XI Jornadas de Ingeniería Telemática

JITEL 2013

Granada 28-30 Octubre

ugr Universidad de Granada

ETSIIT Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

ISTC Departamento de Teoría de la Señal, Telemática y Comunicaciones

at Asociación de Telemática

XI Jornadas de Ingeniería Telemática (JITEL 2013)

Libro de ponencias

Editores:

Jesús E. Díaz Verdejo
Jorge Navarro Ortiz
Juan J. Ramos Muñoz

ugr Universidad de Granada

Asociación de Telemática

ISBN-10: 84-616-5597-4
ISBN-13: 978-84-616-5597-7

Editores: Jesús E. Díaz Verdejo, Jorge Navarro Ortiz, Juan J. Ramos Muñoz
(Universidad de Granada)

Fotografía: Joaquín Valderrama Valenzuela
Portada: Javier Povedano Molina, Rafael A. Rodríguez Gómez, Leovigildo Sánchez Casado y Roberto Magán Carrión.
Maquetación: Juan J. Ramos Muñoz

Presentación

En esta ocasión, es la ciudad de Granada la encargada de servir de anfitriona a las **XI Jornadas de Ingeniería Telemática (JITEL 2013)**, que se celebrarán del 28 al 30 de octubre de 2013.

Las Jornadas de Ingeniería Telemática (JITEL), organizadas por la Asociación de Telemática (ATEL) y el Departamento de Teoría de Señal, Telemática y Comunicaciones de la Universidad de Granada, constituyen un foro propicio de reunión, debate y divulgación para los grupos que imparten docencia e investigan en temas relacionados con las redes y los servicios telemáticos. Con la organización de este evento se pretende fomentar, por un lado el intercambio de experiencias y resultados, además de la comunicación y cooperación entre los grupos de investigación que trabajan en temas relacionados con la Telemática.

Asimismo, en el marco de las jornadas, se organizarán dos workshops, como son las **Jornadas de Innovación Educativa en Ingeniería Telemática (JIE)**, que alcanzan ya la tercera edición, siempre de la mano de JITEL, y **Seguridad en redes inalámbricas ad-hoc (SERIA)**, que se estrena en esta edición.

Este libro recoge las contribuciones que fueron aceptadas para su presentación en las jornadas. Cada una de las contribuciones fue sometida a un riguroso proceso de revisión, bajo la supervisión del Comité de Programa, en el que cada artículo obtuvo tres revisiones independientes. El programa se ha estructurado, de acuerdo a la temática de las contribuciones, en 18 sesiones técnicas: 13 para JITEL, 3 para JIE y 2 para SERIA.

Como punto de encuentro de investigadores y docentes, nos enorgullecemos de contar con la participación y representación de la mayoría de las universidades en las que el área de Ingeniería Telemática tiene presencia a nivel nacional, lo que garantiza el nivel científico-técnico de las jornadas así como la consecución de uno de los objetivos prioritarios: el siempre enriquecedor intercambio de ideas y el establecimiento de colaboraciones entre los participantes. Esperamos que el marco incomparable de la ciudad de Granada, con la Alhambra como estandarte, sirva para aunar esfuerzos en la consecución de los fines tanto científicos como docentes de nuestro colectivo.

Finalmente, es de justicia agradecer la participación activa de todos cuantos han posibilitado este evento tanto a nivel corporativo como individual. Entre los primeros hay que mencionar, especialmente, a la ATEL y al Área de Ing. Telemática de la UGR. A título individual, nuestro más sincero agradecimiento al Comité de Programa, a los investigadores que han participado de forma desinteresada en el proceso de revisión, al Comité Editorial y al Comité organizador local, sin los que el evento no podría haberse llevado a término satisfactoriamente.

El área de Ingeniería Telemática de la Universidad de Granada, como organizadora del evento, les da la bienvenida, tanto a las Jornadas como a la ciudad de Granada.

Jesús E. Díaz Verdejo
Comité Organizador

Comité de programa
Mercedes Amor Pinilla (Universidad de Málaga)
Javier Aracil Rico (Universidad Autónoma de Madrid)
Víctor M. Carneiro Díaz (Universidade da Coruña)
Guiomar Corral Torruella (Universitat Ramon Llull)
Jesús E. Díaz Verdejo (Universidad de Granada)
Yannis Dimitriadis (Universidad de Valladolid)
Rafael M. Estepa Alonso (Universidad de Sevilla)
Santiago Felici Castell (Universitat de Valencia)
Julián Fernández Navajas (Universidad de Zaragoza)
Roberto García Fernández (Universidad de Oviedo)
Sebastián García Galán (Universidad de Jaén)
José Luis González Sánchez (Universidad de Extremadura)
Jesús M. González-Barahona (Universidad Rey Juan Carlos)
Javier Gozálvez (Universidad Miguel Hernández de Elche)
Klaus Hackbart (Universidad de Cantabria)
Xavier Hesselbach Serra (Universidad Politècnica de Catalunya)
Eduardo Jacob Taquet (Euskal Herriko Unibertsitatea)
David Larrabeiti (Universidad Carlos III de Madrid)
José Carlos López Ardao (Universidade de Vigo)
Pilar Manzanares López (Universidad Politécnica de Cartagena)
Iván Marsá Maestre (Universidad de Alcalá)
Jorge Martínez Bauset (Universitat Politècnica de Valencia)
Amaia Méndez (Universidad de Deusto)
Daniel Morató Osés (Universidad Pública de Navarra)
Miquel Oliver Riera (Universitat Pompeu Fabra)
Magdalena Payeras Capellà (Universitat de les Illes Balears)
Pedro M. Ruiz (Universidad de Murcia)
Joaquín Salvachúa (Universidad Politécnica de Madrid)
Luis Sánchez Fernández (Universidad Carlos III de Madrid)
Álvaro Suárez Sarmiento (Universidad de Las Palmas de Gran Canaria)
Miguel Ángel Valero (Universidad Politécnica de Madrid)

Comité ejecutivo
Jesús E. Díaz Verdejo (JITEL 2013)
Klaus Dieter Hackbarth (JITEL 2011)
Álvaro Suárez Sarmiento (ATEL)
Magdalena Payeras Capellá (JITEL 2015)

Comité editorial
Juan Manuel López Soler
Jaime Lloret Mauri

Comité local
Pablo Ameigeiras Gutiérrez
José Camacho Páez
Pedro García Teodoro
Juan Manuel López Soler
José María López Vega
Gabriel Maciá Fernández
Roberto Magán Carrión
Jorge Navarro Ortiz
Javier Povedano Molina
Juan José Ramos Muñoz
Rafael A. Rodríguez Gómez
Antonio Ruiz Moya
Leovigildo Sánchez Casado

Revisores

Agüero Calvo, Ramón
Alarcos Alcázar, Bernardo
Amor Pinilla, Mercedes
Arias Fisteus, Jesús
Asensio Pérez, Juan Ignacio
Astorga, Jasone
Barceló Arroyo, Francisco
Barceló Vicens, Jaume
Barrero López, Aurora
Basanta Val, Pablo
Bikfalvi, Alexander
Bote Lorenzo, Miguel Luis
Cabrero Barros, Sergio
Cacheda Seijo, Fidel
Camacho Páez, José
Campo Vázquez, Celeste
Carmona Murillo, Javier
Carral Pelayo, Juan Antonio
Corral Torruella, Guiomar
Cortés Polo, David
Crespo García, Raquel
de La Cruz Llopis, Luis Javier
Díaz Verdejo, Jesús Esteban
Dimitriadis, Yannis
Draper Gil, Gerard
Egea López, Esteban
Estepa Alonso, Rafael
Felici Castell, Santiago
Fernández García, Norberto
Fernández Masaguer, Francisco
Fernández Navajas, Julián
Formoso López, Vreixo
García, Santiago
García Fernández, Roberto
García Gutiérrez, Alberto Eloy
García Martínez, Luz
García Pañeda, Xabiel
García Rubio, Carlos
García Teodoro, Pedro
García Arranz, Marta
García Sánchez, Antonio Javier
García Sánchez, Felipe
Giménez Guzmán, José Manuel
Gómez Sánchez, Eduardo
González Sánchez, José Luis
González Barahona, Jesús M.
Guerri Cebollada, Juan Carlos
Guijarro Coloma, Luis
Hackbart, Klaus
Hernández Gutiérrez, José Alberto
Higuero Aperribay, Mariví
Hinarejos Campos, M. Francisca
Ibáñez Fernández, Guillermo Agustín
Irastorza Teja, José Ángel
Izal, Mikel
Jacob, Eduardo
Liberal, Fidel
Llamas Nistal, Martín
López Ardao, Carlos
López Millán, Gabriel
López Muñoz, Javier
López Carmona, Miguel Ángel
López Matencio Pérez, Pablo
Maciá Fernández, Gabriel
Macías López, Elsa
Magán Carrión, Roberto
Marín López, Rafael
Marrero Marrero, Domingo
Marsá Maestre, Iván
Martínez Bauset, Jorge
Martínez Cruz, Jesús
Martínez Yelmo, Isaías
Mata Díaz, Jorge
Melendi Palacio, David
Miguel Torres, Luis
Morató Osés, Daniel
Moreno Martín, Manuel
Moreno Martínez, Víctor
Muñoz Gea, Juan Pedro
Muñoz Muñoz, Alfonso
Mut Puigserver, Macià
Narbona Moreno, José Luis
Navarro Ortiz, Jorge
Nieto Jiménez, Ana
Oliver Riera, Miquel
Payeras Capellà, Magdalena
Pérez de Prado, Rocío
Pla Boscà, Vicent
Pozueco Álvarez, Laura
Prieto, Iria
Ramis Bibiloni, Jaume
Ramos de Santiago, Javier
Ramos Muñoz, Juan José
Regueras Santos, Luisa María
Riera Palou, Felip
Rincón Rivera, David
Rodríguez Gómez, Rafael A.
Rodríguez Pérez, Francisco Javier
Ruiz Martínez, Pedro M.
Ruiz Martínez, Antonio
Salazar Riaño, José Luis
Saldaña Medina, José María
Sánchez, Luis
Sánchez Fernández, Luis
Sánchez Casado, Leovigildo
Sanz, Roberto
Seoane Pujol, Isaac
Simmross Wattenberg, Federico
Skarmeta Gómez, Antonio
Soto Campos, Ignacio
Sousa Vieira, María Estrella
Suárez Sarmiento, Álvaro
Urueña Pascual, Manuel
Valero, Miguel Ángel
Vega, Mario
Verdú Pérez, María Jesús
Vidal Ferre, Rafael
Yuste Delgado, Antonio Jesús

Índice de contribuciones

XI Jornadas de Ingeniería Telemática (JITEL)

Aplicaciones y servicios
Sesión JITEL A1

Eficiencia energética en redes
Sesión JITEL A2

Encaminamiento
Sesión JITEL A3

Servicios de seguridad
Sesión JITEL A4

Criptografía y control de acceso
Sesión JITEL A5

Protocolos de comunicaciones
Sesión JITEL A6

Calidad de servicio
Sesión JITEL A7

Modelado y control de tráfico
Sesión JITEL A8

Aplicaciones y servicios: e-salud
Sesión JITEL B2

Redes móviles y de sensores
Sesión JITEL B3

Redes celulares
Sesión JITEL B4

Redes y servicios
Sesión JITEL C1

Seguridad en redes
Sesión JITEL C2

Seguridad en Redes Inalámbricas Ad Hoc (SERIA)

Seguridad en redes inalámbricas Ad-Hoc
Sesión SERIA B5

Seguridad en redes inalámbricas Ad-Hoc (2)
Sesión SERIA B8

III Jornadas de Innovación Educativa en Ingeniería Telemática (JIE)

JITEL

Sistema de pruebas de servicios REST mediante análisis de esquemas inferidos

Alvaro Navas, Pedro Capelastegui, Francisco Huertas, Pablo Alonso-Rodriguez, Juan Carlos Dueñas
Center por Open Middleware
Universidad Politécnica de Madrid
Campus de Montegancedo, E-28223 Pozuelo de Alarcón, Madrid, España
{alvaro.navas, pedro.capelastegui, francisco.huertas, pablo.alonso, juancarlos.duenas}@centeropenmiddleware.com

***Resumen*—El concepto de arquitectura orientada a servicios disfruta de gran consideración en el mundo de la ingeniería del software, lo que se debe a que produce arquitecturas formadas por diversos módulos interconectados entre sí, fácilmente reutilizables para formar nuevos sistemas. Este tipo de diseños no serían posibles sin métodos de interconexión que facilitasen la comunicación entre los módulos mientras reducen al mínimo el acoplamiento entre los mismos, como por ejemplo los servicios REST. Sin embargo, este bajo nivel de acoplamiento trae consigo desventajas, especialmente una falta de transparencia, que dificultan la creación de pruebas de forma sistemática sin requerir conocimiento interno de cómo funciona el servicio. En este artículo presentamos un sistema de detección automática de errores para servicios REST basado en el análisis estadístico de las respuestas producidas al invocar de forma repetida el servicio. De esta forma, se puede probar el servicio de forma sistemática sin conocer su especificación completa, pudiendo detectar errores no identificables con métodos tradicionales de prueba. Esto permite proporcionar una cobertura limitada de pruebas para servicios cuyo formato de respuesta se desconoce, o complementar a otros mecanismos de prueba en otros escenarios.**

***Palabras Clave*—pruebas, SOA, XML, XSD, REST**

I. INTRODUCCIÓN

A lo largo de los últimos años, el paradigma de la arquitectura orientada a servicios ha tenido una gran expansión gracias a la difusión de las tecnologías web e internet. Las ventajas de esta arquitectura se basan en ofrecer diseños modulares con poco acoplamiento entre sí, lo que permite la creación eficiente y sistemática de sistemas distribuidos.

Para que este tipo de arquitectura sea posible, es necesario dotar a los servicios de interfaces de interconexión que permitan encapsular los servicios al mismo tiempo que faciliten el uso de los mismos. Existen varias tecnologías para definir estos interfaces. Entre ellas, los servicios REpresentional State Transfer (REST) están logrando cada vez más aceptación, debido a su capacidad de escalabilidad y la uniformidad de sus interfaces, que permite una mayor separación entre los consumidores y los servicios. Compañías como Yahoo, Google o Twitter definen interfaces REST de acceso a sus servicios, ya sea para consultar mapas (GoogleMaps), imágenes (Flickr) o el correo, lo que permite a terceros desarrollar clientes para sus servicios sin tener que involucrarse en su producción.

Sin embargo, los servicios REST poseen ciertas limitaciones que pueden complicar el desarrollo tanto del propio servicio como de sus clientes. Entre estas limitaciones, destacan la falta de transparencia de la estructura y del código de los servicios, la incertidumbre sobre los componentes invocados durante la ejecución de un servicio, la falta de control sobre la infraestructura y los costes de invocación de servicio. Aunque existen mecanismos para definir formalmente la interfaz del servicio, o bien no se usan, o se trata de desarrollos ajenos al código del servicio y mantenidos de forma paralela, por lo que en ocasiones se pierde la sincronización entre el servicio y su descripción.

Esta falta de transparencia se traduce en que el proceso de creación de un cliente se convierta en un proceso manual que puede requerir cierto conocimiento interno del funcionamiento del servicio, que no siempre está disponible. Además de dificultar el acceso de futuros clientes al nuestro, también dificulta la realización de pruebas. Los sistemas actuales de prueba para servicios REST centran sus esfuerzos en la creación por parte del usuario de casos de prueba, tanto la llamada al servicio como la respuesta esperada, que permitan verificar el correcto funcionamiento del servicio. Y la falta de transparencia inherente a los servicios REST, obliga a que sea el propio desarrollador del servicio el que realice las pruebas. Además, debido a que es el desarrollador el que decide qué se debe probar y qué es correcto (práctica muy extendida), no se realizan pruebas sistemáticas, sino que sólo se escogen los casos que él opina que son susceptibles de producir error.

En este artículo proponemos una solución para la realización automática de pruebas de caja negra a servicios REST, capaz de proporcionar una cobertura de pruebas limitada en escenarios en los que se carezca de la especificacion completa de un servicio, o de complementar a otros mecanismos de prueba cuando si se dispone de esta informacion. La propuesta está basada en el análisis estadístico de las respuestas ofrecidas por el servicio al ser invocado, estudiando dos niveles: sintáctico y semántico. Es decir, el análisis de la estructura de la respuesta y del contenido de la misma.

Aunque el análisis estadístico de los contenidos de la respuesta podría haberse realizado sobre cualquier formato multimedia, hemos decidido centrar nuestras investigaciones en el estudio de servicios que proporcionen respuestas en formato eXtensible Markup Language (XML). Las ventajas de esta decisión son que XML, además de ser un formato muy extendido, impone una estructura estricta y que hay abundante literatura sobre como inferirla a partir de muestras de documentos, facilitando enormemente el análisis sintáctico de las respuestas. Ambas ventajas no son necesariamente ciertas para el resto de formatos soportados por REST (JSON por ejemplo), por lo que XML es el candidato ideal.

El artículo sigue la siguiente estructura. La sección II ofrece una visión completa de las tecnologías usadas para realizar pruebas a servicios REST así como una visión de los

diferentes tipos de inferidores de XML Schema Definition (XSD) existentes. La sección III muestra la arquitectura de la solución propuesta. En la sección IV describimos una serie de experimentos llevados a cabo para demostrar la validez de nuestra solución. Finalmente, la sección V contiene las conclusiones extraídas del desarrollo de este trabajo y las vías de investigación que se nos plantean de cara al futuro.

II. TRABAJOS RELACIONADOS

En esta sección vamos a revisar el estado actual de los sistemas y herramientas que permiten desarrollar pruebas para servicios REST. Así mismo, y ya que el núcleo de nuestra propuesta está basado en la inferencia de la estructura de los archivos XML, hemos considerado oportuno revisar también en qué punto de evolución se encuentran estas tecnologías.

A. Pruebas de servicios REST

Según un estudio reciente [1] , las pruebas de sistemas orientados a servicios son un tema de investigación que ha experimentado un fuerte crecimiento en los últimos años. Sin embargo, el trabajo en este área se ha centrado principalmente en servicios web basados en SOAP, mientras que las pruebas de servicios REST cuentan con un número relativamente escaso de publicaciones.

SoapUI [2] es una herramienta multiplataforma en código abierto para realizar pruebas de servicios web y servicios REST. Soporta pruebas funcionales, de regresión y de carga, e incluye funciones para pruebas de seguridad y simulación de servicios, y permite la generación automática de documentos WADL para la descripción de servicios REST, y la inferencia de esquemas XSD partir de las respuestas de un servicio.

TTR [3] es una herramienta de pruebas para servicios REST con soporte para pruebas funcionales y no funcionales. Se compone de un entorno extensible mediante plug-ins, un lenguaje de especificación para casos de prueba basado en XML, y un método para la composición de casos de prueba. TTR sigue un enfoque de caja negra para las pruebas, y requiere que los servicios a probar se encuentren en entornos controlados.

REST Assured [4] es un lenguaje específico de dominio para Java, desarrollado para simplificar las pruebas de servicios basados en REST. Facilita la construcción de peticiones REST, y permite validar y verificar las respuestas, con herramientas para interpretar documentos JSON y XML, soporte para autenticación, generación de trazas y mapeo de objetos.

En [5], se describe un entorno para pruebas automatizadas de coreografías de servicios web, compatible con servicios REST. Se compone de un mecanismo para la abstracción de coreografías en objetos Java, clientes dinámicos para servicios web (incluyendo un cliente REST basado en REST Assured), y soporte para la intercepción de mensajes y servicios simulados.

[6] presenta un entorno software para la simulación de servicios REST en escenarios de pruebas. Para cada servicio simulado, permite la especificación de interfaces, y parámetros de entrada en forma de documentos XML. Los servicios verifican los parámetros de entrada, y generan respuestas a partir de una combinación de datos pre-grabados, lógicas definidas para el caso de prueba, y perturbación de datos.

En general, las soluciones existentes para pruebas REST presuponen un conocimiento detallado de la especificación del servicio a probar: parámetros de entrada, formato de la respuesta y valores de respuesta esperados. Dado que la motivación del presente trabajo nace de la necesidad de llevar a cabo pruebas de caja negra sobre servicios para no se dispone de la especificación completa, y de reducir el esfuerzo requerido para realizarlas, podemos concluir que ninguno de los sistemas actuales cubre estas necesidades.

B. Inferencia de esquemas XSD

Como se ha indicado, el método de pruebas que proponemos en este artículo incluye el análisis sintáctico de respuestas XML en servicios REST, para lo cual debemos inferir su estructura, representada en forma de esquema. El problema de la inferencia de esquemas a partir de documentos XML se ha tratado en varios estudios a lo largo de los últimos años. Los trabajos iniciales en este área se centraban en la inferencia de esquemas de tipo Document Type Definition (DTD) [7], pero en la actualidad el formato predominante es el XML Schema Definition (XSD), mucho más expresivo, pero también más complejo y difícil de inferir. En esta sección, definimos los requisitos que debe cumplir un motor de inferencia para un sistema de pruebas, resumimos los principales métodos de inferencia encontrados en la literatura, y analizamos las herramientas de inferencia más destacables.

La característica principal que debemos buscar en un sistema de inferencia de esquemas XML es la validabilidad: los esquemas inferidos deben ser tales que todos los documentos XML de entrada validen contra ellos. Por otro lado, el sistema debe ser estricto, de modo que los esquemas inferidos sólo permitan validar documentos cuya estructura sea igual, o lo más parecida posible, a la de los documentos de entrada. Otras propiedades deseables son la corrección y la universalidad: los esquemas generados deben conformarse a la especificación del formato de esquema elegido, y el sistema debe ser capaz de inferir esquemas a partir de cualquier documento XML válido. Finalmente, para el uso de la inferencia en el contexto de nuestro sistema de pruebas, es necesario que el sistema permita la inferencia a partir de grupos numerosos de documentos, que el tiempo de inferencia no sea excesivo, y que sea posible extender el sistema para incorporar funciones de análisis estadístico sobre los documentos y esquemas.

En este artículo solo consideramos la inferencia de esquemas XSD, ya que DTD carece de la expresividad suficiente para generar esquemas estrictos. La inferencia de un esquema XSD requiere la obtención de expresiones regulares a partir de cadenas de elementos, teniendo en cuenta no sólo el nombre de cada elemento, sino también el contexto de su uso. A continuación, resumimos las principales técnicas de inferencia en las que se ha basado nuestra solución.

[8] observa que los sistemas de inferencia XSD que existían previamente no tienen en cuenta el contexto de los elementos XML, lo que resulta en esquemas con la misma estructura y limitada expresividad que DTD. Define el concepto de k-localidad, para referirse a modelos de contenido que dependen de hasta k ancestros de un elemento (donde k=0 para esquemas DTD, y k=2 para la mayoría de XSDs). Su solución introduce una restricción que simplifica la inferencia: usar únicamente expresiones regulares en las que cada nombre de

elemento aparece una sola vez, denominadas Single Occurrences Regular Expression (SOREs) que permiten describir la mayoría de esquemas encontrados en la práctica. Describe el algoritmo iXSD, basado en SOREs, y válido para cualquier k-localidad. Usa autómatas de estados finitos (llamados SOA, Single Occurrence Automatons) como paso intermedio entre el XML y las SORE, y obtiene el esquema a partir de las SOREs. Finalmente, integra una etapa de postprocesado para unificar tipos similares en el XSD obtenido.

Los mismos autores en [9] utilizan un subconjunto de SORE más restrictivo denominado Chain Regular Expression (CHARE), e introducen dos nuevos algoritmos: para la transformación de autómatas en SOREs, y para inferir directamente CHAREs sin recurrir a autómatas, y es especialmente apropiado para escenarios con muy pocos datos XML disponibles. En la misma línea, [10] propone mejoras a los algoritmos y un nuevo mecanismo de mezclado de tipos, que permiten inferir esquemas con el elemento sintáctico <all>, y con tipos asociados a múltiples nombre de etiqueta.

Durante el desarrollo de nuestro trabajo, hemos evaluado varias herramientas de inferencia, con diferentes niveles de prestaciones y madurez. XML Schema Learner [11] es una herramienta PHP en código abierto con capacidad para inferir esquemas DTD y XSD, basada en [10]. Soporta la mayoría de propiedades del lenguaje XSD, y ofrece la inferencia más estricta de entre las herramientas observadas, pero contiene algunos errores de código que resultan en fallos de inferencia.

Trang [12] es una herramienta Java con licencia New BSD capaz de inferir esquemas de distintos formatos, incluyendo DTD y XSD, así como de convertir esquemas de un tipo a otro. Como puntos negativos, sólo considera una k-localidad de cero (es decir, sus XSD son equivalentes a DTD), y los esquemas generados se desvían en ocasiones de la especificación de XSD.

El entorno .NET de Microsoft incluye una API de manejo de XMLs [13] para la inferencia de esquemas XSD, e incluye en su kit de desarrollo una utilidad de inferencia construida sobre esta API. La API toma como entrada un único documento XML y, opcionalmente, un esquema preexistente en el que integrarlo, lo que permite procesar incrementalmente grupos de documentos, pero conlleva una pérdida de información y precisión frente al procesado simultáneo. En nuestras pruebas con la API hemos observado errores de inferencia ocasionales, por ejemplo en escenarios donde elementos comparten nombres con sus ancestros.

SoapUI [2] es una herramienta de pruebas de servicios web que, entre otras funciones, permite la inferencia de esquemas XSD a partir de las respuestas de un servicio REST. Lleva a cabo inferencias con una k-localidad de uno, y al igual que .NET, permite inferir incrementalmente a partir de grupos de documentos. También hemos identificado fallos de inferencia, en casos de desorden de elementos. SoapUI es el único ejemplo previo que hemos encontrado de inferencia de XML aplicada a pruebas REST.

En general, las herramientas observadas sufren o bien de capacidad de inferencia limitada, o bien de errores de inferencia notables en determinados escenarios. Por esto, unido a la dificultad de integrar un módulo de obtención de estadísticas en los sistemas existentes, hemos optado por desarrollar un sistema de inferencia propio, que describimos en los siguientes apartados.

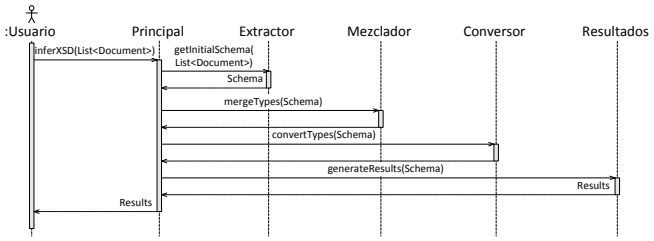


Fig. 1. Diagrama de secuencia de una inferencia de un esquema XSD

III. ARQUITECTURA DEL SISTEMA

En esta sección describiremos la arquitectura de la solución propuesta, empezando por su elemento principal, el inferidor de esquemas XSD.

A. El inferidor de esquemas XSD

El inferidor de esquemas XSD es el núcleo del sistema de detección de anomalías. Este componente es el encargado de reconstruir un esquema XSD contra el que todo el conjunto de documentos sea capaz de validar, así como de generar un conjunto de estadísticas que más tarde permitirán detectar anomalías tanto en la sintaxis de los archivos como en la semántica. Es por ello por lo que antes de explicar la arquitectura global del sistema, debemos describir primero cómo funciona este módulo, sin cuyo crucial trabajo no se entenderían el resto de componentes.

Como ya hemos mencionado anteriormente, después de estudiar en profundidad las diferentes aproximaciones relativas a la inferencia de esquemas, llegamos a la conclusión de que hay pocas herramientas que aprovechen la capacidad descriptiva de XSD para inferir esquemas a partir de un conjunto de documentos. Entre las que lo hacen, la herramienta más completa es la diseñada por Kore Nordmann, XML Schema Learner. Es eso, el diseño de nuestro inferidor está fuertemente basado en el diseño de su herramienta. Sin embargo, y dado que hemos añadido el soporte para la extracción de estadísticas y modificado algunos de sus algoritmos para introducir algunas mejoras, conviene revisar su arquitectura.

El inferidor está diseñado como un componente modular independiente del resto del sistema. La Figura 1 muestra un diagrama de secuencia en el que se muestra la interacción entre los diferentes módulos y los valores que devuelve cada uno cuando se realiza una inferencia. El módulo Principal es el componente coordinador del inferidor. Su función es la de controlar el flujo de datos entre los diferentes módulo. El diseño de Kore Nordmann estaba orientado a tener una serie de fases concretas: un extractor, un mezclador y un conversor de tipos y el módulo que crea el esquema XSD. El módulo Coordinador presenta cuatro interfaces a los que se pueden conectar diferentes módulos que pueden proveer diferentes implementaciones de los mismos. También contiene la definición de las clases del modelo que se irán manipulando durante todo el proceso, como la clase Schema que contendrá la estructura de datos necesaria para inferir el esquema XSD y que se irá modificando en cada fase.

La primera fase es la extracción de tipos que realiza el módulo Extractor cuyo objetivo es transformar el conjunto de documentos XML de entrada a la herramienta en una estructura de objetos que simule la estructura de tipos XSD tanto simples como complejos que debe ser capaz de contener todos los documentos. Nuestra implementación procesa los archivos XML uno a uno. Tras analizar el primer archivo, se crea un objeto Schema que contiene la estructura de elementos detectada, que incluye todos los tipos, simples y complejos, listas de atributos y su pertenencia a un determinado espacio de nombres.

El tratamiento de la mayoría de los tipos es relativamente sencilla, salvo en el caso de los tipos complejos. Estos tipos deben contener la lista de atributos correspondiente a ese tipo, el tipo simple del texto que contengan, de existir, y una representación de la estructura de sus hijos. Debido a que la estructura de estos tipos complejos no tiene por qué ser estática, por ejemplo puede haber elementos o atributos que existan en unos documentos pero no en otros, esta estructura se refleja utilizando autómatas. Permiten describir qué hijos pueden o deben aparecer en el documento y en qué orden. Además, los tipos complejos definen también qué atributos están asociados a cada elemento, incluyendo el tipo simple del atributo y si su aparición es obligatoria o no.

La estructura de elementos almacenada en el objeto Schema hace uso de estos tipos complejos a la hora de definir la secuencia de elementos. Los archivos sucesivos se utilizan para refinar los elementos ya presentes o crear nuevos en caso de ser necesario y para modificar la estructura del documento. El resultado final es un objeto Schema que contiene una versión primitiva del esquema XSD final que contiene una lista de todos los tipos simples y complejos detectados y la lista de los diferentes espacios de nombre encontrados, con todos los prefijos con los que han aparecido.

Una mejora incluida en esta implementación frente a la de Kore Nordmann es la detección de un número mayor de tipos simples que su herramienta, que clasificaba todos los tipos como xs:string. Además, podemos también determinar cuándo un tipo XSD tiene una restricción asociada de tipo Enumeration. También hemos introducido una modificación que nos permite trabajar con diferentes espacios de nombre. Finalmente, debemos mencionar que en cada análisis se extrae información relativa a la aparición de cada elemento y los diferentes valores que puede tomar, que se almacena en una estructura de objetos Java auxiliar dentro del objeto Schema y que nos servirá para elaborar un informe con las estadísticas extraídas del cuerpo de documentos al final del proceso.

A continuación se procede a realizar la mezcla de tipos por medio del módulo Mezclador. La salida del Extractor es un conjunto de objetos Java interrelacionados que conforman un esquema XSD primitivo. El objetivo de este módulo es analizar este esquema y unificar aquellos tipos que son lo suficientemente parecidos como para ser considerados un único tipo XSD, reduciendo enormemente el tamaño del esquema. Este proceso es complejo porque requiere la comparación de todos los tipos. Para los tipos simples eso significa comparar todas las listas de valores. Para los complejos, hay que comparar las estructuras de sus autómatas y las listas de atributos. Además, el proceso debe ser especialmente cuidadoso para poder preservar los datos estadísticos extraídos durante la fase anterior y que no se pierdan durante la mezcla.

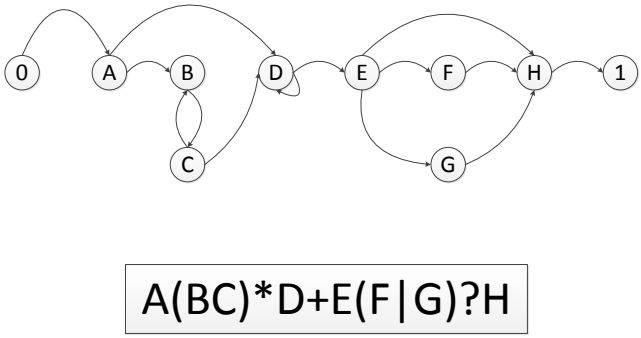


Fig. 2. Conversión de un autómata a expresión regular

El siguiente paso para transformar la estructura de objetos Java en un esquema XSD es convertir la estructura de tipos en una serie de expresiones regulares a partir de las cuales se puede construir el esquema XSD definitivo. Esta tarea corre a cargo del módulo Conversor, que se compone de dos partes diferenciadas. La primera está destinada a crear las expresiones regulares. Para ello se pueden utilizar varios métodos de extracción, principalmente basados en la extracción de SOREs o CHAREs. Ambos tipos de expresiones regulares garantizan una estructura no ambigua y sin dependencias cíclicas, usándose las SOREs por defecto, ya que son más restrictivas, y las CHAREs en caso de que el proceso de creación de la SORE no se pueda completar o cuando se defina así en la configuración de la herramienta. De esta forma nos aseguramos de que el esquema está lo más restringido posible a la estructura de los documentos analizados, evitando dar como válidos documentos que pudieran tener una estructura parecida, pero que no fuera válida.

Las expresiones regulares resultado de extraer utilizando cualquiera de los dos métodos suelen contener información redundante o innecesaria, por lo que la segunda parte de este módulo está dedicada a optimizar las expresiones regulares resultantes hasta que contengan sólo la información mínima necesaria. En concreto, se utilizan optimizadores para eliminar elementos vacíos, para reducir la nomenclatura producida (en especial la concatenación de dos multiplicadores) e incluso para reducir la longitud de algunas secuencias. En la figura 2 se puede observar un ejemplo de autómata convertido a expresión regular siguiendo este método.

Finalmente, el módulo Resultados se encarga de generar los documentos de salida de la herramienta. En concreto, genera un esquema XSD por cada namespace diferente que se haya encontrado dentro del cuerpo de documentos así como un informe estadístico separado en el que se analizan diferentes datos sobre cada elemento. Por cada elemento único encontrado en todo el cuerpo de documentos se calcula su número total de apariciones diferentes, así como su media, máxima y mínima por archivo. Sobre estos datos se puede calcular además la moda y la varianza dependiendo de si el tipo de datos de ese nodo lo admite. Por ejemplo, si es un nodo de tipo XSD Integer, podemos averiguar cual es el valor más común a partir de estos datos y cual es el rango de variación a partir de la desviación.

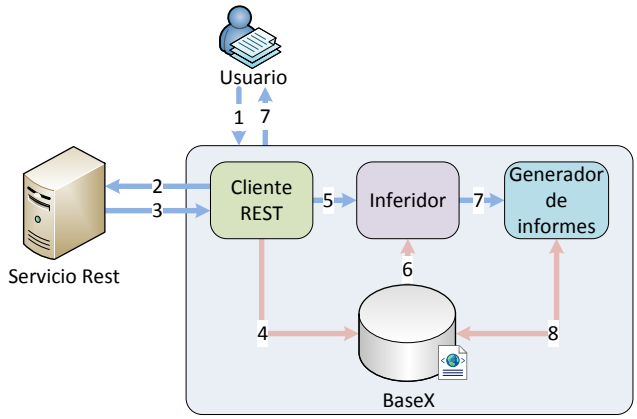


Fig. 3. Arquitectura global de la herramienta

B. Arquitectura global

Una vez explicada la pieza central del sistema y cómo genera las estadísticas, podemos pasar a explicar la arquitectura global del mismo. Recordemos que el objetivo de la herramienta es poder realizar pruebas de caja negra sobre servicios REST, basada en la detección estadística de elementos anómalos. Es por ello que el sistema debe componerse de tres módulos: uno capaz de realizar llamadas a un servicio REST cualquiera y procesar las respuestas; el inferidor, que analiza las respuestas y calcula las estadísticas de cada elemento; y un módulo final que analice las estadísticas extraídas para detectar aquellos elementos, tanto sintácticos como semánticos, que destaquen respecto al resto. La Figura 3 presenta la visión global del sistema así como la secuencia de acciones que se llevan a cabo cuando se quiere ejecutar un análisis de un servicio REST.

El primer paso es la introducción por parte del usuario de un conjunto de datos de prueba. Este conjunto de datos de prueba consiste simplemente en la URL y el método HTTP del servicio que se quiere probar así como un conjunto de parámetros que permitan variar la petición. Cuanto mayor sea este conjunto de parámetros, mejor serán tanto la detección de anomalías como el XSD inferido.

Los datos de entrada llegan al módulo Cliente REST. Este módulo lee estos datos y genera peticiones REST al servicio especificado. Por cada respuesta que recibe, crea un documento XML que asocia esa respuesta a los parámetros utilizados que generaron esa respuesta y almacena ambos en la base de datos del sistema. Para el almacenamiento temporal de los datos hemos utilizado una base de datos orientada a documentos XML llamada BaseX [14], dado que queremos poder realizar búsquedas sobre el cuerpo de documentos sin tener que adaptarlos a un esquema SQL.

Cuando se han finalizado todas las peticiones y todos los resultados se encuentran almacenados en la base de datos, el Cliente REST procede a decirle al Inferidor en que parte de la base de datos puede encontrar el cuerpo de documentos que debe analizar. El funcionamiento del Inferidor ya fue detallado en la sección anterior, por lo que no volveremos a explicar su funcionamiento. Sólo añadiremos que recoge el conjunto de documentos de entrada de la base de datos y almacena los resultados en la misma.

Finalmente, el módulo Generador de Informes procede a analizar los resultados estadísticos recogidos por el Inferidor para detectar anomalías. Para ello se sirve de un conjunto de reglas que aplica a nivel sintáctico y semántico. A nivel sintáctico recorre el esquema XSD para detectar aquellos tipos que tienen un número de apariciones mucho menor que el del resto de elementos. Por ejemplo, si tras analizar 20 documentos encontrásemos un tipo que sólo ha aparecido dos veces, se podría tratar de un error, especialmente si se detecta que es un tipo que existe en otra parte del esquema, lo que indicaría un error humano al crear el documento. A nivel semántico, el descubrimiento de anomalías sigue reglas algo más complejas en las que se comparan diversas estadísticas de los valores que toma cada elemento, tales como la varianza, la moda, el máximo y el mínimo número de apariciones por archivo... Una vez tenemos esos valores, se procede a comparar los mismos entre sí, como en el caso de la varianza y los máximos y mínimos para saber si existe duplicidad de algún valor, o con los de sus valores hermanos, por ejemplo cuando en la lista de valores de un elemento tiene un valor muy distinto al de sus hermanos, ya sea superior o inferior.

Tras descubrir las posibles anomalías, se escribe un informe en el que se recogen todas las anomalías detectadas y su relación con los parámetros de entrada que los produjeron. Para ello se hace uso de las funcionalidades de búsqueda que ofrece BaseX basados en XQuery, un lenguaje de consultas específico para archivos XML. El módulo recoge la ruta XML que generó la anomalía y realiza una búsqueda sobre el conjunto de documentos almacenados en la base de datos. Con los archivos que generaron la anomalía identificados, procede a leer la información introducida por el módulo Cliente REST que ataba esos archivos a parámetros de entrada para reflejar dicha relación en el informe final. Cuando todas las anomalías han sido procesadas, devuelve al usuario tanto el informe como los esquemas XSD que se hayan generado. El motivo de devolver los esquemas XSD no es meramente informativo, ya que al usuario podría usarlos para crear un cliente REST capaz de validar e interpretar todas las respuestas del servidor a partir de los mismos si así lo desea.

IV. RESULTADOS EXPERIMENTALES

Para comprobar la validez de la solución propuesta se han realizado dos tipos de pruebas: pruebas de inferencia y pruebas de sistema. Las primeras se han centrado en validar el funcionamiento de la inferencia de esquemas, pieza central de nuestro sistema. Para ello, hemos comparado los resultados obtenidos por nuestro motor de inferencia con los de las herramientas Trang y SoapUI, a partir de respuestas XML de servicios REST. El segundo tipo de pruebas se ha centrado en probar la validez del sistema completo, utilizándolo para identificar anomalías en servicios REST.

A. Escenario

El escenario de validación consiste en una batería de pruebas de caja negra sobre un servicio REST cuyo funcionamiento interno se desconoce, llevada a cabo con nuestra herramienta de pruebas. Hemos repetido este escenario con dos servicios REST distintos: un servicio público en estado de producción, y un servicio REST propio en desarrollo. El primero nos proporciona un ejemplo de sistema real que se

Tabla I
CARACTERÍSTICAS DE LOS SERVICIOS REST UTILIZADOS

Servicio	Google Places	Servicio REST propio
Proveedor	Google	Propio
Funcionalidad	Encontrar puntos de interés próximos a una posición facilitada	Obtener información de configuración de un servidor web
Tipo de respuesta	corta y homogénea	larga y homogénea
Estado del servicio	Muy estable	En fase de pruebas

puede encontrar en el mercado, y en el que difícilmente se van a encontrar errores, mientras que el segundo aún contiene suficientes errores para demostrar las capacidades del sistema de pruebas. Sus características se muestran en la tabla I. En ambos casos, se han realizado 50 peticiones diferentes a cada uno.

1) Google Places: Como primer servicio REST se ha tomado el servicio público ofrecido por Google, Google Places [15] sobre el cual se han realizado varias consultas para intentar encontrar diferentes tipos de locales en situaciones aleatorias a lo largo de la península ibérica. En cada consulta, se toman como parámetros de entrada una localización, radio de búsqueda, idioma, y tipo de local, con valores seleccionados aleatoriamente dentro de los rangos permitidos.

2) Servicio REST propio: En el segundo escenario hemos elegido un servicio REST de recuperación de configuraciones, actualmente en estado de desarrollo en nuestra organización. El servicio permite consultar la configuración de diversos servidores de aplicación distribuidos en una nube privada. El único parámetro de entrada requerido por el servicio es la dirección del servidor cuya configuración se desea consultar.

B. Validación de la inferencia

Las pruebas de validación de inferencia tienen por objetivo evaluar la capacidad de nuestro motor de inferencia para generar esquemas adecuados a partir de conjuntos de documentos XML. Como métrica de calidad adicional, hemos elegido el tamaño mínimo de inferencia, que se define como el número mínimo de documentos de entrada requeridos para obtener un esquema validable por todos los documentos de un mismo tipo.

La validación se lleva a cabo sobre un conjunto de prueba, compuesto por documentos XML obtenidos de respuestas a un servicio REST, con una estructura común. A partir de este conjunto, se obtiene un subconjunto de análisis, del que se infieren esquemas XSD. El proceso consiste en una serie de iteraciones, cada una con los siguientes pasos:

- Añadir un documento aleatorio del conjunto de prueba al conjunto de análisis.
- Inferir un nuevo esquema a partir del conjunto de análisis.
- Trata de validar el conjunto de prueba contra el esquema obtenido.

Las iteraciones continúan hasta dar con un esquema validable por el conjunto; el tamaño de inferencia es igual al tamaño del conjunto de análisis tras la última iteración.

La validación de inferencia se ha llevado a cabo sobre el servicio REST de Google Places, y el servicio REST propio. En cada caso, se ha repetido el proceso con nuestro motor de inferencia y con las herramienta Trang y SoapUI, utilizando las mismas secuencias aleatorias de documentos y comparando resultados.

1) Google Places: En este escenario todas las herramientas de inferencia son capaces de obtener esquemas XSD validables por la totalidad del conjunto de prueba. Además, para las tres herramientas, los esquemas obtenidos describen adecuadamente la estructura de los documentos, con ligeras diferencias: Trang no recoge las relaciones entre ciertos elementos que siempre aparecen juntos, y tan solo nuestro motor de inferencia identifica adecuadamente las restricciones de enumeración.

En lo que respecta al tamaño mínimo de inferencia, Trang y SoapUI generan un esquema válido para todo el conjunto de prueba a partir de 11 documentos, mientras que nuestro motor requiere de 19 documentos. Esto se debe a que nuestros esquemas son más estrictos, al contener restricciones de enumeración. Hay que tener en cuenta que nuestra herramienta permite una configuración flexible del nivel de detalle de los esquemas inferidos, lo que hace posible, por ejemplo, desactivar la detección de enumeraciones. En este caso, el número de documentos requeridos desciende hasta los 11 observados para otras herramientas.

2) Servicio REST propio: Con nuestro servicio REST de consulta de configuraciones, observamos que resulta imposible obtener ningún esquema utilizando SoapUI. Esto se debe a que los documentos XML de entrada presentan elementos con hijos cuyo orden puede variar, algo con lo que el algoritmo de inferencia utilizado por esta herramienta no es compatible. Así, si el conjunto de análisis incluye para un mismo elemento padre la secuencia de elementos hijos A y B, y posteriormente una secuencia B, A, el programa falla sin llegar a generar un esquema. Este es un tipo de error que también hemos observado en otros sistemas de inferencia estudiados, como el de .NET, que en estos casos genera esquemas incorrectos y no validables.

Por otra parte, Trang sí genera esquemas, pero que no se pueden validar por el conjunto de prueba. El motivo es que la estructura de los documentos incluye distintos elementos con la etiqueta ”configuration”, que Trang es incapaz de distinguir, y agrega en un mismo tipo, lo que resulta en esquemas incorrectos.

Nuestro motor de inferencia, en cambio, reconoce adecuadamente tanto los elementos de orden variable como los tipos con misma etiqueta pero diferente contexto, generando esquemas que se validan para todo el conjunto de prueba. Para ello, necesita un tamaño de conjunto de análisis de 14.

C. Análisis de anomalías

El objetivo de las pruebas ha sido validar la funcionalidad de obtener anomalías a partir de información estadística extraída de las respuestas del servicio. Para ello se han analizado las 50 respuestas del servicio con la herramienta de informes de anomalías; posteriormente, se ha estudiado cada anomalía para determinar su origen y si se trata de un fallo del servicio o no.

1) Google places: En el análisis de las respuestas del servicio REST se ha observado que existe una anomalía. Esta anomalía, figura 4, consiste en un bajo índice de aparición

Fig. 4. Extracto de estadisticas de respuestas de Gooogle Places

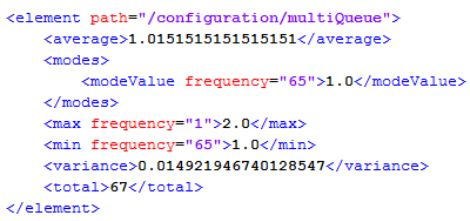


Fig. 5. Elemento repetido.

de un valor en un campo en donde existen pocos valores, en concreto una aparición de 5 ocurrencias sobre 50 con 2 posibles valores para este campo de la respuesta en el servicio REST. Un análisis de las respuestas que generan la anomalía revela que esta se trata de un falso positivo causado por una respuesta poco común, pero válida, del servicio.

2) Servicio REST propio: En este servicio REST se esperaba que la herramienta obtenga anomalías a partir de las respuestas obtenidas. Como resultado de análisis de la herramienta se han obtenido tres tipos de anomalías.

En el primero de anomalía, 5, la frecuencia más común del elemento que produce la anomalía es una única aparición; sin embargo, una de las respuestas tiene dos elementos. Tras estudiar la anomalía se ha determinado que en todos los casos el elemento estaba duplicado y, por lo tanto, era necesario eliminarlo de la respuesta. El valor estadístico que ha identificado esta anomalía ha sido la varianza, la cual tiene un valor muy bajo, sin ser 0.

En la segunda anomalía, se puede observar como existe un

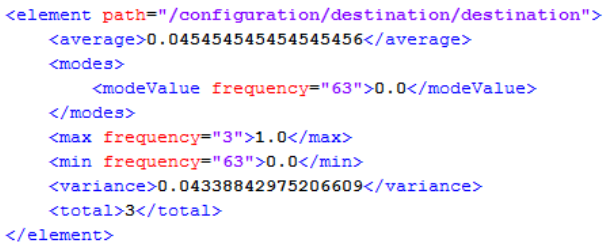


Fig. 6. Elemento incorrecto

elemento en casi todas las respuestas del servicio REST y la frecuencia de aparición en estos casos es siempre uno. Tras su estudio se ha observado que este elemento debería estar en todas las respuestas. El valor estadístico que ha identificado esta anomalía ha sido la varianza la cual tiene un valor muy bajo, sin ser 0.

En el último tipo, figura 6, se presenta en un elemento que aparece solo en un número muy pequeño de resultados del servicio. Hay varias razones para ello: Una de ellas corresponde a un falso positivo, ya que al igual que ocurrió en el análisis del servicio REST Google Places, se trata de respuestas atípicas. Otra razón ha sido que el elemento no debería existir y, por lo tanto, se ha obtenido una respuesta incorrecta del servicio REST. La última de las razones que ha causado una anomalía ha sido un elemento mal situado dentro de la respuesta o un nombre de un elemento incorrecto; en este caso, pese a ser una repuesta incorrecta, ya ha sido detectado en el anterior tipo de anomalía y era producido por elementos que faltaban en las respuestas del servicio. Este tipo de anomalía se ha identificado gracias al conjunto de las variables estadísticas que indican el valor máximo y mínimo de apariciones de los elementos.

Como resultado del análisis de las anomalías se han detectado:

- Tres elementos duplicados en diferentes respuestas XML del servicio.
- Cinco elementos descolocados en varias de las respuestas XML.
- Un elemento correctamente colocado pero cuyo nombre se encuentra modificado en una de las respuestas XML.
- Dos elementos que no deberían aparecer en las respuestas XML del servicio REST analizado.
- Siete casos en los que la anomalía se debía a un falso positivo.

V. CONCLUSIONES Y TRABAJOS FUTUROS

Nuestra solución es capaz de descubrir anomalías que otros sistemas de pruebas no son capaces de detectar con la ventaja de que no se necesita especificar la respuesta esperada para cada petición. Además, obtenemos un esquema XSD de forma más consistente y más específica que otras herramientas de inferencia disponibles en el mercado, lo que permitirá generar de forma automática la especificación WADL del servicio o incluso crear de forma automática las clases de un cliente específico para ese servicio, reduciendo enormemente el tiempo de desarrollo. También hemos podido comprobar que la herramienta es capaz de detectar anomalías que, si bien no son errores, pueden determinar casos especiales, ofreciendo

la posibilidad de utilizar el sistema para identificarlos. Por ejemplo, en el caso de estudio sobre Google Places, podría ser interesante encontrar esos lugares en los que no hay locales alrededor. Esto nos lleva a pensar que se podrían explorar otras funcionalidades para la herramienta.

Sin embargo, este sistema presenta algunas limitaciones. Debido a que el análisis es estadístico, no se puede utilizar para realizar pruebas simples, con pocas peticiones al servicio, ni para detectar errores que no destaquen del funcionamiento normal, es decir, errores que sucedan siempre o en una proporción igual a la de otros errores. Una posible solución a este problema sería la posibilidad de incluir como parámetro de entrada el esquema XSD esperado y compararlo con el obtenido para detectar los elementos anómalos.

Para que esta solución fuese posible, habría que asegurar que el esquema inferido es lo más fiel posible a la realidad. Aunque nuestro inferidor ofrece esquemas muy definidos y atados a los documentos de entrada, se podría mejorar. Por ejemplo, el algoritmo que calcula la distancia entre elementos XML que se utiliza para calcular los elementos que pertenecen a un tipo complejo podría ser sustituida por nuevos algoritmos como el cálculo de la distancia pq-gram [16].

Otra vía de evolución consistiría en estudiar la forma de aplicar el mismo tratamiento a respuestas JSON o en otros formatos. Tanto la solución a esta desventaja como a la anterior representan vías de investigación que nos gustaría abordar en un futuro, ahora que hemos determinado la viabilidad de la solución, para así poder generalizar el uso de la herramienta.

El módulo detector de anomalías y su diagnóstico son también susceptibles de mejorar. El estudio de reglas más complejas y de nuevos mecanismos de detección, como algoritmos de aprendizaje automatizado tales como algoritmos de clasificación o de detección de grupos, supondrían una mejora de la calidad de los resultados ofrecidos.

Para finalizar, pensamos que este sistema es sólo el primer paso para crear un entorno de soporte al desarrollo de servicios REST, ofreciendo la posibilidad no sólo de depurar el servicio sino además ofrecer funcionalidades adicionales como la generación de la definición del servicio o la generación de un cliente.

Referencias

[1] M. Bozkurt, M. Harman, and Y. Hassoun, "Testing and verification in service-oriented architecture: a survey," *Software Testing, Verification and Reliability*, 2012. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/stvr.1470/full

[2] "SoapUI - the home of functional testing," http://www.soapui.org/. [Online]. Available: http://www.soapui.org/

[3] S. Chakrabarti and P. Kumar, "Test-the-REST: an approach to testing RESTful web-services," in *Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns, 2009. COMPUTATIONWORLD '09. Computation World:*, 2009, pp. 302–308.

[4] "rest-assured - java DSL for easy testing of REST services," http://code.google.com/p/rest-assured/. [Online]. Available: http://code.google.com/p/rest-assured/

[5] F. Besson, P. Leal, and F. Kon, "Rehearsal: A framework for automated testing of choreographies," Technical report, University of Sao Paulo, Department of Computer Science, Tech. Rep., 2011. [Online]. Available: http://ccsl.ime.usp.br/baile/files/tech-report-vv_2011.pdf

[6] H. Reza and D. Van Gilst, "A framework for testing RESTful web services," in *2010 Seventh International Conference on Information Technology: New Generations (ITNG)*, 2010, pp. 216–221.

[7] Y. Papakonstantinou and V. Vianu, "DTD inference for views of XML data," in *Proceedings of the nineteenth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, 2000, pp. 35–46.

[8] G. J. Bex, F. Neven, and S. Vansummeren, "Inferring XML schema definitions from XML data," in *Proceedings of the 33rd international conference on Very large data bases*, ser. VLDB '07. VLDB Endowment, 2007, pp. 998–1009. [Online]. Available: http://dl.acm.org/citation.cfm?id=1325851.1325964

[9] G. J. Bex, F. Neven, T. Schwentick, and S. Vansummeren, "Inference of concise regular expressions and DTDs," *ACM Transactions on Database Systems (TODS)*, vol. 35, no. 2, p. 11, 2010. [Online]. Available: http://dl.acm.org/citation.cfm?id=1735890

[10] K. Nordmann, "Algorithmic learning of XML schema definitions from XML data," 2011. [Online]. Available: https://kore-nordmann.de/talks/11_03_learning_xml_schema_definitions_from_xml_data.pdf

[11] "XML-Schema-learner," https://github.com/kore/XML-Schema-learner. [Online]. Available: https://github.com/kore/XML-Schema-learner

[12] "Trang," http://www.thaiopensource.com/relaxng/trang.html. [Online]. Available: http://www.thaiopensource.com/relaxng/trang.html

[13] "Microsoft .NET framework," http://www.microsoft.com/net. [Online]. Available: http://www.microsoft.com/net

[14] C. Grün, S. Gath, A. Holupirek, and M. H. Scholl, *XQuery full text implementation in BaseX*. Springer, 2009.

[15] "Api del servicio web de google places," Website, https://developers.google.com/places/documentation/l.

[16] N. Augsten, M. Böhlen, and J. Gamper, "The pq-gram distance between ordered labeled trees," *ACM Transactions on Database Systems (TODS)*, vol. 35, no. 1, p. 4, 2010.

Arquitectura de VoIP en la Nube con interfaz Web, verde, open source y de bajo coste

Álvaro Suárez[1], Giuseppe Blacio[2], Elsa Macías[1], Boris Ramos[2]

[1]Grupo de Arquitectura y Concurrencia, Departamento de Ingeniería Telemática
Universidad de Las Palmas de Gran Canaria
Campus Universitario de Tafira, Edificio de Electrónica y Telecomunicación, Pabellón C., España

[2]Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral
Campus Gustavo Galindo, Km. 30,5 Vía Perimetral, Guayaquil, Ecuador
asuarez@dit.ulpgc.es, gblacio@espol.edu.ec, emacias@dit.ulpgc.es, bramos@espol.edu.ec

***Resumen*- La *Voz Sobre IP* (*VoIP*) es un servicio esencial de la Sociedad del Conocimiento actualmente. Nuevas formas de proveer dicho servicio son necesarias para facilitar su uso y proporcionar mayores beneficios a los proveedores de servicio y a los usuarios. Proveer dicho servicio a través de la Nube es una forma de permitir el ahorro de costes a los proveedores de servicios, mientras que proveer el servicio mediante interfaces Web hace que los usuarios puedan experimentar un mayor beneficio y comodidad de uso. Actualmente conocemos empresas que tratan de proveer dicho servicio en la Nube y algunos proyectos que independientemente de las empresas anteriores permitirán hacer uso de la VoIP mediante interfaces Web. En este artículo nosotros hacemos una propuesta inicial de diseño de una arquitectura de servicios de VoIP en la Nube que permite, de manera directa, el uso de interfaces Web en los clientes de telefonía que además combina aspectos de seguridad básicos. Una ventaja adicional es que todo el software que se usaría es de libre distribución.**

***Palabras Clave*- VoIP, Nube, WebRTC, WebSocket.**

I. INTRODUCCIÓN

La telefonía es un servicio básico proporcionado a los ciudadanos desde hace más de un siglo. La telefonía analógica [1] tiene aún vigencia en una gran cantidad de hogares, organismos públicos y empresas de todo el Mundo. La telefonía digital [2] hizo su aparición a finales del siglo XX y se sigue usando hoy en día. Aunque este servicio se proporcionó inicialmente sobre medios de comunicación físicos guiados, hoy en día existen muchas más líneas telefónicas de abonados que lo usan sobre medios no guiados. A finales de los años 1970 se comenzó a experimentar con la transmisión de la voz sobre el *Internet Protocol* (*IP*) [3]. Los resultados de esta investigación verían sus frutos comerciales masivos casi 30 años más tarde. Hoy en día Internet es la base del despliegue de muchas formas de comunicar la voz, una de las cuales es la VoIP [4]: un servicio telemático que se despliega en base a IP teniendo a distintos tipos de redes telefónicas como redes de acceso al Núcleo de Internet. Núcleo que ofrece la posibilidad de realizar comunicaciones a escala local y global a un coste económico reducido.

Estos resultados han conllevado el diseño de un sinfín de nuevos protocolos, servicios y arquitecturas que pretenden desplegar la Voz a cualquier dispositivo capaz de soportar la ejecución de programas almacenados y ejecutados por un procesador de relativa baja potencia. La conjunción de estos resultados con la tecnología de software denominada *Open Source* ha producido una cantidad de aplicaciones de libre distribución en los últimos años muy difícil de resumir; entre ellos están: Clientes (*Line*), Servidores (*Asterisk*), Gateways (*GNU Gatekeeper*) y señalización telefónica (*openSS7*).

La importancia de este servicio es variada (desde varios puntos de vista): a) Social, la globalización ha hecho que muchas personas emigren de sus países a otros geográficamente muy lejanos. El abaratamiento de los costes que supone la VoIP hace que sea de gran utilidad y se pueda considerar un servicio esencial de la Sociedad del Conocimiento. b) Académico, la gran complejidad que supone el despliegue de este servicio eficazmente hace que sea un tema esencial para explicar la evolución de las redes de telecomunicación y de Internet: es un ejemplo ideal para analizar los puntos críticos del funcionamiento de una red de comunicación heterogénea: encaminamiento, congestión, ingeniería de tráfico, interconexión de redes heterogéneas.... c) Investigación, a día de hoy sigue existiendo distintos problemas para proveer este servicio de manera eficiente en terminales móviles e inalámbricos y con interfaces universales tipo Web, por ejemplo. d) Comercial, no cabe duda que este servicio sigue siendo uno de los que más rentabilidad proporciona, directa o indirectamente, tanto a los operadores de telecomunicación como a los grandes proveedores de servicios de Internet. Por otro lado, las barreras de Mercado no son altas para pequeñas compañías que quisieran entrar en este Mercado a nivel local.

A pesar del gran despliegue de la VoIP hoy en día y de su gran importancia según los puntos de vista analizados, la provisión del servicio sigue evolucionando por varias razones: a) es necesario que el usuario tenga una interfaz de comunicación muy sencilla (Web) de usar (conseguir un grado de usabilidad elevada), b) las empresas del Sector siguen apostando por proveer un servicio que proporcione mayor *Calidad de Experiencia de usuario* (*QoE*, del inglés

Quality of Experience), puesto que con ello se obtienen más ganancias económicas. Para ello ofertan VoIP con un elevado grado de movilidad del usuario usando comunicaciones móviles e inalámbricas, y c) reducir el consumo energético de los equipos de telecomunicación de una Empresa proveedora de servicios de VoIP haría que se reduzca el *CAPital EXpenditure* (*CAPEX*) y el *OPeration EXPenditure* (*OPEX*) logrando mayor rentabilidad empresarial: algunos autores piensan que esto se puede lograr mediante la VoIP en la Nube.

Hasta donde alcanza nuestro conocimiento del tema, actualmente existen soluciones comerciales de VoIP en la Nube (*Aero*, *Twilio*, *Alteva*…), otras que intentan proporcionar interfaz Web en los equipos terminales (que proporcionan servidores de VoIP gratuitos como *OverSIP* y *JsSIP*) basadas en software libre; pero nunca antes se había propuesto una arquitectura de servicios que combine ambos tipos de soluciones. La idea principal de este artículo es proponer el diseño de un servicio de VoIP en la Nube, aplicable a distintos tipos de nubes con cambios muy pequeños, con interfaces Web de acceso en los equipos terminales. Esta solución es eficaz porque reduce el CAPEX y el OPEX, es segura y permite el ahorro energético (verde) y acceso móvil ubicuo.

En este artículo primero revisamos soluciones de VoIP en la Nube y presentamos las ideas básicas de nuestra propuesta en relación a este aspecto. Después analizamos algunas soluciones muy recientes que permiten acceder al servicio de VoIP usando únicamente interfaz Web. Por último, mostramos nuestra propuesta de servicio de VoIP en la Nube con interfaces Web teniendo en cuenta todos los aspectos de nuestra solución y presentamos algunas conclusiones.

II. Servicio de VoIP en la Nube

Dos aspectos importantes de la VoIP son: la señalización y la comunicación de la voz. Para la señalización en Internet tradicionalmente se han utilizado un conjunto amplio de protocolos como la familia de *H.323* [5], el *Inter Asterisk eXchange 2* (*IAX2*) [6] y el de propósito general *Session Initiation Protocol* (*SIP*) [7]. Los dos últimos son los que mayor uso tienen debido a que se utilizan con *Private Branch eXchange* (*PBX*) de software libre y existen muchas distribuciones de código abierto. El *Real Time Protocol* (*RTP*) se utiliza universalmente para transportar la señal de voz digitalizada y empaquetada procedente de los *COdificadores-DECodificadores* (*CODEC*s) y siguiendo alguno de los perfiles predefinidos por este protocolo. El uso masivo de RTP y SIP en los hogares y empresas en los que se instala *Network Address Translation* (*NAT*) es posible gracias a mecanismos de red como *Session Border Controller* (*SBC*) o bien protocolos como *Traversal Using Relays around NAT* (*TURN*), *Session Traversal Utilities for NAT* (*STUN*) e *Interactive Connectivity Establishment* (*ICE*).

La Nube es un paradigma de provisión de servicios (Infraestructuras, Plataforma o Software) [8] asociado a Internet y la Web directamente. Por tanto, a nivel técnico, el despliegue de la VoIP en la Nube es independiente de los protocolos de señalización y comunicación de datos que se use en Internet. Esto es, dichos protocolos pueden ser usados de manera directa para VoIP en la Nube. O lo que es lo mismo, quizás el detalle más relevante a resolver es el de la señalización de todas las llamadas y la mayor tasa de bits requerida sea el apropiado (en servidores centralizados en la Nube). Además para interconectar las redes telefónicas a Internet se pueden usar las arquitecturas de protocolos estandar: *Signalling System number 7* (*SS7*), *Media Gateway Control Protocol* (*MGCP*), *Signalling Transport* (*SIGTRAN*) ... [9]. Por tanto, a nivel técnico el aspecto más importante del diseño de la VoIP en la Nube es el diseño del centro de cálculo que acoja a los servidores de VoIP y su dimensionado para que sean capaces de soportar un número de llamadas dado (haciendo posible su escalabilidad). Dependiendo del uso que se de a estos servidores, este dimensionado tendría un impacto u otro. Por ello distinguimos tres tipos de servidores de VoIP alojados en una nube: a) *pública*, mediante la cual una organización ofrece servicios al público en general [10], b) *privada*, mediante la cual una organización ofrece servicios sólamente a sus empleados o socios. Normalmente, las máquinas de este tipo de nube se aloja en los límites de la organización propietaria (con conexión directa a un encaminador extremo de Internet) o bien en las instalaciones de un proveedor externo (en este caso habitualmente mediante virtualización) [10]. Difieren principalmente de las nubes públicas en el que la infraestructura asociada a esa nube no se comparte con alguna otra empresa o entidad, y c) *híbrida* [11] que combinan acceso público restringido y acceso particular: pueden ser un modelo de paso entre una nube privada a una nube pública en la que la seguridad del acceso de usuarios debe estar garantizado en un grado elevado.

Obviamente, el Núcleo de Internet debe ser capaz de soportar el volumen de tráfico de VoIP proyectado y nosotros suponemos que como parte de la conexión de estos servidores a Internet se ha hecho el *Service Level Agreement* (*SLA*) que sería capaz de contrastar la QoS determinada en estos casos.

La razón de que se busque proveer un servicio de VoIP en la Nube a nivel económico es variado según distintos objetivos. A título de ejemplo nombramos tres: a) un organismo público que desee "controlar" su servicio de telefonía para ahorrar costes (por ejemplo una universidad grande), podría desplegar un servicio de nube privada en su centro de cálculo y comunicaciones. Con el debido SLA con proveedores de VoIP internacionales podría ahorrar costes en las facturas de telefonía. A la vez que dentro del organismo todas las comunicaciones de voz se hacen sobre su red privada. La ventaja de esto es que se puede asegurar la privacidad y desplegar servicios de VoIP experimentales que incluso puedan ser liberados comercialmente posteriormente, b) una Empresa proveedora de Servicios de VoIP, lo desplegaría en una nube pública para ofrecer un servicio ágil en el que fácilmente se podrían desplegar nuevos servicios de VoIP o se podrían particularizar por grupos de clientes dinámicamente o bien redefinir algunos de esos servicios simplemente instalando nuevo software en función de la demanda de servicios. Por otro lado, también podría alquilar sus servicios como plataforma a terceros o incluso ofrecer software de VoIP como servicio, y c) una *Pequeña y Mediana Empresa* (*PYME*) con varias sedes geográficamente distantes (dentro de un mismo país) podría manejar todas sus comunicaciones internas (y otras provenientes de la telefonía convencional) usando un servidor en su nube privada con lo cual ahorraría en la instalación de varios servidores

distribuidos (esta suele ser la solución típica) y ahorrar en costes de mantenimiento... Nótese que la experiencia que gane una PYME tecnológica en el uso de VoIP entre sus empleados puede servir como base para crear una nube híbrida con la que ir liberando productos de VoIP incrementalmente con vistas a su comercialización.

En cualquiera de los casos anteriores, el servicio de VoIP en la Nube soportaría usuarios en movilidad de manera directa simplemente accediendo al servicio instalado en la Nube (en un lugar de Internet), configurando el acceso de los clientes de VoIP (SIP) en distintos terminales. Disponer de los perfiles de los usuarios en la Nube representa una ventaja grande de este tipo de soluciones por cuanto simplifica enormemente la configuración de los clientes de VoIP. Nótese que la movilidad podría darse dentro de las instalaciones de un organismo o PYME o bien fuera de sus instalaciones.

En la tabla I presentamos las ventajas de la VoIP en la Nube frente a una arquitectura tradicional de VoIP y a la telefonía tradicional (entendiendo por ésta la que se produce en las redes nativas de telefonía por medios de comunicación guiados o no guiados).

Hasta donde nosotros conocemos, las empresas que ofertan servicios de VoIP en la Nube únicamente proveen estos servicios pero no facilitan la conexión de los usuarios mediante interfaces de telefonía que les simplifique la conexión telefónica, como podrían ser las interfaces Web.

III. Clientes de VoIP con interfaz Web

Que un organismo o PYME o incluso usuarios individuales contraten un servicio de VoIP en la Nube les evita tener que destinar recursos humanos y físicos para controlar y alojar a los servidores de VoIP y la electrónica de Red necesaria (conmutadores habilitados para voz, encaminadores, Gateways, SBCs...). Esto supone un ahorro en CAPEX y OPEX así como energético (que libremente podríamos denominar *VoIP verde*). Sin embargo, todavía deben disponer de equipos terminales de telefonía o bien softphones (clientes) que les permitan acceder al servicio cómodamente y sin necesidad de instalar software en sus equipos terminales. Esto tiene el inconveniente de que usuarios no expertos tienen una curva de aprendizaje del funcionamiento de estos equipos elevados y suelen tener problemas con su uso debido a la complejidad que tienen (son mucho más complejos que un simple equipo de telefonía tradicional). Por ello, las empresas u organismos deben destinar recursos humanos técnicos al entrenamiento y solución de problemas con el uso de estos equipos terminales.

Uno de los objetivos de la VoIP con terminales de telefonía con interfaz Web es conseguir que los usuarios puedan usar de una forma muy simple y cómoda este servicio usando únicamente navegadores Web (normalmente gratuitos). Con ello se consigue reducir los costes de mantenimiento de los softphones (no Web) y también de entrenamiento y solución de problemas de su uso (para usuarios no expertos). Para poder disponer de interfaces potentes que permitan utilizar todos los servicios de VoIP es necesario usar el *Hiper Text Markup Language 5* (*HTML5*). Con las tecnologías de HTML5 es posible diseñar interfaces Web de VoIP amigas del usuario y muy simples de manejar. Además, sería incluso posible que el usuario final diseñara el tipo y funcionalidad adicional del terminal que quisiera usar; pudiendo por ejemplo, definir únicamente aquella funcionalidad que realmente vaya a utilizar (reduciendo de esta manera la curva de aprendizaje).

Para la utilización de VoIP con interfaz Web es necesario llevar a cabo la señalización y la comunicación de voz empleando los protocolos de la Web. Para ello existen dos proyectos recientes: los *WebSockets* y el *WebRTC*.

El HTTP crea una conexión *Transmission Control Protocol* (*TCP*) cada vez que el cliente (navegador) Web inicia la conexión con el servidor Web [12]. En cambio, un WebSocket define un protocolo que habilita la comunicación full-duplex entre un cliente y un servidor Web usando una única conexión TCP para sucesivas conexiones entre ellos. De esta manera un WebSocket, implantado en *Javascript* dentro de una página HTML5, simplifica el manejo de la comunicación entre cliente y servidor Web permitiendo que todas se lleven a cabo mediante una conexión TCP (canal

Tabla I
Comparación de sistemas de telefonía

	Telefonía tradicional	VoIP	VoIP en la Nube
Conmutación	*Circuitos*	*Paquetes*	*Paquetes*
Gestión llamadas	*Independiente*	*Independiente/dependiente*	*Dependiente*
Personalización	*Alta*	*Alta*	*Baja*
Escalabilidad	*Baja*	*Media*	*Alta*
Calidad Voz	*Alta*	*Media*	*Media*
Tasa bits	*Fija 64 Kbps*	*Variable 16-128 Kbps*	*Variable 16-128 Kbps*
Estándares	*Bien definidos*	*Compiten entre sí*	*Compiten entre sí*
Servicios	*Tradicionales*	*Tradicionales y añadidos*	*Tradicionales y añadidos*
Infraestructura	*Dedicada*	*Compartida con otros tipos de datos*	*Compartida también*
Operadores	*Uno sólo*	*Varios*	*Varios*
Numeración	*Dependiente ubicación*	*Independiente*	*Independiente*
Números emergencia	*Se ubica al llamante directamente*	*No se puede ubicar directamente*	*No se puede ubicar directamente*
Flexibilidad	*Baja*	*Media*	*Alta*
Gestión ENUM	-	*Independiente*	*Dependiente*
CAPEX	*Alto*	*Alto*	*Bajo*
OPEX	*Alto*	*Medio*	*Bajo*

lógico). Sin embargo, su uso puede plantear problemas para el manejo de la sincronización en VoIP en el que se suelen necesitar más de un canal lógico de señalización. Aunque su uso representa un avance importante para dicha señalización debido a que el servidor puede enviar datos sin ser pedidos al navegador Web (con los protocolos tradicionales de HTTP esto se puede hacer pero de manera muy laboriosa y compleja en algunos casos). Además, el WebSocket proporciona una enorme reducción en el tráfico innecesario en la red y el retraso en comparación con Polling y Streaming, que se utilizan para emular una conexión full-duplex [13]. El funcionamiento básico del protocolo de WebSockets se puede resumir en los siguientes pasos:

1) La conexión WebSocket inicia su ciclo de vida como una conexión HTTP, lo que garantiza la plena compatibilidad con los sistemas pre-WebSocket.
2) El navegador envía una petición (*WebSocket handshake*) al servidor indicando que quiere cambiar de HTTP al protocolo de WebSocket actualizando la cabecera (*upgradeheader*).
3) La conexión HTTP cambia a la conexión WebSocket sobre la misma conexión TCP utilizando los mismos puertos estándar de HTTP (80) y HTTPS (443), de manera predeterminada [12].

En [14] se puede encontrar un mecanismo de transporte de mensajes SIP sobre Websockets. En la fase de handshake, el cliente debe incluir el valor de SIP en su cabecera. En [15] se muestra un ejemplo ilustrativo completo de sincronización SIP a través de Web Sockets usando conexiones P2P y a través de un *Proxy*.

El proyecto WebRTC lo estandariza actualmente el grupo *RTCWeb* del *Internet Engineering Task Force* (*IETF*) y su *Aplication Programming Interface* (*API*) la estandariza el *WebRTC Working Group* [16] del *World Wide Web Consortium* (*W3C*) [17]. La idea básica de este proyecto es lograr la comunicación de voz entre terminales o navegadores [16] [18], sin instalar *plugins* o *native apps*, usando APIs en HTML5 y transportando la voz en *Secure RTP* (*SRTP*) [19]. Los CODECs a implementar para asegurar la comunicación por WebRTC son [20]: *Opus* (soporta audio de alta calidad), *G.711* (apropiado para conexión con la red telefónica clásica) y *Telephoneevent* (transmisión de tonos *Dual Tone Multi Frecuency* (*DTMF*) en paquetes IP). Los pasos básicos mediante los cuales se hace una sesión WebRTC son:

1) Acceso al audio y vídeo local usando la *Media Stream API* y solicitando el acceso mediante *getUserMedia*.
2) Establecimiento de la conexión entre terminales (navegadores o terminales telefónicos) usando la *RTCPeerConnection API* la cual puede hacer uso de: ICE, TURN y STUN para atravesar *firewalls* y NAT.
3) Intercambio de flujos de voz generando inicialmente la descripción de la sesión mediante el objeto *SessionDescription*: objeto que describe una sesión mediante *Session Description Protocol* (*SDP*). Para cerrar la conexión, se invoca al método *close* del objeto *RTCPeerConnection*.
4) Cerrar la conexión.

IV. PROPUESTA DE ARQUITECTURA DE SERVICIOS DE VOIP

Una vez revisadas las ideas básicas de la VoIP en la Nube, y los protocolos de sincronización y comunicación de voz a través de la Web, en este apartado presentamos nuestra propuesta de VoIP en la Nube que incluye dispositivos terminales que usarían WebRTC y WebSockets que se ha estudiado en profundidad en [15]: en ese trabajo hemos presentado una arquitectura completa de VoIP en la Nube con interfaces Web teniendo en cuenta además aspectos de la seguridad de la provisión del servicio en la Nube.

Para el diseño del servicio de VoIP en la Nube se ha seguido un diseño de la interconexión de dispositivos de red y especialización de funciones mediante un modelado jerárquico [21]. Un objetivo de este modelo es especializar distintas partes de la red (normalmente una *Local Area Network* (*LAN*) o tipo de red asimilada) y mantener la funcionalidad de los equipos lo más simple posible haciendo descansar la complejidad en las relaciones entre las distintas partes de la red. Para obtener la organización de los componentes físicos y lógicos de la arquitectura de la red se utiliza un esquema *top-down* distinguiendo una serie de partes bien diferenciadas:

1. El Nivel de acceso provee la conectividad de equipos terminales y servidores, así como una posible clasificación en grupos de trabajo (organizados en *Virtual LAN*s (*VLAN*s) por ejemplo) y herramientas de seguridad.
2. El Nivel de distribución provee conectividad basada en políticas de entrega de tráfico, filtrado de seguridad, balanceo de cargas, QoS, encaminamiento entre VLAN y demás políticas de una organización. También se utiliza para aislar problemas en la red.
3. El Nivel del núcleo provee un backbone de alta velocidad para los conmutadores de distribución. Al ser este nivel crítico para las comunicaciones debe proveer una elevada confiabilidad de la red y adaptarse muy rápido a los cambios.

Cada nivel proporciona la funcionalidad necesaria para la red. Cabe mencionar que no es estrictamente necesario implementar cada nivel por separado en entidades físicas diferentes sino que pueden compartir recursos en un mismo equipo, pero cuando el número de usuarios, y por lo tanto el tráfico, aumenta de manera considerable, se recomienda su separación, para una gestión más eficaz.

Este diseño de LAN debe conectarse a Internet mediante las tecnologías de acceso de alta velocidad existentes en el Mercado. Además sobre esas conexiones se debe proveer la posibilidad de construir *Virtual Private Networks* (*VPN*), sobre Internet, que permita la provisión de VoIP segura. Además se deben proveer acceso a las redes telefónicas clásicas.

En la LAN debe existir una *zona desmilitarizada* (*DMZ*, del inglés *DesMilitarized Zone*) [22] en la que se alojan servidores internos y datos de acceso público. Los servidores de VoIP (WebRTC) serán alojados en esta zona desmilitarizada a la que sólo pueden acceder usuarios autorizados previamente.

Adaptando los modelos de [23] hemos determinado las distintas partes de la LAN: Módulo de red interna (LAN), Módulo de borde de distribución, Módulo de borde corporativo, Módulo de red de acceso y Módulo equipos

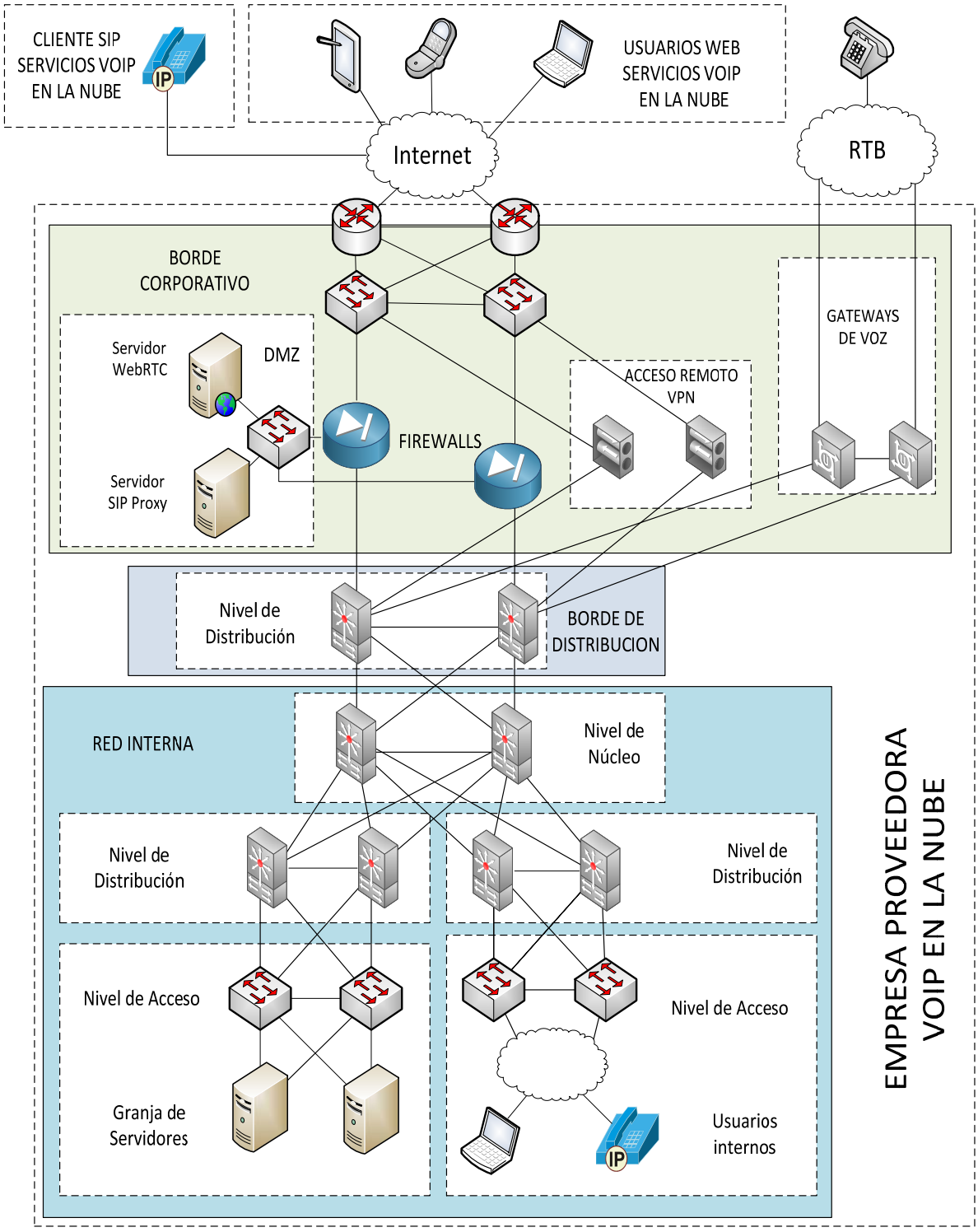


Fig. 1. Arquitectura de Servicios de VoIP en la Nube con interfaz Web en los clientes.

terminales. La ventaja de este diseño modular es que para cambiar de un tipo de nube privada a híbrida y a pública, en general sólo es necesario hacer cambios en el Módulo de acceso, porque la funcionalidad del resto de módulos se mantiene prácticamente invariante.

En la Fig. 1 se muestra un esquema general de la solución que proponemos.

En esta arquitectura de servicios de VoIP, los usuarios con teléfonos móviles inteligentes, tabletas, o computadores, pueden acceder al servicio por medio de la Web a través de HTML5; el usuario se registra en el servidor WebRTC, y a continuación puede realizar una solicitud de llamada sea a otro usuario Web, a un teléfono IP físico SIP en Internet, o a un número convencional de la red telefónica clásica. El servidor WebRTC debería estar en una DMZ. Otra posibilidad de registro consiste en que el usuario solicitara el registro a través de acceso remoto por VPN si la necesidad de seguridad es mayor para la empresa que provee el

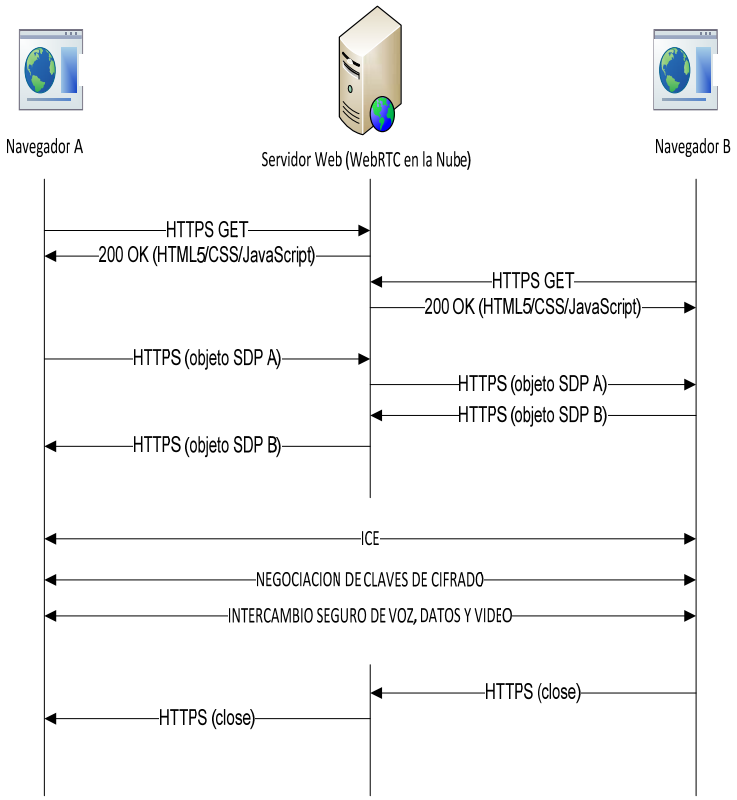


Fig. 2. Diálogo básico entre dos navegadores Web (clientes de VoIP) a través de un servidor Web habilitado con WebRTC.

servicio. Se recomienda que el acceso a la red telefónica clásica y las bases de datos de los usuarios estén detrás de un firewall, para maximizar en lo posible las medidas de seguridad. Nótese que este esquema puede ser utilizado para nubes privadas e hibridas. Las diferencias entre ellas es que los usuarios se registrarían de forma diferente: en la nube privada por ejemplo existiría un registro masivo controlado de todos los usuarios de la Organización o PYME, registro que lo haría el gestor del servidor WebRTC.

Para ilustrar como se llevaría a cabo la comunicación en nuestra arquitectura de servicios de VoIP mostramos un ejemplo de diálogo en la Fig. 2 entre dos navegadores Web (el servidor Web se supone que está habilitado con WebRTC). A continuación se analiza el flujo de mensajes entre dos navegadores habilitados para WebRTC que hiciera uso del servidor de VoIP en la Nube que hemos presentado:

1. El navegador A solicita una página Web al servidor Web.
2. El servidor Web proporciona la página Web con *WebRTCJavaScript* al navegador A.
3. El navegador B solicita una página Web al servidor Web.
4. El servidor Web proporciona la página Web con *WebRTC JavaScript* al navegador B.
5. El navegador A decide comunicarse con B, entonces el navegador A envía una solicitud por medio de un objeto *SDP* de A al servidor Web.
6. El servidor Web envía el objeto SDP de A en *JavaScript* a B.
7. Usando *JavaScript* en el navegador B, se envía una respuesta por medio de un objeto SDP al servidor WebRTC.
8. El servidor WebRTC envía el objeto SDP de B usando *JavaScript* a A.
9. A y B comienzan un proceso para determinar la mejor ruta para alcanzarse directamente usando ICE.
10. A y B hacen el intercambio de claves para la comunicación segura de la voz.
11. A y B comienzan en intercambio de voz, datos y video.
12. El navegador B cierra la conexión mediante HTTP seguro (*HTTPS*)

Nótese que en el caso de que un terminal no pueda implantar el navegador Web entonces se debe usar un proxy que si lo pueda implantar, y se deberían añadir los pasos adicionales de la comunicación con el proxy. Como ejemplo, en la Fig. 3 hemos considerado un navegador A y un Cliente SIP estándar. Como se aprecia, en primer lugar se produce una negociación entre el navegador A y el servidor Web para pactar el tipo de CODEC, velocidades de transmisión… Esta negociación comienza cuando el servidor Web proporciona la página Web con *WebRTC JavaScript* al navegador A, una vez que éste lo ha solicitado a través de un mensaje GET de *HTTP Secure* (*HTTPS*).

Un aspecto a considerar es que cuando el usuario del Navegador A decide realizar la comunicación, el código JavaScript del navegador habilita restricciones de acceso basada en la descripción de la información multimedia a ser manejada (voz o vídeo), solicita los medios de comunicación, y consigue permiso del usuario. La información multimedia deseada se captura en un objeto SDP, se envía al cliente SIP B por medio del servidor Web y se re-envía al *SIP Proxy* en el que se encuentra registrado el cliente SIP B.

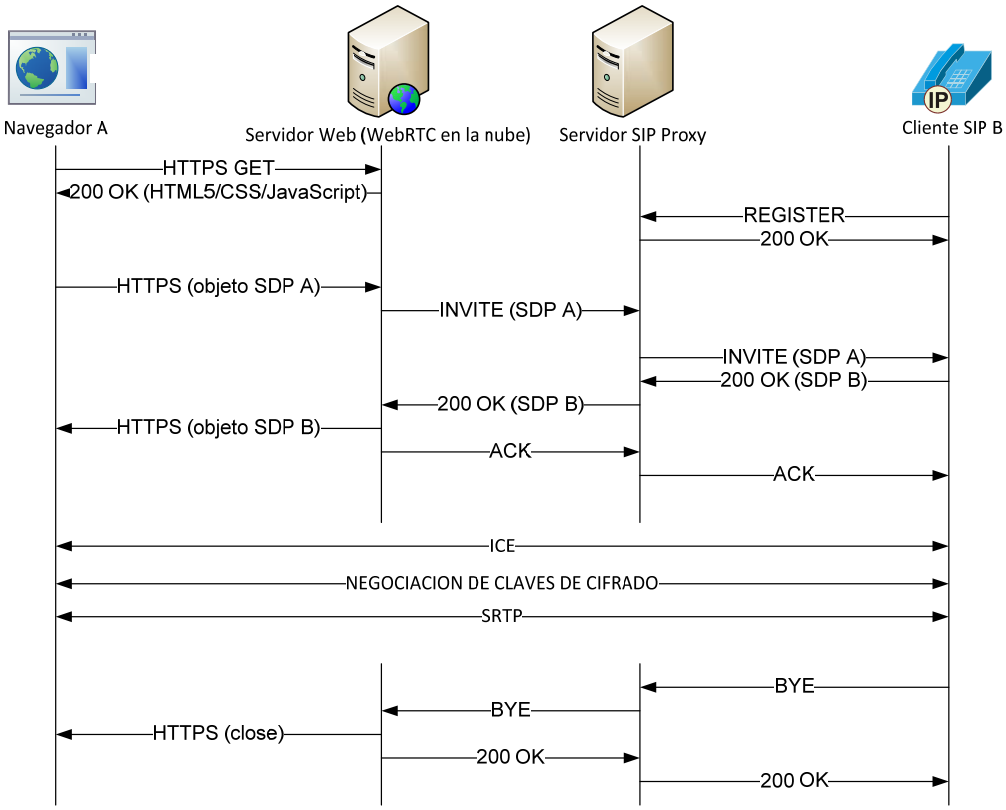


Fig. 3. Diálogo entre un navegador sin WebRTC y un cliente estándar de SIP.

Es importante notar que WebRTC no estandariza la forma en cómo estos navegadores envían estas peticiones y ofertas (aún está en desarrollo).

Entonces, el Cliente SIP B recibe la invitación (mensaje SIP *INVITE*), y respondería por medio de un mensaje SIP *200 OK*, el cual sería enviado en formato SIP convencional hasta el servidor Web, donde será traducido por medio de *WebSockets SIP*.

Otro detalle a mencionar es que el Navegador A no envía al cliente SIP B un mensaje de confirmación ACK, sino que el servidor Web lo realiza por él.

Una vez realizado este proceso se produce la comunicación directa entre ambos clientes, a través de ICE. Acto seguido empieza un proceso de intercambio de claves de cifrado del tráfico de voz. El intercambio el tráfico de datos, será transportado por medio del *SRTP*, entre los clientes directamente.

Cuando la llamada de voz finaliza el cliente SIP B envía un mensaje SIP *BYE* a su *SIP Proxy* el cual lo re-envía al servidor B y este lo traduce a un formato HTTPS para cierre de la conexión. E igualmente el servidor Web confirma por el Navegador A al cliente SIP B.

V. Conclusiones

El servicio de VoIP es un ejemplo de éxito de los círculos de innovación con tres ejes sintonizados: Universidad, Empresa y Mercado. Las iteraciones de innovación en este Círculo aún no han terminado porque: aún es posible iterar sobre nuevos retos de investigación que conllevan a nuevos modelos de uso en la Empresa y estrategias de Mercado para descubrir nuevas formas de explotar comercialmente dicho Servicio proyectando la investigación que se haga en la Universidad.

En este artículo hemos presentado un trabajo inicial en el que se analiza el despliegue de una nueva forma de ofertar el servicio de VoIP. La idea básica fue diseñar una infraestructura de VoIP en la Nube (válida para nubes privadas, híbridas y públicas) en la que la seguridad sale reforzada y además se logra reducir el CAPEX, provee seguridad de uso y ahorro energético a PYMES que optaran por instalar sus PBXs en sus instalaciones. Puede proveer un servicio como Software, Plataforma o Infraestructura. Además, consideramos que las interfaces del servicio se proveerían a través de Web de manera integrada con la solución de la VoIP en la Nube. Esto mejora el OPEX de equipos terminales considerablemente al no existir la necesidad de instalar y configurar complejos softphones para usuarios no expertos. No conocemos ninguna solución similar a la que hemos presentado.

Este trabajo inicial se debe completar para considerar los problemas reales que se plantean en una arquitectura de servicios de este tipo. Por ejemplo, el acceso inalámbrico y móvil a través de Web a la arquitectura del servicio de VoIP tiene varios retos que deberían ser abordados, entre ellos:

1) Medir la sobrecarga de señalización en la Red y el impacto que provocaría los WebSockets sobre los canales móviles.
2) En el campo de las interfaces Web sería interesante estudiar una forma muy rápida de generar automáticamente distintos tipos de softphones para distintos tipos de usuarios según su experiencia usando el servicio: por ejemplo, un usuario que no

tiene ninguna experiencia automáticamente podría generar una interfaz muy simple y a medida que va ganando en experiencia podría ir generando cada vez (automáticamente) softphones más complejos de usar (con más opciones para usar distintos tipos de servicios de VoIP). La generación de estos softphones debería adaptarse a los recursos de pantalla escasos de los teléfonos móviles inteligentes.

3) Un tema muy interesante para estudiar es la escalabilidad de la arquitectura de provisión de servicios de VoIP que hemos planteado. En principio, la arquitectura planteada debería soportar sin problema una gran cantidad de llamadas, esto es, para una PYME típica esta arquitectura es más que suficiente. Sin embargo, cuando se trata de una organización de mayor tamaño se ha de tener en cuenta la posibilidad de no poder dar soporte a una gran cantidad de llamadas simultáneamente. Por ello es necesario llevar a cabo un estudio detallado de la posibilidad de escalar la arquitectura calculando la potencia máxima de los computadores que alojan los servicios en la Nube. Otra posibilidad es hacer replicación interna y virtualización dinámica de los computadores que alojarían a los servidores. Por último otra posibilidad sería hacer una redistribución geográfica de los servidores en distintos puntos geográficos (lo cual es más adecuado para nubes públicas con un elevado número de usuarios). En cualquier caso se necesita un estudio detallado más profundo que ponga de manifiesto las ventajas e inconvenientes de cada uno de estos métodos de escalabilidad.

REFERENCIAS

[1] Herrera, E. *Fundamentos de Ingeniería Telefónica*. Editorial Limusa, 1983.

[2] Bellamy J., *Digital telephony*, John Wiley & Sons Australia, Limited, 1982.

[3] Danny Cohen, *Specifications For The Network Voice Protocol (NVP)*, Request For Comments 741, noviembre 1977.

[4] Nagireddi, S., *VoIP Voice and Fax Signal Processing*, John Wiley & Sons, 2008.

[5] James F. Durkin, *Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security*, CISCO Press, 2010.

[6] Mohamed Boucadair, Inter-Asterisk Exchange: Deployment Scenarios in SIP-Enabled Networks, John Wiley & Sons, 2009.

[7] Christina Hattingh, Darryl Sladden and ATM Zakaria Swapan, *SIP Trunking*, CISCO Press, 2010.

[8] Kris A. Jamsa, *Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More*, Jones and Bartlett Learning, 2013.

[9] Johnston, A., *SIP*: *Understanding the Session Initiation Protocol*, Artech House (Artech House Telecommunications Library), 2004.

[10] Krutz, R. y Vines, R.V., *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley Publishing Inc., 2010.

[11] Sosinsky, B., *Cloud Computing Bible*, Amazon Kindle, 2011.

[12] Fette, I. y Melnikov, A., *The WebSocket Protocol*, Request For Comments 6455, 2011.

[13] Lubbers P. y Greco, F., *HTML5 Web Sockets: A Quantum Leap in Scalability for the Web*, disponible en http://www.websocket.org/quantum.html, 2013.

[14] Baz, I. y Millan J., *The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)*, draft-ietf-sipcore-sip-websocket-06, disponible en https://datatracker.ietf.org/doc/draft-ietf-sipcore-sip-websocket/?include_text=1, marzo 2013.

[15] Blacio Giuseppe, *Diseño de una Red para Voz Sobre IP en la Nube y Posible Implementación con HTML5*, Tesis de Grado, Magister en Telecomunicaciones, Facultad de Ingeniería en Electricidad y Computación (FIEC), dirigida por Álvaro Suárez Sarmiento, abril 2013.

[16] Johnston, A. y Burnett, D., *WebRTC*: *APIs and RTCWEB Protocols of the HTML5 Real-Time Web* (second edititon), Digital Codex LLC, 2013.

[17] Hickson, I., *The WebSocketAPI, W3C Candidate Recommendation*, September 2012 extraído desde http://www.w3.org/TR/*WebSockets*/, 2012.

[18] Dutton, S., *WebRTC Plugin-free real-time communication*, Slides disponibles en http://www.samdutton.com/webrtc.pdf, 2012.

[19] PKE Consulting, *Introduction to WebRTC*, extraído desde http://www.pkeconsulting.com/pke*WebRTC*.pdf, 2012.

[20] Valin, JM. y Bran, C., WebRTC Audio Codec and Processing Requirements, draft-ietf-rtcweb-audio-01, disponible en http://tools.ietf.org/pdf/draft-ietf-rtcweb-audio-01.pdf, noviembre 2012.

[21] Bruno, A. y Jordan, S., *CCDA 640-864 Official Cert Guide*, Cisco Systems, Inc., 2011.

[22] Frahim, J. y Santos, O., *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*, Cisco Systems, Inc., 2005.

[23] Teare, D., *Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide*, CISCO Press, 2010.

Arquitectura de red para despliegues masivos de Infraestructuras de Medición Avanzada

Gregorio López[1], Francisco J. Herrera[1], José I. Moreno[1], Fernando Martín[2], Marta Bocos[3]
[1]Universidad Carlos III de Madrid, [gregorio.lopez| franciscojose.herrera.luque|joseignacio.moreno]@uc3m.es
[2]Unión Fenosa Distribución, fmartins@gasnatural.com
[3]Iberdrola, mbla@iberdrola.es

Resumen **- La transición de las infraestructuras eléctricas actuales a las denominadas Redes Eléctricas Inteligentes (*Smart Grids*) representa uno de los proyectos ingenieriles más complejos que jamás se haya afrontado, por lo que ha de llevarse a cabo paulatinamente. Actualmente nos encontramos en las etapas más tempranas de dicho proceso, donde destacan los despliegues de infraestructuras de medición avanzada (*Advanced Metering Infrastructures*) como primeros pasos hacia la *Smart Grid*. El proyecto PRICE-GEN representa un referente, a nivel nacional e internacional, de proyecto de infraestructuras de medición avanzada. PRICE-GEN pretende diseñar una arquitectura de red óptima e interoperable, desarrollar nuevos equipos de medida inteligente e implantar y validar esta plataforma a través de un piloto que involucra en torno a 200.000 contadores desplegados en la zona del Corredor de Henares. El objetivo de este artículo es presentar y analizar dicha arquitectura de red junto con su arquitectura de protocolos asociada.**

Palabras Clave **- AMI (*Advanced Metering Infrastructure*); Arquitectura de red; Arquitectura de protocolos; M2M (*Machine-to-Machine*); PRIME (*PoweRline Intelligent Metering Evolution*); *Smart Grid***

I. INTRODUCCIÓN

Las denominadas Redes Eléctricas Inteligentes (en inglés, *Smart Grids*) pueden definirse como redes eléctricas que hacen uso de las TIC (Tecnologías de la Información y la Comunicación) para coordinar las necesidades y capacidades de todas las entidades que las componen, con el fin de proporcionar un suministro eléctrico económicamente eficiente, sostenible, con bajas pérdidas y elevados niveles de calidad y seguridad [1].

Aunque el concepto de *Smart Grid* pueda sintetizarse en un párrafo, llevarlo a la práctica representa uno de los proyectos ingenieriles más complejos que jamás se haya afrontado, ya que supone una revolución a todos los niveles en un sistema tan complejo y crítico como el eléctrico, que lleva décadas sin evolucionar desde un punto de vista estructural.

Dicha revolución pretende, básicamente, transformar un sistema altamente centralizado y estático, en el que un número reducido de generadores a gran escala suministran electricidad a un número elevado de consumidores sin que exista comunicación en tiempo real entre ambos [2], en un sistema altamente distribuido y dinámico, en el que haya un mayor número de generadores, de menor escala y distribuidos, que puedan comunicarse en tiempo real con los consumidores para optimizar generación y consumo [3].

En consecuencia, la transición de la red eléctrica tradicional a la *Smart Grid* ha de ser gradual, hablándose en la literatura de tres generaciones de *Smart Grid* [4]. La primera generación (*Smart Grid 1.0*) se centra en la monitorización y el control del consumo, involucrando sistemas y aplicaciones como EMS (*Energy Management Systems*), AMI (*Advanced Metering Infrastructures*) y DR (*Demand Response*). La segunda generación (*Smart Grid 2.0*) se centra, en cambio, en la generación distribuida, involucrando elementos como el almacenamiento (clave para poder ajustar consumo y generación) o el coche eléctrico (que puede actuar tanto como consumidor, generador o almacenador de energía). Por último, la tercera generación (*Smart Grid* 3.0) se centra en la parte operativa del sistema, contemplando un mercado eléctrico dinámico y entre iguales.

Actualmente nos encontramos en las etapas más tempranas de dicha evolución, donde destacan los despliegues de AMI como primeros pasos hacia la *Smart Grid*. En las AMI existe una comunicación bidireccional entre los contadores inteligentes y los sistemas de información, por la que los primeros dejan de ser meros sensores y pasan a formar parte del núcleo de la infraestructura de distribución eléctrica. Las AMI aportan beneficios tanto para los operadores eléctricos (*utilities*) como para los consumidores. A las *utilities* les facilita tanto el mantenimiento como la operación de su infraestructura, permitiéndoles ejecutar acciones como altas o bajas remotas de contadores, tele-carga de *firmware* o lecturas remotas de contadores (periódicas o bajo demanda). Los consumidores pueden tener acceso a información detallada sobre su consumo o beneficiarse de tarifas diferenciadas dinámicas.

PRICE-GEN es el proyecto de AMI de referencia en España y se espera que se convierta también en un referente a nivel internacional [5]. PRICE-GEN pretende diseñar una arquitectura de red óptima e interoperable, desarrollar nuevos equipos de medida inteligente que proporcionen información puntual de los consumos y de la generación, tanto de los clientes como del propio estado de la red eléctrica, e implantar y validar esta plataforma a través de un piloto que involucra en torno a 200.000 contadores desplegados en la zona del Corredor de Henares. El objetivo de este artículo es presentar y analizar dicha arquitectura de red junto con su arquitectura de protocolos asociada.

El resto del artículo está organizado de la siguiente manera. La sección II discute brevemente los requisitos que deben cumplir las infraestructuras de comunicaciones para *Smart Grid*, en general, y para AMI, en particular. La sección

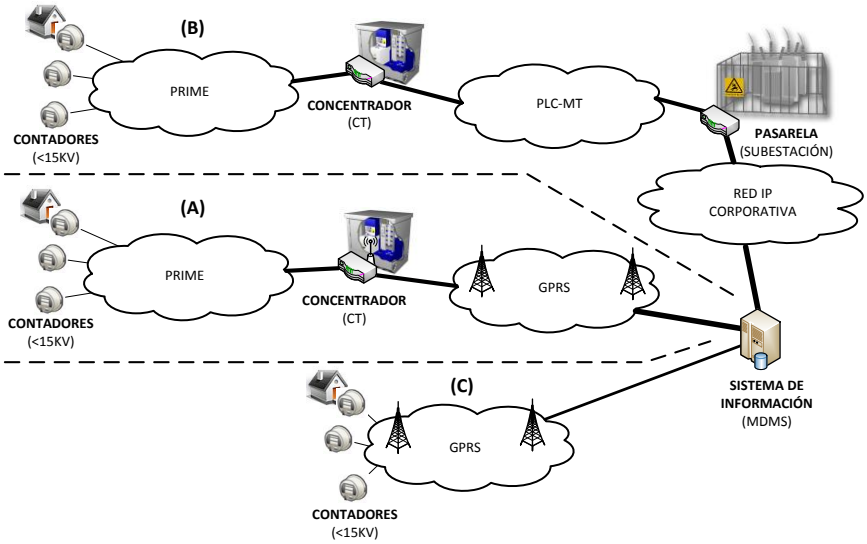


Fig. 1. Visión global de la arquitectura de red del proyecto PRICE-GEN.

III presenta la arquitectura de comunicaciones diseñada para ajustarse a dichos requisitos así como a las características específicas de los diferentes escenarios presentes en entornos reales. La sección IV resume las principales características de la arquitectura de red del proyecto PRICE-GEN y la compara con otros trabajos relacionados. Por último, la sección V presenta las principales conclusiones y trabajos futuros.

II. Requisitos

En esta sección se listan algunos requisitos clave que deben tenerse en cuenta a la hora de diseñar la arquitectura de comunicaciones de aplicaciones comprendidas dentro del ámbito de las *Smart Grids*, tales como las AMI [6],[7]:

- QoS (*Quality of Service*). La infraestructura de comunicaciones deberá proporcionar un cierto nivel de QoS que se adecúe a la aplicación objetivo. Más concretamente, las políticas de QoS están principalmente orientadas a la priorización de tráficos ante situaciones de congestión y a la reserva de capacidad cuando la tecnología lo permite. Algunos parámetros que se utilizan para cuantificar dicho nivel de QoS son:
  - Latencia. Puede describirse como el retardo de los datos transmitidos extremo-a-extremo. La latencia es un parámetro clave en aplicaciones de protección y control a nivel de subestación, en las que debe garantizarse que en ningún caso superará un determinado valor (típicamente, 4 ms). Sin embargo, en aplicaciones AMI para entornos residenciales, la latencia no supone un parámetro crítico.
  - Ancho de banda y Tasa de transmisión. La infraestructura de comunicaciones debe proporcionar una tasa de transmisión lo suficientemente alta como para cursar el tráfico asociado a una determinada aplicación. En general, esto dependerá del volumen de dispositivos así como del tamaño de la información que envían y de la frecuencia con la que lo hacen.
  - Fiabilidad y Disponibilidad. La infraestructura de comunicaciones debe garantizar que funciona correctamente un porcentaje de tiempo respecto al total del año, siendo necesario que dicho porcentaje sea tanto más alto cuánto más crítica sea la información transportada para el correcto funcionamiento de la infraestructura eléctrica.
- Interoperabilidad. La infraestructura de comunicaciones debe permitir que dispositivos de distintos fabricantes interactúen de manera transparente. Para conseguir este objetivo es necesario definir y estandarizar los bloques funcionales que componen la infraestructura de comunicaciones así como los interfaces entre ellos. La utilización de estándares es clave para alcanzar la interoperabilidad requerida, que posibilita la libre competencia en un mercado global, lo que acaba repercutiendo en productos más fiables a precios más bajos.
- Escalabilidad. La infraestructura de comunicaciones tiene que garantizar la escalabilidad tanto desde un punto de vista técnico como desde un punto de vista económico. Por un lado, teniendo en cuenta el elevado número de dispositivos que involucran este tipo de sistemas, las tecnologías de comunicaciones utilizadas deben minimizar los costes de despliegue, mantenimiento y operación, para que el factor económico no suponga una barrera. Por otro lado, la arquitectura de comunicaciones debe ser lo suficientemente flexible como para soportar un número muy elevado y variable de dispositivos así como para acomodar nuevos servicios.
- Seguridad y Privacidad. Debido a que la información que se maneja en este tipo de sistemas es extremadamente sensible, la seguridad (tanto la física como la ciber-seguridad) y la privacidad representan un requisito clave para su despliegue y aceptación [8]. Por lo tanto, es imprescindible que la infraestructura de comunicaciones proporcione un nivel de seguridad adecuado a la aplicación objetivo. En cuanto a la privacidad, queda fuera del ámbito del proyecto PRICE-GEN y, por tanto, de este artículo.

III. Arquitectura de Red

La Fig. 1 muestra una visión global de la arquitectura de comunicaciones para AMI del proyecto PRICE-GEN, diseñada para ajustarse a los requisitos presentados en la sección II así como a las diferentes tipologías de red presentes en este tipo de despliegues (urbana, semi-urbana y

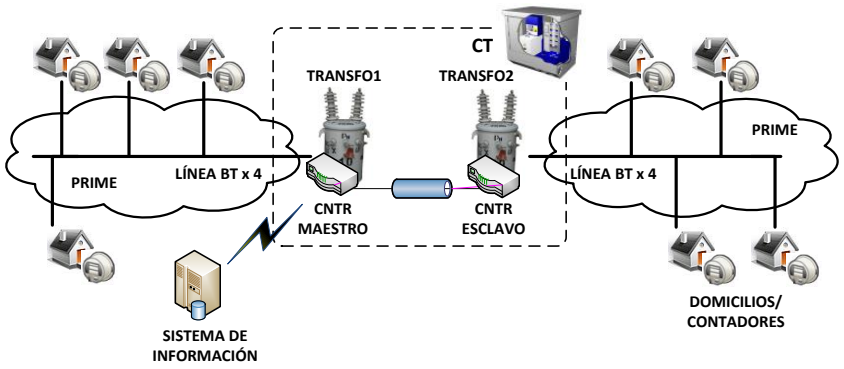


Fig. 2. Mapeo de la infraestructura de comunicaciones y la infraestructura de distribución eléctrica para la arquitectura *Comunicación a través de Concentrador*.

rural). Se trata de una arquitectura de red heterogénea en tanto en cuanto comprende a su vez tres arquitecturas de red (identificadas como (A), (B) y (C) en la Fig. 1), cada una de las cuales está compuesta por diferentes segmentos de red, en los que se emplean diferentes tecnologías de comunicación.

Estas tres arquitecturas influyen en la comunicación entre los Contadores y el Sistema de Información (también nombrado en la literatura como MDMS – *Metering Data Management System*), pudiendo distinguirse entre:

A. Comunicación a través de Concentrador;
B. Comunicación a través de Concentrador y Pasarela;
C. Comunicación directa.

La *Comunicación a través de Concentrador* representa la arquitectura de red básica del proyecto PRICE-GEN, diseñada especialmente para entornos urbanos y semi-urbanos dotados de una red de BT (Baja Tensión) de calidad media-alta. Se trata de una arquitectura jerárquica a dos niveles que aprovecha la propia infraestructura eléctrica con el objetivo de agilizar el despliegue y favorecer la escalabilidad.

La Fig. 2 ilustra cómo se mapea esta arquitectura de red con la infraestructura de distribución eléctrica. Como se puede ver, los Contadores están instalados en los domicilios mientras que los CNTR (Concentradores) están instalados en los CT (Centros de Transformación). Domicilios y CT están conectados eléctricamente a través de la infraestructura de BT.

Un CT puede estar equipado con uno, dos o tres transformadores de MT (Media Tensión) a BT. Cada transformador presenta típicamente 4 salidas de BT y cada una de estas líneas de BT da servicio a una serie de domicilios según una topología en bus.

Dentro de un CT, los CNTR están asociados concretamente a los transformadores, habiendo un CNTR por cada transformador. En el caso de que haya varios CNTR dentro de un mismo CT, uno funcionará como maestro, desde el punto de vista de las comunicaciones, mientras que el resto funcionarán como esclavos. La comunicación entre CNTR maestro y CNTR esclavo/s se basa en tecnología cableada (p. ej., Ethernet).

La principal funcionalidad del CNTR desde el punto de vista de AMI es agregar los datos que envían los Contadores, lo que favorece la escalabilidad de la plataforma. El CNTR principal o maestro de un CT es el que gestiona la comunicación con el Sistema de Información, que no está asociado con ningún elemento de la infraestructura eléctrica concreto, estando localizado típicamente en un CPD (Centro de Procesamiento de Datos) de la *utility*.

La *Comunicación a través de Concentrador y Pasarela* es una arquitectura de red jerárquica a tres niveles que se ajusta a la propia jerarquía de la red eléctrica de distribución, con el objetivo de sacar el máximo partido de la infraestructura eléctrica como medio de comunicación. Así, los Contadores están asociados a los domicilios, los CNTR a los CT y la Pasarela a la Subestación que controla la red de distribución eléctrica en cuestión. Al igual que en el caso de la *Comunicación a través de Concentrador*, domicilios y CT están conectados eléctricamente a través de la red de BT (Fig. 2). Por otro lado, una Subestación y los CT que dependen de ella están conectados eléctricamente a través de la red de MT. Por lo tanto, esta arquitectura de red aprovecha tanto las líneas de BT como las líneas de MT como medio de comunicación.

Por último, la *Comunicación directa* se trata de una solución especialmente indicada para casos singulares tales como entornos donde la red de BT no es de suficiente calidad o para CT con muy pocos clientes (entornos rurales). Esta configuración consta de un único segmento de red, lo que perjudica la escalabilidad, aunque en los entornos a los que está orientada esta arquitectura no se trate de un parámetro crítico.

Las siguientes subsecciones proporcionan más detalles de estas arquitecturas, centrándose en cómo se ajustan a los requisitos presentados en la sección II y en las tecnologías de comunicación y la arquitectura de protocolos que utilizan.

A. Comunicación a través de Concentrador

La Fig. 3 muestra las tecnologías de comunicaciones y la torre de protocolos completa a utilizar en cada uno de los segmentos de red de esta arquitectura, indicando el nombre de los mismos según se definen en [9].

La comunicación entre Contadores y CNTR se basa en PRIME (*PoweRline Intelligent Metering Evolution*) [10]. PRIME es una solución NB-PLC (*Narrow Band - Power Line Communications*) de segunda generación que, como ya se ha comentado, utiliza como medio de transmisión la propia infraestructura eléctrica de BT, lo que reduce los costes de despliegue de este segmento de red.

PRIME alcanza tasas de transmisión de hasta 130 Kbps, lo que en principio parece suficiente para aplicaciones AMI. La fiabilidad y disponibilidad de esta tecnología está muy ligada a la calidad de la red de BT, pudiendo presentar

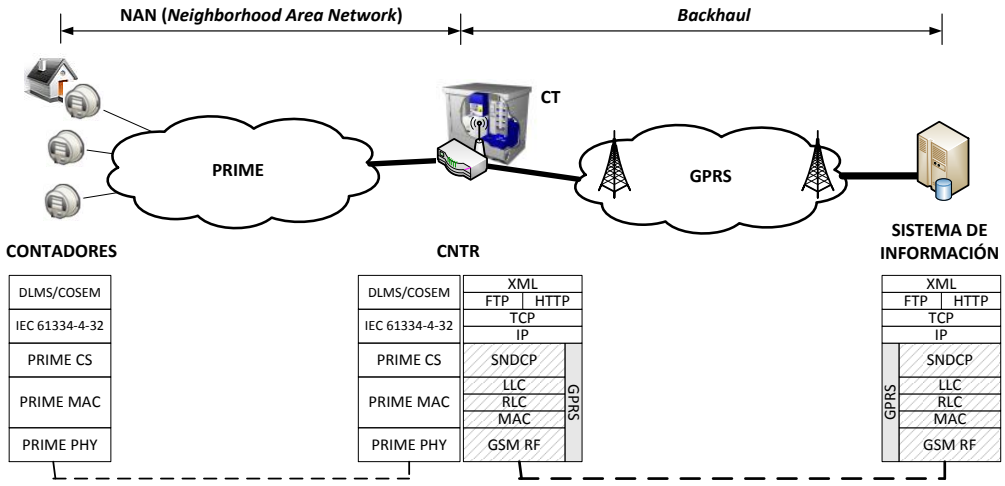


Fig. 3. Tecnologías de comunicación y torre de protocolos para la arquitectura *Comunicación a través de Concentrador*.

problemas principalmente asociados a la atenuación y al ruido [11]. Esta arquitectura de red está recomendada para entornos dotados de una red de BT de calidad media-alta precisamente para minimizar los efectos de dichos problemas, maximizando así la fiabilidad y disponibilidad.

Al contrario que otras soluciones disponibles en el mercado para este segmento, la especificación PRIME es abierta y gratuita, lo que permite que cualquier fabricante pueda desarrollar productos que se ajusten a ella, favoreciendo notablemente la interoperabilidad. De hecho, durante los últimos años se han llevado a cabo pruebas de interoperabilidad en campo con resultados satisfactorios [12]. Además, la especificación PRIME soporta seguridad a diferentes niveles de la torre de protocolos, como se comentará más en detalle a lo largo de esta subsección.

La arquitectura de protocolos definida en PRIME se compone de tres capas: capa física (*PHYsical layer*), capa de enlace (*Data Link layer* - MAC) y capa de convergencia (*Convergence layer* - CS).

La capa física de PRIME es responsable de la transmisión y recepción de tramas procedentes de la capa de enlace entre nodos vecinos a través de los cables de BT. Emplea el formato de modulación OFDM (*Orthogonal Frequency Division Multiplexing*) en la banda de frecuencias CENELEC-A (concretamente entre los 41 KHz y los 89 KHz).

La capa de enlace de PRIME se encarga del control de acceso al medio, la asignación de tasa binaria de transmisión, la gestión de conexiones entre equipos interconectados y la resolución de topologías.

PRIME define dos tipos de nodos: Nodo Base y Nodo de Servicio, que se interconectan bajo el paradigma de orientación a conexión en modo maestro-esclavo. En cada red PRIME hay un único Nodo Base que ejerce las funciones de maestro en la gestión de las conexiones con otros nodos y que constituye inicialmente la red en sí mismo. Siguiendo un procedimiento de registro, otros nodos (Nodos de Servicio) se le pueden unir para formar parte de la red. En el despliegue del proyecto PRICE-GEN la funcionalidad de Nodo Base en cada subred PRIME la desempeñan los CNTR, mientras que la funcionalidad de Nodo de Servicio la desempeñan los Contadores. PRIME también contempla que un Nodo de Servicio pueda funcionar como Repetidor, para mitigar los efectos de la atenuación.

Tanto el Nodo Base como los Nodos de Servicio de una subred PRIME pueden acceder al canal durante el período con contienda (SCP – *Shared-Contention Period*) o solicitar transmitir durante el período libre de contienda (CFP - *Contention-Free Period*). La técnica de acceso al medio que se emplea durante el período con contienda es CSMA-CA (*Carrier Sense Multiple Access-Collision Avoidance*).

La capa de convergencia clasifica el tráfico intercambiado entre diferentes equipos asociándolo con la conexión de la capa de enlace correspondiente. Para ello realiza el encapsulado de cualquier tipo de información proveniente de las capas superiores de la arquitectura de protocolos de comunicaciones para generar MAC SDU (*Media Access Control Service Data Units*), pudiendo incluir la funcionalidad de supresión de la cabecera de la PDU (*Protocol Data Unit*) del nivel superior. La capa de convergencia se divide a su vez en dos subcapas:

- CPCS (*Common Part Convergence Sublayer*), responsable de la fragmentación y el ensamblado de PDU del nivel superior para adecuarlas a la SDU de la capa de enlace;
- SSCS (*Service Specific Convergence Sublayer*), que permite gestionar de modo diferenciado distintos tipos de tráfico de nivel superior. PRIME dispone de versiones específicas para IPv4, IPv6, IEC 61334-4-32 y una versión genérica para cualquier otro protocolo de nivel superior.

En el proyecto PRICE-GEN se utiliza la subcapa de convergencia de PRIME asociada al protocolo IEC 61334-4-32 para el transporte de unidades de datos del protocolo de aplicación DLMS/COSEM (*Device Language Message Specification*/*Companion Specification for Energy Metering*). IEC 61334-4-32 es un servicio de transporte no orientado a conexión disponible en modalidades con y sin acuse de recibo. Las razones por las que se decide usar este protocolo frente a otros protocolos de transporte basados en IP (*Internet Protocol*) son las siguientes:

- Los servicios que ofrece IEC 61334-4-32 al nivel superior son de baja complejidad y, al mismo tiempo, suficientes para satisfacer las demandas de los Contadores, lo que simplifica su funcionamiento y reduce su coste, favoreciendo la escalabilidad económica de esta solución.
- La sobrecarga que introduce IEC 61334-4-32 es mucho menor que la de otros protocolos de transporte basados en

IP. Una PDU IEC 61334-4-32 añade 24 bits de cabecera a los mensajes DLMS/COSEM. La utilización de UDP/IP (*User Datagram Protocol*), por ejemplo, implicaría añadir entre 320 bits y 288 bits, que podrían llegar a reducirse a 104 si se implementa la funcionalidad de compresión de cabecera IP, lo que requeriría equipos con mayores capacidades y, por tanto, de mayor coste.

- El hecho de que los CNTR agreguen el tráfico procedente de los Contadores implica que los CNTR inspeccionan los paquetes procedentes de los Contadores hasta la capa de aplicación, desencapsulan los datos y los procesan para minimizar el volumen de datos enviado a través de GPRS. Esto a su vez implica que la conectividad transparente extremo-a-extremo que proporciona IP, que representa una de sus principales ventajas, pierde su valor.

COSEM (IEC 62056-61/62) es un perfil del protocolo de aplicación DLMS (IEC 62056-53) específicamente diseñado para contadores inteligentes [13],[14]. Se trata de un modelo de datos orientado a objetos que define la representación de diferentes tipos de información relativa a contadores inteligentes de electricidad, calefacción, agua y gas. Además, dispone de un mecanismo de comunicación basado en mensajes para transmitir la información contenida en el modelo de datos. Una interacción típica en DLMS/COSEM consiste en una consulta del valor que toma un atributo específico en el Contador y una respuesta de éste con el valor codificado según las reglas de codificación A-XDR (*eXternal Data Representation*).

La arquitectura de protocolos de este segmento de red dispone de servicios de seguridad tanto en la capa de enlace de PRIME como en el nivel de aplicación (DLMS/COSEM). La especificación de PRIME proporciona, como servicios de seguridad, privacidad, autentificación e integridad de los datos a nivel de la subcapa MAC, mediante un método de conexión segura y una política de gestión de claves. PRIME define dos perfiles posibles de seguridad con diferentes características:

- Perfil de Seguridad 0, basado en la transmisión de MAC SDU sin ningún tipo de cifrado. Con este perfil están deshabilitados todos los servicios de seguridad.
- Perfil de Seguridad 1, basado en la transmisión con cifrado AES (*Advanced Encryption Standard*) de 128 bits tanto de los datos como del CRC (*Cyclic Redundancy Check*) asociado.

Aunque para la transmisión de datos puede elegirse el Perfil de Seguridad 0, la especificación obliga a la transmisión cifrada de los mensajes de control de la subcapa MAC. Los mensajes baliza y los asociados al proceso de Promoción de los Nodos de Servicio se transmiten sin cifrar.

Las especificaciones más recientes de DLMS/COSEM soportan también de forma opcional funcionalidades de seguridad [15]. Dichas funcionalidades pueden agruparse en tres ámbitos diferentes: 1) el control del acceso a la información; 2) el mantenimiento de un registro de eventos relacionados con la seguridad; y 3) el cifrado de mensajes. El control del acceso a la información se puede realizar a dos niveles: 1) el de autenticación de los interlocutores de la comunicación y 2) el de definición de vistas con diferentes niveles de acceso a la información contenida en los objetos. Respecto al cifrado de mensajes, pueden implementarse algoritmos de generación de funciones *hash* y algoritmos de cifrado tanto simétrico como asimétrico.

La comunicación entre CNTR y Sistema de Información se basa en GPRS (*General Packet Radio Service*). GPRS es una tecnología celular madura y ampliamente desplegada que proporciona cobertura en prácticamente todo el territorio nacional (ocurriendo lo mismo en muchos otros países), lo que facilita el despliegue y puesta en funcionamiento de la plataforma y garantiza la interoperabilidad.

GPRS proporciona tasas de bajada reales en torno a 110 Kbps frente a tasas de subida reales en torno a 26.8 Kbps [16]. La infraestructura de comunicaciones GPRS estará gestionada por un operador de red o proveedor de servicio de comunicaciones, por lo que los costes de despliegue se limitan a la compra de tarjetas SIM (*Subscriber Identity Module*) y no existen costes de mantenimiento.

El hecho de que los CNTR agreguen los datos procedentes de los Contadores favorece que la plataforma escale tanto desde el punto de vista técnico (permitiendo reducir el volumen de datos en el canal de subida de este segmento, lo que a su vez favorece la adaptación de PRIME a GPRS) como desde el punto de vista económico (reduciendo los costes de operación).

Para maximizar la disponibilidad de este segmento, los CNTR estarán equipados con tarjetas SIM “blancas” que les proporcionarán conectividad con el Sistema de Información a través de varios operadores de red (típicamente dos).

En cuanto a la seguridad, GPRS soporta mecanismos de seguridad extremadamente robustos. Además, entre los CNTR y el sistema de información se podrá establecer una VPN (*Virtual Private Network*), a nivel de enlace (utilizando L2TP – *Layer 2 Tunneling Protocol*), a nivel de red (utilizando IPSec – *Internet Protocol Security*) o a nivel de transporte (utilizando TLS/SSL – *Transport Layer Security* / *Secure Sockets Layer*) [17].

En el plano de control, la comunicación entre el Sistema de Información y los CNTR se basa en Servicios Web sobre FTP/TCP (*File Transfer Protocol* / *Transmission Control Protocol*), definiéndose los comandos y notificaciones oportunos en formato XML (*eXtensible Markup Language*). El Sistema de Información funciona como servidor FTP mientras que los CNTR funcionan como clientes FTP.

En el plano de datos, la comunicación entre el Sistema de Información y los CNTR también se basa en Servicios Web sobre FTP/TCP. En el caso particular del volcado de datos de los CNTR al Sistema de Información, los CNTR agrupan los datos asociados a cada Contador para eliminar redundancias y codifican la información agregada de todos los Contadores en formato XML. Como ya se ha comentado, en el caso de que haya varios CNTR en un mismo CT, el maestro es el único que se comunica con el Sistema de Información (pudiendo haber dos maestros virtuales para CT con un número muy alto de Contadores).

Actualmente, este volcado de información de los CNTR al Sistema de Información se realiza una vez al día, lo que pone de manifiesto que el retardo no es un parámetro crítico en este tipo acciones, siendo además complicado alcanzar retardos muy bajos cuando la comunicación entre los Contadores y el Sistema de Información se realiza a través de CNTR. Sin embargo, si los datos recogidos se utilizaran como entrada para otras aplicaciones, tales como DR, la

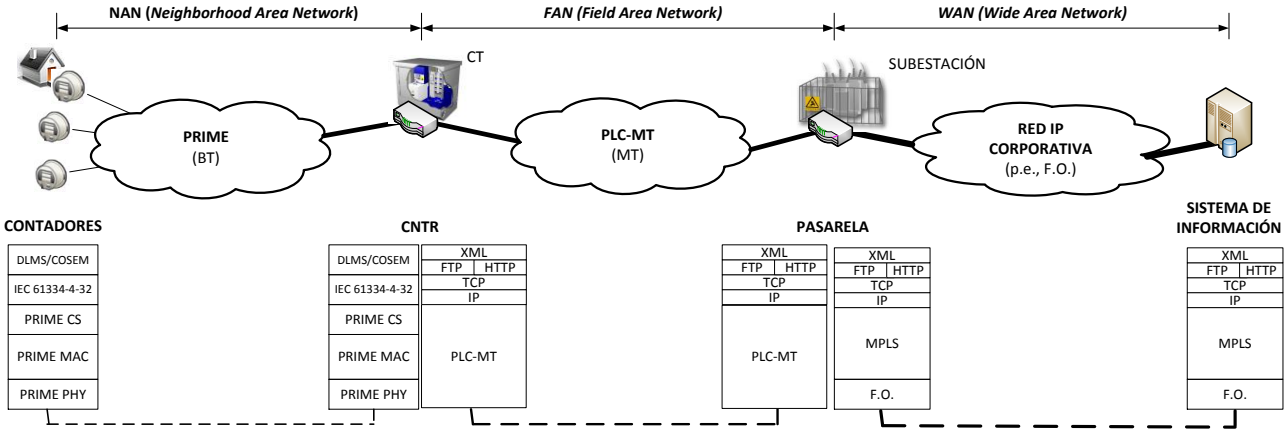


Fig. 4. Tecnologías de comunicación y torre de protocolos para la arquitectura *Comunicación a través de Concentrador y Pasarela*.

periodicidad de este volcado de información podría reducirse hasta la periodicidad de envío de los Contadores. Asimismo, las operaciones remotas sobre el Contador (p. ej., cortes, enganches, cambios de potencia) funcionan en tiempo real.

B. Comunicación a través de Concentrador y Pasarela

La Fig. 4 muestra las tecnologías de comunicaciones y la torre de protocolos completa a utilizar en cada uno de los segmentos de red de esta arquitectura, indicando el nombre de los mismos según se definen en [9].

Los Contadores siguen comunicándose con el CNTR utilizando PRIME, por lo que también está indicada para ser desplegada en entornos urbanos o semi-urbanos dotados de una red de BT de calidad media-alta.

Los CNTR localizados en los CT se comunican con la Pasarela, localizada en la Subestación, utilizando para ello PLC-MT (PLC de Media Tensión).

Finalmente, la Pasarela se comunica con el Sistema de Información utilizando la red IP corporativa que conecta las Subestaciones de la *utility*. Este tipo de redes suelen ser redes cableadas de banda ancha basadas en MPLS (*MultiProtocol Label Switching)*. MPLS soporta QoS, ingeniería de tráfico y VPN, permitiendo asociar una etiqueta determinada al tráfico AMI para distinguirlo del resto y tratarlo de la manera más adecuada.

Los costes de despliegue de esta arquitectura son muy bajos, ya que utiliza la propia red de distribución eléctrica como medio de comunicación. Los costes operacionales serán inferiores a los de la arquitectura presentada en la sección III.A, ya que no hay que pagar a un tercero en base al volumen de datos. Sin embargo, los costes de mantenimiento (que podrían incluirse dentro de los de operación) serán superiores.

El segmento de red clave en la disponibilidad de la comunicación entre CNTR y Sistema de Información en esta arquitectura es el que utiliza la red de MT y dicho parámetro dependerá de la calidad de ésta. En principio, la disponibilidad de la comunicación entre CNTR y Sistema de Información sería inferior en este caso que en el caso de utilizar GPRS con conectividad a través de varios operadores de red.

C. Comunicación Directa

La Fig. 5 muestra las tecnologías de comunicaciones y la torre de protocolos completa a utilizar en cada uno de los segmentos de red de esta arquitectura, indicando el nombre de los mismos según se definen en [9].

Como se ha comentado al principio de esta sección, dentro del ámbito del proyecto PRICE-GEN esta arquitectura se considera una solución extraordinaria indicada para casos muy particulares, tales como entornos donde la red de BT no es de suficiente calidad o para CT con muy pocos clientes (entornos rurales), ya que presenta múltiples inconvenientes:

- Como se observa en la Fig. 5, esta solución implica que el Sistema de Información interprete mensajes DLMS/COSEM. Sin embargo, a pesar de que los despliegues AMI en general puedan presentar una arquitectura de red heterogénea que resulte de una combinación de las tres soluciones descritas a lo largo de esta sección, lo ideal es que el tratamiento de los datos se realice de manera uniforme independientemente del origen de los mismos. Para solucionar este problema se pueden implementar CNTR virtuales en el Sistema de Información, tal y como también muestra la Fig. 5.
- Aumenta los costes de despliegue en tanto en cuanto el número de tarjetas SIM necesarias aumenta en torno a dos órdenes de magnitud.
- Aumenta el volumen de datos cursado por la red GPRS, ya que no hay agregación de información, aumentando por tanto los costes de operación.

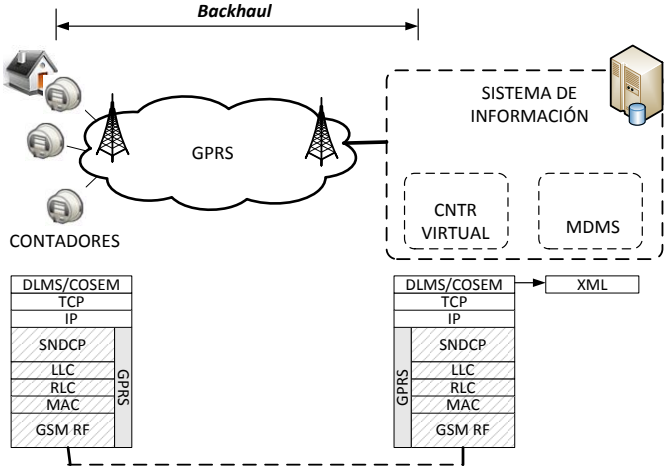


Fig. 5. Tecnologías de comunicación y torre de protocolos para la arquitectura *Comunicación Directa*.

Tabla I. Comparativa de las arquitecturas de red consideradas en el proyecto PRICE -GEN

	A. A través de CNTR	B. A través de CNTR y Pasarela	C. Directa
Tecnologías Comunicación	*NAN*: PRIME *Backhaul*: GPRS	*NAN*: PRIME *FAN*: PLC-MT *WAN*: Red IP Corporativa	*Backhaul*: GPRS
Fiabilidad	✓✓✓ ✓✓✓	✓✓ ✓✓✓	✓✓ ✓✓
Interoperabilidad			
Costes de despliegue	€€	€	€€€€
Costes de operación	€€	€	€€€€
Costes de mantenimiento	€	€€	€
Escalabilidad	✓✓✓	✓✓✓	✓
Seguridad	✓✓✓	✓✓✓	✓✓ (No VPN)

- En el caso de utilizar mecanismos de seguridad a nivel de transporte o red (VPN), la sobrecarga introducida es mayor, ya que no se aplicarían sobre datos asociados a un grupo de Contadores sino sobre datos asociados a un único Contador, lo que podría aumentar los costes de operación. Además, este requisito podría incrementar la complejidad de los Contadores y, por ende, su coste, lo que tendría un impacto considerable en los costes de despliegue.

Para evitar estos problemas, dentro del ámbito del proyecto PRICE-GEN se está investigando la posibilidad de desplegar en este tipo de entornos la arquitectura presentada en la sección III.A, pero utilizando un CNTR especialmente diseñado para ellos.

IV. Discusión

La Tabla I resume y compara de forma cuantitativa las características de las arquitecturas de comunicaciones presentadas en la sección III.

A pesar de que, como se ha comentado, la comunicación directa entre Contadores y Sistema de Información presenta varios inconvenientes, esta arquitectura se utiliza con bastante frecuencia en la literatura para evaluar infraestructuras de comunicaciones para AMI.

Así, [19] evalúa el retardo y el ancho de banda en una red UMTS (*Universal Mobile Telecommunications System*) que transporta tráfico generado por Contadores junto con tráfico de usuario (voz y datos), utilizando para ello OPNET Modeler 14.5. Las principales conclusiones a las que llega este trabajo son: 1) que cuando el número de Contadores aumenta, el retardo también aumenta, sugiriendo la utilización de algoritmos de planificación que permitan priorizar el tráfico con requisitos de tiempo real; y 2) que es necesario reservar ancho de banda suficiente para transportar los dos tipos de tráfico considerados sin problema. Notar que las conclusiones a las que llega este estudio respecto al retardo no son válidas en una arquitectura que utilice CNTR para agregar la información de un grupo de Contadores. En este caso, el retardo se desacopla del número total de Contadores y pasa a depender principalmente de la periodicidad de volcado de información de los CNTR.

La referencia [16], en cambio, no se basa en simulaciones, sino que evalúa la comunicación directa entre Contadores y Sistema de Información en redes GPRS, HSDPA (*High-Speed Downlink Packet Access*) y LTE (*Long Term Evolution*) reales, utilizando como métricas el RTT (*Round-Trip Time*) y el *jitter* (variación del retardo). Las principales conclusiones a las que llega este trabajo van en la línea de que el rendimiento es tanto mejor cuanto más alta es la generación celular que se utilice. Sin embargo, dichas conclusiones no consideran limitaciones asociadas a los costes ni a la disponibilidad de la tecnología. Además, este estudio no se basa en datos de volumen de Contadores procedente de despliegues reales. Por último, notar que la importancia del *jitter* disminuye cuando la comunicación entre Contadores y Sistema de Información se realiza a través de CNTR.

La referencia [20] analiza ventajas e inconvenientes de dos arquitecturas de comunicación basadas en tecnologías inalámbricas 4G (LTE y WiMAX - *Worldwide Interoperability for Microwave Access*). En primer lugar, también considera la comunicación directa entre Contadores y Sistema de Información, centrándose en los problemas que presenta desde el punto de vista de la red de comunicaciones. Así, este artículo destaca la ineficiencia de los procedimientos de establecimiento de conexión y autenticación teniendo en cuenta el patrón de tráfico de los Contadores a nivel individual y apunta algunos problemas que tendría que afrontar el operador de red, tales como la mejora de la red de acceso radio para evitar problemas de falta de ancho de banda o de cobertura debidos al elevado número de Contadores. Para solucionar dichos problemas, propone la comunicación a través de CNTR, a los que llama AP (*Aggregation Points*). Para la comunicación entre Contadores y dichos AP propone utilizar tecnologías inalámbricas como Zigbee o Wi-Fi. La principal desventaja de esta segunda solución con respecto a la primera es que el introducir un segmento de red la hace más frágil frente a posibles ataques de seguridad.

También existen en la literatura soluciones de "última milla" basadas en arquitecturas inalámbricas malladas [21]. Este enfoque presenta ventajas desde el punto de vista de gestión y mantenimiento de la infraestructura, aunque los riesgos de seguridad en principio aumentan.

En cuanto a arquitecturas híbridas que combinan tecnologías inalámbricas y cableadas, PLC parece encontrarse en una situación privilegiada como tecnología cableada de "última milla" para aplicaciones relacionadas con *Smart Grid* [22], por los motivos que ya se han comentado a lo largo de este artículo. Dentro de esta familia de tecnologías de comunicación, hay una tendencia considerable en el mercado a la adopción de PRIME, debido a que es un protocolo abierto y gratuito liderado por importantes fabricantes y *utilities* y a los numerosos despliegues en los que se está utilizando con éxito [23].

Respecto al impacto en la infraestructura de comunicaciones de una arquitectura centralizada frente a una totalmente distribuida, [24] evalúa este problema centrándose en la escalabilidad como figura de mérito del sistema y utilizando como métricas los costes de despliegue y el ABDP (*Accumulated Bandwidth-Distance Product*). La principal conclusión a la que llega es que las simulaciones realizadas indican que una arquitectura distribuida presenta beneficios para la infraestructura de comunicaciones respecto a una arquitectura centralizada. Éste es también el enfoque de las soluciones basadas en agentes [25]. Sin embargo, y probablemente debido de nuevo a riesgos de seguridad, la tendencia que se observa en el mercado no va en la línea de distribuir el procesado de la información a lo largo de la infraestructura de comunicaciones (lo que en principio reduciría el tránsito de información), sino de realizarlo en una misma entidad lógica aplicando procesamiento "en la nube" y herramientas de *Big Data*.

V. Conclusiones

Este artículo presenta una arquitectura de red heterogénea para AMI desde un punto de vista práctico y operacional, centrándose en: 1) las tecnologías de comunicación y la torre de protocolos que se utiliza en cada una de las arquitecturas de red que la componen; y en 2) las ventajas e inconvenientes de cada una de ellas y, en consecuencia, los entornos reales de despliegue a los que mejor se adecúan.

Esta arquitectura servirá como soporte para las simulaciones que se llevarán a cabo durante la ejecución del proyecto con el objetivo de obtener guías para el diseño y despliegue de infraestructuras de comunicaciones para AMI. En estas simulaciones se pretende seguir una metodología similar a la presentada en [26]. La herramienta a utilizar para realizar dichas simulaciones se decidirá una vez definidos los escenarios de interés (instancias particulares de la arquitectura presentada en este artículo), en base a sus características y a los parámetros a evaluar.

Agradecimientos

Este trabajo ha sido financiado parcialmente por el Ministerio de Economía y Competitividad a través del programa INNPACTO dentro del proyecto PRICE-GEN (IPT-2011-1507-920000).

Los autores de este artículo agradecen el apoyo y colaboración del resto de socios del consorcio PRICE-GEN: Arteche, CIRCE, Current Iberia, Iberdrola Distribución, UC3M, Unión Fenosa Distribución y ZIV Metering Solutions.

Referencias

[1] International Energy Agency. "Technology roadmap: Smart Grids". 2011. On-line: http://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf

[2] H. Farhangi, "The path of the Smart Grid", IEEE Power & Energy Magazine, Vol. 8, No. 1, pp. 18-28, 2010.

[3] L. Hernández *et al*, "A multi-agent system architecture for smart grid management and forecasting of energy demand in virtual power plants", IEEE Communications Magazine, Vol. 51, No 1, pp 106 - 113, 2013.

[4] A. Carvallo, J. Cooper, "The Advanced Smart Grid: Edge Power Driving Sustainability", Ed. Artech House, 2011.

[5] Página oficial del proyecto PRICE: http://www.priceproject.es/es

[6] Y. Yan, Y. Quian, H. Sharif, D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges", IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, pp. 5-20, 2013.

[7] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, C.P. Hancke, "A Survey on Smart Grid Potential Applications and Communication Requirements", IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, pp. 28-42, 2013.

[8] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. Chen, "Cyber Security and Privacy Issues in Smart Grids", IEEE Communications Surveys & Tutorials, Vol. 14, No.4, pp. 981-997, 2012.

[9] IEEE Std 2030. "IEEE 2030 Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads". 2011.

[10] ITU-T G.9904. "Narrowband orthogonal frequency division multiplexing power line communication transceivers for PRIME networks". 2012.

[11] J. M. Domingo, S. Alexandres, C. Rodríguez-Morcillo, "PRIME performance in power line communication channel", IEEE ISPLC, Udine, Italy, 2011.

[12] A. Arzuaga, I. Berganza, A. Sendin, M. Sharma, "PRIME interoperability tests and results from field", IEEE SmartGridComm, Gaithersburg, USA, 2010.

[13] DLMS User Association, "Excerpt from DLMS/COSEM Architecture and Protocols". Ed. 7.0, 2009. On-line: http://dlms.com/documents/Excerpt_GB7.pdf

[14] DLMS User Association, "Excerpt from COSEM Identification System and Interface Classes". Ed. 10.0, 2010. On-line: http://dlms.com/documents/Excerpt_BB10.pdf

[15] DLMS User Association, "DLMS/COSEM over PLC – security of meter data exchange over open networks". Presentación en "Metering Europe", 2007. On-line: http://www.dlms.com/downloads/dlmscosemoverplcviennagk070921.pdf

[16] G. M. Shrestha, J. Jasperneite, "Performance Evaluation of Cellular Communication Systems for M2M Communication in Smart Grid Applications", Computer Networks, pp- 352-359. Springer Berlin Heidelberg, 2012.

[17] S. Khanvilkar, A. Khokhar, "Virtual Private Networks: An Overview with Performance Evaluation", IEEE Communications Magazine, Vol. 42, No10, pp. 146-154, 2004.

[18] V. Oksman, J. Zhang, "G.HNEM: the new ITU-T standard on narrowband PLC technology", IEEE Communications Magazine, Vol. 49, No. 12, pp. 36-44, 2011.

[19] S. Abdul Salam, S. Mahmud, G. Khan, H. Al-Raweshidy, "M2M communication in Smart Grids: Implementation scenarios and performance analysis", IEEE WCNC Workshops, Paris, France, 2012.

[20] R. Mao, V. Julka, "Wireless Broadband Architecture Supporting Advanced Metering Infrastructure", IEEE VTC Spring, Budapest, Hungary, 2011.

[21] P. Kulkarni, S. Gormus, F. Zhong, F. Ramos, "AMI Mesh Networks—A Practical Solution and Its Performance Evaluation", IEEE Transactions on Smart Grid, Vol 3. No. 3, pp. 1469-1481, 2012.

[22] A. Zaballos, A. Vallejo, J. M. Selga, "Heterogeneous communication architecture for the smart grid", IEEE Network, Vol. 25, No. 5, pp. 30-37, 2011.

[23] Página oficial de la *PRIME Alliance*: //www.prime-alliance.org/

[24] J. Zhou, R. Quingyang, Y. Qian, "Scalable Distributed Communication Architectures to Support Advanced Metering Infrastructures in Smart Grid", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 9, pp. 1632-1642, 2012.

[25] B. C. S. Sanches, A. F. M. Batista, I. R. S. Casella, "Smart Grid for the Masses: An Agent-based system for remote measurement", IEEE SMFG 2011, Bologna, Italy, 2011.

[26] G. López, P. Moura, V. Custodio, J. I. Moreno, "Modeling the Neighborhood Area Networks of the Smart Grid", IEEE ICC, Ottawa, Canada, 2012.

Técnicas de Optimización para la Ejecución de Secuencias de Navegación

Jose Losada, Juan Raposo, Alberto Pan, Paula Montoto
Departamento de Tecnologías de la Información y las Comunicaciones
Universidade da Coruña
Facultad de Informática, Campus de Elviña, s/n, 15071, A Coruña (España)
jlosada@udc.es, jrs@udc.es, apan@udc.es, pmontoto@udc.es

Resumen. Hoy en día, las aplicaciones de automatización Web se utilizan para diferentes propósitos, tales como vigilancia tecnológica, extracción masiva, mashups, metabuscadores o pruebas automatizadas de aplicaciones Web. En la mayoría de los sistemas, el componente de navegación automático se desarrolla utilizando las APIs de navegadores convencionales (ej. Internet Explorer o Firefox). El principal inconveniente de estos sistemas es el rendimiento en tareas que requieren respuestas en tiempo real y/o requieren un número significativo de ejecuciones en paralelo. En este trabajo, se proponen un conjunto de técnicas para construir un componente de navegación capaz de ejecutar de forma eficiente secuencias de navegación Web. Estas técnicas permiten detectar los elementos de las páginas HTML que son necesarios para ejecutar correctamente la secuencia, descartando las partes no necesarias. Utilizando estas técnicas de optimización, las pruebas realizadas sobre sitios Web reales se ejecutan significativamente más rápido, consumiendo además un menor volumen de recursos.

I. INTRODUCCIÓN

La mayoría de los sitios Web han sido diseñados para ser utilizados por personas, por lo que no proporcionan interfaces programáticas para interactuar con ellos. Por ese motivo, recientemente, ha surgido un gran interés en la automatización de interacciones con sitios Web mediante la utilización de las llamadas aplicaciones de automatización Web. Estas aplicaciones son capaces de navegar de forma automática a través de sitios Web simulando el comportamiento de un usuario humano. Por ejemplo, una aplicación de metabúsqueda de vuelos, puede utilizar un componente de automatización Web para buscar vuelos en los sitios Web de las diferentes aerolíneas o agencias de viajes. Actualmente, las aplicaciones de automatización Web son ampliamente utilizadas para propósitos muy diferentes tales como vigilancia tecnológica, extracción masiva de información, tecnologías de metabúsqueda en Internet, mashups o pruebas automatizadas de aplicaciones Web.

Las aplicaciones de automatización Web permiten la ejecución de forma automática de secuencias de navegación Web. Una secuencia de navegación Web automática consiste en una sucesión de pasos que representan acciones a realizar por un usuario humano sobre un navegador Web con el objetivo de alcanzar un determinado estado en una página. La Figura 1 ilustra un ejemplo de una secuencia de navegación Web que accede al contenido del primer mensaje en la carpeta Inbox de una cuenta de Gmail.

Este trabajo se enfoca en mejorar en el rendimiento de la ejecución automática de secuencias de navegación. La aproximación seguida por la mayoría de los sistemas de

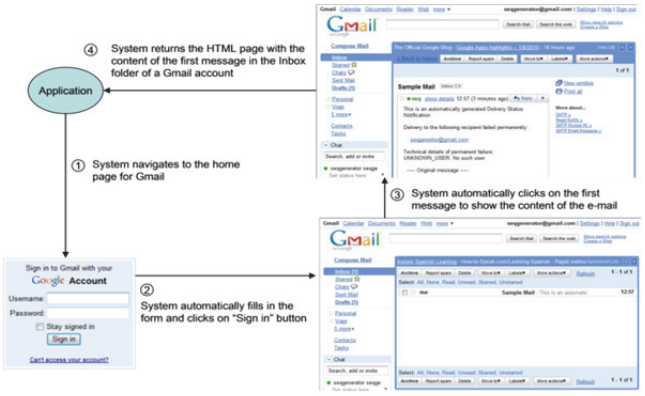


Fig. 1. Ejemplo de secuencia de navegación

navegación Web automática [1] [2] [3] [4] [5] consiste en la utilización de APIs de navegadores Web convencionales para la automatización de estas secuencias. Esta aproximación tiene la ventaja de que no requiere del desarrollo de un componente de navegación propietario, y garantiza que las páginas Web accedidas se comportarán de la misma forma que cuando son accedidas por un usuario humano mediante la utilización de un navegador "real".

A pesar de que esta aproximación es adecuada para algunas aplicaciones de automatización Web, presenta problemas de rendimiento si las tareas de automatización Web requieren respuestas en tiempo real y/o ejecutan en paralelo las secuencias de navegación un número significativo de veces. Esto es debido a que los navegadores Web comerciales están diseñados para ser aplicaciones del lado cliente, y por lo tanto, consumen una cantidad significativa de recursos: memoria, ancho de banda y CPU. En este trabajo se aborda este problema a través de la utilización de un navegador a medida, construido especialmente para ejecutar tareas de automatización Web. Este navegador es capaz de mejorar los tiempos de respuesta, consiguiendo además minimizar significativamente la utilización de recursos (memoria, CPU y ancho de banda). Para ello, se han desarrollado un conjunto de técnicas y algoritmos que permiten optimizar de forma automática las secuencias de navegación, detectando qué partes de las páginas accedidas durante la ejecución de una secuencia de navegación pueden ser descartadas (no cargadas) y qué eventos pueden ser omitidos (no disparados) sin que ello afecte a la correcta ejecución de la secuencia.

Existen otros sistemas que también utilizan navegadores Web desarrollados específicamente para ejecutar secuencias de navegación Web [6] [7]. Estos sistemas no están

orientados a su utilización por parte de humanos, y por lo tanto, pueden evitar la realización de ciertas tareas (como por ejemplo, el "renderizado" que se encarga de interpretar el contenido de una página HTML y mostrarlo formateado en la ventana del navegador). Sin embargo, dichos sistemas funcionan como un navegador convencional al cargar y construir la representación interna de las páginas Web, tareas que suponen la parte más importante en términos de uso de recursos computacionales (memoria y CPU), y por lo tanto, las mejoras de rendimiento son mucho menores que las conseguidas con el enfoque propuesto en este trabajo.

El resto del artículo se organiza de la siguiente forma. La sección 2 describe brevemente los modelos en los que se basa esta aproximación. La sección 3 presenta un resumen de la solución. La sección 4 explica en detalle las técnicas diseñadas. La sección 5 describe la evaluación experimental de la aproximación. La sección 6 discute los trabajos relacionados y finalmente, la sección 7 resume las conclusiones.

II. Modelo

El modelo principal en el que se basa este trabajo es el Document Object Model (DOM) [8]. Este modelo describe cómo los navegadores representan internamente la página Web HTML que tienen cargada en memoria y cómo responden a las acciones realizadas por el usuario sobre ella. Una página HTML se modela como un árbol, dónde cada elemento HTML se representa con un tipo específico de nodo. Un tipo de nodo importante son los nodos *script,* utilizados para situar y ejecutar un código de script sobre el documento (típicamente escritos en un lenguaje interpretado como *JavaScript*). Los nodos *script* pueden contener el código directamente o pueden referenciar un fichero externo que lo contiene. Dichos *scripts* son procesados cuando se carga la página y pueden contener declaraciones de elementos (por ejemplo, una función o una variable que podrán ser utilizadas desde otros nodos).

Adicionalmente, cada nodo del árbol puede recibir eventos producidos (directa o indirectamente) por las acciones de usuario. Existen diferentes tipos de eventos para acciones, tales como el clic con el ratón sobre un elemento (*click*), mover el cursor del ratón sobre un elemento (*mouseover*), o indicar que una página nueva se ha cargado (*load*), entre otros muchos. Cada nodo puede registrar para cada tipo de evento, un conjunto de "*escuchadores de eventos*" (*event listeners*), denominados también manejadores (*handlers*).

El ciclo de vida para el procesamiento de un evento puede resumirse de la siguiente forma: el evento es enviado siguiendo un camino desde el nodo raíz del árbol al nodo destino. El envío del evento (también denominado como propagación del evento) se realiza en dos fases diferentes, las cuales se realizan en el siguiente orden:

Capture: el evento sigue una ruta que empieza en la raíz del árbol y que llega hasta el nodo destino pasando por todos sus ancestros.

Bubbling: el evento sigue una ruta que empieza en el nodo destino y que llega hasta la raíz del árbol pasando también por todos sus ancestros. Esta fase tiene una propiedad adicional: la propagación puede ser cancelada localmente en el nodo destino o en cualquiera de sus ancestros en el árbol.

Cuando se registra el manejador de un nodo se debe indicar si pertenece a la fase de *capture* o de *bubbling*. Los eventos registrados para la fase de *capture* se ejecutan antes que los eventos ejecutados para la fase de *bubbling*.

Un manejador ejecuta código arbitrario (generalmente escrito en un lenguaje de *scripting* como *Javascript*). Los manejadores tienen acceso al árbol completo de la página y pueden realizar acciones sobre ella como por ejemplo, modificar nodos existentes, eliminarlos, crear nodos nuevos o incluso se pueden emitir nuevos eventos.

Además de los eventos provocados por acciones de usuario sobre la página, existen también algunos eventos que el navegador dispara de forma automática. El ejemplo más representativo es el evento *load*, emitido por el navegador sobre el elemento *body* de la página HTML una vez ha finalizado el proceso de carga de ésta. A partir de ahora, estos eventos se denominarán "eventos automáticos".

III. Visión General

Esta sección presenta una visión general de la propuesta realizada en este trabajo.

La entrada para el componente de navegación Web automático es la especificación de una secuencia de navegación. En la mayoría de los sistemas, esta especificación se genera a partir de un ejemplo: el usuario realiza un ejemplo de la secuencia de navegación deseada utilizando un navegador Web modificado (por ejemplo, utilizando un plugin sobre un navegador convencional); en el navegador Web se graban los eventos realizados por el usuario y se genera una especificación de la secuencia que puede ser reproducida automáticamente por un componente de ejecución. El formato exacto utilizado para especificar secuencias de navegación es diferente en cada sistema de automatización Web, pero en la mayoría de ellos esta secuencia de navegación consiste en una lista de eventos que debe ser emitida sobre determinados elementos de las páginas del sitio Web a las que se va accediendo. Es importante indicar que, entre la ejecución de una acción y la siguiente, es necesario esperar a que finalicen todos los efectos producidos por la primera de ellas (por ejemplo, esperar a que se cargue una nueva página en el navegador). Ver [9] para una discusión de las diferentes aproximaciones para grabar y ejecutar secuencias de navegación Web.

La idea básica que se presenta a continuación consiste en detectar qué partes de las páginas accedidas pueden ser descartadas (no cargadas) y qué eventos pueden ser omitidos (no emitidos) sin que ello afecte a la ejecución de la secuencia de navegación. Básicamente, esta aproximación consta de dos fases:

- Fase de optimización: el componente de navegación automático ejecuta por primera vez la secuencia de navegación para calcular qué nodos del árbol HTML DOM [8] de cada página cargada son necesarios para ejecutar la secuencia, y cuáles pueden ser descartados. Una vez finalizada esta primera ejecución, el componente de navegación almacena cierta información que le permite identificar dichos nodos en posteriores ejecuciones de la misma secuencia (la información para identificar los nodos debería ser resistente a pequeños cambios en la página). Al mismo tiempo, el componente de navegación calcula qué eventos automáticos es

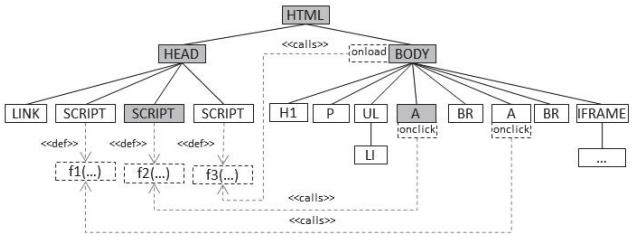


Fig. 2. Árbol DOM de una página de ejemplo

necesario emitir cada vez que se carga una página durante la ejecución de la secuencia de navegación.

- Fase de ejecución: el componente de navegación ejecuta la secuencia utilizando la información de optimización calculada en la fase previa. Cuando se carga cada página, se construye un árbol HTML DOM reducido, que contiene únicamente los nodos relevantes necesarios para ejecutar la secuencia, y sólo se emiten los eventos automáticos que la fase anterior ha identificado como necesarios para la correcta ejecución de la secuencia de navegación.

La Figura 2 muestra el árbol DOM de una sencilla página de ejemplo. Se utilizan cajas para representar los nodos en el árbol y líneas continuas para representar las relaciones de padre-hijo. Por otro lado, los manejadores de eventos se representan como cajas con líneas punteadas y adyacentes a su nodo en el árbol (*onclick*, *onload*). Las flechas con líneas discontinuas se utilizan para indicar las funciones definidas en nodos *script* (<*def*>) y las funciones definidas en nodos *script* que se invocan desde manejadores (<*calls*>). Sobre este árbol DOM, podría ejecutarse una secuencia de navegación con una única acción que podría consistir en un clic sobre el primer nodo *A*. Cuando se emite el evento *click*, se ejecuta el manejador de evento *onclick*, y la función *f2* realiza una navegación a la página deseada (por ejemplo, mediante la ejecución del siguiente código *javascript*: *window.location = 'http://acme.com';*).

Los nodos marcados en gris son los necesarios para simular la acción clic y ejecutar correctamente la navegación a la siguiente página (que denominaremos como "*nodos relevantes*"). En este ejemplo, los nodos relevantes son: el nodo *A* que es el objeto del evento *click* emitido por esta secuencia de navegación, el nodo *SCRIPT* que define la función *f2* ejecutada por el manejador de evento *onclick*, y sus respectivos ancestros (las reglas que han sido utilizadas para calcular los nodos relevantes serán descritas más adelante). El resto de los nodos pueden ser descartados (no cargados) sin que ello afecte a la ejecución (a estos nodos los denominaremos "*nodos irrelevantes*"). Además, no se necesita disparar el evento automático *load* cuando se carga la página, porque no es necesario ejecutar el código del manejador de evento *onload* para reproducir la secuencia de forma correcta.

Esta aproximación producirá mejoras significativas en el rendimiento y el uso de recursos:

— Se producirá un ahorro de memoria, porque se representarán muchos menos nodos en el árbol DOM.

— Se utilizará menos tiempo de CPU porque no se ejecutarán los scripts innecesarios. En el ejemplo anterior, no es necesario ejecutar los nodos *script* que no se muestran en gris.

— Se producirá un ahorro en ancho de banda porque no se realizarán las navegaciones que son innecesarias. En el ejemplo anterior, no se realizarán las navegaciones especificadas por los nodos LINK e IFRAME.

El principal problema reside en cómo calcular lo que denominamos "*dependencias de nodos*". En el ejemplo anterior, el nodo *SCRIPT* que define *f2* es una dependencia del nodo *A* cuando se emite el evento *click* sobre dicho nodo. Es importante indicar que en el modelo DOM, los *scripts* son "cajas negras" y por tanto, dichas dependencias no pueden ser inferidas a priori. Sin embargo, al utilizar un navegador desarrollado específicamente para estas tareas, es posible controlar el motor de ejecución de *scripts* al más bajo nivel y por lo tanto, es posible detectar esas dependencias que estarían ocultas al utilizar el API de más alto nivel de un navegador comercial.

También es necesario resaltar el hecho de que las dependencias pueden llegar a ser mucho más complejas que las descritas en el escenario anterior. Por ejemplo, la emisión de un evento *click* sobre un enlace puede producir la ejecución de un *script* que requiera la ejecución previa del código *scripting* definido en otro nodo diferente del árbol DOM. Otro ejemplo con mayor dificultad sería aquel en el que el manejador de evento *load* del nodo *BODY* generase contenido dinámico, incluyendo un nodo *A* sobre el cual se podría emitir posteriormente un evento *click*. Podría ocurrir incluso que un *script* haga uso de elementos definidos en otro *script* y este último podría estar definido en un marco diferente (*iframe*). En la siguiente sección se describe cómo se pueden abordar estos problemas.

IV. Técnicas Propuestas

En esta sección se presentan, en primer lugar, algunas definiciones y propiedades (sección IV.A) para modelar todas las posibles dependencias entre los nodos del árbol DOM. A continuación, se describen las técnicas utilizadas durante la fase de optimización (sección IV.B). Posteriormente, se explica brevemente la metodología utilizada para la generación de las expresiones que permiten identificar a los nodos irrelevantes (sección IV.C) y finalmente, se perfilan las operaciones que se llevan a cabo durante la fase de ejecución (sección IV.D).

A. Dependencias de Nodos

Definición 1: se dice que existe una dependencia entre dos nodos *n1* y *n2* cuando el nodo *n2* es necesario para la correcta ejecución del nodo *n1*. Se dice que el nodo *n2* es una dependencia del nodo *n1* y se denota *n1*→ *n2*. Las siguientes reglas definen este tipo de dependencias:

- Si el código *script* de un nodo *s1* utiliza un elemento declarado en un nodo *SCRIPT s2* (por ejemplo, una función o una variable), entonces *s1*→ *s2*. Justificación: para poder ejecutar el código de *script* del nodo *s1*, debe ejecutarse con anterioridad el nodo *s2*.

- Si el código *script* de un nodo *s* utiliza un nodo *n*, entonces *s*→ *n*. Justificación: para poder ejecutar el

código *script* del nodo *s*, debe cargarse previamente el nodo *n*. Por ejemplo, si *s* obtiene una referencia al nodo *A* utilizando la función *JavaScript document.getElementById* y navega a la URL especificada en su atributo *href*, entonces no se podrá ejecutar correctamente el código de *script* de *s* si no se carga previamente el nodo *A*.

- Si el código *script* de un nodo *s* realiza una modificación en un nodo *n*, entonces $n \rightarrow s$. Justificación: la acción realizada por *s* puede ser necesaria en una acción posterior sobre el nodo *n*. Por ejemplo, si *s* modifica el atributo *action* de un nodo *FORM* para establecer la URL destino, entonces no podrá realizarse el envío del formulario a no ser que *s* se ejecute previamente.

Definición 2: se dice que existe una dependencia condicionada a que el evento *e* se dispare sobre el nodo *n*, entre dos nodos *n1* y *n2*, cuando el nodo *n2* es necesario para la correcta ejecución del nodo *n1*, cuando se dispara el evento *e* sobre el nodo *n*. Se denota como $n1 \rightarrow^{e|n} n2$. Este tipo de dependencias se definen mediante un conjunto de reglas análogas a las explicadas en la definición anterior, con la diferencia de que en este caso, involucran nodos que contienen manejadores de eventos:

- Si el código *script* de un manejador de eventos *l* para el evento *e* sobre el nodo *n* utiliza un elemento declarado en un nodo *script s* (por ejemplo, una función o una variable), entonces $n \rightarrow^{e|n} s$. Justificación: si el evento *e* se emite sobre el nodo *n*, entonces se ejecutará el manejador de eventos *l* el cual requiere que se ejecute previamente el nodo *SCRIPT s*.

- Si el código *script* de un manejador de eventos *l* para el evento *e* sobre el nodo *n1* utiliza un nodo *n2*, entonces $n1 \rightarrow^{e|n1} n2$. Justificación: si se emite el evento *e* sobre *n1*, entonces se ejecutará el manejador de evento *l* y por tanto, se deberá cargar previamente el nodo *n2*.

- Si el código *script* de un manejador de eventos *l* para el evento *e* sobre el nodo *n1* realiza una modificación en un nodo *n2*, entonces $n2 \rightarrow^{e|n1} n1$. Justificación: la acción realizada por *l* puede ser necesaria para que *n2* sea utilizado posteriormente. Por ejemplo, si *l* modifica el atributo *action* de un nodo *FORM* para establecer la URL destino, entonces no será posible enviar el formulario a no ser que se ejecute previamente *l*. Debido a que *l* únicamente será ejecutado cuando se dispare el evento *e* sobre *n1*, entonces *n1* es necesario.

Las siguientes propiedades de transitividad son aplicables a las dependencias entre nodos (cada una de ellas será explicada con un ejemplo).

Propiedad 1: Si $n1 \rightarrow n2$ y $n2 \rightarrow n3$ entonces $n1 \rightarrow n3$.

El ejemplo de la Figura 3.a muestra un fragmento del árbol DOM de una página en la que el código *script* del nodo *SCRIPT1* invoca a la función *f1*, definida en el nodo *SCRIPT2* (*SCRIPT1→ SCRIPT2*), y el código de la función *f1* invoca a la función *f2,* definida en el nodo *SCRIPT3* (*SCRIPT2→ SCRIPT3*). Para una correcta ejecución del código *script* del nodo *SCRIPT1*, son necesarios tanto el segundo como el tercer nodo *SCRIPT*, por tanto ambos son dependencias de éste (*SCRIPT1→ SCRIPT3*).

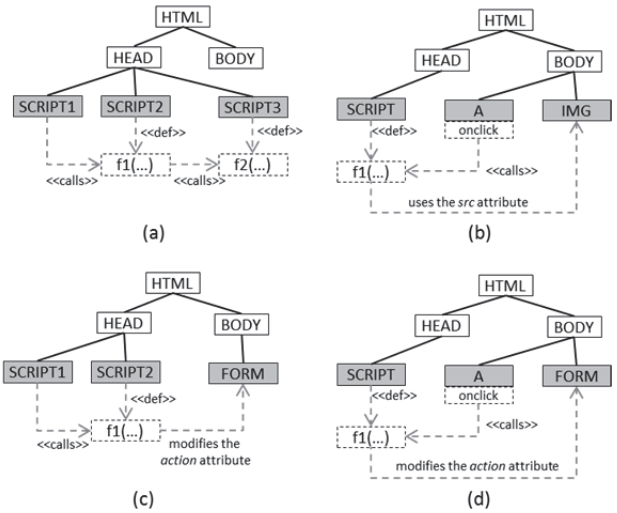


Fig. 3. Ejemplos de dependencias transitivas

Propiedad 2: Si $n1 \rightarrow^{e|n} n2$ y $n2 \rightarrow n3$ entonces $n1 \rightarrow^{e|n} n3$.

El ejemplo de la Figura 3.b muestra un fragmento del árbol DOM de una página donde el manejador de evento *click* de un nodo *A* invoca a la función *f1*, definida en el nodo *SCRIPT* ($A \rightarrow^{click|A} SCRIPT$), y el código de la función *f1* utiliza el atributo *src* del nodo *IMG* (*SCRIPT→ IMG*). Para realizar un procesamiento correcto del nodo *A* cuando se emite el evento *click* sobre él, son necesarios tanto el nodo *SCRIPT* como el nodo *IMG*, y por lo tanto ambos son dependencias del nodo *A* ($A \rightarrow^{click|A} IMG$).

Propiedad 3: Si $n1 \rightarrow n2$, y $n3 \rightarrow n2$ porque *n2* es un nodo script que realiza una modificación en *n3*, entonces $n3 \rightarrow n1$.

El ejemplo de la Figura 3.c muestra un fragmento del árbol DOM de la página donde el código del nodo *SCRIPT1* invoca a una función *f1*, definida en el nodo *SCRIPT2* (*SCRIPT1→ SCRIPT2*), y el código de la función *f1* modifica el atributo *action* del nodo *FORM* (*FORM→ SCRIPT2*). Para el correcto procesamiento del nodo *FORM* (por ejemplo, para que el formulario se envíe correctamente), es necesario definir y ejecutar previamente la función *f1* (esto implica que son necesarios los nodos *SCRIPT1* y *SCRIPT2*). Por lo tanto, ambos nodos son dependencias del elemento *FORM* (*FORM→ SCRIPT1*).

Propiedad 4: Si $n1 \rightarrow^{e|n} n2$ y $n3 \rightarrow n2$ porque *n2* es un nodo *script* que realiza una modificación en *n3*, entonces $n3 \rightarrow^{e|n} n1$.

El ejemplo de la Figura 3.d muestra un fragmento del árbol DOM de una página en la que el manejador de evento *click* del nodo *A* invoca la función *f1*, definida en el nodo *SCRIPT* ($A \rightarrow^{click|A} SCRIPT$), y el código de la función *f1* modifica el atributo *action* del nodo *FORM* (*FORM→ SCRIPT*). Para que el nodo FORM sea procesado correctamente cuando se emite el evento *click* sobre el nodo *A* (por ejemplo, para enviar el formulario), son necesarios tanto el nodo *SCRIPT* como el nodo *A*, es decir, ambos son dependencias del nodo *FORM* ($FORM \rightarrow^{click|A} A$).

B. Cálculo de nodos y eventos automáticos relevantes

El principal objetivo de la fase de optimización es identificar el conjunto de nodos relevantes, todos ellos necesarios para la correcta ejecución de la secuencia de navegación. Durante esta fase, el navegador opera de manera similar a cómo lo hace un navegador convencional: se carga la página completa, se genera el árbol DOM, se descargan todos los elementos externos (por ejemplo, las hojas de estilo y los ficheros de *script*) y se ejecutan todos los nodos *script* definidos en la página. Además, también se disparan todos los eventos automáticos (ver la sección 2 para recordar la definición de eventos automáticos) que el navegador emite automáticamente cuando se carga completamente cada nueva página (por ejemplo, el evento *load* se emite sobre el elemento *body*). Posteriormente, el navegador reproducirá la secuencia de navegación previamente definida, disparando los eventos necesarios en los elementos adecuados para emular la interacción del usuario con la página (por ejemplo, realizando un clic sobre un elemento, moviendo el ratón sobre un nodo de la página, etc.), hasta que se inicia una navegación a una nueva página.

Durante todo este proceso, el navegador interactúa con el motor de ejecución de *scripts* para detectar las dependencias entre los nodos (en este desarrollo se utiliza Mozilla Rhino). Para obtener estas dependencias se utilizan las reglas definidas en la sección anterior. Por ejemplo, cuando se ejecuta un nodo *script*, el navegador interactúa con el motor de ejecución para monitorizar qué funciones son invocadas durante su ejecución. De acuerdo con la primera regla de la Definición 1, el nodo que previamente ha definido dichas funciones, se marca como dependencias del nodo *script* que se está ejecutando. De forma análoga, si el código del nodo *script* crea o modifica otro nodo, de acuerdo a la regla 3 de la Definición 1, este nodo *script* será una dependencia del nodo modificado.

De forma análoga, cuando se emite un evento (ya sea automático o generado por la secuencia de navegación), el navegador monitoriza, por un lado, los nodos utilizados durante la ejecución de los manejadores asociados al evento y por otro lado, también monitoriza si se generan otros eventos y qué nodos se modifican durante la ejecución de estos. Es decir, se generarán las dependencias apropiadas de acuerdo a las reglas de la Definición 2.

Una vez calculadas todas las dependencias, se construye el conjunto de nodos relevantes y para ello se utilizan las siguientes reglas:

1. Los nodos que se utilizan directamente en la secuencia de navegación ejecutada son relevantes. Por ejemplo, si un paso de la secuencia de navegación genera un evento *click* sobre un nodo *A*, entonces ese nodo *A* es relevante.

2. Si un nodo *n* es relevante, todos sus ancestros son relevantes. Es necesario tener en cuenta que los ancestros podrían ser necesarios debido a las fases de *capture* y *bubbling* del modelo de eventos del árbol DOM (ver sección 2).

3. Por definición, si el nodo *n1* es relevante y $n1 \rightarrow n2$ entonces *n2* es relevante (es decir, todas las dependencias de un nodo relevante son relevantes también).

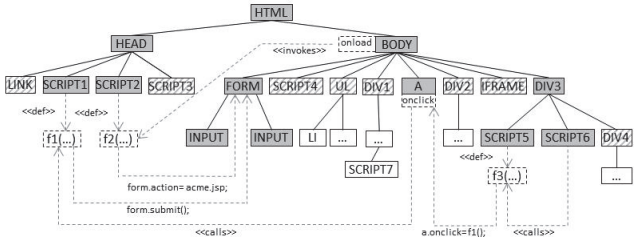


Fig. 4. Ejemplo

4. Por definición, si un nodo *n1* es relevante, $n1 \rightarrow^{e|n} n2$, y el evento *e* fue disparado sobre el nodo *n*, entonces *n2* es relevante (es decir, si se emite el evento *e* sobre el nodo *n*, todas las dependencias condicionadas a que el evento *e* se dispare sobre *n* son también relevantes).

5. Con el objetivo de enviar correctamente los formularios, se aplican algunas reglas especiales sobre los nodos relacionados con estos: (a) si un nodo formulario es relevante, también son relevantes todos los nodos de entrada (nodos *input*) y de selección (nodos *select*) que están contenidos en el formulario, (b) si un nodo *input* o *select* es relevante, el nodo formulario que lo contiene es relevante, (c) si un nodo selección es relevante, todos sus nodos hijos *option* son relevantes.

6. Un pequeño conjunto de nodos correspondientes a algunos tipos especiales de elementos se consideran siempre como relevantes. Estos nodos son necesarios para procesar de forma adecuada otros nodos del árbol DOM de la página. Por ejemplo, el elemento *base* establece la URL base, lo que significa que las URLs especificadas por otros elementos son relativas al valor que indica dicho elemento.

A partir del conjunto de nodos relevantes, se puede calcular fácilmente el conjunto de nodos irrelevantes que pueden ser eliminados durante la fase de ejecución. En primer lugar, todos nodos del árbol DOM que no están contenidos en el conjunto de nodos relevantes se añaden al conjunto de nodos irrelevantes. Posteriormente, se eliminan del conjunto de irrelevantes todos aquellos nodos que tienen un ancestro que también está contenido en dicho conjunto. Como resultado se obtienen únicamente los nodos raíz de los subárboles cuyos descendientes son todos irrelevantes. Dicho conjunto se denomina conjunto de subárboles irrelevantes.

Finalmente, para determinar cuáles de los eventos automáticos son necesarios para la correcta ejecución de la secuencia, el sistema comprueba, por cada evento automático, si alguno de los nodos relevantes tiene una dependencia derivada de ese evento (es decir, comprueba si algún nodo relevante ha sido afectado por uno de los manejadores ejecutados como resultado de haber disparado el evento). Si se produce esto, entones el evento es añadido a la lista de eventos automáticos que deberían ser emitidos en tiempo de ejecución cuando se carga la página HTML.

A continuación se muestra un ejemplo. La Figura 4 muestra un fragmento del árbol DOM de una página. La secuencia que se ejecuta sobre esta página emite un evento *click* sobre el nodo *A*. Los nodos relevantes para esta interacción se muestran en gris en la figura. Estos nodos relevantes han sido calculados de la siguiente manera:

- De acuerdo con la regla 1, el nodo *A* es relevante (porque es el objetivo de la acción).

- De acuerdo con la regla 2, todos los ancestros de *A* son relevantes: *BODY* y *HTML*.

- De acuerdo con la regla 3, todas las dependencia de *A* son relevantes: *SCRIPT5* y *SCRIPT6* (y sus ancestros: *DIV3*). En este caso son necesarios porque ejecutan el código *script* que modifica el manejador de evento *click* del nodo *A* cuando se carga la página.

  — La función *f3* (definida en *SCRIPT5*) modifica el manejador del evento *click* del nodo *A*, por tanto *A →SCRIPT5*.

  — *SCRIPT6*, que se ejecuta cuando se carga la página, invoca a la función *f3*, por tanto *SCRIPT6→ SCRIPT5*, y debido a las reglas de transitividad explicadas en la sección 2, *A→ SCRIPT6*.

- De acuerdo con la regla 4, también son relevantes todas las dependencias de *A* condicionadas a que el evento *click* se dispare sobre el nodo *A*: *SCRIPT1* y *FORM* (y todos sus ancestros: *HEAD*). Dichos nodos son necesarios porque el manejador del evento *click* del nodo *A* invoca la función definida en *SCRIPT1* y esta función es la que envía el formulario *FORM*.

  — El manejador de evento *onclick* del nodo *A* invoca la función *f1* definida en *SCRIPT1*, por tanto $A \rightarrow^{click|A}$ *SCRIPT1*.

  — La función *f1* utiliza el nodo *FORM*, por tanto *SCRIPT1→FORM*, y debido a las reglas de transitividad explicadas en la sección 2, $A \rightarrow^{click|A}$ *FORM*.

- De acuerdo a la regla 5, si un nodo *FORM* es relevante, son relevantes todos nos nodos *INPUT* contenidos en el formulario: *INPUT1* y *INPUT2*. Para enviar correctamente el formulario, todos sus campos de entrada son necesarios.

- De acuerdo a la regla 3, todas las dependencias del nodo *FORM* son relevantes: *SCRIPT2* y *BODY* (y todos sus ancestros, que ya están incluidos en el conjunto de nodos relevantes). Dichos elementos son necesarios porque el manejador de evento *load* del nodo *BODY* invoca una función definida en *SCRIPT2* y esta función modifica el atributo *action* del nodo *FORM*.

  — El manejador de evento *onload* del nodo *BODY* invoca la function *f2* definida en *SCRIPT2*, por tanto $BODY \rightarrow^{load|body}$ *SCRIPT2*.

  — La function *f2* (definida en *SCRIPT2*) modifica el atributo *action* del nodo *FORM*, por tanto *FORM →SCRIPT2*, y debido a las reglas de transitividad explicadas en la sección 2, $FORM \rightarrow^{load|body}$ *BODY*.

Los nodos que se muestran a rayas en la Figura 4 son los nodos que han sido identificados como raíces de subárboles irrelevantes, los cuales pueden ser descartados en posteriores ejecuciones de la secuencia.

El evento automático *load*, emitido sobre el nodo *BODY*, debe ser añadido a la lista de eventos automáticos necesarios, porque el nodo *FORM*, que es un nodo relevante, tiene una dependencia derivada de él ($FORM \rightarrow^{load|body}$ *BODY*). Es necesario tener en cuenta que, para enviar correctamente el formulario, el manejador del evento *load* del elemento *BODY* (*onload*) debe ser ejecutado, porque invoca a la función *f2* y esta función establece el atributo *action* del formulario.

C. Identificación de los Subárboles Irrelevantes en la Fase de Ejecución

Una vez que se han calculado los nodos raíces de los subárboles irrelevantes, es necesario generar expresiones para identificar a cada uno de estos subárboles durante la fase de ejecución. Existen dos requisitos para este proceso. Por un lado, las expresiones generadas deberían ser resistentes a pequeños cambios en la página, porque en los sitios Web reales hay generalmente pequeñas diferencias entre el árbol DOM de la misma página cargada en diferentes momentos (por ejemplo, puede aparecer un nuevo anuncio de publicidad o se pueden mostrar registros de datos diferentes). Por otro lado, la comprobación de si un nodo encaja con una expresión, debe ser un proceso muy eficiente, porque durante la fase de ejecución se comprueba si cada uno de los nodos encaja con alguna de esas expresiones.

Para identificar unívocamente un nodo en el árbol DOM se utiliza una expresión de tipo XPath [10]. Cada una de las expresiones generadas debe identificar a un único nodo en todo el árbol, pero además, estas expresiones no deberían ser demasiado específicas como para que se vean afectadas por pequeños cambios en la página. Por ese motivo, se utiliza una versión mejorada del algoritmo explicado en [9], que no se explica en detalle debido a las limitaciones de espacio.

D. Fase de Ejecución

El funcionamiento general del componente de navegación en esta fase es el siguiente: antes de cargar cada una de las páginas, se comprueba si existe información de optimización asociada a esa página, es decir, si existe un conjunto de expresiones para identificar los nodos raíz de los subárboles irrelevantes. Esa información se utiliza para construir una versión reducida del árbol DOM HTML. Esta versión reducida del árbol contiene únicamente los nodos relevantes. Posteriormente, se comprueban si existe información relativa a los eventos automáticos que deberían ser disparados en esa página. En caso de que esta información exista, sólo se emiten los eventos ahí indicados.

El proceso que comprueba si un nodo es raíz de un subárbol irrelevante debe ser muy eficiente porque esa comprobación se realiza para cada uno de los elementos presentes en la página, con el objetivo de decidir si debe o no añadirse al árbol DOM HTML. Por esta razón, no se utiliza un algoritmo convencional de emparejamiento de expresiones XPath. En su lugar, se utiliza un algoritmo diseñado específicamente, que aprovecha el hecho de que el tipo de expresiones XPath que se generan, utilizan tan solo un subconjunto estricto de XPath y siempre verifica ciertas restricciones. Este algoritmo específico es mucho más rápido para estas expresiones particulares y consiste, a grandes

Tabla I
COMPARACIÓN DE EJECUCIÓN NORMAL Y OPTIMIZADA

	HTML DOM nodes created	Scripts executed	Frames and Windows	HTML pages downloaded	External objects downloaded	AJAX requests
Alexa	1176/144	48/20	1/1	2/2	27/16	0/0
Amazon	7965/4047	176/77	6/2	9/4	13/5	2/1
AppleStore	2611/79	69/1	1/1	3/3	15/11	2/0
Barnes&Noble	3989/136	26/26	1/1	4/4	14/14	0/0
Bloomberg	6281/187	243/28	14/11	8/7	53/6	0/0
CNET	3395/157	113/56	7/4	9/6	52/24	0/0
CNN	4539/40	103/8	6/1	7/3	30/5	0/0
Ebay	4932/3175	80/37	4/1	8/4	25/9	0/0
Flickr	1332/61	61/9	2/1	5/4	19/1	0/0
GoogleNews	7460/114	48/11	2/1	4/4	9/3	0/0
Imdb	2608/485	183/56	28/1	8/3	34/10	4/3
Linkedin	2095/167	52/12	3/1	5/3	20/5	3/0
Reference	2709/579	152/29	7/2	9/3	33/11	0/0
Reuters	2797/298	265/50	11/2	12/3	156/41	4/1
Softonic	4932/250	79/6	12/1	15/4	17/3	0/0
Spiegel	3361/139	92/25	20/3	21/4	22/7	1/0
StackOverflow	3950/153	43/9	1/1	3/3	21/5	4/1
Taringa	2530/256	209/15	10/1	13/3	47/8	7/0
Theguardian	4519/248	257/70	5/1	4/3	76/28	0/0
Tripadvisor	6769/88	92/14	1/1	4/4	6/0	0/0
W3CSchools	2380/32	89/0	8/1	8/3	33/0	0/0
Walmart	6926/385	208/29	15/3	4/3	42/13	4/3
Wikipedia	5078/143	52/24	1/1	4/4	37/21	0/0
Wordpress	472/37	56/21	6/1	7/2	18/10	0/0
WSJournal	6303/1148	204/118	39/24	60/35	78/50	0/0
Yahoo	1946/85	127/33	7/1	8/2	16/2	0/0
Yelp	2815/508	52/6	7/1	2/2	14/0	0/0
Total	**105870/13141 (12,41%)**	**3179/790 (24,85%)**	**225/70 (31,11%)**	**246/125 (50,81%)**	**927/308 (33,23%)**	**31/9 (29,03%)**

Tabla II
TIEMPOS DE EJECUCIÓN MEDIOS EXPRESADOS EN MILISEGUNDOS

	Custom browser with optimization	Custom browser without optimization	HtmlUnit	Internet Explorer	Mozilla Firefox
Alexa	2782	4426 (159%)	5329 (192%)	13902 (500%)	13152 (473%)
Amazon	5019	8549 (170%)	10927 (218%)	22320 (445%)	18584 (370%)
AppleStore	2009	4228 (210%)	5043 (251%)	16953 (844%)	16253 (809%)
Barnes&Noble	5094	7187 (141%)	6422 (126%)	27578 (541%)	26390 (518%)
Bloomberg	1593	7908 (496%)	18081 (1135%)	34744 (2181%)	26710 (1677%)
CNET	7065	11563 (164%)	17537 (248%)	26615 (377%)	21389 (303%)
CNN	2779	9294 (334%)	21763 (783%)	20392 (734%)	14649 (527%)
Ebay	5274	8377 (159%)	12286 (233%)	22993 (436%)	17894 (339%)
Flickr	4055	9338 (230%)	11813 (291%)	21277 (525%)	14124 (348%)
GoogleNews	2414	5810 (241%)	8599 (356%)	27337 (1132%)	16783 (695%)
Imdb	4279	9361 (219%)	11429 (267%)	21530 (503%)	16629 (389%)
Linkedin	2839	6230 (219%)	5839 (206%)	17941 (632%)	13135 (463%)
Reference	4694	12639 (269%)	19650 (419%)	17849 (380%)	17364 (370%)
Reuters	5621	19341 (344%)	22261 (396%)	20323 (362%)	19562 (348%)
Softonic	3272	6579 (201%)	14048 (429%)	16600 (507%)	18893 (577%)
Spiegel	4297	9570 (223%)	12948 (301%)	14562 (339%)	14513 (338%)
StackOverflow	2341	6770 (289%)	6377 (272%)	19113 (816%)	13681 (584%)
Taringa	4546	13746 (302%)	14614 (321%)	18690 (411%)	17569 (386%)
Theguardian	5604	12219 (218%)	18490 (330%)	23730 (423%)	27909 (498%)
Tripadvisor	3353	4921 (147%)	14942 (446%)	24896 (742%)	18772 (560%)
W3CSchools	1251	8143 (651%)	8793 (703%)	19049 (1523%)	12407 (992%)
Walmart	5633	12554 (223%)	20183 (358%)	20998 (373%)	20896 (371%)
Wikipedia	4309	7192 (167%)	10711 (249%)	18742 (435%)	14524 (337%)
Wordpress	2792	5776 (207%)	6373 (228%)	16020 (574%)	14177 (508%)
WSJournal	13621	21028 (154%)	19201 (141%)	21719 (159%)	19087 (140%)
Yahoo	4013	8875 (221%)	13496 (336%)	21816 (544%)	16639 (415%)
Yelp	2906	6706 (231%)	10228 (352%)	20035 (689%)	19828 (682%)
Average		244%	355%	634%	519%
Standard Dev.		109 (45%)	210 (59%)	404 (64%)	284 (55%)
Average ± Stdev.		201%	248%	449%	385%
Median		219%	301%	507%	463%

rasgos, en chequear si existen nodos, en el camino que va desde el nodo que se está procesando hasta la raíz del árbol, que se puedan emparejar con todas las "expresiones individuales" que componen la expresión XPath.

V. EVALUACIÓN

Para comprobar la validez de las técnicas anteriormente descritas, se ha desarrollado un navegador a medida que implementa los algoritmos propuestos en los apartados anteriores y se han realizado una serie de experimentos que se detallan a continuación. Este navegador a medida ha sido desarrollado en Java utilizando librerías de código abierto incluyendo *Apache Commons-Httpclient* para el manejo de peticiones HTTP, el analizador sintáctico *Neko HTML* para construir las estructuras DOM y *Mozilla Rhino* como motor de ejecución de *JavaScript*.

Esta sección explica el conjunto de experimentos que han sido realizados y para ello, se ha seleccionado un conjunto de sitios Web de diferentes dominios, todos ellos incluidos en el ranking de Alexa [11] de los 500 sitios Web más visitados. En cada sitio Web se ha grabado una secuencia de navegación representativa de su función principal (por ejemplo, en un sitio de Web de comercio electrónico, se ha realizado una búsqueda de un producto). Cada secuencia ejecuta eventos para rellenar y enviar formularios, eventos para navegar a través de hipervínculos, y en algunos casos, eventos para mostrar el contenido que se obtiene tras la ejecución de peticiones AJAX.

En el primer experimento, se comparan los recursos que consume el navegador desarrollado a medida cuando utiliza sus capacidades de optimización con los recursos que consume durante una ejecución normal (esta segunda ejecución emula el comportamiento de un navegador comercial, cargando al completo todas las páginas accedidas y disparando todos los eventos automáticos). En este experimento, se ha ejecutado previamente la secuencia de navegación para obtener la información de optimización. Posteriormente, se han realizado dos ejecuciones más de esta misma secuencia, en la primera de ellas no se ha utilizado la información de optimización, y en la segunda sí se utilizado dicha información. La Tabla 1 muestra los valores obtenidos en cada una de las ejecuciones para los sitios Web que han sido seleccionados (cada celda de la tabla muestra el resultado de la ejecución normal seguido del resultado de la ejecución optimizada). Para evitar el problema de pequeñas variaciones en el acceso a las páginas Web cuando se realiza en diferentes momentos, cada secuencia se ha ejecutado 10 veces y el resultado es la media de las 10 ejecuciones.

Al medir los recursos utilizados en la ejecución de todas las secuencias de navegación, las ejecuciones optimizadas únicamente requieren crear el 12,41% de los nodos de los árboles DOM de las páginas cargadas. Al descartar nodos, el navegador también evita las descargas innecesarias y la ejecución de *scripts* innecesarios, de tal forma que el uso de memoria y CPU se minimiza de forma significativa. La ejecución optimizada únicamente ejecuta el 24,85% de los *scripts*, crea el 31,11% de los marcos (*frames*) y ventanas, descarga el 50,81% de los documentos HTML y el 33,23% de objetos externos (e.g. *scripts* y hojas de estilo CSS), y ejecuta el 29,03% de las peticiones AJAX.

En el segundo experimento se compara el tiempo de ejecución del navegador a medida cuando utiliza y cuando no utiliza sus capacidades de optimización, con el tiempo de ejecución de otros componentes de navegación representativos. Se ha seleccionado, por una parte, un componente de navegación basado en otro navegador a medida, en este caso, HtmlUnit [6], proyecto de código abierto que también soporta *JavaScript* y CSS. Y por otra parte, se han seleccionado dos componentes de navegación que utilizan las APIs de dos navegadores comerciales, en este caso Microsoft Internet Explorer 9 y Mozilla Firefox 19. La Tabla 2 muestra el tiempo de ejecución medio de 20 ejecuciones consecutivas de cada una de las secuencias de navegación de prueba, descartando aquellas que no se encuentran dentro del rango de la desviación estándar. La Tabla 2 también muestra el porcentaje de tiempo en comparación con el tiempo de ejecución del navegador a medida cuando utiliza sus capacidades de optimización.

En general, tanto el navegador a medida como HtmlUnit obtienen mejores resultados que Firefox e Internet Explorer. Esto se debe a que estos componentes, al no estar orientados a su utilización por humanos, no necesitan ejecutar algunas tareas que sí se ejecutan en los navegadores convencionales,

por ejemplo, la renderización de la página en el interfaz de usuario.

El tiempo de ejecución del navegador a medida, cuando utiliza sus capacidades de optimización, siempre ha sido mejor en comparación con los tiempos obtenidos para el resto de componentes de navegación. Comparados con la ejecución sin optimización, los tiempos de ejecución varían desde 141% en el peor de los casos hasta el 651% en el mejor de los casos. Al calcular la media de porcentajes, descartando aquellos que no quedan dentro del rango de la media ± desviación típica (la desviación típica es del 45%), el tiempo de ejecución del navegador propietario sin optimización es 2,01 veces más lento (201%) que el tiempo de ejecución con optimización. La mediana de las ejecuciones indica que el navegador propietario sin optimización es 2,19 veces más lento. Realizando los mismos cálculos, el componente de navegación basado en HtmlUnit es, de media, 2,48 veces más lento (248%) que el navegador propietario con optimización y la mediana de las ejecuciones indica que es 3,01 veces más lento. En el caso del componente de navegación basado en Microsoft Internet Explorer, el tiempo medio de ejecución es 4,49 veces más lento (449%) que el tiempo de ejecución del navegador propietario con optimización y la mediana de las ejecuciones indica que es 5,07 veces más lento. Por último, el componente de navegación basado en Mozilla Firefox es 3,85 veces más lento (385%) que el tiempo de ejecución del navegador propietario con optimización y la mediana de las ejecuciones indica que es 4,63 veces más lento.

VI. Trabajos Relacionados

Actualmente las aplicaciones de automatización Web son ampliamente utilizadas para diferentes propósitos. La aproximación seguida por la mayoría de los sistemas de automatización Web, como Smart Bookmarks [1], Wargo [2], QEngine [3], Sahi [4], Selenium [5], and Montoto et al. [9] consiste en utilizar las APIs de navegadores Web convencionales para automatizar la ejecución de secuencias.

Esta aproximación tiene dos ventajas importantes: por un lado, no requiere del desarrollo de un nuevo navegador a medida (este desarrollo es complejo y supone un gran esfuerzo) y por otro lado, está garantizado que las páginas se comportarán del mismo modo que cuando un usuario humano accede a ellas utilizando su navegador. Sin embargo, esta aproximación presenta problemas de rendimiento para tareas de automatización Web intensivas que requieren respuestas en tiempo real y/o requieren de la ejecución en paralelo de un número significativo de secuencias de navegación. Esto se debe a que los navegadores Web convencionales están diseñados para ser aplicaciones del lado cliente y, por tanto, consumen una cantidad significativa de recursos.

Otros sistemas utilizan la aproximación de crear navegadores a medida simplificados, especialmente construidos para esa tarea. WebVCR [12] y WebMacros [13] se basan en la utilización de clientes HTTP simples que carecen de la posibilidad de ejecutar código de *scripting* complejo y tampoco soportan peticiones AJAX. El navegador a medida desarrollado para este trabajo, soporta todas esas funcionalidades más complejas.

HtmlUnit [6] y Kapow [7] utilizan un navegador a medida con soporte para muchas funcionalidades AJAX y *Javascript*. Dichos sistemas son más eficientes que los navegadores Web comerciales, porque no están orientados a ser utilizados por humanos y por lo tanto pueden evitar la realización de ciertas tareas (como por ejemplo, el "renderizado" que se encarga de interpretar el contenido de una página HTML y mostrarlo formateado en la ventana del navegador). Sin embargo, HtmlUnit funciona como un navegador comercial al cargar y construir la representación interna de las páginas Web. Por otro lado, la última versión de Kapow no se encuentra disponible para descarga, pero según nuestro conocimiento, también carga y construye la representación interna de la página al igual que un navegador convencional. Como el proceso de carga de la página HTML es la parte más importante en cuanto a la utilización de recursos computacionales, las mejoras en el rendimiento obtenidos por estos sistemas, son mucho menores que los conseguidos con el enfoque que se propone en este trabajo.

VII. Conclusiones

En este trabajo se presenta un conjunto original de técnicas y algoritmos para ejecutar eficientemente secuencias de navegación Web. Esta aproximación realiza una ejecución previa de la secuencia de navegación Web y en esta primera ejecución se obtiene la información sobre los elementos de las páginas HTML que no son necesarios para la correcta ejecución de la secuencia. Posteriormente, esa información se utiliza en las siguientes ejecuciones de la misma secuencia y ello permite construir el árbol DOM de las páginas HTML utilizando solamente los elementos imprescindibles, y emitir únicamente los eventos que son estrictamente necesarios. De acuerdo con los experimentos realizados, estas técnicas son altamente efectivas: se construyen árboles DOM más pequeños, no se ejecutan *scripts* innecesarios y no se realizan muchas de las navegaciones. De esta manera, las técnicas propuestas permiten ahorrar ancho de banda, memoria y CPU, y por lo tanto, permiten la ejecución de las secuencias de navegación de manera más rápida y eficiente.

VIII. Referencias

[1] Hupp D., Miller R.C.: Smart Bookmarks: automatic retroactive macro recording on the web. In: Proceedings of the 20th Annual ACM Symposium on User Interface Software and Technology, pp. 81-90. ACM New York, Newport (2007)

[2] Pan A., Raposo J., Álvarez M., Hidalgo J., Viña A.: Semi automatic wrapper-generation for commercial web sources. In: IFIP WG8.1 Working Conference on Engineering Information Systems in the Internet Context, pp. 265-283. Kluwer, B.V. Deventer, Japan (2002)

[3] QEngine, http://www.adventnet.com/products/qengine/index.html

[4] Sahi, http://sahi.co.in/w/

[5] Selenium, http://seleniumhq.org/

[6] HtmlUnit, http://htmlunit.sourceforge.net/

[7] Kapow, http://www.openkapow.com

[8] Document Object Model (DOM). http://www.w3.org/DOM/

[9] Montoto P., Pan A., Raposo J., Bellas F, López J.: Automated browsing in AJAX websites. Data Knowl. Eng. 70(3), 269-283 (2011)

[10] XML Path Language (XPath), http://www.w3.org/TR/xpath

[11] Alexa, The Web Information Company. http://www.alexa.com

[12] Anupam V., Freire J., Kumar B., Lieuwen D., Automating web navigation with the WebVCR, Computer Networks 33(1-6), 503-517 (2000)

[13] Safonov A., Konstan J., Carlis J.: Beyond Hard-to-Reach Pages: Interactive, Parametric Web Macros. In: 7th Conference on Human Factors & the Web. Madison 2001

Discretización de la adaptación de rate para la mejora de la eficiencia energética en redes cableadas

J. Galán-Jiménez, A. Gazo-Cervero
Universidad de Extremadura
jaime@unex.es, agazo@unex.es

***Resumen*—Mejorar la eficiencia energética asociada al funcionamiento del equipamiento de red se ha convertido recientemente en un objetivo a lograr por parte de la comunidad investigadora. Uno de los puntos clave es que el equipamiento actual se encuentra restringido por las limitaciones impuestas por la tecnología. Por ello, los fabricantes necesitan de nuevos métodos que permitan que sus dispositivos presenten un menor consumo energético. Este artículo estudia el compromiso entre la cantidad de energía que es posible ahorrar en las redes cableadas y el número discreto de niveles de energía a implementar en las tarjetas de línea por parte de los fabricantes. Los resultados muestran que no es necesario fabricar tarjetas de línea que soporten un gran número de niveles de energía diferentes, ya que un número limitado como puede ser cuatro niveles de energía es suficiente para conseguir una reducción significativa en el consumo energético.**

***Index Terms*—Eficiencia energética, nivel de energía, distribución de energía, redes de área extensa.**

I. Introducción

En la actualidad se estima que el consumo asociado al equipamiento TIC (Tecnologías de la Información y las Comunicaciones) se encuentra entre un 2-10 % de la energía eléctrica mundial. Se estima que la infraestructura de redes de comunicaciones de los EEUU supone un consumo de entre 5 y 24 TWh/año [1], lo que se traduce en un coste anual de entre 0,5 y 2,4 billones de dólares. Además se prevé que en el año 2017 el consumo de energía de las redes de comunicaciones crecerá globalmente más de un 200 % [2]. En Europa, concretamente, se prevén valores en torno a 35,8 TWh en 2020 [3], mientras que en Japón, los routers consumirán el 9 % de la electricidad del país en 2015 [4].

Por otro lado, las TIC suponen alrededor de un 2-4 % de las emisiones de dióxido de carbono (CO_2) a nivel mundial [5]. De ese porcentaje, el 37 % proviene de las redes de comunicaciones y del equipamiento de red [6] y se estima que para el año 2020 se multiplique por dos si no se aplican iniciativas para la reducción del impacto ambiental. Sin embargo, para que la temperatura global del planeta no aumente más de un 2 % en dicho año, es necesario que el volumen de emisión de los gases de efecto invernadero se reduzca del 15 al 30 % [7]. Se trata, por tanto, de una crítica contradicción que la investigación tanto académica como industrial debe solucionar.

Afortunadamente, las TIC son una de las áreas más prometedoras en las que conseguir una reducción significativa del consumo de energía global. En concreto, existen oportunidades para conseguir una reducción considerable del consumo energético de las redes de comunicaciones [1], [8], [9]. A pesar de que el consumo del equipamiento de red ha recibido una mayor atención desde los inicios de la investigación en este ámbito, actualmente se está empezando a dedicar esfuerzo al hecho de reducir el consumo energético de Internet de forma global. En [9] se presenta una posible clasificación para categorizar los métodos que permiten ahorrar energía en redes de comunicaciones cableadas. Esta clasificación establece las tres siguientes áreas: 1) Diseño de red e Ingeniería de tráfico. 2) Diseño de sistemas y Optimización de componentes hardware. 3) Diseño de protocolos y Coordinación global.

Son varios los autores que se centran en el estudio de diferentes mecanismos de ahorro de energía basados en métodos que determinan el mínimo conjunto de recursos que han de ser utilizados para satisfacer una demanda de tráfico dada. Para ello, utilizan dos técnicas basadas en hardware: Sleeping (los componentes que no son necesarios pasan a dormir) y Rate Adaptation (los componentes se adaptan a las necesidades puntuales de la red). Además, se asume ampliamente en la literatura que los dispositivos hardware de red soportarán en el futuro características de ahorro de energía, mediante la posibilidad de disponer de una serie de interfaces que puedan operar a diferentes velocidades de envío [1], [10]. La unión de ambos aspectos genera la oportunidad de proponer mecanismos de ahorro energético en los que, mediante la adaptación de la velocidad de las tarjetas de línea a los requisitos de la red en cada instante, se consiga una significante reducción de la energía consumida por la misma.

Nuestro trabajo se centra en la actuación sobre los componentes hardware de la red, mediante la cual es posible conseguir un relevante ahorro energético en redes cableadas. Aunque las otras dos áreas de clasificación de [9] (diseño de red y diseño de protocolos) no son el foco de nuestro trabajo, si entendemos los mecanismos utilizados en la literatura para reducir el consumo energético en redes cableadas, podremos realizar propuestas de ahorro energético basadas en el diseño de los componentes de la red. De este modo, proponemos la utilización de un número limitado de niveles de energía para conseguir una reducción significativa del consumo energético en redes cableadas. Mediante simulaciones sobre escenarios de topologías de red reales, obtenemos el porcentaje de ahorro energético para distintas funciones de energía, asumiendo que los enlaces de la red pueden configurarse usando diferentes niveles de energía.

El resto del artículo está organizado como sigue: La Sección II describe brevemente los trabajos relacionados con el acometido en el presente documento. La Sección III define el proble-

ma que se desea resolver, mientras que las dos metodologías de ahorro de energía basadas en algoritmos bio-inspirados se presentan en las Secciones IV y V respectivamente. Los resultados experimentales obtenidos tras la realización de simulaciones sobre distintos escenarios son presentados en la Sección VI, para finalizar con la Sección VII de conclusiones.

II. Trabajos relacionados

La conciencia por el ahorro energético en las TIC se inicia en el diseño de las comunicaciones inalámbricas, con un punto de partida ligado a la aparición de los dispositivos móviles [11]. Los dispositivos móviles presentan capacidades de procesamiento limitadas y funcionan mediante baterías con un ciclo de trabajo pequeño en el que se suceden periodos cortos de tiempo a un rendimiento elevado y posteriores intervalos de inactividad continuada. De ahí que el consumo de la transmisión de datos a través de las redes inalámbricas sea menor que el consumo de la transmisión de datos en Internet [12].

Sin embargo, la actividad investigadora en términos de ahorro energético para redes cableadas es muy reciente. Además, los mecanismos existentes para la reducción del consumo energético en redes inalámbricas no son fácilmente extrapolables a las redes cableadas. Por ejemplo, aunque ciertos dispositivos del borde de las redes cableadas pueden utilizar el modo de operación anterior, la mayoría de ellos pueden presentar valores bajos de utilización media, de modo que se encuentren en un estado de completo reposo durante intervalos de tiempo muy cortos. Trabajos como los de [1], [13] indican que el consumo energético de dispositivos de red como tarjetas de línea se puede reducir al disminuir la velocidad a la que éstas trabajan. Esto se debe a que un dispositivo que trabaja a una menor frecuencia puede reducir su consumo energético por dos razones. Primeramente, un funcionamiento más lento hace que se consigan ahorros substanciales. La segunda razón hace referencia al hecho en el que trabajar a una menor frecuencia también permite el uso del escalado de voltaje dinámico (Dynamic Voltage Scaling, DVS) [14], [15], que permite reducir el voltaje de operación y, en consecuencia, la energía consumida por los dispositivos de red.

Nedevschi et al. tratan de buscar una zona de decisión con respecto a qué técnica basada en hardware (Sleeping o Rate Adaptation) utilizar en función de las características concretas de la red. Para ello, investigan la relación entre la velocidad de operación de los enlaces y su consumo energético para diferentes distribuciones de velocidades [1], entre las que se encuentran una distribución uniforme de velocidades (función de energía lineal) y una distribución exponencial (10 Gbps, 1 Gbps, 100 Mbps, 10 Mbps). Esta última aproximación la estudian al considerar que actualmente existe tecnología hardware para dar soporte a dichas velocidades (tecnología Ethernet). De los resultados se extrae que el tipo de distribución más apropiada para conseguir una mayor reducción en la velocidad de operación de los enlaces y, por consiguiente, un menor consumo energético, es una distribución de tipo uniforme. Además, indican que tanto Sleeping como Rate Adaptation son dos técnicas eficaces dependiendo principalmente del perfil energético del equipamiento de la red y de la utilización de la misma.

En un paso más, Vasic et al. realizan un estudio basado en [1] en el que comparan el ahorro energético en redes cableadas tras aplicar las técnicas Sleeping y Rate Adaptation en función del consumo base de los componentes de la red a nivel individual, es decir, en base a la cantidad de energía que es consumida por un elemento de la red sin tener en cuenta su velocidad de operación [10]. Para el caso en que el consumo base de los elementos de la red sea alto, interesa mantener el menor número de enlaces activos (Sleeping). Por el contrario, si el consumo base de los elementos de la red presenta valores pequeños, la técnica Rate Adaptation es la más apropiada. En este segundo caso, puesto que los autores se basan en los resultados de [1], también asumen y utilizan una distribución de velocidades uniforme en sus experimentos.

Por otro lado, los autores de [9] realizan diversos experimentos para medir el consumo energético de dos routers Cisco diferentes: GSR 12008 y 7507; ambos con sus sistemas base (chasis más procesador del router) y tarjetas de línea. Sin embargo, de los resultados obtenidos en este caso se puede extraer que la función de energía que describe el consumo de las tarjetas de línea de dichos routers toma valores discretos, de forma que podamos asumir su adaptación a una distribución de tipo logarítmico.

Rodgers, a su vez, utiliza un Intel 82579 Gigabit Ethernet PHY y obtiene los valores de consumo energético para enlaces de 100 Mbps y 1 Gbps [13]. En este caso, realiza mediciones para cada uno de los tres modos de operación en los que se pueden encontrar configurados los enlaces: Activo, Idle y LPI (Low Power Idle del estándar IEEE 802.3az). De los resultados obtenidos tras las mediciones, podemos extraer cuál es el consumo de un enlace cuando no porta tráfico alguno (LPI) en función de su consumo cuando está activo. Así pues, podemos asumir que el consumo de un enlace en modo LPI o Sleeping toma valores de entre un 5-10 % de su consumo cuando se encuentra en modo activo.

Una vez conocidos los trabajos y las distintas funciones de energía utilizadas en la literatura, podemos decir desde nuestro conocimiento que no existe ningún trabajo que trate de evaluar cuál es el número discreto de niveles de energía más apropiado para poder ser implementado en las tarjetas de línea, de forma que mediante la técnica Rate Adaptation se consiga un significativo ahorro de energía sin exigir demasiado al hardware al evitar utilizar un número de niveles elevado. En lugar de decantarnos por un tipo de función de energía concreto, nos centramos en comparar el ahorro de energía conseguido al utilizar distintas funciones de energía. Para ello, aplicamos los mecanismos de optimización propuestos en las siguientes secciones, que minimizan la energía consumida por la red siguiendo la filosofía de las técnicas basadas en hardware Sleeping y Rate Adaptation.

III. Configuración de red para el ahorro de energía

III-A. Definición del problema

Dada una infraestructura de red $G = (V, E, R)$ de nodos $v \in V$, conectados por un conjunto de enlaces unidireccionales

$e \in E$ asociados a un conjunto de niveles de energía $r \in R$ y una matriz de demanda de tráfico $M_{(i,j)}, \forall i,j \in V$ con una demanda de tráfico de $d_{(s,d)} \in M_{(i,j)}$ unidades desde el nodo origen $s \in V$ hasta el nodo destino $d \in V$, encontrar la configuración de red que minimice el consumo de energía requerido.

Un enlace dirigido desde el nodo $i \in V$ hacia el nodo $j \in V$ se denota por $e_{i \to j}$ y está asociado a un nivel de energía $r \in R$ durante un intervalo de tiempo T, que representa la velocidad configurada para la tarjeta de línea del enlace durante dicho intervalo. La función $powerL\left(e_{i \to j}, r, T\right)$ calcula el consumo de energía instantáneo en Vatios de la tarjeta de línea correspondiente al enlace dirigido $e_{i \to j}$, que se encuentra configurada con un nivel de energía $r \in R$ durante un intervalo de tiempo T. Finalmente, c_r hace referencia al consumo instantáneo de la tarjeta de línea correspondiente al enlace $e_{i \to j}$ durante un intervalo de tiempo T cuando se encuentra configurada con un nivel de energía r.

Así pues, se minimiza el consumo instantáneo de la red para un conjunto de intervalos de tiempo, de forma que todos juntos constituyen una secuencia que proporciona una completa cobertura sobre el ciclo diario. Por lo tanto, el consumo energético instantáneo IPC de una configuración de red $C \in G$ durante un intervalo de tiempo T viene determinado por el sumatorio del consumo energético instantáneo de cada tarjeta de línea activa (1), el cual depende del nivel de energía con el que éstas se encuentran configuradas (2):

$$\min IPC\left(C,T\right) = \sum_{e_{i \to j} \in E} powerL\left(e_{i \to j}, r, T\right) \qquad (1)$$

donde

$$powerL\left(e_{i \to j}, r, T\right) = c_r T, \forall e_{i \to j} \in E, \forall r \in R \qquad (2)$$

III-B. Definición de nivel de energía

Dada una función de energía $f(x)$, donde x corresponde a la velocidad de operación del enlace y $f(x)$ corresponde al consumo de energía para la velocidad x, consideramos nivel de energía al par $r = (x, f(x))$.

Un nivel de energía relaciona, por tanto, la velocidad de operación de un enlace con su consumo energético. El mínimo número de niveles de energía que un enlace puede soportar es uno: activo, que hace referencia a la capacidad nominal del enlace y su consumo de energía asociado. El método "Sleeping" [1] añade otro posible nivel de energía en el que el enlace no procesa ningún tipo de tráfico, de forma similar a un modo "Standby". Los enlaces que se encuentran en un nivel de energía "Sleeping" permiten ahorrar energía al no transportar paquetes de datos, aunque permanecen operativos para ser despertados si es necesario. En este modo operativo, los enlaces consumen un pequeño porcentaje de energía: entre el 5-10 % de su consumo si se encuentran configurados con el máximo nivel de energía [13]. Por otro lado, un enlace puede operar utilizando diferentes niveles de energía por medio del método basado en hardware Rate Adaptation [1]. Además, los autores de [10] indican que el hardware de red soportará probablemente en un futuro cercano características de ahorro de energía mediante la posibilidad de proporcionar un conjunto de interfaces que puedan operar a diferentes velocidades. La Tabla I muestra un ejemplo en el que un enlace puede soportar hasta cinco niveles de energía. De esta forma, en nuestra propuesta asumimos que un enlace puede soportar un número determinado de niveles de energía diferentes. Asumimos también asimetría para los enlaces, es decir, los dos arcos unidireccionales que constituyen un enlace bidireccional pueden estar configurados con distintos niveles de energía.

Tabla I
EJEMPLO DE NIVELES DE ENERGÍA SOPORTADOS POR UN ENLACE

Nivel de Energía	Velocidad de operación
0	Sleeping, "Dormido"
1	10 Mbps
2	100 Mbps
3	1 Gbps
4	10 Gbps

III-C. Definición de distribución de energía

Dado un número discreto de niveles de energía, n, definimos distribución de energía, l, a la sucesión de n niveles de energía, r_i, con los que pueden estar configurados los enlaces de la red. Se trata de una sucesión creciente de velocidades de operación que se encuentran asociadas a cada uno de los niveles de energía:

$$l = \left\{r_0, r_1, r_2, ..., r_{n-1}\right\}, \forall r_i < r_{i+1} \in R \qquad (3)$$

Si denotamos $rate_{max}$ a la mayor velocidad de operación soportada por los enlaces de la red, los valores de r_i para una distribución de energía lineal vienen dados por la siguiente ecuación:

$$r_i = \frac{i}{n-1} rate_{max} \qquad (4)$$

Por otro lado, si asumimos que:

$$rate_{max} = b^x, \forall rate_{max} > 0, \forall b > 0, b \neq 1, \forall x \in \mathbb{R} \qquad (5)$$

con b como base logarítmica y aplicamos la definición de logaritmo:

$$\log_b\left(rate_{max}\right) = x \Leftrightarrow rate_{max} = b^x \qquad (6)$$

determinamos que los valores de r_i para una distribución de energía logarítmica vienen dados por la siguiente ecuación:

$$r_i = \frac{rate_{max}}{b^{\left[x - \left(x \frac{i}{n-1}\right)\right]}} \qquad (7)$$

De este modo, si tenemos un número de niveles de energía igual a dos $(n = 2)$ y una distribución de energía lineal o logarítmica, los enlaces pueden estar dormidos u operando a la máxima velocidad, $rate_{max}$, es decir, el conjunto de posibles valores a tomar es $l = \{r_0, r_1\} = \{sleeping, rate_{max}\}$.

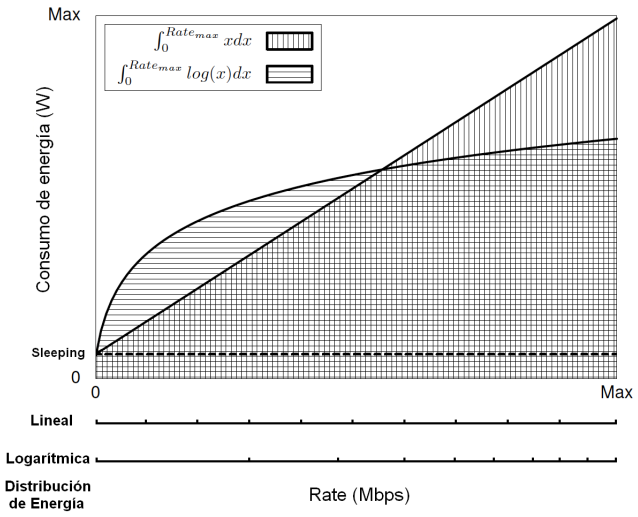


Fig. 1. Adaptación de áreas de las funciones de energía.

III-D. Caracterización de las funciones de energía

Para calcular el consumo de energía instantáneo de cada una de las tarjetas de línea asociadas a los enlaces activos, es necesario seleccionar una función de energía $f(x)$. Sin embargo, en lugar de centrarnos en una función de energía particular, comparamos los valores de ahorro de energía obtenidos al utilizar diferentes tipos de funciones de energía a través de un framework que nos permite su comparación por pares:

$$\int_0^{Rate_{max}} f_a(x)dx = \int_0^{Rate_{max}} f_b(x)dx \tag{8}$$

Para realizar esta comparación normalizada, las áreas delimitadas por las dos funciones de energía con respecto al eje de abscisas deben ser iguales (Fig. 1). Con el objetivo de obtener resultados consistentes, consideramos dos tipos de funciones de energía concretas: lineal ($f_a(x) = x$) y logarítmica ($f_b(x) = log(x)$). Una vez que se ha realizado este paso previo, podemos calcular el consumo instantáneo de las tarjetas de línea según la función de energía utilizada y aplicar los métodos de optimización basados en algoritmos bio-inspirados que se describen en las Secciones IV y V.

IV. Algoritmos genéticos para el cálculo de niveles de energía

Los tiempos de cálculo que son generalmente necesarios en los mecanismos de optimización de red son elevados [16], especialmente para redes muy grandes debido a su complejidad computacional. Afortunadamente, existen métodos que se apoyan en heurísticas para la resolución de este tipo de problemas dentro de un tiempo dado, limitando drásticamente el número de datos a utilizar, aunque para ello sacrifiquen la garantía de obtención de soluciones óptimas. En nuestro trabajo hemos optado inicialmente por utilizar los denominados algoritmos genéticos (GAs, Genetic Algorithms).

Los GAs son métodos adaptativos utilizados normalmente para dar solución a complejos problemas de optimización. Se basan en los mecanismos de la evolución natural, donde los individuos se reproducen y únicamente los más aptos sobreviven [17]. Están constituidos por un conjunto de soluciones potenciales o cromosomas (población) y una serie de operadores que se inspiran en la biología (selección, cruzamiento y mutación) [18]. Cada cromosoma tiene un valor de aptitud (fitness) que indica el grado de bondad con respecto a la solución que representa. Los operadores anteriormente mencionados son aplicados sobre la población para intentar conseguir mejores soluciones potenciales y crear nuevas generaciones. De acuerdo con la Teoría de la Evolución, únicamente aquéllos individuos de la población que mejor se adaptan al entorno en el que viven tienden a sobrevivir, al transmitir su superior información genética a las nuevas generaciones [17].

El problema de optimización descrito en la Sección III es un problema MCMF (MultiCommodity Maximum Flow) perteneciente a la clase de problemas NP-hard [16]. Para resolverlo, utilizamos un GA con el objetivo de encontrar configuraciones de red casi óptimas que minimicen la energía consumida en función de la demanda de tráfico entre cada par origen-destino. El objetivo principal es, por tanto, minimizar el conjunto de recursos de la red que deben estar activos para satisfacer una demanda de tráfico dada. Estos recursos pasarán a un nivel de energía inferior cuando no sea necesario que continúen operando en su "alto nivel de energía". Esto implica que algunos enlaces pasen a estar más cargados para que otros cambien su modo de operación y consigan ahorrar energía. Los recursos de la red que pueden "dormirse" o pasar a un menor nivel de energía son tanto los routers como los enlaces (tarjetas de línea) [1], [9], [10], [16].

IV-A. Codificación del cromosoma

Un cromosoma, c, está constituido por una sucesión de valores (genes, g_i) que representan la velocidad de operación de los niveles de energía asociados a cada uno de los enlaces unidireccionales de la red durante un intervalo de tiempo dado:

$$c = \{g_0, g_1, g_2, ..., g_N\}, \forall g_i \in [0, 1] \in \mathbb{R} \tag{9}$$

Los valores que pueden tomar los genes se corresponden con el eje de abscisas de las funciones de energía utilizadas en nuestra propuesta (Fig. 1, Sección III-D), de forma que para cada valor en dicho intervalo cerrado (velocidad de operación) existe un valor en el eje de ordenadas que hace referencia al correspondiente consumo instantáneo. Cada cromosoma representa, por tanto, una configuración de red con su conjunto de enlaces, los cuales están configurados con una velocidad de operación concreta durante un intervalo de tiempo determinado. Para determinar si la configuración de red codificada por un cromosoma satisface la correspondiente demanda de tráfico durante dicho intervalo, se utiliza el algoritmo de encaminamiento del camino más corto (SPF, Shortest Path-First). Cada demanda de tráfico desde cada nodo origen hacia cada nodo destino debe ser encaminada de forma correcta por la configuración de red en cuestión para que su cromosoma asociado pueda ser considerado como una solución por parte del GA. De esta forma, si la configuración de red es capaz de encaminar el tráfico con la restricción de

no superar la capacidad efectiva de cada enlace unidireccional, el cromosoma en cuestión se convierte en una solución para dicho intervalo de tiempo. Si por el contrario la configuración de red no puede satisfacer la demanda de tráfico, esta solución potencial no es válida y no puede ser evaluada por la función de fitness. Este tipo de soluciones no válidas son descartadas por el GA. El algoritmo utilizado para esta comprobación de viabilidad de soluciones presenta una complejidad algorítmica $O(n^4)$ para cada cromosoma evaluado por el GA.

IV-B. Función de fitness

Una vez que se ha obtenido una solución, es decir, una configuración de red válida, evaluamos su calidad a través de la función de fitness para determinar la "bondad" del cromosoma. Puesto que lo que finalmente se pretende obtener es la configuración de red válida que presente un menor consumo de energía para un intervalo de tiempo concreto, debemos encontrar un compromiso entre minimizar el número de enlaces activos y activar aquellos enlaces con un consumo menor. En definitiva, el cromosoma que presente un mejor fitness será aquél que incluya genes con valores más cercanos a 0 que a 1, además de satisfacer los requisitos de demanda de tráfico y capacidad efectiva de cada uno de los enlaces de la red. La función de fitness utilizada para evaluar un determinado cromosoma durante un intervalo de tiempo concreto viene dada por la Ec. (1), descrita en la Sección III-A, que calcula el consumo de energía instantáneo de la configuración de red para dicho intervalo.

El GA realiza una serie de iteraciones mediante la aplicación de los dos operadores genéticos básicos: cruzamiento y mutación. De este modo, evalúa las soluciones obtenidas y trata de encontrar otras mejores mediante la minimización del valor obtenido por la función de fitness. Este proceso se repite para un número de iteraciones (generaciones) previamente definido o hasta que se cumpla la condición de terminación.

V. Optimización por enjambre de partículas para el cálculo de niveles de energía

Con el objetivo de comparar el rendimiento obtenido al aplicar distintos algoritmos bio-inspirados sobre el problema de ahorro de energía en las redes de comunicaciones cableadas, decidimos utilizar también la optimización por enjambre de partículas (PSO, Particle Swarm Optimization). PSO es otra forma de computación basada en la biología inicialmente inspirada en el comportamiento de las bandadas de pájaros y los bancos de peces, con una naturaleza estocástica parecida a los GAs [19]. El principal objetivo es imitar el proceso de comunicación natural y de conocimiento individual dentro de un grupo, donde la opinión de un individuo del grupo tiende a converger hacia la opinión del propio grupo.

Más formalmente, PSO es una metaheurística basada en población que utiliza un conjunto de soluciones potenciales para resolver un problema de optimización concreto. La población está constituida por un conjunto de partículas (soluciones potenciales) que vuelan sobre un espacio de búsqueda multidimensional. La agregación de estas partículas en cada iteración del algoritmo constituye el enjambre. Cada partícula del enjambre representa un punto en el espacio de búsqueda del problema y tiene asociado un valor de fitness. El principal objetivo es, por tanto, explorar este espacio de búsqueda de forma eficiente y esto se consigue gracias al movimiento del enjambre hacia la mejor solución encontrada en las iteraciones anteriores. A lo largo del proceso se van obteniendo soluciones potenciales (mejor valor de fitness) para converger finalmente en una solución con un error mínimo. Para ello, cada partícula conoce la mejor posición que ha encontrado $(localbest, p_i)$ y la mejor posición que el resto de partículas del enjambre han encontrado $(globalbest, G)$ desde el inicio del algoritmo. La velocidad de la partícula, v_i, y su posición, x_i, se actualizan en cada iteración (tiempo $k+1$) a través de las Ec. (10) y (11), en las que α_1 y α_2 son constantes de aceleración. La primera constante asocia la propia experiencia de la partícula con su posición actual, mientras que la segunda hace referencia a la interacción social entre las partículas del vecindario. La función de inercia se representa por φ, mientras que γ_{1i} y γ_{2i} son números aleatorios distribuidos uniformemente entre 0 y 1 que se aplican a la partícula i-ésima.

$$v_i(k+1) = \varphi(k)v_i(k)+\alpha_1[\gamma_{1i}(p_i-x_i(k))]+\alpha_2[\gamma_{2i}(G-x_i(k))] \quad (10)$$

$$x_i(k+1) = x_i(k) + v_i(k+1) \quad (11)$$

En esta ocasión, el objetivo es el mismo que el perseguido al utilizar los GAs de la Sección IV: encontrar configuraciones de red casi óptimas que minimicen la energía consumida en función de la demanda de tráfico entre cada par origen-destino. Para este propósito, pasamos a explicar la aplicación de PSO para resolver el problema descrito en la Sección III, mediante la descripción de la codificación de las partículas que conforman el enjambre y el modo de operación de la función de fitness.

V-A. Codificación de las partículas

Una topología de red compuesta por n enlaces unidireccionales se representa por un espacio de búsqueda n-dimensional donde el enjambre de partículas se mueve hacia la solución a encontrar. Una partícula, i, está constituida por una sucesión de n valores (D_j), uno por cada dimensión, que representan la velocidad de operación de los niveles de energía asociados a cada uno de los enlaces unidireccionales de la red durante un intervalo de tiempo dado:

$$i = \{D_0, D_1, D_2, ..., D_n\}, \forall D_j \in [0,1] \in \mathbb{R} \quad (12)$$

De hecho, una partícula (PSO) es equivalente a un cromosoma (GA) en nuestra propuesta: ambos elementos representan una configuración de red concreta durante un intervalo de tiempo determinado. Los genes de los cromosomas en GA son ahora concebidos como valores de las dimensiones del espacio de búsqueda en PSO. Tal es así, que las partículas pueden representar configuraciones de red con enlaces que soporten un número finito o infinito de niveles de energía, de forma similar a lo descrito en la Sección IV para GAs.

Tabla II
CARACTERÍSTICAS DE LOS ENLACES DE LAS TRES TOPOLOGÍAS

Topología	Velocidad de operación	Enlaces
Géant	10 Gbps	32
	2,4 Gbps	34
	155 Mbps	8
NSFNet	155 Mbps	42
AT&T	9,6 Gbps	10
	2,5 Gbps	90
	622 Mbps	261
	45 Mbps	6

V-B. *Función de fitness*

Con el objetivo de determinar si la configuración de red representada por una partícula satisface la correspondiente demanda de tráfico para un intervalo de tiempo concreto, se utiliza de nuevo el algoritmo de encaminamiento SPF. Si la configuración de red es capaz de encaminar el tráfico con la restricción de no exceder la capacidad efectiva de ningún enlace unidireccional, la partícula asociada se convierte en solución. Del mismo modo que en GAs, el algoritmo utilizado para esta comprobación de viabilidad de soluciones presenta una complejidad algorítmica $O(n^4)$ para cada partícula evaluada. PSO lleva a cabo una serie de iteraciones para encontrar la mejor solución dentro del espacio de búsqueda multidimensional al aplicar la misma función de fitness que la utilizada en GAs (Ec. (1) de la Sección III-A). Esta función de fitness calcula el consumo de energía instantáneo de la configuración de red representada por la partícula en cuestión durante un intervalo de tiempo concreto. Una vez encontrada la mejor solución para el intervalo de tiempo actual, se repite el proceso para todos los intervalos de tiempo del ciclo diario, con el propósito de obtener las configuraciones de red más apropiadas en términos de ahorro de energía a lo largo del día.

VI. RESULTADOS EXPERIMENTALES

Para evaluar nuestra propuesta hemos utilizado un conjunto de datos correspondientes a una serie de matrices de tráfico para las redes Géant, NSFNet y AT&T. La Tabla II muestra la distribución de enlaces para cada una de las topologías utilizadas. Con respecto a la carga de tráfico, se han usado matrices de tráfico reales tomadas a intervalos de 15 minutos durante cuatro meses consecutivos de observación para Géant. Por otro lado, se ha aplicado una carga sintética sobre NSFNet y AT&T que está basada en la función sinusoidal para la generación de tráfico utilizada en [16], con intervalos de tiempo tomados cada 5 minutos. La Fig. 2 muestra el porcentaje de carga de tráfico diario para cada topología. Se puede observar que existe una considerable variación que distingue la componente diurna de la nocturna, patrón que se repite día tras día.

Asumiendo el consumo de energía del equipamiento de red de [9], los escenarios están constituidos por un conjunto de routers Cisco 7507 conectados entre sí por una serie de enlaces unidireccionales configurados en un nivel de energía concreto. Estos enlaces unidireccionales pueden cambiar de nivel de energía de forma independiente para adaptar su velocidad de operación a la carga de la red. El consumo de energía de un

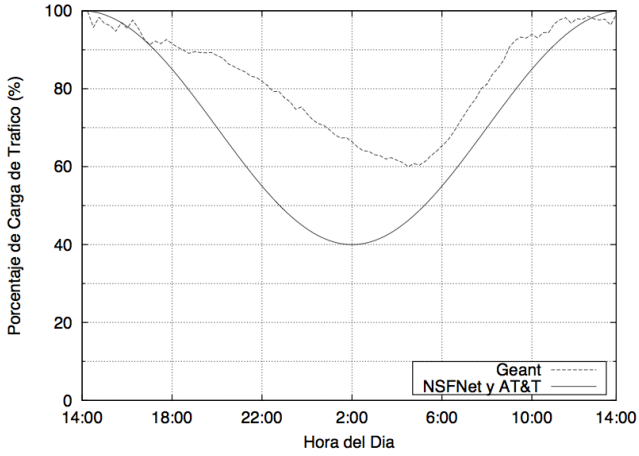


Fig. 2. Carga de tráfico agregada a lo largo del ciclo diario para las tres topologías.

enlace se calcula en función del nivel de energía en el que se encuentre configurado y de la función de energía utilizada (lineal o logarítmica). Con el objetivo de conocer el impacto que supone el hecho de utilizar enlaces que dispongan de la posibilidad de operar según diferentes niveles de energía, ejecutamos varias veces ambos métodos bio-inspirados utilizando distinto número de niveles de energía, n, y siguiendo una distribución de energía determinada. Además, comparamos los resultados obtenidos con el caso en el que suponemos un número infinito de niveles de energía $(n = \infty)$, es decir, el caso en el que los enlaces se pueden configurar con el nivel de energía más apropiado. En este caso ideal, la red consumiría la menor cantidad de energía posible.

Para calcular intervalos de confianza y realizar un análisis estadístico completo, se han realizado 50 ejecuciones independientes para cada tupla del tipo (T, DE, FE, CA) con T: Topología, DE: Distribución de Energía, FE: Función de Energía, CA: Configuración del Algoritmo. La Fig. 3 muestra un gráfico acumulativo que relaciona el número de niveles de energía utilizados, n, y el porcentaje de ahorro de energía logrado por las distintas combinaciones de tuplas. Los resultados indican que el porcentaje de ahorro de energía para 2, 3 y 4 niveles de energía crece de manera cuasi-uniforme para cada caso. También se puede comprobar que si se utilizan más de 4 niveles de energía se obtiene una mejora mínima en términos de ahorro de energía.

Para confirmar estadísticamente esta observación, se ha realizado un análisis multivariante para ambos algoritmos de forma que podamos conocer el impacto de cada variable independiente: grado de conectividad, distribución de energía, función de energía y número de niveles de energía sobre la variable dependiente: ahorro de energía. La Tabla III recoge los resultados obtenidos para la regresión de Mínimos Cuadrados Ordinarios (MCO) realizada, que presenta un R^2 de 0,944. Todas las variables independientes del análisis son categóricas excepto el grado de conectividad, que es continuo. Los coeficientes no estandarizados (columna B) indican que un incremento en una unidad en el grado de conectividad está asociado de forma significativa con un incremento de más del

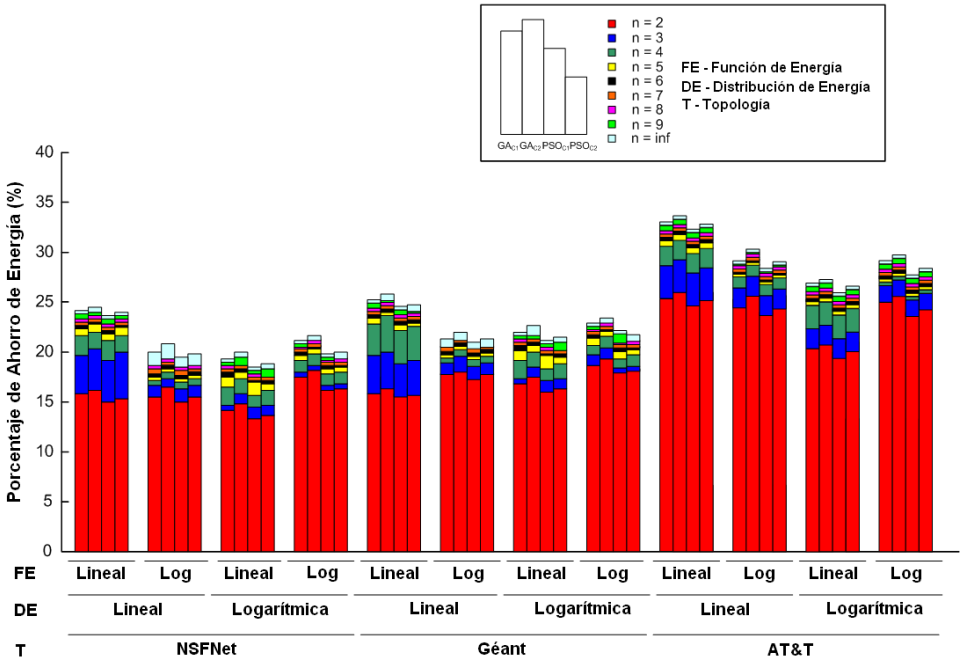


Fig. 3. Porcentaje de ahorro de energía en función del número de niveles de energía.

Tabla III
COEFICIENTES[A]

Modelo	Tipo de Variable	Coefs. no Estandarizados		Coefs. Estand.	t	Sig.
		B	Error Est.	Beta		
1 (Constante)		-22,283	2,303		-9,677	0,000
GradoConectividad	Continua	7,387	0,735	0,121	10,045	0,000
DistribuciónEnergíaLog	Categórica	-0,843	0,160	-0,064	-5,286	0,000
FunciónEnergíaLog	Categórica	-0,514	0,160	-0,039	-3,224	0,001
NivelesEnergía2	Categórica	16,969	0,357	0,768	47,556	0,000
NivelesEnergía3	Categórica	18,701	0,357	0,846	52,409	0,000
NivelesEnergía4	Categórica	20,201	0,357	0,914	56,611	0,000
NivelesEnergía5	Categórica	20,684	0,357	0,936	57,965	0,000
NivelesEnergía6	Categórica	21,030	0,357	0,951	58,936	0,000
NivelesEnergía7	Categórica	21,458	0,357	0,971	60,136	0,000
NivelesEnergía8	Categórica	21,692	0,357	0,981	60,790	0,000
NivelesEnergía9	Categórica	21,886	0,357	0,990	61,336	0,000
NivelesEnergíaInf	Categórica	22,664	0,357	1,025	63,515	0,000

[A] Variable Dependiente: AhorroEnergía
Variables de Referencia: DistribuciónEnergíaLineal, FunciónEnergíaLineal, NivelesEnergía1

7 % en el ahorro de energía. Este valor supone una relación directamente proporcional entre el grado de conectividad y la cantidad de ahorro de energía, es decir, a mayor grado de conectividad, mayor ahorro de energía respecto al consumo de energía global de la red. Además, tanto la distribución de energía logarítmica como la función de energía logarítmica tienen una influencia pequeña y negativa, aunque estadísticamente significativa, sobre los valores de ahorro de energía con respecto a la distribución de energía y función de energía lineales.

Se puede observar también el porcentaje de ahorro de energía obtenido por nuestra propuesta cuando se utiliza un número determinado de niveles de energía. Estos valores son comparados con el caso en el que no se utilizan mecanismos de ahorro energético por parte de la red, es decir, el caso en el que únicamente existe un solo nivel de energía (enlace 100 % activo). Así, el uso de dos niveles de energía supone alrededor del 17 % de ahorro con respecto a la situación en la que no se utilizan técnicas de ahorro de energía. Además, se puede observar que las mayores mejoras en términos de ahorro entre dos niveles adyacentes se logran cuando el número es inferior a 4. Por ello, podemos afirmar que el incremento de niveles de energía por encima de este número no supone grandes beneficios con respecto a la reducción del consumo energético de la red.

Con el objetivo de conocer el impacto que produce el valor del criterio de parada (número de generaciones en GA y número máximo de iteraciones en PSO) y el tamaño de la

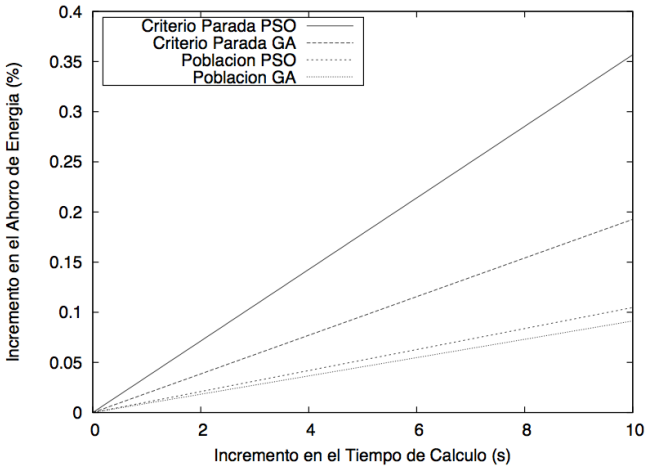


Fig. 4. Compromiso ahorro de energía-tiempo de cálculo para ambos algoritmos bio-inspirados.

población sobre el ahorro de energía y el tiempo de cálculo en ambos algoritmos, se ha realizado un segundo análisis multivariante. La Fig. 4 muestra la influencia de las dos variables independientes a comparar (criterio de parada y población) sobre las variables dependientes (ahorro de energía y tiempo de cálculo) para ambos algoritmos bio-inspirados. Es deseable que las cuatro líneas sean lo más verticales posibles, ya que, en ese caso, el ahorro de energía aumentaría en gran medida mientras que únicamente se emplearía un tiempo mínimo para conseguirlo. En nuestro caso, el hecho de incrementar el valor del criterio de parada en ambos algoritmos es más interesante que incrementar el tamaño de la población desde el punto de vista del compromiso ahorro de energía-tiempo de cálculo. Además, PSO proporciona mejores resultados que GA para dicho compromiso, mientras que si únicamente consideramos la cantidad de energía ahorrada, GA presenta los mejores resultados.

VII. Conclusiones

En este artículo se propone la utilización de un número limitado de niveles de energía para conseguir una reducción significativa del consumo energético de las redes cableadas. Para ello, se han utilizado los denominados algoritmos bio-inspirados y un conjunto de topologías de red reales tales como NSFNet, Géant y AT&T. Los experimentos realizados se basan en simulaciones donde los enlaces pueden configurarse según distintos niveles de energía y en las que se utilizan diversos tipos de funciones de energía. Los resultados demuestran que se puede mejorar en gran medida la eficiencia energética de una red mediante la utilización de un reducido número de niveles de energía. Concretamente, no es necesario que los fabricantes construyan tarjetas de línea que soporten un gran número de niveles de energía diferentes, ya que un número igual a 4 es suficiente para lograr una reducción significativa del consumo de energía. Por otro lado, si no es posible utilizar el método Rate Adaptation, se podría usar el método denominado Sleeping dependiendo del perfil energético de la red. Los resultados indican también que a mayor grado de conectividad se consigue un mayor ahorro de energía respecto del consumo global de la red. Finalmente, ni el tipo de distribución de energía ni el tipo de función de energía tienen un gran impacto en términos de ahorro energético.

Agradecimientos

Este trabajo ha sido financiado en parte por la Consejería de Empleo, Empresa e Innovación del Gobierno de Extremadura y el Fondo Social Europeo (PRE09184 y GRU10116).

Referencias

[1] S. Nedevschi, L. Popa, G. Iannaccone, S. Ratnasamy, D. Wetherall, "Reducing Network Energy Consumption via Sleeping and Rate-Adaptation", USENIX NSDI 2008, pp. 323-336, San Francisco (EEUU), 16-18 Abril, 2008.

[2] Y. Zhang, P. Chowdhury, M. Tornatore, B. Mukherjee, "Energy Efficiency in Telecom Optical Networks", IEEE Communications Surveys & Tutorials, vol. 12, n. 4, pp. 441-458, 2008.

[3] Global e-Sustainibility Initiative (GeSI), "SMART 2020: Enabling the low carbon economy in the information age". http://www.smart2020.org/_assets/files/02_Smart2020Report.pdf. Último Acceso: 19 Septiembre 2013.

[4] M. Nakamura, "Advanced photonic technologies for the information era", Nature Photonics Technology Conference 2007, Tokio (Japón), 23-25 Oct. 2007.

[5] M. Pickavet et al., "Worldwide Energy Needs for ICT: The Rise of Power-Aware Networking", 2nd International Symposium on Advanced Networks and Telecommunication Systems, pp. 1-3, Mumbai (India), 15-17 Dic. 2008.

[6] J. Mankoff, R. Kravets, E. Blevis, "Some Computer Science Issues in Creating a Sustainable World", IEEE Computer, vol. 41, n. 8, pp. 102-105, 2008.

[7] D. Pamlin, K. Szomolányi, "Saving the Climate @ the Speed of Light-First Roadmap for Reduced CO2 Emissions in the EU and Beyond", World Wildlife Fund and European Telecommunications Network Operators' Association, Abril 2007.

[8] IEEE P802.3az Energy Efficient Ethernet Task Force. http://www.ieee802.org/3/az. Último Acceso: 19 Septiembre 2013.

[9] J. Chabarek, J. Sommers, P. Barford, C. Estan, D. Tsiang, S. Wright, "Power Awareness in Network Design and Routing", IEEE INFOCOM 2008, pp. 457-465, Phoenix (EEUU), 13-18 Abril, 2008.

[10] N. Vasic, D. Kostic, "Energy-Aware Traffic Engineering", e-Energy 2010, pp. 169-178, Passau (Alemania), 13-15 Abril, 2010.

[11] Y. Agarwal, R. Chandra, A. Wolman, P. Bahl, K. Chin, R. Gupta, "Wireless Wakeups Revisited: Energy Management for VoIP over Wi-Fi Smartphones", ACM MobiSys 2007, pp. 179-191, San Juan (Puerto Rico), 11-14 Junio, 2007.

[12] M. Gupta, S. Singh, "Greening of the Internet", ACM SIGCOMM 2003, pp. 19-26, Karlsruhe (Alemania), 25-29 Agosto, 2003.

[13] J. Rodgers, "Energy Efficient Ethernet: Technology, Application and Why You Should Care". http://intel.ly/LNffEP. Último Acceso: 19 Septiembre 2013.

[14] B. Zhai, D. Blaauw, D. Sylvester, K. Flautner, "Theoretical and Practical Limits of Dynamic Voltage Scaling", DAC 2004, pp. 868-873, San Diego (EEUU), 7-11 Junio, 2004.

[15] M. Weiser, B. Welch, A. Demers, S. Shenker, "Scheduling for Reduced CPU Energy", USENIX OSDI 1994, pp. 13-23, Monterey (EEUU), 14-17 Nov. 1994.

[16] L. Chiaraviglio, M. Mellia, F. Neri, "Energy-Aware Backbone Networks: A Case Study", IEEE ICC Workshops 2009, pp. 1-5, Dresden (Alemania), 14-18 Junio, 2009.

[17] C. Darwin, "On the Origin of Species by Means of Natural Selection", John Murray, Londres (1859).

[18] D.E. Goldberg, "Genetic Algorithms in Search, Optimization and Machine Learning", Addison-Wesley, Reading, MA (1989).

[19] J. Kennedy, R. Eberhart, "Particle Swarm Optimization", IEEE International Conference on Neural Networks 1995, pp. 1942-1948, Perth (Australia), 27 Nov. - 1. Dic. 1995.

Análisis del impacto de la configuración de un dispositivo 802.11g sobre su consumo energético.

A. Bravo-Vicente, J. Galán-Jiménez y A. Gazo-Cervero.
Universidad de Extremadura.
Avda. de la Universidad s/n, 10003, Cáceres, España.
abelbv@unex.es, jaime@unex.es, agazo@unex.es.

***Resumen*—Debido al auge de las comunicaciones inalámbricas, reducir su consumo se ha transformado en un punto clave de estudio. Este artículo analiza la influencia de la configuración de un dispositivo inalámbrico en su consumo energético. Para ello se estudian cinco parámetros operacionales en un dispositivo WiFi: dos parámetros de configuración de la conexión de red (tamaño de datagrama y velocidad de transmisión de datos), controlador de dispositivo, Power Save Mode (PSM) y potencia de señal. Este análisis determina la influencia de cada uno de los parámetros en la energía consumida, analizando qué valores favorecen el ahorro. Los resultados indican que la correcta configuración del dispositivo puede suponer un ahorro de hasta un 83% sobre su consumo energético.**

***Palabras Clave*—Ahorro energético, configuración de dispositivo, 802.11g, tamaño de datagrama, velocidad de transmisión, PSM, potencia de señal, controlador de dispositivo.**

I. INTRODUCCIÓN

En los últimos años se viene observando un incremento en la popularidad de las redes inalámbricas de área local (Wireless Local Area Network, WLAN). Se estima que en 2017 siete mil millones de personas alrededor del mundo utilizarán siete trillones de dispositivos móviles [1]. Evidentemente, un incremento en el número de dispositivos supondrá una mayor demanda energética.

Hasta un 10% del consumo energético de un ordenador portátil es producido por el interfaz de red inalámbrico [2]. Además, recientes estudios han demostrado que en torno a un 50% de la energía consumida por equipamiento TIC (Tecnologías de la Información y la Comunicación) se produce en redes inalámbricas [3], [4]. Por tanto, optimizando el consumo energético en dispositivos WLAN se podría reducir significativamente la huella de carbono [5].

En este artículo se han analizado diversas variables involucradas en el rendimiento energético de un dispositivo USB WiFi con el objetivo de determinar la influencia de cada una de ellas sobre el valor de energía consumida.

Se ha desarrollado una metodología de medida que permitiese determinar los parámetros modificables que afectan al consumo energético del dispositivo bus universal en serie (USB). Mediante análisis estadístico se ha estudiado la influencia de cada uno de los parámetros en el valor de energía consumida y se han determinado los intervalos de confianza para cada valor obtenido.

Se ha estudiado cómo afecta la variación de cinco parámetros operacionales, los cuales son fácilmente modificables en cualquier dispositivo de este tipo: tamaño de datagrama, velocidad de transmisión de datos, controlador del dispositivo, Power Save Mode (PSM) y potencia de la señal emitida por el dispositivo.

El resto del artículo se organiza como sigue: en la sección II se estudian los trabajos existentes en la literatura relacionados con la investigación realizada. En la sección III se exponen los objetivos, la sección IV describe la metodología propuesta para la realización de las distintas pruebas de obtención de resultados de consumo energético expuestas en la sección V y, finalmente, las conclusiones se reflejan en la sección VI.

II. TRABAJOS RELACIONADOS

El interés que despierta el estudio del consumo energético en dispositivos inalámbricos crece año tras año. En este sentido los trabajos pretenden ayudar a crear modelos de consumo energético que puedan ser utilizados para la mejora de protocolos y algoritmos en WLANs de modo que su eficiencia energética se vea incrementada. Todos los estudios que se presentan a continuación, igual que el desarrollado en este artículo, intentan dar algún tipo de solución a esta problemática.

En [6] los autores estudian la relación existente entre tráfico de red y consumo energético en el estándar IEEE 802.11. Presentan una caracterización de la potencia consumida en dispositivos WiFi en términos de tráfico enviado y recibido, modulación, codificación utilizada y tamaño de los datagramas. El escenario desarrollado para la realización de las diversas mediciones se compone de un Punto de Acceso (AP) 802.11, un ordenador portátil y un dispositivo de medición energética.

Los autores de [7] presentan el resultado obtenido de analizar el consumo energético de una tarjeta PCMCIA basada en el estándar 802.11b. Se analizan tres modos operacionales: envío, recepción y reposo, variando para cada uno de ellos tres parámetros: tamaño de datagrama, velocidad de transmisión de datos y potencia de la señal de radiofrecuencia. Las mediciones se realizan haciendo uso del modo ad-hoc entre dos equipos. Tras la realización de las mediciones, los autores proponen que no se utilice la opción de fragmentación de paquetes, que la velocidad de transmisión de datos sea tan alta como sea posible y que la potencia de la señal sea configurada al nivel más bajo para conseguir un mayor ahorro energético.

En el estudio presentado por Mahadevan et al. [8] se evalúa el consumo energético en una gran variedad de dispositivos de red como hubs, switches, routers y WiFi APs, con el objetivo de desarrollar un modelo de consumo energético de los mismos. Además, elaboran una comparativa con datos de consumo energético para una gran cantidad de configuraciones comunes a cualquier switch o router. En dicha comparativa se observa cómo el consumo en miliwatios / velocidad de transmisión máxima en Mbps presenta grandes variaciones en

función del dispositivo analizado. Por ejemplo, el consumo energético de un AP WiFi es 11,21 órdenes de magnitud superior al de un switch de núcleo de la red, o 12,77 órdenes de magnitud superior en el caso de un switch de borde.

Tomando como punto de partida los trabajos expuestos en los anteriores párrafos, se ha desarrollado el estudio que se presenta en este artículo. Para su realización se ha utilizado un dispositivo 802.11g, ya que permiten una mayor velocidad de transmisión con respecto a anteriores estándares. Además de realizar un análisis de la influencia de la velocidad de transmisión, del tamaño de datagrama y de la potencia de la señal de radiofrecuencia, similar a los casos anteriormente citados, se estudia la efectividad de PSM y la influencia del controlador de dispositivo en el valor de consumo energético. Para garantizar la fiabilidad de los resultados, se realizó un análisis estadístico multivariante de forma que podamos conocer el impacto de cada una de las variables estudiadas en el valor de ahorro energético obtenido.

El modo de ahorro energético PSM ha demostrado su eficiencia transmitiendo a tasas de transferencia no muy elevadas, por lo que este será un factor determinante a la hora de decidir si se usa o no este mecanismo.

La cantidad de información transmitida y la velocidad de la misma serán factores cruciales a la hora de seleccionar la configuración de los parámetros operacionales estudiados que favorezcan el ahorro energético.

III. OBJETIVO

Este estudio se realiza con el objetivo de analizar y determinar cómo la configuración de varios parámetros influyen en el consumo energético de un dispositivo WiFi, el cual se conecta por USB a un ordenador personal.

Para esto se han definido cinco parámetros operacionales del enlace inalámbrico sobre los cuales versará el estudio. Se utilizará el siguiente orden a lo largo de todo el artículo:

1) Tamaño de datagrama (L).
2) Velocidad de transmisión (B).
3) Controlador de dispositivo inalámbrico (D).
4) PSM implementado en el estándar 802.11 [9].
5) Potencia de la señal transmitida (P).

Se estudió cómo afecta la variación de cada uno de los parámetros anteriores en el consumo energético. De este modo fue posible concluir qué valores han supuesto decrementos e incrementos en el gasto energético del dispositivo USB WiFi. Una vez analizado este comportamiento se podrá determinar qué configuraciones ejercen una influencia directa sobre el consumo energético y por lo tanto permiten el mayor ahorro de energía en función de los requerimientos.

IV. METODOLOGÍA DE MEDIDA

A. Testbed para la realización de los experimentos

Se ha desarrollado un escenario para el llevar a cabo los diversos experimentos (Figura 1), para facilitar su comprensión a la hora de mencionar a los elementos se indica la letra o número que lo referencia en dicha figura. Compuesto por un AP 802.11g (E), dos ordenadores portátiles utilizados para establecer una comunicación entre ambos (B) y (C). El Equipo 2 (C) ha enviado / recibido tráfico a través del Switch (D) el cual se conecta al AP (E) gracias a un cable de red. Será el AP (E) el encargado de enviar datos de forma inalámbrica al dispositivo USB WiFi conectado al Equipo 1 (B). Las mediciones de consumo energético se han realizado sobre el dispositivo USB WiFi.

La obtención de datos de consumo energético se han realizado usando un multímetro modelo PCE DM22 (A), con puerto serie RS-232 (3) mediante el cual se obtuvieron los valores de consumo energético medidos para su posterior tratamiento. Estas mediciones son transferidas directamente al Equipo 1 (B).

Para medir el consumo energético directamente de los pines del puerto USB, se desarrolló un cable de conexión que conecta el dispositivo USB WiFi (F) con el multímetro (A). Dicho cable permitirá obtener resultados de mediciones instantáneas sin que se pierda conectividad entre el dispositivo USB WiFi (F) y el equipo. El cable a su vez está conectado a una fuente de 5V que proporciona energía al dispositivo, éste no utiliza la alimentación del puerto USB de modo que se consigue estabilizar la corriente que llega al dispositivo USB.

Para procesar la información suministrada por el multímetro (A), se ha desarrollado una aplicación. Servirá para conocer la información enviada, recibida, controlar la sincronización entre dos computadores. Ademas de realizar cálculos para determinar valores de consumo energético y su posterior almacenamiento.

El Equipo (B) ejecuta una aplicación desarrollada en lenguaje Java compuesta por diversos módulos. A continuación se listan dichos módulos. La numeración que se expone a continuación se corresponde con la representada en la Figura 1. Las líneas que indican flujos de datos entre los distintos módulos están representadas por líneas discontinuas. El sentido de los flujos de datos se refleja mediante flechas.

- **(1)** Escrito en lenguaje Shell y su cometido es configurar la velocidad tanto el punto de acceso como en el dispositivo USB.
- **(2)** Clase Java que se encarga de realizar conexiones ssh de forma automática entre los equipos 1 y 2. Esta conexión es necesaria para el envío de comandos de un equipo a otro y para el cierre de la conexión.
- **(3)** Clase Java encargada de la comunicación con el puerto serie RS-232, obtención de los datos suministrados a través de dicho puerto y almacenamiento en formato CSV para su posterior tratamiento estadístico.
- **(4)** Desarrollado en lenguajes AWK y Shell. Genera un archivo que contiene datos acerca de la información transmitida/recibida para el posterior análisis estadístico.
- **(5)** Externo a la aplicación Java, en este caso han sido desarrollado en Phyton y lenguaje estadístico R, su función será generar las diversas gráficas y datos estadísticos que componen el estudio.

B. Metodología

Se debe analizar y controlar tanto el tráfico de la conexión inalámbrica establecida como el consumo energético del dispositivo, de modo se pueda concluir cuál es el consumo del dispositivo por unidad de información (bit) para su posterior análisis.

Partiendo del escenario reflejado en la Figura 1, se establece un enlace de datos entre los equipos, cuyas características vendrán definidas por los parámetros operacionales a estudiar.

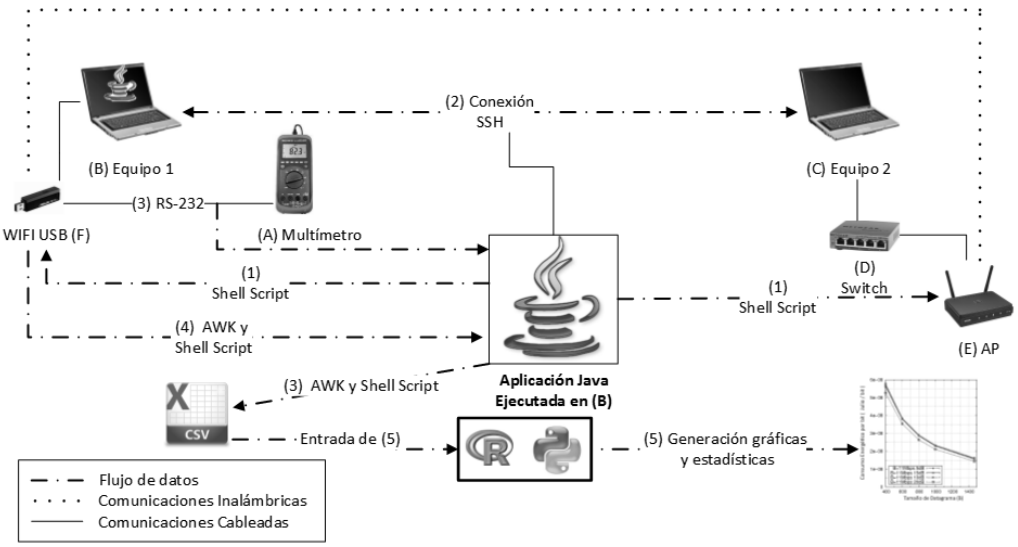


Fig. 1. Diagrama de funcionamiento de la aplicación desarrollada.

Uno de los equipos actúa como emisor de datos y el otro como receptor. El equipo emisor transmite un flujo de datos UDP con una tasa de bits constante. El equipo receptor establece un enlace inalámbrico, mediante un dispositivo USB WiFi, a través de un AP WiFi a diferentes velocidades de transmisión y con tamaños de datagrama determinados.

Se han seleccionado tres valores de B para la realización de las pruebas: 11 Mbps, 24 Mbps y 54 Mbps. Para cada una de estas velocidades se utilizarán 5 tamaños de datagramas basándonos en el estudio [10], que determina los valores de L más utilizados en internet: 400 bytes, 600 bytes, 800 bytes, 1000 bytes y 1470 bytes. Según dicho estudio la mayor frecuencia de aparición se presenta en los datagramas de 0 a 400 bytes, con casi un 40% y los de 1470 bytes se sitúan en un 20%. Para obtener resultados lo más fiable posible, cada una de las pruebas realizadas se ha repetido hasta en diez ocasiones, obteniendo el valor medio para cada caso y los intervalos de confianza.

Se han estudiado los parámetros PSM, P y D del dispositivo, en los modos: emisión, recepción y reposo. Se ha analizado para cada uno de ellos el consumo energético para cada par de la combinación B - L.

En cada caso se ha determinado el consumo energético por bit (Ec. 1). Definimos E_{bit} (Julios / bit) como el valor medio del consumo energético en el periodo t (segundos) $\overline{C}_t[W]$, dividido entre el tráfico transmitido en ese mismo periodo Th_t (Bit/segundo).

$$E_{bit}[J/bit] = \frac{\overline{C}_t[W]}{Th_t[bit/s]} \quad (1)$$

Anteriormente a la realización de cada uno de los experimentos que componen los distintos apartados, se comprueban los valores de la diferencia de potencial. Se midió hasta en diez ocasiones para cada una de las velocidades de transmisión configurada, obteniendo como resultado un valor promedio de 5,167 Voltios (V) con una desviación estándar de 0,011.

V. RESULTADOS EXPERIMENTALES

En este apartado se exponen los resultados obtenidos para cada uno de los parámetros estudiados. Se realizó un análisis para conocer el estado de partida. Se modificaron las siguientes variables para conocer las variaciones en el consumo energético: el controlador del dispositivo, la activación del modo de ahorro energético PSM y para finalizar se varió la potencia de la señal de radiofrecuencia. En todos los casos también sufrieron modificaciones el tamaño de datagrama y la velocidad de conexión.

A. Estado de partida

Este estado se caracteriza por mantener los siguientes valores por defecto en el sistema operativo: controlador de dispositivo libre bajo licencia GPL, que pasaremos a denominar D_L, PSM inactivo y potencia configurada a 20 dB.

Para analizar el comportamiento energético del dispositivo en el estado de partida, primeramente se comprobó el consumo del dispositivo USB WiFi en estado de reposo. Se pudo observar que el consumo energético del dispositivo se mantuvo estable durante todo el tiempo de realización de cada una de las pruebas, estableciéndose en un promedio 0,7 Julios (J) con una desviación estándar de 0,010, independientemente del tamaño de datagrama y la velocidad configurada en la conexión. Al no existir transferencia de datos, estos dos parámetros no intervienen en el consumo energético del dispositivo.

La Figura 2 muestra los resultados correspondientes al caso en que el dispositivo USB WiFi actúa como receptor de información. Se comprueba que el dispositivo consumió menor cantidad de energía en modo recepción que en emisión.

B. Evaluación del consumo energético con respecto al tamaño de datagrama

Podemos observar en la Figura 2 que incrementar el valor de L supone a su vez reducir el consumo energético. Esto es debido a la disminución de la cantidad de datagramas transmitidos y por lo tanto el overhead.

C. Evaluación del consumo energético con respecto a la velocidad de transmisión

Se observó analizando los resultados reflejados en la Figura 2 que el dispositivo consumió menor cantidad de energía en

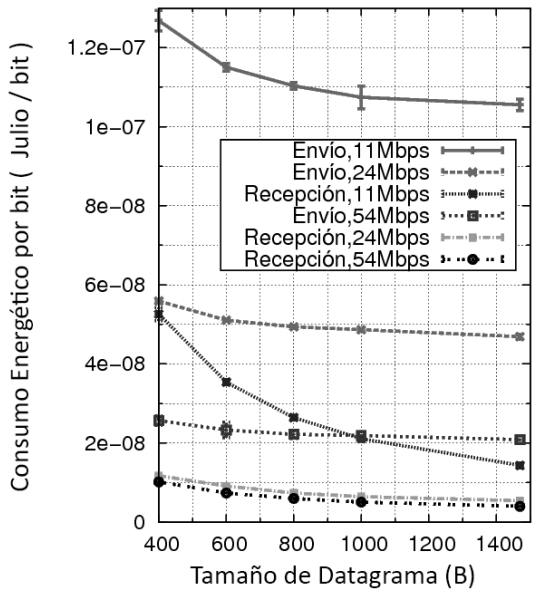


Fig. 2. Consumo energético por bit en el estado de partida

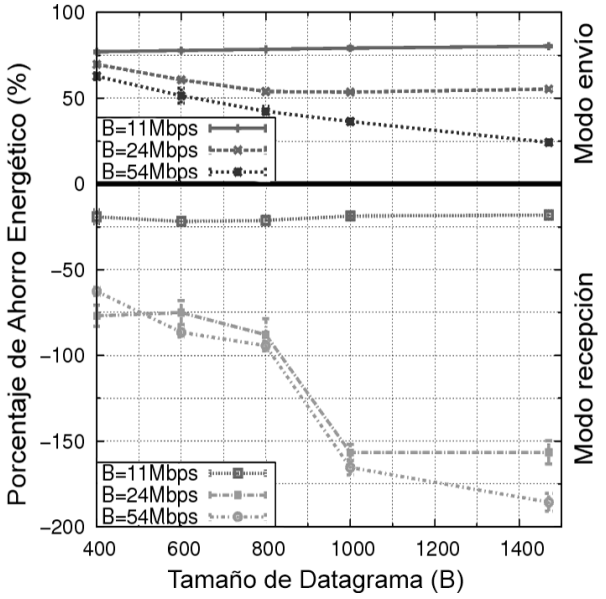


Fig. 3. Porcentaje de ahorro energético al cambiar el controlador del dispositivo

modo recepción que en emisión. Incrementar los valores de B y L supuso que el consumo energético por bit sufriese un decremento en su valor.

Comprobamos que caso de realizar envío de datos, del equipo 1 (B) al equipo 2 (C), el valor más alto de consumo energético por bit se produce al configurar la velocidad de transmisión a un valor bajo, debido a que el número de datagramas transmitidos decrece.

Tanto en lo referente a esta sección como a la anterior, se observa una conducta similar que en [6] y [7], en los cuales se aparece el mismo patrón de comportamiento tanto en emisión como recepción con respecto al consumo energético producido por el interfaz USB WiFi.

D. Evaluación del consumo energético con respecto al controlador del dispositivo utilizado.

Se ha procedido a modificar el controlador del dispositivo D_L, por la versión privativa facilitada por el fabricante (Ralink) en su versión 2.4.0.1, que pasaremos a denominar D_P. Nuestro objetivo consiste en conocer si realmente la utilización de un controlador del dispositivo u otro influye en gran medida en la energía consumida por el dispositivo USB WiFi.

Los resultados arrojados con D_P comparados con los del estado de partida con D_L pueden ser observados en la Figura 3. El dispositivo presenta un consumo energético en reposo de 0,11 J, lo que supone que la modificación del controlador del dispositivo ha supuesto una reducción del 84,28% de la energía consumida manteniendo el dispositivo USB WiFi en reposo.

Realizando transferencia de datos (modo envío), los resultados de la Figura 3 reflejan que D_P presenta una gran influencia sobre el consumo energético del dispositivo. En este sentido, supone un ahorro de energía por bit de hasta un 77% con respecto al estado de partida. Como se observa, para lograr este ahorro es necesario decrementar el valor de B e incrementar L. Se comprueba que si B toma el valor de 54 Mbps incrementar el valor de L supone una reducción del ahorro energético por bit.

Analizando los datos obtenidos en modo recepción, observamos una situación totalmente diferente a la anterior. El consumo energético con D_P sufre un incremento de hasta el 182% con respecto a D_L, el cual disminuye cuando el valor de L disminuye y B toma un valor bajo. Podemos concluir de los resultados obtenidos que la modificación que sufre D con respecto al estado inicial ha supuesto una disminución en el consumo energético del dispositivo cuando se transmite información. Así pues, también se observa que en caso de que el dispositivo actúe únicamente como receptor de datos, se produce un incremento en el consumo energético con respecto al utilizado en primer lugar.

E. Análisis del efecto de Power Save Mode

PSM está enfocado a maximizar ahorro energético (incluido en el estándar IEEE 802.11 [9]). Estudiaremos en este apartado cómo afecta la carga de la red en el ahorro de energía cuando la funcionalidad PSM se mantiene activa.

Se consideran cuatro valores de escalado (S) sobre el ancho de banda máximo alcanzable: 100%, 50%, 25% y 10%.

En este caso, el tráfico únicamente se analizará en recepción debido al comportamiento inherente de PSM, ya que sólo es efectivo en esta dirección del flujo de datos [9].

En la Figura 4 se ofrecen los resultados obtenidos al configurar el parámetro B a 54 Mbps. El comportamiento observado en este caso fue similar que el obtenido al configurar B a 11 Mbps y 24 Mbps. Mediante la observación de los resultados obtenidos se comprueba que se produce un incremento en el ahorro de energía al aumentar el valor del porcentaje de escalado de tráfico transmitido S. Este valor de escalado indica el porcentaje de reducción de la cantidad de tráfico transmitido sobre el máximo alcanzable. Por otra parte, se puede observar que cuando este parámetro incrementa su valor los resultados comienzan a ser similares a los obtenidos con el mecanismo de ahorro de energía PSM inactivo. En el mejor

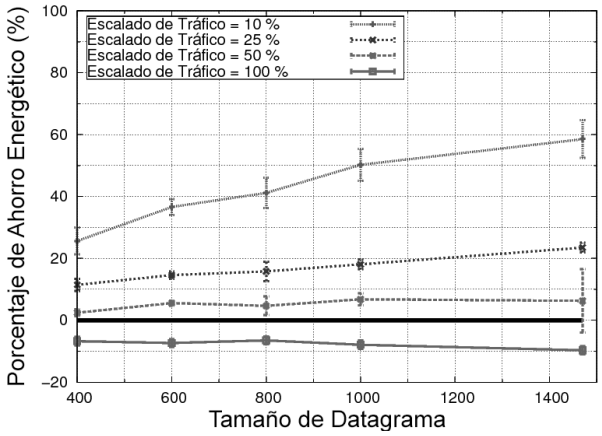


Fig. 4. Porcentaje de ahorro energético configurando la velocidad de transmisión de datos a 54Mbps.

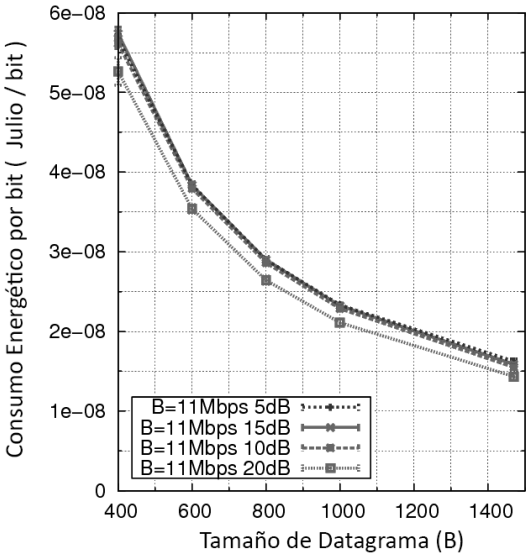


Fig. 5. Consumo energético en modo recepción variando el valor de potencia de señal.

de los casos incrementar L a su máximo y disminuir S puede suponer un ahorro energético en torno al 60 %.

Por tanto, podemos afirmar para todos los casos, que la eficiencia de PSM se incrementa con el decremento de la carga de la red y el aumento de L.

F. Variación en la potencia de la señal de radiofrecuencia.

Se ha analizado la influencia de la potencia configurada en el dispositivo USB WiFi sobre su consumo energético. En este caso, se realizaron pruebas utilizando tres valores de P: 5 dB, 10 dB, 15 dB y 20 dB. La selección se mueve en un rango de valores desde el máximo al mínimo pasando por uno intermedio, de modo que fuesen representativos en relación al rango de posibilidades de configuración.

Los resultados obtenidos en modo transmisión se podrían resumir en dos puntos: 1) En todos los casos, si se produce un decremento en la potencia de transmisión, la energía consumida por el dispositivo USB WiFi crece con respecto al estado de partida, siendo en el mejor de los casos este del 2 % con una potencia de señal de 5 dB y en el peor del 10 % configurando una potencia de señal de 15 dB. 2) Incrementar el valor de L supone un decremento en el consumo energético en el módulo WiFi.

Para el modo recepción el comportamiento con respecto al consumo energético observado es totalmente contrario al anterior. Decrementar la potencia hasta 5 dB puede suponer con respecto al estado de partida un incremento de hasta un 17,41 % en el caso de tamaños de datagrama de 1480 bytes, el cual se reduce hasta un 10 % al disminuir la potencia de tranmisión a 5 dB con un tamaño de datagrama de 400 bytes.

Si comparamos los resultados obtenidos con los ofrecidos en el trabajo [7] se observa patrón similar en el comportamiento de la transmisión: A mayor potencia de la señal de radiofrecuencia mayor consumo y a mayor tamaño de datagrama, menor consumo.

En el trabajo [7] se indica que en modo recepción no se observa variaciones en el consumo. Sin embargo, en los resultados que se observan en la Figura 5 al disminuir la potencia de transmisión se elevó el consumo energético. Este incremento en el consumo se agrava al incrementar el tamaño de datagrama.

G. Discusión de resultados.

Se estudió la influencia ejercida por cinco parámetros operacionales de un enlace WiFi en el consumo energético de un dispositivo USB.

Partiendo de una situación en la cual se establece una configuración por defecto, el cual se ha denominado estado de partida y se encuentra definido en la sección V-A, se han realizado variaciones en los parámetros especificados en la sección III. Comparando los resultados obtenidos con el estado de partida se determinaron los incrementos / decrementos sobre el consumo de energía, y por tanto, las combinaciones de parámetros que resultan más eficientes en términos energéticos.

Con el fin de determinar las condiciones que favorecen el ahorro energético los datos obtenidos se sometieron a un análisis multivariante. Se ha considerado como variable independiente cada uno de los parámetros estudiados. Los resultados arrojados se exponen en la Tabla I. Tanto en la tabla como en el presente apartado se ha utilizado la nomenclatura expuesta en la sección III.

La columna de coeficientes no estandarizados (columna B) de la Tabla 1 muestra que un incremento de 1 Mbps en velocidad de transmisión se asocia de un modo estadísticamente significativo con un decremento en el ahorro energético de un 1,95% en recepción y 0,7% en envío.

Para todos los casos la influencia con respecto al valor de ahorro energético final en L es inferior a B tal y como se puede observar en el en la tabla I.

Se ha verificado que el controlador de dispositivo USB WiFi presenta un vínculo muy estrecho con el consumo energético. Ya que se observó al modificar el controlador de dispositivo un incremento en el consumo energético cuando el dispositivo recibe gran cantidad de información. Sin embargo, sucede lo contrario cuando actúa en modo emisor.

El estudio del modo de ahorro energético PSM determinó que la eficiencia del mecanismo se ve decrementada cuando aumenta la carga de red. Esto se puede comprobar en la sección PSM de la Tabla I. La columna de coeficientes no

estandarizados muestra que un incremento de una unidad en el escalado de tráfico (Parámetro S) se relaciona de un modo estadísticamente significativo con una disminución de 0,485% sobre el ahorro energético obtenido.

En lo referente a la potencia de señal de radiofrecuencia difieren los datos en cuanto a envío y recepción. Realizando transmisión de datos se ha observado un incremento en el consumo energético, el cual se ve reducido al incrementar el tamaño de datagrama. Si se realiza recepción de información elevar el valor de potencia de señal ayuda a reducir el consumo energético.

El valor de P establecido es un factor que será determinante en función del sentido que tome la transmisión de información.

Se comprobó en modo recepción que el incremento de P supone disminuir el ahorro energético obtenido, sin embargo, en envío sucede lo contrario, se aprecia un gran incremento en el ahorro energético al aumentar el valor de P, como se puede observar en la Tabla I.

Tabla I
COEFICIENTES DEL ANÁLISIS MULTIVARIANTE.

		B	Error	Beta	t	Sig
	PSM					
	(Constante)	30,911	2,476		12,486	,000
	B	-,112	,041	-,092	-2,735	,007
	L	,011	,002	,197	5,867	,000
	S	-,485	,021	-,788	-23,479	,000
	D					
Recepción	(Constante)	34,619	13,207		2,621	,011
	B	-1,950	,243	-,614	-8,028	,000
	L	-,070	,012	-,451	-5,895	,000
	P					
	(Constante)	9,444	,815		11,595	,000
	B	-,015	,012	-,076	-1,295	,197
	L	,004	,001	,373	6,360	,000
	P	-,268	,051	-,306	-5,215	,000
	D					
	(Constante)	95,367	2,794		34,138	,000
	B	-,763	,051	-,822	-14,853	,000
	L	-,015	,003	-,322	-5,828	,000
Envío	P					
	(Constante)	-1,772	1,257		-1,410	,160
	B	,220	,018	,544	12,256	,000
	L	-,004	,001	-,223	-5,030	,000
	P	,836	,079	,468	10,564	,000

VI. CONCLUSIONES

Se estudió el efecto que tienen cinco características de las redes inalámbricas sobre su consumo energético, utilizando para ello el testbed que se observa en la Figura 1.

Se obtuvieron valores de consumo energético en función de diversas configuraciones. Se determinó el ahorro energético obtenido mediante comparaciones con el estado que se denominó inicial (sección V-A).

Los resultados muestran cómo el tamaño de datagrama, la velocidad de transmisión, el controlador de dispositivo utilizado, el mecanismo de ahorro energético PSM y la potencia de la señal de radiofrecuencia influyen en el consumo energético.

Con respecto al tamaño de dagrama, los mejores resultados se obtienen con el máximo de los tamaños, siempre y cuando no se produzca fragmentación. A su vez, se incrementa la reducción en el consumo energético al aumentar la velocidad de conexión.

El controlador de dispositivo juega un papel importante, ya que al utilizar D_P se obtiene gran ahorro energético al realizar envío de datos, aunque en recepción sucede lo contrario.

PSM ofrece una disminución del consumo energético al activar el mecanismo en modo recepción y recibir datos a velocidad baja.

Incrementar la potencia de señal en modo envío de datos supone un incremento en el consumo energético, en modo recepción sucede lo contrario.

Al igual que en [6], hemos podido verificar que tanto la carga de la red como el tamaño del datagrama presentan un gran influencia en el valor final de consumo energético del dispositivo inalámbrico. En ambos casos un incremento en estos parámetros implica un crecimiento en el consumo energético.

La selección del controlador adecuado supone un 40% sobre el potencial de ahorro. Seleccionar una buena combinación de todos los parámetros estudiados puede contribuir a que el consumo energético del dispositivo USB WiFi se vea reducido hasta en un 83%.

REFERENCIAS

[1] K. David, *Technologies for the Wireless Future: Wireless World Research Forum, Volume 3*. Wiley Publishing, 2008.

[2] G. Anastasi, M. Conti, E. Gregori, and A. Passarella, "802.11 power-saving mode for mobile computing in wi-fi hotspots: limitations, enhacements and open issues", *Wirel. Netw., vol. 14, no. 6*, pp. 745-768, dec 2008. [Online]. Available: http://dx.doi.org/10.1007/s11276-006-0010-9

[3] J. Lorincz, A. Capone, and M. Bogarelli, "Energy savings in wireless access networks through optimized network management", Wireless Pervasive Computing (ISWPC), *5th IEEE International Symposium on*, pp. 449-454, 2010.

[4] H. O. Scheck, "ICT & wireless networks and their impact on global warming", *European Wireless Conference (EW)* , pp. 911-915, 2010.

[5] Y. Al-Hazmi, H. de Meer, K. A. Hummel, H. Meyer, M. Meo and D. Remondo, "Energy-efficient wireless mesh infrastructures", *IEEE Network Magazine, vol. 25, no. 2*, pp. 32-38, 2011.

[6] K. Gomez, R. Riggio, T. Rasheed and F. Granelli, "Analysing the energy consumption behaviour of wifi networks", *Online Conference on Green Communications (GreenCom),IEEE*, pp. 98-104, 2011.

[7] J. P. Ebert, B. Burns and A. Wolisz, "A trace-based approach for determining the energy consumption of a WLAN network interface", *Proc. of the European Wireless Conference*, pp. 230-236, 2002.

[8] P. Mahadevan, P. Sharma, S. Banerjee, and P. Rangathan, "A power benchmarking framework for network devices", *Proceedings of the 8th International IFIP-TC 6 Networking Conference*, pp. 795-808 , 2009.

[9] "IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wiereless lan medium access control (MAC), and physical layer (PHY) specifications", pp. 1-1076, 2007.

[10] R. Sinha, C. Papadopoulos, and J. Heidemann, "Internet packet size distributions: Some observations", USC/Information Sciences Institute, *Tech. Rep. ISI-TR-2007-643*, May 2007, originally released October 2005 as web page http://netweb.usc.edu/ rsinha/pkt-sizes/. [Online]. Available: http://www.isi.edu/ johnh/PAPERS/Sinha07a.html

Influencia de los códecs de VoIP en el consumo energético de los Smartphones.

Pablo Carrillo Alvarez, Antonio Estepa Alonso, Rafael Estepa Alonso, Juan M. Vozmediano Torres.
Área de Ingeniería Telemática
Universidad de Sevilla
C/ Camino de los Descubrimientos s/n
pablo.carrillo.alvarez@gmail.com, {aestepa,rafa,jvt}@trajano.us.es.

***Abstract*—En este artículo se presentan los resultados de un estudio realizado para caracterizar el perfil de consumo energético de los codecs usados en VoIP. En un estudio preliminar ya detectamos que existen diferencias significativas entre codecs y que éstas son principalmente atribuibles al uso intensivo del procesador cuando no se usa el modo de ahorro de energía de WiFi, lo que ocurre comúnmente. En este nuevo estudio experimental se mide el uso del procesador realizado por cada codec así como su influencia sobre el consumo de batería en un terminal iphone 4S. Los resultados muestran diferencias significativas entre codecs, y pensamos que éstas diferencias son extrapolables a cualquier terminal móvil. Por ello, la selección del codec a usar en los terminales móviles debería incluir el consumo energético como un factor más a tener en cuenta.**

***Index Terms*—Energía, códecs, VoIP, 802.11**

I. Introducción

Los dispositivos móviles tales como *smartphones*, *netbooks*, o *tablets* han experimentado a lo largo de los últimos años un fuerte crecimiento en el mercado residencial español [1]. Los factores que han contribuido a este éxito son tanto tecnológicos como económicos y sociales. Sin embargo, todos estos dispositivos comparten una limitación común: el tiempo máximo de uso en movilidad o, lo que es equivalente, el tiempo de operación hasta que se agota la batería.

Por otra parte, el uso cada vez más habitual de aplicaciones multimedia en los dispositivos móviles (en especial smartphones), hace que resulte interesante preguntarse qué influencia tienen este tipo de aplicaciones en el consumo energético del dispositivo. Aunque existen estudios sobre el consumo energético de aplicaciones de *streaming* de audio/vídeo [2], [3], existe aún poca investigación sobre las aplicaciones de VoIP, donde los estudios existentes suelen centrarse en el consumo del interfaz WiFi [4], [5].

En un trabajo previo [6], realizamos un primer análisis preliminar sobre el impacto que los diferentes codecs de VoIP tienen sobre el consumo de batería de un ordenador portátil, encontrando que cada codec tiene un consumo energético diferenciado. El procesador del dispositivo y la tarjeta WiFi son los dos componentes electrónicos que más influyen en estas diferencias. En particular, respecto al consumo energético en la tarjeta WiFi obtuvimos las siguientes conclusiones:

- Los paquetes generados por la aplicación de VoIP sólo mantienen a la interfaz WiFi en estados activos (TX/RX) aproximadamente el 2% de su tiempo.
- Si se usa el modo de ahorro energético (PSM), el consumo de la tarjeta WiFi es muy reducido comparado con el procesador, aunque presenta variaciones mas apreciables entre codecs.
- Si no se usa el modo PSM, apenas existen diferencias en cuanto a la energía consumida en la interfaz WiFi por los diferentes codecs. Este escenario es el más habitual y en él, el uso del procesador marcará las diferencias energéticas entre codecs.

Por ello en este trabajo nos centraremos en determinar experimentalmente las diferencias existentes entre codecs respecto al consumo energético del procesador de un teléfono móvil actual (iphone 4S). A través de medidas, se analizará para cada codec el tiempo de uso del procesador del teléfono al codificar conversaciones reales, así como el gasto de batería asociado. Aunque los resultados en términos absolutos son sólo aplicables a este terminal, pensamos que el ranking energético obtenido será válido para cualquier dispositivo ya que el uso del procesador depende principalmente de la complejidad algorítmica de cada codec. Entendemos que los resultados de este estudio son de aplicación en el diseño de las aplicaciones de VoIP, que podrían seleccionar de forma dinámica parámetros como el codec a utilizar (o su configuración), evaluando entre otros factores, la disponibilidad energética del dispositivo.

La organización del resto del artículo es la siguiente. En la sección II se ofrece un breve resumen sobre las principales características de los códecs bajo estudio en el presente trabajo. La sección III realiza un breve análisis sobre la influencia que tienen los códecs en los diferentes componentes electrónicos con impacto en el consumo. La sección IV explica el experimento realizado para la medición de los recursos consumidos por los códecs bajo estudio. La sección V presenta los resultados obtenidos y, finalmente, la sección VI ofrece las conclusiones principales y las futuras líneas de avance.

II. Códecs en aplicaciones de VoIP

La Figura 1 representa los principales elementos involucrados en el flujo de la comunicación en un extremo de una aplicación de VoIP. La tarjeta de sonido del dispositivo genera periódicamente muestras digitales (PCM 16 bits) del sonido percibido por el micrófono, que incluye ruido de fondo. Estas muestras son procesadas por el codec, componente clave del proceso de aplicación. El codec, en su modo de operación básico, opera sobre un grupo de muestras generando un bloque de datos llamado *trama* a intervalos periódicos. Tanto el tamaño de la trama generada como el tiempo necesario para generar una nueva trama dependen del algoritmo de codificación particular de cada codec. Las tramas generadas son posteriormente encapsuladas para su envío hacia el otro

extremo donde serán decodificadas. El proceso de encapsulado incluye el uso de los protocolos RTP, UDP e IP. Para mejorar la eficiencia es posible encapsular varias tramas en un mismo paquete IP, aunque la mayoría de aplicaciones suelen usar un intervalo de generación de paquetes de 20 ms tal y como sugiere el perfil RTP de la mayoría de codecs [7]. Los paquetes IP son finalmente enviados a través de la interfaz de comunicación (WiFi en nuestro estudio) del dispositivo.

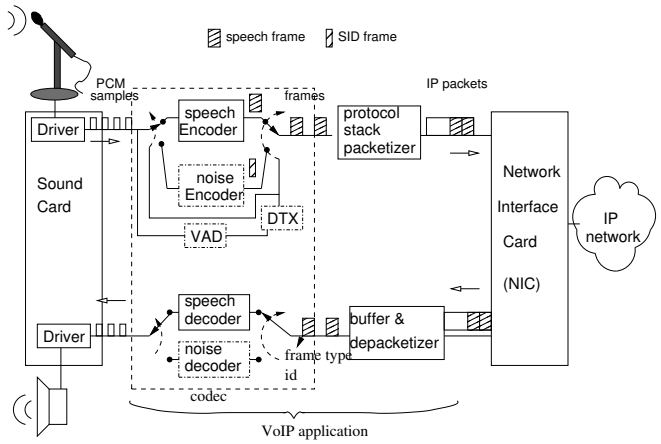


Fig. 1. Esquema de un extremo de la comunicación en una aplicación de VoIP

En el otro extremo, los paquetes IP recibidos por la tarjeta de red se almacenan temporalmente en un buffer gestionado por la aplicación de VoIP, que permite compensar fluctuaciones de retardo (*jitter*) en la red. Una vez esperado un tiempo inicial para el llenado de este buffer, la aplicación de VoIP comienza a extraer tramas de forma periódica para su descodificación. Después de la descodificación se obtienen de nuevo un conjunto de muestras PCM de 16 bits que reconstruyen la señal original con una cierta distorsión. Los codecs se diferencian principalmente en la calidad del sonido reproducido (distorsión frente a la señal original), el caudal requerido (tamaño y frecuencia de las tramas generadas) y el algoritmo de codificación/decodificación (complejidad computacional).

Por lo explicado anteriormente, los codecs generan paquetes de tamaño constante a intervalos fijos de tiempo (tráfico CBR). Sin embargo, algunos codecs pueden actuar como fuente de tasa variable (VBR) a fin de reducir el caudal de tráfico generado a través de las siguientes técnicas:

- *Supresión de Silencios*. Esta característica evita que se generen nuevas tramas durante los períodos de inactividad de la voz. Ello puede suponer una reducción de hasta el 50% del ancho de banda. Se basa en un algoritmo detector de actividad vocal (*Voice Activity Detector* o VAD) que clasifica cada grupo de muestras de sonido como voz o como ruido de fondo. Cuando el algoritmo VAD clasifica una trama como ruido de fondo, otro algoritmo (DTX) determinará cuándo enviar una muestra del ruido al extremo receptor para que éste sea reproducido durante los intervalos de silencio para mayor confort del oyente. Estas tramas que describen el ruido de fondo se denominan *Silence Insertion Descriptor* (SID) y son codificadas de manera diferente a la voz. Entre el 3 y el 7% de las tramas generadas en una conversación son de tipo SID, dependiendo del codec. Los codecs G.729b, G.723.1 y AMR ofrecen Supresión de Silencios a elección del usuario.
- *Multi-tasa*. Algunos codecs ofrecen varias tasas de compresión (modos de operación). Cada modo de operación se diferenciará en el tamaño de la trama generada o en el periodo de generación entre tramas, lo cual supone que un usuario podría elegir el caudal que mejor se ajuste a sus necesidades. Evidentemente, mientras mayor compresión se utilice se obtendrá una peor calidad de sonido dentro de un mismo codec. Los codecs G.723.1, AMR e iLBC son ejemplos de codecs multi-modo.

La tabla I resume las características principales de los códecs a utilizar en el presente estudio. La columna que mide el índice de opinión media (MOS) o calidad ha sido calculada utilizando el método de evaluación de la calidad vocal por percepción, PESQ, normalizado en la Recomendación P.862 de la ITU-T, bajo un escenario sin pérdidas de paquetes ni retrasos. La última columna refleja la implementación en lenguaje C que se ha utilizado en el presente estudio para cada codec. Como puede comprobarse, las implementaciones utilizadas son las ofrecidas por los propios estándares.

III. Componentes de la Energía asociada a un códec de VoIP

Los principales componentes electrónicos utilizados por una aplicación de VoIP son:

- *Procesador*. Usado en los procesos de codificación y descodificación de cada trama. Además del algoritmo de codificación de voz, también el algoritmo VAD y la codificación de tramas SID consumirán ciclos de procesador en aquellos códecs que presentan esta característica. El tiempo que un procesador particular necesita para generar una trama dependerá básicamente del algoritmo de codificación del códec, debiendo ser siempre significativamente menor que periodo de generación de tramas del codec si se utilizan en entornos de tiempo real como un conversación de VoIP.
- *La interfaz WiFi*. Usada para transmitir las tramas generadas y recibir las tramas procedentes del otro extremo de la conversación [1]. Aunque la generación y consumo de de tramas se puede considerar periódico, los codecs con VAD evitan el envío durante los períodos de inactividad vocal, a excepción de las esporádicas tramas de descripción de ruido de fondo (tramas SID) que se usan en el generador de ruido de confort.
- *Otros componentes*. Componentes como el display, la memoria o la tarjeta de sonido también son usados por la aplicación de VoIP e influyen en el consumo de energía. Sin embargo nuestro estudio se centra en averiguar las diferencias de consumo energético de distintos codecs en su tarea de codificación / descodificación, y no en ofrecer valores absolutos de consumo (que no serían extrapolables entre diferentes dispositivos). Asumimos que los codecs bajo estudio no presentan diferencias

[1]El uso de la interfaz WiFi también requiere de una mínima atención de la CPU que será despreciada en nuestro estudio.

Códec	Tasa de muestreo (kHz)	Tasa de bits (Kbit/s)	Tamaño de trama (ms)	Bits por trama de voz	Bits por trama SID	Algoritmos de codificación	DTX	MOS	Código fuente C descargable de
G.711	8	64	-	640	-	PCM	No	4.39	http://www.itu.int/rec/T-REC-G.711/es [8]
G.723.1	8	6.3 5.3	30	192 160	32	MP-MLQ ACELP	Yes	3.69 3.49	http://www.itu.int/rec/T-REC-G.723.1/es [9]
G.729	8	8	10	80	-	CS-ACELP	No	3.75	http://www.itu.int/rec/T-REC-G.729/es [10]
G.729A	8	8	10	80	-	CS-ACELP	No	3.67	http://www.itu.int/rec/T-REC-G.729/es [10]
G.729B	8	8	10	80	10	CS-ACELP	Yes	3.51	http://www.itu.int/rec/T-REC-G.729/es [10]
G.729AB	8	8	10	80	10	CS-ACELP	Yes	3.55	http://www.itu.int/rec/T-REC-G.729/es [10]
AMR	8	12.2 10.2 7.95 7.4 6.7 5.9 5.15 4.75	20	244 204 159 148 134 118 103 95	39	MR-ACELP	Yes	3.97 3.93 3.69 3.71 3.64 3.55 3.44 3.39	http://www.3gpp.org/ftp/Specs/html-info/26073.htm [11]
iLBC	8	15.2 13.3	20 30	303 399	-	iLBC	No	3.86 3.82	http://www.ietf.org/rfc/rfc3951.txt [12]

TABLA I
PRINCIPALES CARACTERÍSTICAS DE LOS CÓDECS DE VOIP.

significativas en cuanto al uso de estos componentes electrónicos por lo que no los incluiremos en el estudio[2].

Como se indicó en la Sección 1, en [6] se concluye que las tarjetas WiFi se encuentran en estado *no activo* (ocioso, o dormido si se usa PSM) más del 98% del tiempo de una conversación debido fundamentalmente a la diferencia entre el tiempo requerido para transmitir o recibir una trama en las tarjetas actuales (p.e. $\sim$1.4 μs para 54Mbps) y el tiempo entre tramas (20 ms generalmente). Por tanto, el gasto energético de la tarjeta WiFi apenas va a depender del codec utilizado y si de la configuración de ahorro de energía de la misma (elevado en el caso de no usar PSM y reducido si se usa). Por este motivo el presente estudio estará centrado en medir el tiempo de uso del procesador por parte de cada codec.

IV. EXPERIMENTO

Hemos diseñado un experimento, basado en medidas software en un terminal *iPhone 4S*, para valorar el tiempo de uso del procesador de cada uno de los codecs (y modos) de la tabla I durante la codificación/descodificación de una serie de conversaciones de referencia. Estas conversaciones han sido obtenidas de un banco de conversaciones de referencia internacional, *Linguistic Data Consortium* [13]. En particular hemos usado el CR-ROM LDC 97S42 que incluye 120 conversaciones telefónicas en inglés americano. Cada conversación tiene una duración entre 15 min y 30 min, y se encuentra compuesta por dos canales (uno en cada sentido de la conversación) de manera que, separando ambos canales, es posible obtener el audio que se recibiría (descodificaría) y transmitiría (codificaría) en cada extremo de la conversación. Hemos utilizado 5 de estas conversaciones, que, en su conjunto, cuentan con una duración aproximada de 2 horas, no encontrando diferencias en los resultados al añadir nuevas conversaciones que alargasen más el proceso.

A. ¿Qué se mide?

La estrategia que seguiremos es la medida del tiempo de uso del procesador de un terminal durante la codificación y descodificación de ambos extremos de conversaciones reales. El tiempo de uso puede ser traducido a energía utilizando datos de potencia de la circuiteria del dispositivo en particular. Es decir, asumiremos un comportamiento lineal simple como modelo de la energía consumida por el procesador:

$$\text{Energía}_{CPU} = P_{HW} \cdot t \quad (1)$$

donde P_{HW} es una constante de potencia que dependerá de un procesador particular y t es el tiempo de ejecución de una tarea (p.e. codificación o descodificación de las tramas de una conversación) para un codec particular en un procesador particular. t dependerá del número de operaciones requeridas para completar la tarea así como de las prestaciones del procesador (p.e. Gigaflops). Si asumimos que la constante P_{HW} no depende del codec, entonces podríamos comparar diferentes codecs midiendo el tiempo que tardan en completar una misma tarea. Aunque existen otros modelos mas complejos en la literatura, creemos que este modelo lineal es suficiente para cubrir los propósitos del estudio de comparar las diferencias entre codecs.

Para determinar el consumo de energía también vamos a medir el gasto en la batería del teléfono por unidad de tiempo, lo que nos dará una pendiente de descarga de batería equivalente a nuestra constante P_{HW}. Los resultados obtenidos podrían ser trasladados a otros dispositivos siempre que conozcamos el valor de P_{HW} en el nuevo dispositivo y la relación entre la prestación de su procesador y el procesador utilizado en nuestro experimento[3]

B. ¿Cómo se mide?

Se ha desarrollado una aplicación para un terminal *iPhone 4S*. El terminal no ha tenido uso previo con lo que la batería se encuentra en perfecto estado.

Para la medida del tiempo de uso del procesador, se ha creado una aplicación para cada codec tal y como se puede apreciar en la figura 2. Para un codec concreto se han desarrollado cuatro pantallas:

[2]Hemos realizado medidas de uso de memoria no encontrando diferencias significativas entre codecs.

[3]Las prestaciones del procesador (p.e. Gigaflops) pueden ser obtenidas en las especificaciones técnicas.

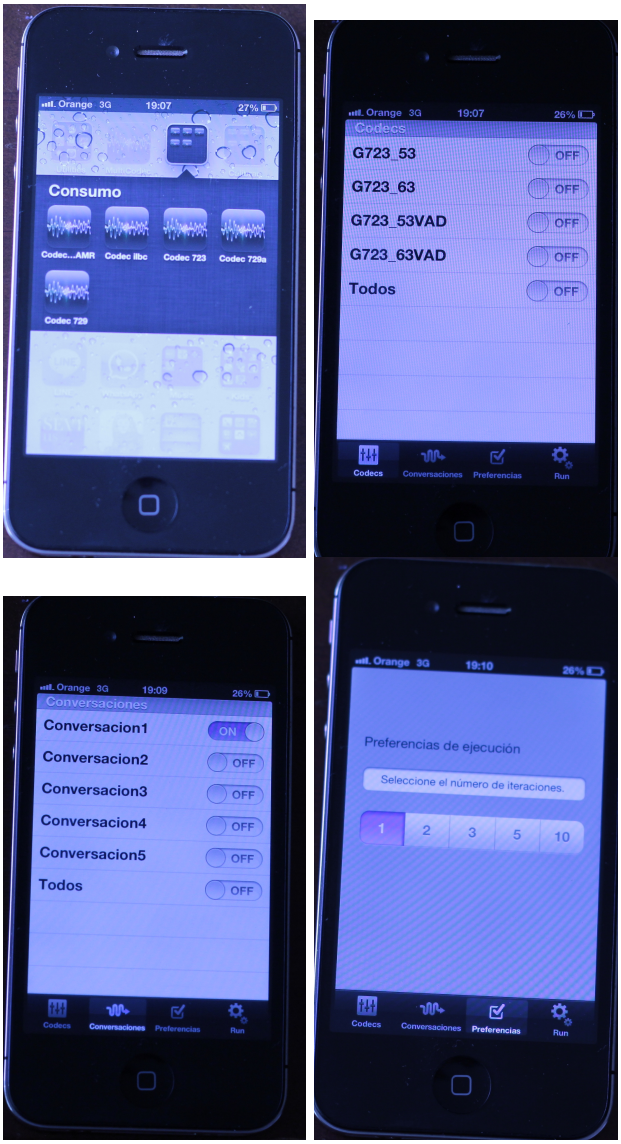


Fig. 2. Pantallas de la aplicación ejecutándose en el terminal

1. Codec: una interfaz donde se permite seleccionar todas las variantes posibles de un mismo codec (p.e. modos de operación o supresión de silencio) para el proceso de codificación / descodificación.
2. Conversaciones: una interfaz donde se permite seleccionar la(s) conversación(es) a codificar/descodificar. El programa realiza la codificación de un canal de la conversación y la descodificación del otro canal. También realiza la operación inversa, obteniéndose así el tiempo de uso del procesador en cada extremo de la conversación.
3. Iteraciones: esta pantalla permite al usuario indicar el número de iteraciones a realizar (repetición del experimento).
4. Ejecución: Esta pantalla nos permite ejecutar el experimento así como indicar que los resultados generados sean enviados por email a través del propio teléfono. Los resultados consisten en una tabla de datos con el tiempo de procesador empleado en el proceso de codificación en ambos extremos así como el tiempo empleado en el proceso de descodificación en ambos extremos, para cada iteración, conversación y codec/modo empleado.

Para medir el tiempo de uso del procesador hemos modificado el código fuente de los codecs[4] listados en la tabla I para que utilice la función getrusage. Esta función estándar de la biblioteca GNU C solicita al sistema operativo que tome una medida del número de ciclos de procesador que utiliza un proceso. La función getrusage es invocada al principio del proceso de codificación/descodificación y junto con el tiempo que toma se guarda el número de tramas procesadas (tanto en la codificación como en la descodificación).

Además de la aplicación anterior, también se ha creado otra aplicación cuyo objetivo es medir el proceso de descarga de batería. Para medir el estado de la batería, utilizamos una llamada standard al sistema operativo que registra automáticamente el tiempo del sistema cada vez que cambia el porcentaje de batería en el dispositivo (a intervalos de 5%). El experimento consiste en codificar de forma continuada partiendo de una batería llena (la medición del tiempo comienza cuando la batería pasa al 95%) registrando los instantes de cambio de la batería (o sea: 95%,90%,85%,...) hasta llegar al 5%. El dispositivo móvil se encontrará en modo avión, sin ningún otro proceso de aplicación en ejecución y con el display a un nivel máximo de brillo[5]. En las mismas condiciones se medirá la pendiente de descarga de la batería antes de realizar el experimento para poder restársela a los datos obtenidos durante el experimento.

V. Resultados

A. Tiempo de uso del procesador

El procesador es utilizado tanto para la codificación de las tramas que se generan como para la descodificación de aquellas tramas que se recibirían del otro extremo de la conversación. Los resultados presentados provienen de ejecutar el experimento anteriormente descrito: codificación/decodificación de 5 conversaciones (10 ficheros de audio, uno por canal) y 2 iteraciones.

1) Codificación: La Tabla II muestra los resultados obtenidos en el proceso de codificación (resultados agregados de todas las iteraciones y conversaciones). La columna 2 muestra cuántos segundos de procesador son necesarios para codificar un segundo de conversación.

En los resultados de la tabla anterior podemos apreciar lo siguiente:

- Existe una variación muy significativa entre codecs. El codec G.723 (modo 6.3) requiere casi 10 veces más uso del procesador que el codec iLBC20.
- Los codecs que presentan supresión de silencios (VAD) tienen una mayor varianza en cuanto a los resultados obtenidos. Esto es lógico ya que las tramas codificadas dependen de la actividad vocal de cada conversación.

[4]Algunas compañías han desarrollado implementaciones de bajo consumo para varios de estos códecs, pero ante las dificultades para obtenerlas este estudio considerará sólo la implementación referencia, asumiendo que todos los códecs pueden ser objeto de mejoras similares

[5]Se ha optado por esta aproximación por permitir un *feedback* visual del proceso en la pantalla y por que haya una mayor similitud con el escenario utilizado para medir el gasto energético

TABLA II
PROCESO DE CODIFICACIÓN

Codec(modo)	segundos de procesador / segundo de sonido	Intervalo de Confianza 95%
AMR4.75	0,8502953799	±0,0009592408
AMR7.4	0,8300669507	±0,0009570168
AMR12.2	0,8982567083	±0,0008550941
AMR4.75VAD	0,6322348211	±0,0643953333
AMR7.4VAD	0,6204528754	±0,0638037916
AMR12.2VAD	0,6814535964	±0,0546551214
G729	0,9389504731	±0,0011112069
G729b	0,6548824928	±0,0534129596
G729a	0,5500213477	±0,0010696579
G729ab	0,4203116089	±0,0616307063
G723_53	1,1129556496	±0,001343638
G723_63	1,4852095776	±0,0022399295
G723_53VAD	0,8222049267	±0,0473987498
G723_63VAD	1,0737613371	±0,0434156726
ILBC20	0,149301743	±0,0010704197
ILBC30	0,1749364185	±0,0010225189

2) Descodificación: La Tabla III muestra los resultados obtenidos en el proceso de descodificación (resultados agregados de todas las iteraciones y conversaciones). La columna 2 muestra cuántos segundos de procesador son necesarios para descodificar un segundo de conversación.

TABLA III
PROCESO DE DESCODIFICACIÓN

Codec(modo)	segundos de procesador / segundo de audio descodificado	Intervalo de Confianza 95%
AMR4.75	0,1290933184	±0,0094600544
AMR7.4	0,126136726	±0,00325231
AMR12.2	0,1288370973	±0,0051735467
AMR4.75VAD	0,1106649996	±0,1683620648
AMR7.4VAD	0,1093002901	±0,1561918419
AMR12.2VAD	0,1120522623	±0,1518197683
G729	0,1921093154	±0,0127892634
G729b	0,1720820412	±0,0686124707
G729a	0,1211894625	±0,0051007214
G729ab	0,1270814609	±0,0264587193
G723_53	0,1011909108	±0,0074405467
G723_63	0,1010665702	±0,0068016988
G723_53VAD	0,090501021	±0,0074405467
G723_63VAD	0,0903858505	±0,1436614353
ILBC20	0,0610137474	±0,0300987959
ILBC30	0,0639086916	±0,0260178325

De los resultados de la tabla III se desprende que el proceso de descodificación de cualquier codec requiere significativamente menos uso de procesador que el proceso de codificación.

Si sumamos el tiempo de uso de procesador en cada extremo de cada conversación (tiempo requerido para codificar todo el audio del micrófono y descodificar el sonido previamente codificado por el otro extremo de la conversación) obtenemos los resultados medios mostrados en la Figura 3, donde se nos muestra el ranking de los codecs utilizados en el experimento (de menor a mayor tiempo de uso de procesador).

Tal y como se puede apreciar en el ranking anterior,

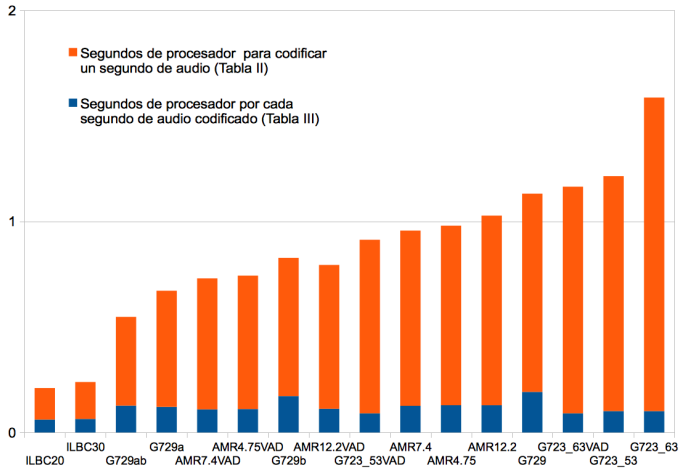


Fig. 3. Tiempo de uso de procesador de la aplicación de VoIP (debido al codec) en un extremo de una conversación

aquellos codecs cuyo tiempo total de uso sea superior a 1 seg.[6] no podrán ser utilizados en el dispositivo[7] en su implementación original (p.e. G.723 sin usar VAD, o G.729).

B. Energía consumida por el procesador

Nuestra aplicación también realiza una estimación de la energía total consumida por las tareas de codificación y descodificación. Esto nos permitirá calcular el factor P_{HW} de la ecuación 1. Tal y como se describió en el apartado anterior el proceso consiste en codificar continuamente una conversación durante tanto tiempo como sea necesario para descargar la batería. Nuestra aplicación irá registrando todos los instantes en los que cambie el nivel de carga de la batería (a intervalos de 5%) desde el 95% hasta llegar al 5%. Esta misma pendiente de descarga se ha calculado sin el proceso de aplicación para restar el gasto ordinario del sistema operativo y la pantalla.

Los resultados obtenidos son:

- La batería se descarga una media de $\mathbf{0,42\%}$ por cada minuto de uso del procesador en la tarea de codificación. Con unas diferencias de $\pm 0,01$ según el codec utilizado[8].
- Si restamos la pendiente de descarga si no se hubiese ejecutado la aplicación de codificación, obtenemos que el gasto de batería debido al proceso de codificación (procesador) es del $\mathbf{0,197\%}$ por minuto, (con diferencias de $\pm 0,01$ entre codecs).

Así pues, el procesador del teléfono podría estar funcionando 526,3 minutos codificando si fuese el único componente que utilizase la batería (según sus especificaciones de

[6]Nótese que se toma como referencia 1 seg. de conversación

[7]Al hacer esta afirmación estamos asumiendo que ambos extremos de la conversación utilizan el mismo codec

[8]Para verificar que esta pendiente de descarga no depende del codec hemos realizado esta mima prueba con todos los codecs bajo estudio, obteniendo pequeñas variaciones que pueden explicarse por las diferencias de rendimiento de los codecs, en cuanto a segundos de sonido por segundos de procesador, que implican un número diferente de lecturas (p.e. para producir un gasto del 80% de la batería, el codec ilbc20 necesita codificar la misma conversación 60 veces mientras que el codec AMR 12.2 sólo necesita codificarla 15 veces, ello implica que el codec ilBC va a realizar mas operaciones de lectura y esto tendrá una pequeña influencia en el gasto en batería. Por otra parte para minimizar estas diferencias en el estudio se ha evitado escribir los archivos codificados/descodificados

1432mAh (5.3Wh)), o hasta 238 minutos (unas 4 horas) si no descontamos el gasto del teléfono en reposo. Ello se traduce en diferentes tiempos de uso según el codec ya que por cada segundo de uso de cpu es posible codificar mas o menos segundos de audio según el codec tal y como se indica en la tabla II. La tabla IV refleja el tiempo máximo de la aplicación de VoIP en función de estos dos parámetros tomando como referencia el gasto total de batería (es decir, 0,42% por cada minuto de procesador) y el tiempo que procesador que requiere cada extremo de la conversación por cada segundo de conversación (tablas II y III).

TABLA IV
TIEMPO MÁXIMO DE USO EN CONVERSACIÓN.

Codec(modo)	tiempo de procesador / segundo de conversación	tiempo máximo de uso (min. conversación)
G723_63	1,586276*	150,0369 min
G723_53	1,214146*	196,0224 min
G723_63VAD	1,164147*	204,4415 min
G729	1,131059*	210,4221 min
AMR12.2	1,027093*	231,7217 min
AMR4.75	0,979388	243,0087 min
AMR7.4	0,956203	248,9009 min
G723_53VAD	0,912705	260,7630 min
G729b	0,82696	287,7995 min
AMR12.2VAD	0,793505	299,9347 min
AMR4.75VAD	0,742899	320,3662 min
AMR7.4VAD	0,729753	326,1376 min
G729a	0,671210	354,5830 min
G729ab	0,547393	434,7881 min
ILBC30	0,2388	996,4616 min
ILBC20	0,210315	1.131,6332 min

* Nótese que los codecs marcados con * no podrían implementarse en este terminal ya que cada segundo de conversación requiere mas de un segundo de procesador.

Como puede observarse en la Tabla IV, existen grandes diferencias en cuanto a la duración máxima de uso de una aplicación de VoIP en función del codec seleccionado por el desarrollador el usuario. Pensamos que las diferencias entre codecs obtenidas si contásemos otros componentes (p.e. tarjetas radio) no reflejarían diferencias significativas con respecto a los resultados obtenidos ya que las diferencias en el gasto energético apenas dependería del codec[9]. También pensamos que estos resultados (no en términos absolutos, si no en términos de diferencias entre codecs) deberían mantenerse en otros terminales ya que las diferencias son debidas a la complejidad computacional de los algoritmos respectivos.

VI. CONCLUSIONES Y LÍNEAS DE AVANCE

Hemos realizado un estudio sobre la influencia de los diferentes códecs de VoIP en el consumo de batería de un smartphone actual (iphone 4S) debido al uso del procesador. Los resultados reflejan que el codec (y modo) utilizado por el desarrollador o el usuario tendrá una gran influencia en cuanto a la duración de la batería llegando a diferencias de entre 5 y 6 veces entre los codecs implementables que mas consumen (p.e. G729, AMR sin supresión de silencios) y los que menos consumen (p.e. iLBC). El ranking de consumo de los codecs obtenido es extrapolable a cualquier dispositivo ya que dependen principalmente de la complejidad algorítmica de cada codec. Por ello, pensamos que el perfil energético de cada codec debería ser tenido en cuenta en el futuro junto con otros factores como el ancho de banda o la calidad.

En el futuro pretendemos realizar un estudio con un modelo energético mas complejo que incluya medidas de campo de otros componentes como la memoria y tarjetas radio así como realizar un algoritmo de selección de codec que incluya su perfil energético como un factor mas, junto al consumo de ancho de banda o la calidad.

[9]Aunque existen claras diferencias en el patrón de tráfico que generaría cada codec, en general la tarjeta radio va a estar el 98% del tiempo ociosa con lo que tales diferencias apenas se sustancian en diferencias de consumo energético

AGRADECIMIENTOS

Esta investigación ha sido financiada parcialmente por los proyectos TEC2010-20861 y TIC-6339, del Ministerio de Ciencia e Innovación y la Junta de Andalucía respectivamente.

REFERENCIAS

[1] "eespaña 2011 ,informe anual sobre el desarrollo de la sociedad de la información en españa." Fundacion Orange, Recommendation G.729, January 2011. [Online]. Available: http://www.informeeespana.es/docs/eE2011.pdf

[2] D. W. MA Viredaz, "Power evaluation of a handheld computer," in *IEEE Micro*, 2003, pp. 66–74.

[3] V. Raghunathan, T. Pering, R. Want, A. Nguyen, and P. Jensen, "Experience with a low power wireless mobile computing platform," in *ISLPED '04: Proceedings of the 2004 international symposium on Low power electronics and design*. New York, NY, USA: ACM, 2004, pp. 363–368.

[4] T. Shiao-Li and H. Chung-Huei, "A survey of energy efficient mac protocols for ieee 802.11 wlan," *Computer Communications*, vol. 34, no. 1, pp. 54 – 67, 2011.

[5] V. Namboodiri and L. Gao, "Towards energy efficient voip over wireless lans," in *MobiHoc '08: Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*. New York, NY, USA: ACM, 2008, pp. 169–178.

[6] A. J. Estepa, J. M. Vozmediano, J. López, and R. M. Estepa, "Impact of voip codecs on the energy consumption of portable devices," in *Proceedings of the 6th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, ser. PM2HW2N '11. New York, NY, USA: ACM, 2011, pp. 123–130. [Online]. Available: http://doi.acm.org/10.1145/2069087.2069104

[7] H. Schulzrinne and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control," RFC 3551 (Standard), Internet Engineering Task Force, Jul. 2003, updated by RFC 5761. [Online]. Available: http://www.ietf.org/rfc/rfc3551.txt

[8] "Pulse code modulation (pcm) of voice frequencies," ITU-T, Recommendation G.711, November 1988. [Online]. Available: http://www.itu.int/rec/T-REC-G.711-198811-I/en

[9] "Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s," ITU-T, Recommendation G.723.1, May 2006. [Online]. Available: http://www.itu.int/rec/T-REC-G.723.1-200605-I/en

[10] "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (cs-acelp)," ITU-T, Recommendation G.729, January 2007. [Online]. Available: http://www.itu.int/rec/T-REC-G.729-200701-I/en

[11] S. Andersen, H. Astrom, R. Hagen, R. Hagen, W. Kleijn, and J. Linden, "Adaptative multi-rate speech codec; c-source code," ETSI, Recommendation TS 126 073, December 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/26073.htm

[12] S. Andersen, A. Duric, H. Astrom, R. Hagen, W. Kleijn, and J. Linden, "Internet low bit rate codec (ilbc)," IETF, Recommendation RFC 3951, December 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3951.txt

[13] A. Canavan, D. Graff, and G. Zipperlen, "Callhome american english speech," in *LDC97S42*, ser. Linguistic Data Consortium, 1997.

Energy and carbon emissions aware services allocation with delay for Data Centers

Bernat Guillén*, Xavier Hesselbach*, Xavier Muñoz*, Sonja Klingert†
*Telematics Engineering Department
Universitat Politecnica de Catalunya
C/Jordi Girona, 1 i 3 Modul C3 - Campus Nord
08034 Barcelona
†Software Engineering Group
University of Mannheim
A5,6 Building B
D-68131 Mannheim

***Abstract*—This paper presents a new approach to service assignment in Data Centers (DC), relating it to a classical combinatory problem called Bin Packing Problem and adding the possibility of delay and collaboration with users and energy providers. This possibility proves to reduce in much the energy consumption of the DC as well as the CO_2 emissions.**

***Keywords*—virtualization, energy savings, carbon emissions, Data Centers, allocation**

I. INTRODUCTION

Electricity consumed in Data Centers (DC), air cooling devices (AC) and uninterruptable power supply systems (UPS), is foreseen as a major contributor to the electricity consumed in the commercial sector in the near future, especially with the cloud computing trend still on the rise .

The project All4Green analyses the relationship between the IT Customer (ITC) and DC (DC) or DC federation in conjunction with the relationship between the different parts of the DC seeking a hollistic way of improving energetical efficiency and CO_2 emissions.

Instead of focusing on the energy optimization of single ITC elements, or subsets of the ITC elements making up a data center, this paper broadens the scope of energy savings to the full ecosystem in which data centers operate, fostering collaboration between all entities in this ecosystem with the common goal of saving energy and emissions through special contracts between them, following the work in [1], [2] and [3].

With the proposed technology, energy savings generated in the data center through the new relation with ITC users are magnified at the very source of the electricity transformation process through the coordinated collaboration of all the actors inside the ecosystem.

This collaboration is not only beneficial for the environment, but also economically sustainable, and therefore not limited to customers with a strong green/ecological conscience.

The main benefits of the envisioned ecosystems results from the interplay between data centers and energy providers. On the one hand, data centers, as important customers of energy providers, can have a great impact on the emergence and avoidance of energy usage peaks, and on the other hand, energy providers can reduce the impact of such peaks by using the optimal balance of energy sources based on their flexibility and CO2 emissions, including renewable energy sources like solar or wind, which have traditionally been difficult to be fully integrated into the electricity grid due to their long-term unpredictability.

The european FP7 All4Green project addresses this problem by coordinating energy supply and demand by encouraging extensive collaboration between energy providers and data centers as major energy consumers.

II. FORMULATION OF THE PROBLEM

Giving a whole mathematical model of a DC and the processes that take place in it is an enormous task and it can mislead to unprofitable results. Therefore, some hypothesis must be made when modelling the DC in order to simplify the problem, while not losing information about itself.

The EP has a contract with the DC called Green Supply Demand Agreement or GreenSDA. In this contract there are "green clauses" such as:

- Maximum amount of power consumption reduction per request $\beta_{max} < 1$, e.g. $\beta_{max} = 0.1$ implies that the EP can ask a reduction in the power consumed of maximum 10% (it must be specified if it is with respect to the hired power or to the previously used power).
- Maximum number of energy consumption reduction requests per month.
- Rate of CO_2 emissions prediction.

Plus the "regular clauses", e.g.:

- Maximum power hired P_h.

These are the clauses important to this paper. For example, the DC will always have a prediction in the CO_2 emission factor for the next hour given by the EP, namely $CEF(i)$ (Carbon Emissions Factor in the slot i). The EP will also provide $\beta(i)$, i.e. the reduction in power consumption requested in the slot i.

The DC network forms a graph V, each of its elements being a server. The set of all the users is $\mathcal{U}$ and the set of all possible services is $\mathcal{S}$. The set of all possible pairs user-service (allowed by each user's contract) is $\mathcal{D} \subseteq \mathcal{U} \times \mathcal{S}$.

At the same time, the ITC has a contract with the DC called Green Service Level Agreement, or GreenSLA. In this

contract there are regular clauses (QoS, price per service, etc.) as in a regular SLA and "green clauses":

- Agreeded possible reduction in the QoS time-depending (for example, reducing the availability of a web server in weekends) and reward.
- Agreeded possible reduction in the QoS state-depending (for example, reducing the availability of a web server if the DC is in "Energy Saving State") and reward.
- Agreeded possible reduction in the QoS after negotiations, meaning that the DC can negotiate with the ITC for a reduction in some special moments (for example, if the EP has asked a reduction in the energy consumption) and reward/penalty.
- Agreeded maximum amount of times per month a DC can negotiate with an ITC for a reduction in the QoS.
- Agreeded maximum amount of times per month a DC can delay or pause the execution of a service or VM for an ITC u: $d_{max}(u)$.
- Agreeded maximum amount of delays a user can suffer given a particular state of the DC or moment, according to the GreenSLA, e.g. "Every weekend or when the DC is in Energy Saving State the user can see at most two of his services' executions delayed": $d_{max}(u, i)$

Each service in $\mathcal{D}$ will consume an instantaneous amount of CPU workload, memory usage and hard drive space. However, it will be summarized as a percentage of "computer usage" averaged through a "time slot": $0 < a_{(u,s)}(\Delta t) \leq 1$ is this average of the relative workload (relative to using 100% of a server) during Δt. Each service will also have assigned a duration: The number of slots that it will be consuming. This duration: $0 < n_{(u,s)}(\Delta t)$ will be also known in the offline version of the problem. From now on Δt will not be mentioned in the "workload" charge or the duration for conciseness.

A server that is online but idle will consume power, namely P_{idle}, and a server at maximum utilization will consume P_{MAX}. Moreover, the air conditioning (AC) consumes P_{AC}. A service consuming $a_{(u,s)}$ "workload" will give an energy consumption given by Eq. 1 in Δt time.

$$E_{service}(u, s) = (P_{MAX} - P_{idle})a_{(u,s)}\Delta t \quad (1)$$

The DC can choose between two actions regarding the execution of a service:

- Run the service instantaneously.
- Pause or delay the execution of the service.

The objective is to choose the one that will result in less energy consumed and CO_2 emitted overall, i.e. at the end of the month/year.

A few more assumptions must be made from services:

- A service will always use less or equal than a server (no redundancy). Otherwise, the heuristics proposed would not change significantly but the analysis of the algorithm would increase in complexity.
- Even in the online version, it will be known (or at least estimated) whether the service execution will end in the following two slots or not.

Finally, it is assumed that the consolidation of the services does not consume any extra energy, and the equation for calculating the Temperature in the room in the slot i can be seen in Eq. 2

$$T(i) = GT(i-1) + c_1(P_{servers}(i)) - c_2 P_{AC}(i) \quad (2)$$

The terms in Eq. 2 are defined as follows.

$T(i)$ is the temperature in the slot i, i.e. $t_0 + i\Delta t$, G is a constant dependent on the geometry of the room, c_j are constants dependent on the temperature in the past, i.e. $c_j(T(i-1))$, that relate the power consumption of the servers and AC to a change in heat. This parameters should be estimated by the DC. $P_{servers}(i)$ is the power consumed by the servers in the slot i, that means, summing the power consumed by the idle servers and all the power consumed by the running services. $P_{AC}(i)$ is the power consumed by the AC in the slot i. The temperature can only vary between T_{min} and T_{max} given by the hardware specifications, and only in increments of ΔT_{max}. Thus, the current temperature is related to the temperature in the past (which involves $P_{AC}(i-1)$), to the servers currently working and to the power spent in the AC. This model is academical, and shall be changed by the DC, but it serves for illustrating the restrictions in minimum power spent in AC. Furthermore, it reflects the fact that spending more power in the AC now can save power in the future, therefore reducing the carbon emissions.

The model of the temperature might as well be changed, this is only a simple version for academic purpose only.

A summary of the parameters involved in this paper can be seen in Table I.

Table I
PARAMETERS INVOLVED IN THE ALL4GREEN SYSTEM

Parameter	Defined by	Constraints
P_{idle}	Hardware	
P_{MAX}	Hardware	
Δt	Design	
P_{AC}	Variable	Temperature and power limits
G	Geometry	Used in temperature calculation
$CEF(i)$	GreenSDA / EP	
P_h	GreenSDA	
β_{max}	GreensDA	
$\beta(i)$	EP	
$d_{max}(u)$	GreenSLA	GreenSLA
$d_{max}(u, i)$	GreenSLA / DC state	
$a_{(u,s)}$	Hardware / Design	≤ 1
T_{min}/T_{max}	Hardware	
ΔT_{max}	Hardware	

III. ONLINE DECISION PROBLEMS

An optimization problem Q is [4] a 4-tuple $\langle I_Q, S_Q, f_Q, opt_Q \rangle$ where I_Q is the set of input instances, S_Q gives a set of feasible solutions for every input instance in I_Q, f_Q is a real-valued function of every instance in I_Q and $opt_Q \in \{max_Q, min_Q\}$ indicates if we want to maximize or minimize f_Q. A decision problem is a special kind of optimization problem where f_Q only has two values (namely "yes" or "no"). A decision problem can be derivated from an optimization problem asking the question: "Is there any solution $y \in S_Q(x)$ $x \in I_Q$ such that $f_Q(x, y)$ is smaller or greater (depending on opt_Q) than C?".

The NP-completeness theory studies decision problems and their tractability. A problem is said to be in the class P if there is an algorithm that solves it in polynomial time, and

in class NP if there is an algorithm that "checks a solution" in polinomial time (for further definitions, see [4]). It is not known, but it is a general belief, that some problems that are in NP are not in P. This belief is due to the fact that many problems can easily be shown to be in NP but until now there has been no way to see if they are in P, i.e. no polynomial time algorithm has been made that solves them.

Some NP problems admit algorithms that find approximate solutions to them (find $(1+\epsilon)OPT$ instead of OPT, in a worst-case situation) or asymptotically approximate solutions, i.e. they find $(1+\epsilon)OPT$ when OPT is big enough, in a worst-case situation.

An online decision problem is a decision problem in which we do not know the whole I_Q but it is updated in real time (see [5]). If $x \in I_Q, x = \{constraints, data\}$, we could say that in the online version of the problem the constraints change in time and data is added and removed systematically. Therefore, an algorithm that solves the online version of a problem will make the decision based only in the data received until that moment and the current constraints. There is a very important concept related to online decision problems: The competitive ratio. For $x \in I_Q$ let $OPT(x)$ be the offline optimal solution of a problem, that is if all the data was known at the beginning. Let $A(x)$ be the output of the algorithm that tries to solve the online problem for that data. Then (Eq. 3), the competitive ratio is the worst-case relation between the offline optimal solution and the solution given by the online algorithm.

$$c(A) = sup_{x \in I_Q} \frac{A(x)}{OPT(x)} \tag{3}$$

Here, worst-case is the keyword. There is another way of analyzing the outcome of the algorithms (offline or online) in an average situation [6], but it requires further probabilistic and statistic study (compared to the combinatoric approach of a worst-case study). However, some problems that appear to be very hard and have very bad boundaries on the worst-case scenario, might admit an algorithm that will give the optimal solution in an average scenario.

IV. BIN PACKING PROBLEM AND VARIATIONS

A very famous NP-hard [4, p. 210] problem is the so-called Bin Packing Problem (BPP). Using the formal definition, the problem is formulated as:

- I_Q: the set of tuples $\alpha =< s_1, \ldots, s_n; T >\in I_Q$, with $s_i \leq T \forall i$
- $S_Q(\alpha)$: the set of partitions ("packings") $Y = (B_1, \ldots, B_r)$ of $\{s_1, \ldots, s_n\}$ such that $\sum_{s_i \in B_j} s_i \leq T$ for all j
- $f_Q(\alpha, Y)$: the number of subsets ("packs") in the partition Y of α.
- $opt_Q = min$

The items s_i are the items that we pack in bins of size B. Our objective is to minimize the number of bins used (or the total waste in the used bins). This problem has been used many times to model scheduling problems, and it seems to fit quite well as will be shown in the next section. The problem has many variations and a short introduction to them is needed because one of them will be key for the development of the model.

This problem doesn't admit any approximation schemes, in fact the best polynomial time algorithm that approaches this problem can not guarantee a solution better than 1.5 times the optimal.

The first algorithm that tried to solve the problem is called First-Fit: for each s_i from $i = 1$ to n, put the item s_i in the first bin it fits. This is not a very good algorithm (its approximation ratio is 2) but if we first order the items from biggest to smallest we have the First-Fit-Decreasing algorithm.

The First-Fit-Decreasing (FFD) algorithm has a worst-case performance of $1.22 \cdot OPT + 4$ and runs in $O(n^2)$. It can be shown that there is an assymptotic fully polynomial time approximation scheme to the Bin Packing Problem, however, an average case analysis [7] of the problem shows that the FFD algorithm's expected waste is assymptotically the same as the optimal algorithm's expected waste.

The online version of the Bin Packing Problem forbids the use of algorithms such as FFD, due to the impossibility of ordering the items before packing. Some algorithms have been developed to solve the online problem (or the offline problem without the possibility of reordering items). An exhaustive survey can be found in [8].

Some interesting variants of the BPP are:

- Dynamic BPP. It is an online version of the BPP in which the items not only arrive but also depart. In this one, no item can be moved after it is placed.
- Fully Dynamic BPP. It is a dynamic BPP in which the items can be replaced. An efficient and fast algorithm for this problem can be found in [9].
- BPP with variable cost. In this variant there are different bins with different costs (all of them have the same size). Putting an element in a bin can be more expensive than opening a new bin of another kind.

V. MATHEMATICAL MODEL OF THE PROBLEM

The objective is to minimize the total energy consumption and CO_2 emissions in a period of time. It can be a day or a month, let it be called T. This period will be divided in slots Δt. It would be more precise to divide it into many slots, but for the sake of simplicity only two are being observed at each moment: The present slot and the immediately next. This is also justified in the online version: The further in time one observes, the less information one has. Therefore taking into account "only" the present and the immediate future is rigorous enough. However, one must notice that the future acts in this case as a trend, i.e. if $CEF(i+1) > CEF(i)$ one must assume that the future will tend to be more expensive than the present. For this reason, some variables are defined in a "smart" way. The variables used are:

- A binary variable $\delta_v^{(u,s)}(i) \in \{0,1\}$ indicating whether the service (u,s) has been assigned to the server $v \in V$ (in the slot i) or not.
- $O_v(i) \in \{0,1\}$, with $v \in V$ is a binary variable indicating whether the server v has a service assigned in the slot i (1) or not (0).
- A binary variable $d^{(u,s)}(i)$ indicating whether the service (u,s) is delayed or not in the slot i.
- A variable $d^u(i)$ indicating how many times a user has suffered a delay or pause of a service during a long period of time (e.g. a month)

- The power used by the AC: $P_{AC}(i)$.
- For conciseness, $P_0 = P_{MAX} - P_{idle}$
- The set of all services that are working in the slot i is $W(i) \subset D$. The set of all services delayed/paused in the slot i is $P(i) \subset D$. The set of all "active" services is $A(i) = W(i) \cup P(i)$.

The energy consumed during the slot i by the server v can be expressed as seen in Eq. 4

$$\frac{E_v(i)}{\Delta t} = P_{idle} O_v(i) + P_0 \sum_{(u,s)\in W(i)} \delta_v^{(u,s)}(i) a_{(u,s)} \quad (4)$$

The energy consumed by the DC during the slot i is modelled as seen in Eq. 5

$$E(i) = \sum_{v\in V} E_v(i) + \Delta t P_{AC}(i) \quad (5)$$

The final objective is to minimize the energy consumption throughout a given time starting at slot i (for example a month), namely $N\Delta t$, where each slot will be weighted by the $CEF(i)$ and a design weighting factor $\alpha(j)$. The function to minimize is seen in Eq. 6.

$$f_0 : \sum_{j=0}^{N} \alpha(j) CEF(i+j) E(i+j) \quad (6)$$

The restrictions are written in the following equations. Eq. 7 refers to the maximum workload of a server (it can not exceed 100%). Eq. 8 refers to the natural impossibility of running the same service more than once. Eq. 9 and Eq. 10 refer to the restrictions in temperature (see Eq. 2).

$$\sum_{(u,s)\in W(i)} \delta_v^{(u,s)}(i) a_{(u,s)} \leq O_v(i) \; \forall v \in V \quad (7)$$

$$d^{(u,s)}(i) + \sum_{v\in V} \delta_v^{(u,s)}(i) = 1 \; \forall (u,s) \in A(i) \quad (8)$$

$$T_{min} \leq T(i) \leq T_{max} \quad (9)$$

$$T(i) - T(i-1) \leq \Delta T_{max} \quad (10)$$

More restrictions involving delays and power limits follow in Eq. 11, Eq. 12 and Eq. 13, and Eq. 14 restricts the number of consecutive delays of a service (it is written as an example, the number of consecutive allowed delays will be left to designers).

$$\sum_{\{s:(u,s)\in A(i)\}} d^{(u,s)}(i) + d^u(i) \leq d_{max}(u) \quad (11)$$

$$\sum_{\{s:(u,s)\in A(i)\}} d^{(u,s)}(i) \leq d_{max}(u,i) \quad (12)$$

$$\frac{E(i)}{\Delta t} \leq \beta(i) P_h \quad (13)$$

$$d^{(u,s)}(i-1) + d^{(u,s)}(i) \leq 1 \quad (14)$$

As has been said in the beginning of the section, $\alpha(j) = 0 \, \forall j > 1$, i.e. the model will only consider two slots (present and immediate future). It is very important to remark that the action of delaying can only take place in the slot i, otherwise it will always be better to delay or pause a service in the slot $i+1$ and the solution would not make sense.

In this sense, the approach is already a bit "online", the immediate future is relevant because the model needs to know whether $CEF(i+1) > CEF(i)$ or not, or if there is any service about to end in the slot $i+1$, but it should be blind to what services requests will come in the slot $i+1$.

Now, a simple set of manipulations of Eq. 6 will allow this problem to be understood as a more complex version of the Bin Packing Problem. First of all, notice that the Energy Consumption due to the services executed is a constant once the delayed services are chosen (Eq. 15). Moreover, the delayed services plus the working services are the total amount of services. Notice also that a service $a_{(u,s)}$ is in $P(i)$ if and only if $d^{(u,s)}(i) = 1$ (Eq. 16).

$$\sum_{v\in V} \sum_{(u,s)\in A(i)} \delta_v^{(u,s)}(i) a_{(u,s)} = \sum_{(u,s)\in W(i)} a_{(u,s)} \quad (15)$$

$$\sum_{v\in V} \sum_{(u,s)\in A(i)} \delta_v^{(u,s)}(i) a_{(u,s)} + \\ + \sum_{(u,s)\in A(i)} d^{(u,s)}(i) a_{(u,s)} = \sum_{(u,s)\in A(i)} a_{(u,s)} \quad (16)$$

Thus, defining P_d as in Eq. 17 we can change Eq. 5 and re-write it as in Eq. 18, because when optimizing the constant factors can be eliminated, but remembering that we have to add the delayed services back in $E(i+1)$ as seen in Eq. 19.

$$P_d(i) = P_0 \sum_{(u,s)\in A(i)} d^{(u,s)}(i) a_{u,s} \quad (17)$$

$$\frac{E'(i)}{\Delta t} = P_{idle} \sum_{v\in V} O_v(i) - P_d(i) + \Delta t P_{AC}(i) \quad (18)$$

$$\frac{E'(i+1)}{\Delta t} = P_{idle} \sum_{v\in V} O_v(i+1) + P_d(i) + \Delta t P_{AC}(i+1) \quad (19)$$

Writing f_0 this way, one can easily see that if there were no P_{AC}, no delaying and no variable cost the problem is exactly the same as a Bin Packing Problem (dynamic). The final f_0 obtained from these formulas and normalizing by $CEF(i)\alpha(0)$ would be Eq. 20.

$$f_0 : \; E'(i) + \alpha(1) \frac{CEF(i+1)}{CEF(i)} E'(i+1) \quad (20)$$

Regarding P_{AC}, clearly only three restrictions affect its value. On the one hand, the power limit (Eq. 13) limits the maximum power that can be spent in $P_{AC}(i)$ given the power spent on the servers. On the other hand, the temperature restrictions (Eqs. 9 and 10) limit the minimum power that can be spent in $P_{AC}(i)$ in order to keep the temperature between some limits.

If the approach were to be hollistic the problem faced would be treated as a Mixed Integer Programming (MIP) problem. These problems tend to be very complex and unpractical.

However, this particular problem requires further study to see to what extent it requires MIP techniques.

First of all, notice that objective is to minimize the total energy consumption and therefore, it is to be expected that Eq. 13 is accomplished always, and if it does not follow, the heuristical approach will try to solve it. The only way to not being able to accomplish Eq. 13 is either by not delaying any

service and having a too "narrow" request from the EP in the slot i, or delaying too many services and having this request in the slot $i+1$. Nevertheless if there is a narrow request from the EP in the slot i or $i+1$, it is reasonable to expect high values of $CEF(i)$ or $CEF(i+1)$, respectively, thus being improbable that many services will be not delayed or will be delayed, respectively. The point is that the problem formulation and heuristics themselves should avoid solutions in which Eq. 13 does not follow.

Moreover, let Q' be a similar problem, with neither the restrictions that affect P_{AC} nor the requirement to minimize P_{AC}, i.e. the only problem is assigning services to servers (BPP). Let $E'(i)$ and $E'(i+1)$ be as in Eq. 18 and Eq. 19 without the P_{AC} term. Let Y'^* be the optimal assignment for Q', with $E'^*(i)$ and $E'^*(i+1)$ the energy consumption of this assignment. Let Q'' be another problem where the services are already assigned with the assignment Y^* and the only thing left to do is select P_{AC} *with* the restrictions. This is a Linear Programming Problem and can be solved with many methods. Let P''^*_{AC} be the optimal solution (as a vector $(P''^*_{AC}(i), P''^*_{AC}(i+1))$) to Q''. Notice that it might not exist if we take into account the power consumption restriction, but as explained in the previous paragraph we will assume that there is a feasible solution. With this assumptions, and using Linear Programming, one can see that two possible solutions for P_{AC} can exist. Either $P_{AC}(i+1) = 0$ and $T(i) < T_{MAX}$ or both $T(i)$ and $T(i+1)$ are equal to T_{MAX}. Let $f'_0(Y'^*)$ be the value of f_0 with the assignment Y'^* and the AC power at P''^*_{AC} The question is, is Y'^*, P''^*_{AC} the optimal solution to the original problem? The answer is: Not necessarily. However, studying the problem and the possible perturbations of the global optimum with respect to the "local" optimum (optimum for Q' and Q'') leads to many conditions and ideas for the heuristic solutions.

One can distinguish two major situations, between many others:

- $CEF(i) \geq \alpha(1)CEF(i+1)$: Apparently the best solution is to delay as many services as possible. However, sometimes not delaying can be better (in terms of P_{AC} if, for example, it implies using less servers. Moreover, using less servers might change the strategy of AC usage.
- $CEF(i) < \alpha(1)CEF(i+1)$: The inverse situation takes place. Again, the best solution is not always that which does not delay any service.

The heuristics proposed should take into account these and more different conclusions that can be reached from simple manipulation of the equations. In the next section the necessary conditions will reveal and be used in one or several heuristics, in order to give boundaries or at least a taste of what the competitive ratio of the algorithms would be.

VI. RESULTS

The heuristics proposed will approach the problem in three phases:

1) Decide which services will be delayed and which are not going to be delayed.
2) Assign the services to the servers.
3) Decide the power used by the AC.

These phases might be mixed and repeated more than once (for example, once for each service) or done separately for each group of services. This separation of tasks allows a different approach for each part, and the reuse of several techniques, specially in the second phase (assigning services), where classical techniques for the BPP can be used.

Special care must be taken with three situations:

1) Services that are about to finish. Each heuristic will treat this situation differently.
2) Deciding whether to consolidate or not (if no continuous migration can be made). The choice will be made according to some parameters, independently of the three other phases.
3) Facing power shortages, thus forcing the system to delay more services.

The heuristics here proposed will be explained following a structure. First, the heuristic will be summarized and then explained in detail. Second, a "bad-case" scenario will be explained to illustrate the problems of the heuristic. Third, a more general explanation covering some aspects of the whole problem will be given.

The first heuristic H_1 proposed is a very naive heuristic that acts like a switch. It works as following:

1) Delaying: If $CEF(i+1)\alpha(1) < CEF(i)$ delay all services that can be delayed. Otherwise, don't delay any service.
2) If even then Eq. 13 is not achieved, reject the request from the EP to lower the energy consumption.
3) Assigning processes: Each slot acts as an independent BPP problem. If migration of the services is allowed, use the algorithm provided by [9]. Otherwise use another online BPP algorithm, Best Fit or a Harmonic Algorithm being the most recommended.
4) P_{AC}: Solve the Linear Programming (LP) problem $min\ P_{AC}(i) + \frac{C(i+1)\alpha(i)}{C(i)} P_{AC}(i+1)$ with the restrictions Eq. 9, 10, 13.
5) If there is no feasible solution, first try to consolidate with a FFD algorithm. If there still is no feasible solution do the opposite and start again.
6) If even then there is no feasible solution, try to consolidate with a FFD algorithm. If it still does not work, reject the request from the EP to lower the energy consumption.
7) If migration is not always allowed and is not imposed by an external agent, decide to consolidate when a certain threshold of servers have less than 50% usage. Recollocate the services in this servers using a First Fit Decreasing algorithm.

H_1 is one of the most simple heuristics that can be thought of. However, simple as it is it may not deliver an optimal solution in many cases. For example, let $C(i+1)\alpha(1) = C(i)$. Imagine the following situation: In the slot i there are N servers full, however N services with sizes $(\frac{1}{2} + \epsilon)$ arrive. In the slot $i+1$, N services with sizes $(\frac{1}{2} + \epsilon)$ that are already in the N servers will end. If H_1 is followed, and migration is not allowed, a total of $4N$ servers will be used: $2N$ in the slot i (N were used and N more are required for the new services) and $2N$ in the slot $i+1$ (although if migration was allowed only N servers would be used). However, the

optimal solution would only use $2N$ servers in total, delaying the incoming services. As can be trivially deduced, this means that $sup_I \frac{H_1(I)}{OPT(I)}$ is at least 2 if no migration is allowed, and 1.5 if it is allowed.

Even more, during the course of the long period (month, week, etc.) it is very likely that the delays of the users are depleted long before the end of the term. This means that at some point no service will be able to be delayed and therefore the problem will turn to a Dynamic BPP. For example, a user demands a service a (that only lasts 1 slot) $2d^u_{max}$ times and always when $CEF(i+1)\alpha(1) < CEF(i)$. The first d^u_{max} times it is delayed, although it could fit in a server in the slot i but requires to open a new server in the slot $i+1$. After the third time it is the opposite way: If it was delayed it would consume less and need no new server, but not being delayed it requires to open a new server only for this service. In Eq. 21 can be seen the ratio between the solution proposed by H_1 and the optimal (note: $C(i+1) = \frac{CEF(i+1)\alpha(1)}{CEF(i)}$ and P_0 is $P_{MAX} - P_{idle}$). Again, this ratio is $\frac{3}{2}$ in the worst case($C(i+1) = 1$) so we can say that the competitive ratio is at least 1.5.

$$\frac{3P_{idle} - aP_0 + C(i+1)(3P_{idle} + aP_0)}{2P_{idle} - aP_0 + C(i+1)(2P_{idle} + aP_0)} \tag{21}$$

Finally, if the algorithm chooses "delay" and by any chance a user has more services at one moment working than those that can be delayed, delaying the biggest ones seems to be the most reasonable option, arguments similar to those that prove that FFD is better than FF would apply.

The second heuristic H_2 is more dynamical as it checks service by service whether it is better to delay or not. The procedure is different according to whether it is possible to migrate services or not.

1) List all the services that can be delayed.
2) If migrating services is not possible:
   a) Put in the first place the services that are already working (those that would be paused).
   b) For each of these services, check whether it is cheaper to leave them where they are or pausing them (if they can be paused, taking into account if another service from the same user has been paused yet). Do not count as power consuming those processes that have not been assigned yet. For example, if two services can be paused, when the first one is chosen to be delayed or not it won't take into account where the second service is. However the seccond will take into account where the first one has been put.
3) After this, or if migrating services is possible, for each service remaining, check whether it is cheaper to put it in the slot i or the slot $i+1$.
4) If a service is to be assigned, except for the particular case of the services that must remain in the same place, proceed as in the Dynamic Bin Packing Problem algorithm chosen or the Fully Dynamic BPP (depending on whether migration is allowed or not).
5) After having assigned the services, decide P_{AC} as in H_1.
6) If, after all the solution is not feasible (Eq. 13 can not follow) try to consolidate. If it still does not work, see if it is the slot i or $i+1$ that break the condition. Starting from the biggest service, change $d^{(u,s)} \leftarrow 1 - d^{(u,s)}$ and update P_{AC} until the condition follows. If there is no way to achieve it, reject the request from the EP.
7) Consolidation works as in H_1.

This algorithm is more complex and looks better. First of all, it is easy to check that the problems mentioned above for H_1 will not affect H_2. It is less probable that Eq. 13 does not follow. However, it is not perfect, and it has similar problems to the offline algorithm First Fit. The order matters. For example, if $C(i+1) < 1$, imagine there are N servers with $\epsilon < \frac{1}{2}$ space. Then $2N$ services arrive that will only last 1 slot. The first N have size ϵ, the other $1-\epsilon$. The servers are going to be all free in the slot $i+1$. For the first N services, H_2 decides to place them now, if a condition on $C(i+1)$ holds: $C(i+1) > \frac{1}{\frac{P_{idle}}{\epsilon P_0}+1}$ (remember $P_{idle} > P_0$). For the second N services, it is better to put them later. However the optimal solution is to delay them all. In the worst case situation, namely $\epsilon \leftrightarrow \frac{1}{2}$ and $C \leftrightarrow \frac{1}{\frac{P_{idle}}{\epsilon P_0}+1}$, the ratio of the two solutions is the one displayed in Eq. 22. As can be seen, it is smaller than the ratio in H_1 as long as $P_{MAX} < 2P_{idle}$. Notice that in this scenario, H_1 would give a better performance.

$$1 + \frac{\frac{P_{MAX}}{P_{idle}} - 1}{2} \tag{22}$$

It is important to remark that $C(i+1)$ should be an indicator of the trend and therefore sometimes the heuristic might give a solution that is not optimal. For example, choosing not to open a server in the present but open it in the future might seem to be the best option if the service is very small. That is why a small trick will be needed: Counting $O_v(i+1)$ twice if it is not supposed to be closed in the state $i+2$. This avoids the problem and has an explanation, it would be the same as adding $E(i+2)$ to the computation without counting $P_{AC}(i+2)$ nor being able to delay any service yet in the slot $i+1$, thus making everything except whether the server will be on or not a constant. It seems a rather coarse addition but seems the best way to approach the problem.

As for a competitive ratio, until now there has been no way to find a bad case scenario as clear as in H_1. It could happen however, that for example some time it is better to delay and in the future there would come a moment when delaying would help to save even more energy. However, being this totally unknown, any policy possible (dividing $C(i+1)$ in categories, etc.) might lead to bad solutions. Which of them would be the least bad, remains yet an open problem.

Notice that the results in both heuristics depend as well on the performance of the algorithms that assign. However, comparing the outcome of a problem that won't allow delay with this problem gives an idea of the energy and CO_2 emissions that might be saved.

As a final comment, selecting the AC strategy in the end might lead to wrong results: there might be a solution worse in terms of service assignment but better overall. However, some algebra shows that it depends on the coefficients in the temperature calculations as well as $C(i+1)$. For this reason, until the moment no examples of those situation have been found that don't depend on a lot of parameters.

VII. CONCLUSIONS AND FUTURE RESULTS

This paper presents the problem of assigning services to servers aiming to minimize the total energy consumption and relates it to the Bin Packing Problem, presenting a new version of the BPP where delays are allowed. It presents two different fast heuristics that give a solution to the problem and gives some boundaries on the performance of both heuristics.

There are more possibilities but no numerical results on the heuristics commented in this section have been obtained. The natural heuristics that follow the ones explained before are:

1) H_3: Same as H_2 but first ordering from biggest to smallest the processes. The studies made on FF and FFD for the classical BPP suggest that it should improve the performance.
2) H_4: Again following the indications of the classical BPP problem, a classification of the services in size similar to that in the harmonic algorithms could improve the performance.
3) H_{ia}: Similar to H_i, but the AC is calculated in each iteration (it is a direct formula). It seems that it would give a much better answer, however no analysis has been done until now.

Finally, an approach using Genetic Algorithms or Simulated Annealing or another metaheuristic may be very well suited to this problem. As has been explained, sometimes locally worse solutions (in terms of assignment) may lead to globally better solutions when P_{AC} is calculated. The binary natural description of the delayed (or not) services makes a Genetic Algorithm very easy to implement for this purpose.

VIII. ACKNOWLEDGEMENTS

This work has been partially supported by the Spanish Government, MICINN, under research grant TIN2010-20136-C03 and by the European FP7 All4Green project (Grant agreement No. 288674).

REFERENCES

[1] P. Wieder, R. Yahyapour, and W. Ziegler, Eds., *Grids and Service-Oriented Architectures for Service Level Agreements*. Boston, MA: Springer US, 2010.
[2] C. Bunse, S. Klingert, and T. Schulze, "GreenSLAs for the Energy-efficient Management of DCs," *Energy Efficient Data Centers*, vol. 7396, 2012.
[3] S. Klingert, T. Schulze, and C. Bunse, "GreenSLAs for the Energy-efficient Management of DCs." presented in 2nd International Conference on Energy-Efficient Computing and Networking, Columbia University, New York, 2011.
[4] J. Chen, "Introduction to Tractability and Approximability of Optimization problems," *Lecture Notes, Department of Computer Science*, 2002. [Online]. Available: http://faculty.cs.tamu.edu/chen/notes/opt.pdf
[5] A. M. Koster and X. Muoz, *Graphs and Algorithms in Communication Networks: Studies in Broadband, Optical, Wireless and Ad Hoc Networks*, 1st ed. Springer Publishing Company, Incorporated, 2009, ISBN: 978-3-642-02249-4z.
[6] W. Szpankowski, *Average case analysis of algorithms*, 2010.
[7] E. C. Jr, D. Johnson, G. Lueker, and P. Shor, "Probabilistic analysis of packing and related partitioning problems," *Statistical Science*, 1993.
[8] E. G. Coffman, Jr., J. Csirik, and G. J. Woeginger, "Approximate solutions to bin packing problems," WOE-29, INSTITUT FR MATHEMATIK B, TU GRAZ, STEYRERGASSE 30, A-8010, Tech. Rep., 1999.
[9] Z. Ivkovic and E. Lloyd, "Fully dynamic algorithms for bin packing: Being (mostly) myopic helps," *SIAM Journal on Computing*, vol. 28, no. 2, pp. 574–611, 1998.

Familia *All-Path*: Caminos de Mínima Latencia, Escalabilidad y Balanceo de Carga para Redes Ethernet

Elisa Rojas, Guillermo Ibáñez, José Manuel Giménez-Guzmán, Juan A. Carral
Departamento de Automática
Universidad de Alcalá
Escuela Politécnica. Campus universitario. Ctra. Madrid-Barcelona, Km. 33,600
elisa.rojas.sanchez@gmail.com, guillermo.ibanez@uah.es, josem.gimenez@uah.es, juanantonio.carral@uah.es

***Resumen*- El notable crecimiento en los últimos años de Ethernet dada su buena relación calidad/precio y facilidad de configuración, ha originado que esta tecnología se imponga frente a otras en el caso de las redes empresariales, y específicamente de las redes de centros de datos. Este documento presenta un estudio de la familia de protocolos de *bridging* puro *All-Path*, que toma el nombre del hecho de que todos los caminos (*all paths*) en la red se exploran de manera simultánea aprovechando las tramas broadcast que se intercambian los dispositivos finales de la topología. Esta propuesta nace como simplificación de la tendencia actual del uso de protocolos de estado de enlace en encaminamiento, como es el caso de los recientes estándares Shortest Path Bridges (IEEE 802.1aq) y TRILL (IETF) Rbridges, demostrando así que es posible conseguir caminos de mínima latencia y balanceo de carga de una manera mucho más sencilla.**

***Palabras Clave*- Ethernet, Switching, Bridging, Caminos Mínimos, Baja Latencia, Centros de Datos**

I. INTRODUCCIÓN

Las redes de *bridging* o *switching* Ethernet (denominadas así por el uso de puentes transparentes, del inglés *bridge* o *switch*, como dispositivos de encaminamiento en la red) ofrecen importantes ventajas de coste y rendimiento para redes de pequeño y mediano tamaño, en las que se incluyen las redes empresariales y de centros de datos, además de gran compatibilidad y configuración más sencilla que el uso de redes *routing*, bajo IP. Sin embargo, Shortest Path Bridging (SPB) [1] y los RBridges de TRILL [2], actuales propuestas para superar las limitaciones del protocolo de árbol expandido (STP/RSTP) [3], recientemente estandarizadas, basan su funcionamiento en la utilización de protocolos de estado de enlace en el encaminamiento tal y como se procede en capa 3, lo que provoca que los puentes pierdan parte de su facilidad de configuración y asimismo no garantizan de este modo que el balanceo de carga sea el óptimo, ya que el cálculo de rutas se realiza de manera estática al inicio y no tiene en cuenta el tráfico que se intercambiará en la red [4].

Dada la situación, los mecanismos de exploración de caminos para el cálculo de rutas, que siguen el fundamento base de los puentes transparentes y que sorprendentemente apenas han sido valorados en la comunidad científica, se presentan como la mejor alternativa y ofrecen admirables ventajas: simplicidad, balanceo de carga y caminos de mínima latencia. De este modo comienza el desarrollo de la familia *All-Path*, familia de protocolos basada en la inundación de la red mediante tramas broadcast para calcular así caminos de mínima latencia, teniendo en cuenta el estado de la red en el momento del cálculo y no un mecanismo aleatorio como en el caso de los dos estándares previamente mencionados.

El protocolo ARP-Path es el primero que se desarrolló dentro de la familia. El alto nivel de diversidad de caminos (selección de caminos sensible al nivel de carga en la red) alcanzado por este protocolo produce resultados excelentes tanto en términos de latencia como de rendimiento o *throughput* [5], pero hay ciertos escenarios donde el resultado puede no ser óptimo porque se busca primar el balanceo de carga o la escalabilidad frente a otros parámetros, o porque quizás los patrones de tráfico son muy asimétricos. Para estos casos surgen Flow-Path y Bridge-Path, que completan la familia junto a ARP-Path, y que pretenden aportar la posibilidad de ajuste fino de la red en base a ciertos parámetros y conservando las características principales de caminos de baja latencia y configuración sencilla o nula.

A continuación se presenta esta familia y cómo considerar el uso de uno u otro protocolo según los requerimientos de la red o del proveedor, del tipo de topología y del tipo de tráfico. Para ello, en el apartado II se describe cada protocolo y las diferencias entre ellos, en el apartado III se formula teóricamente el balanceo de carga y la escalabilidad de cada uno y en el apartado IV se realiza un breve análisis práctico con un par de topologías sencillas. Finalmente el apartado V contiene las conclusiones.

II. FAMILIA ALL-PATH

Para comprender el funcionamiento de la familia All-Path es necesario conocer primero el protocolo ARP-Path [5], dado que es el que inició la familia y cuyo funcionamiento base es aplicable al resto de protocolos. ARP-Path obtiene su nombre del protocolo de resolución de direcciones ARP, invocado en IPv4 de manera previa a toda comunicación entre un par de sistemas finales, del cual aprovecha la necesidad de explorar la red para construir los caminos entre dichos sistemas finales. De esta manera, ARP-Path explora todos los posibles caminos de la red entre el dispositivo origen y el destino, y selecciona el camino de mínima latencia sólo inspeccionando los mensajes del diálogo ARP (mensajes *ARP Request* y *ARP Reply*), sin necesidad de modificarlo, ni cambiar nada de los sistemas finales. Además,

no utiliza información IP, por lo que su equivalente en IPv6, el protocolo *Neighbour Discovery* (NDP) podría ser utilizado de manera análoga para explorar dichos caminos.

A continuación se describe el funcionamiento de ARP-Path. El protocolo Flow-Path se describe en el apartado posterior, el cual sigue pasos similares en la generación de los caminos, pero crea caminos únicos por pares de hosts o por flujo (en inglés *flow*) en lugar de ser compartidos por diferentes sistemas finales, caso de ARP-Path. Y finalmente se describe Bridge-Path, en el que los caminos se crean por cada puente frontera (en inglés *edge bridge*) en la topología, donde se considera que un puente frontera es aquel que no sólo dispone de conexiones con otros puentes en la red, sino también con sistemas finales, de manera que en la práctica se estarán generando caminos para grupos de hosts conectados a un conmutador común.

A. *ARP-Path*

Cuando un sistema origen A quiere comunicarse con otro destino B, A emitirá un *ARP Request* que será respondido por B con un *ARP Reply* que contendrá la dirección MAC de B que solicitaba previamente A.

El primer mensaje es de tipo broadcast, por lo que cuando llega al primer conmutador, en el caso de la Fig. 1 sería el puente 1, éste bloquea, o más correctamente, "asigna un cerrojo" con la dirección origen A al puerto por el cual llega la trama (pasa a estado '*locked*') e inunda el resto de enlaces con el mensaje, difundiéndolo así por toda la red. Este ARP Request entonces alcanzará los puentes 2 y 4, que realizarán la misma acción, que básicamente es apuntar el puerto por el que llegó la trama por primera vez, es decir, la copia de la trama más rápida, y seguir difundiendo el mensaje por la topología. Cuando uno de estos puentes vuelve a recibir otra copia del mismo mensaje por otro puerto, ésta se descarta al considerarse una copia lenta y de esta manera se evitan los bucles y las tormentas de tramas en la red.

Finalmente, una de las copias, la más rápida, alcanzará el destino B y habrá dejado tras de sí una serie de puertos en estado '*locked*' en cada puente, que indicarán un camino para alcanzar el dispositivo A, tal y como se muestra en la Fig. 1. Dichos estados poseen un temporizador que les hará pasar automáticamente a un estado '*learnt*' (aprendido) y que mostrarán el camino generado. El matiz de tener dos estados es que el primero sólo tiene como misión evitar los bucles en la red de los mensajes broadcast, es fijo y de corta duración, mientras que el segundo muestra el camino aprendido, es flexible a futuros aprendizajes y su duración es mayor.

Cuando B responde con el mensaje *ARP Reply*, éste será de tipo unicast y podrá seguir el camino ya explorado previamente y, a la vez, construir un camino hacia B. Para ello, cada puente encamina dicha trama por el puerto asociado al destino A tal y como haría con cualquier trama unicast, pero además asocia el puerto de entrada a la dirección B. La asociación es de estado '*learnt*', puesto que ya no es necesario realizar el cerrojo previo al no haber posibilidad de bucles. Por lo tanto, el conmutador 3 recibiría el mensaje, asociaría el origen B en su puerto de entrada y enviaría el mismo por el puerto asociado al destino A, pasando así por 2 y 1 que realizarían la misma acción, hasta alcanzar A, tal y como se ve en la Fig. 2.

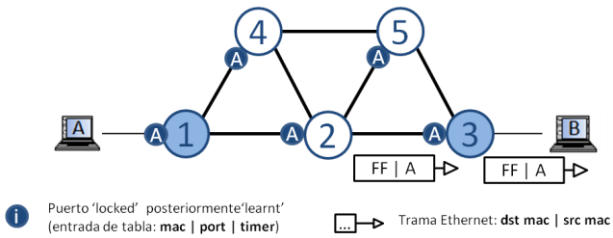


Fig. 1. Aprendizaje del camino hacia A por inspección del mensaje *ARP Request* emitido por A

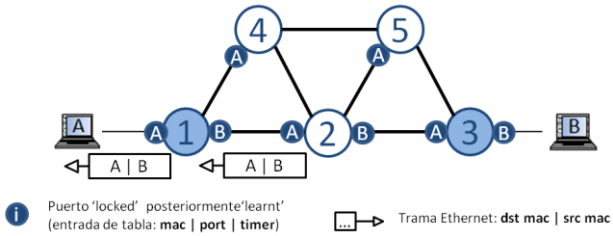


Fig. 2. Aprendizaje del camino hacia B por inspección del mensaje *ARP Reply* emitido por B con destino A

Tras el intercambio de mensajes ARP se inicia la comunicación deseada entre A y B, posible gracias a que existe un camino recientemente generado, que es el compuesto por los puentes 1-2-3. Además, estas entradas pueden ser compartidas entre diversos sistemas finales, es decir, si conectado al puente 3 hubiese otro host C, éste utilizaría el mismo camino para enviar tráfico hacia A que el que usa B.

B. *Flow-Path*

El protocolo Flow-Path sigue la misma filosofía de inspección de los mensajes ARP para construir los caminos, sólo que en este caso no se comparten caminos al ser estos únicos entre pares de hosts.

En la Fig. 3 se observa cómo se crean los cerrojos del flujo en dirección A con el mensaje *ARP Request*. Dado que la dirección B todavía es desconocida, pues es misión del protocolo ARP descubrirla, en Flow-Path se apuntan temporalmente las IPs asociadas a A y B para caracterizar el flujo a la hora de confirmar el camino de vuelta y mientras tanto, se indica la entrada con un 'A?' donde el interrogante indica la dirección B que está por ser descubierta aún.

Tal y como se ve en la Fig. 4, de manera análoga a ARP-Path, el mensaje *ARP Reply* aprende los puertos del camino asociados al flujo en dirección hacia B, denominados 'BA', y confirma a la vez aquellos 'A?' pasándolos a estado aprendido y con valor 'AB', dado que ya se conoce el destino del flujo. Así ya se puede realizar la comunicación entre A y B, que tiene como ruta los puentes 1-2-3.

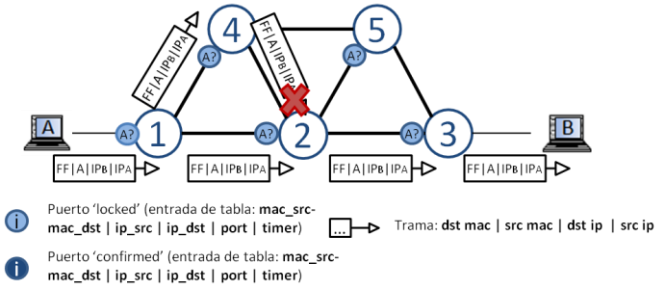


Fig. 3. Aprendizaje del camino hacia A del flujo AB por inspección del mensaje *ARP Request* emitido por A

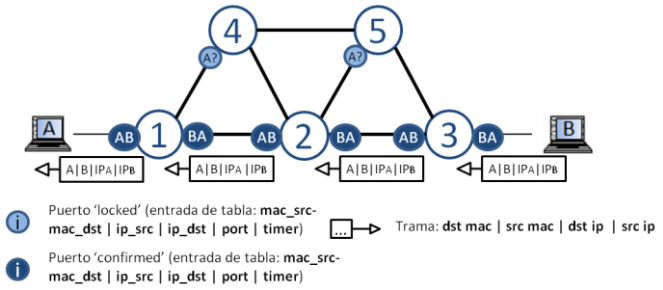


Fig. 4. Aprendizaje del camino hacia B del flujo AB por inspección del mensaje *ARP Reply* emitido por B con destino A

La diferencia con ARP-Path es que si hubiese otro host C conectado al puente 3, éste quizás no utilizaría el mismo camino para enviar tráfico hacia A que el que usa B, es decir, se crearía un camino independiente con entradas denominadas 'AC' y 'CA' y éstas quizás podrían coincidir o no con las ya aprendidas para el flujo entre A y B, según sea la utilización de los enlaces en la red, pues es posible que el nuevo camino de mínima latencia sea distinto.

Por lo tanto, Flow-Path asegura independencia de flujos que puede a su vez garantizar el reparto de tráfico en el caso de que cierto host A intercambie información con más de un destino, pero a cambio también incrementa el tamaño de las tablas de aprendizaje y es posible que las rutas independientes no sean necesarias debido a que el tráfico existente sea bajo, lo que provocaría que se seleccionara el mismo camino de mínima latencia para todos los casos.

C. *Bridge-Path*

El caso del protocolo Bridge-Path es justo el opuesto de Flow-Path, en lugar de crear más caminos independientes para diversificar el tráfico, el objetivo es compartir un mayor número de caminos que ARP-Path al construirse los mismos por puente frontera y no por dispositivo final, de modo que se ahorra en número de entradas de tabla y coste de almacenamiento en la red. Para conseguir esta propuesta sin modificar los mensajes ARP existen actualmente tres alternativas:

- Reutilizar la etiqueta VLAN (ARP-PathV)
- Encapsular la trama con MAC-in-MAC (ARP-PathM)
- Traducir la dirección del host en una jerárquica en la que cierto campo indique la identidad del puente (Path-Moose [6]).

Las dos primeras siguen la filosofía de encapsulamiento de SPBV y SPBM respectivamente [1], mientras que la tercera se basa en el protocolo MOOSE [7].

Para explicar el funcionamiento de Bridge-Path tomaremos el caso concreto de ARP-PathM. Cuando un dispositivo A quiere comunicarse con otro B, el mensaje emitido por el origen (ya sea de tipo ARP o no) se encapsulará en el puente que le sirve con una nueva cabecera Ethernet, que indicará el destino y el origen en formato de MAC o identidad del puente frontera. El resto de puentes actuarán de manera idéntica al protocolo ARP-Path hasta llegar al puente que sirve al destino, que quitará dicha cabecera y entregará el mensaje al destino. Es decir, que la única diferencia está en los puentes frontera y la encapsulación, generando caminos agrupados.

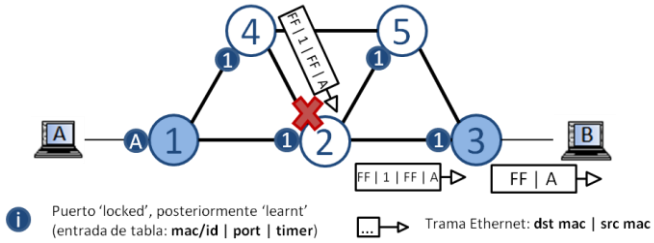


Fig. 5. Aprendizaje del camino hacia el puente 1, frontera de A, por inspección del mensaje *ARP Request* emitido por A

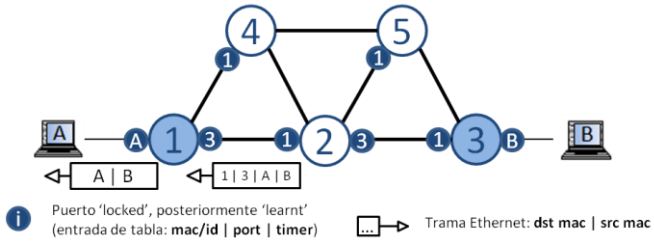


Fig. 6. Aprendizaje del camino hacia el puente 3, frontera de B, por inspección del mensaje *ARP Reply* emitido por B con destino A

En la Fig. 5 y la Fig. 6 está indicado cómo se realiza el aprendizaje en Bridge-Path con los mensajes *ARP Request* y *ARP Reply*, respectivamente. Se puede ver cómo los mensajes broadcast no varían en el encapsulamiento su dirección destino, pero sí la origen, que en la Fig. 5 pasa de ser A a encapsularse con la dirección 1, que puede ser la MAC de su puente frontera o simplemente un identificador del mismo. Mientras que para el caso de los mensajes unicast, ambas direcciones se "traducen" a su puente frontera correspondiente. En la Fig. 6 el host B pasa a ser 3 y el host A, conocido previamente gracias al mensaje *ARP Request*, pasa a ser 1 y el encaminamiento en los conmutadores de la red se realiza en base a dichas identidades aprendidas. Finalmente el *ARP Reply* alcanza el puente 1, que desencapsula el mensaje y se lo entrega al sistema A, no sin antes aprender la asociación "sistema final B conectado a puente frontera 3" para futuras comunicaciones.

En el caso de Bridge-Path, si existiese un host C conectado al puente 3 que se comunicara con A, compartiría el mismo camino de B a A, aquel marcado con las entradas en tablas del puente 1, pero además también lo compartiría en caso de comunicarse con un cuarto sistema D conectado al mismo puente que A. De esta forma los caminos se comparten por grupos de hosts y se garantiza la escalabilidad de la red a cambio de una independencia de caminos menor.

D. *Otros protocolos de la familia All-Path*

La familia *All-Path* dispone de otros protocolos actualmente bajo estudio en el grupo de investigación GIST-Netserv de la Universidad de Alcalá [8] que combinan de diferentes formas esos dos parámetros: escalabilidad y balanceo de carga. Uno de estos protocolos es por ejemplo, ARP-Path*, pero que dejaremos fuera del estudio de este documento.

III. Estudio Teórico de Escalabilidad y Balanceo de Carga

Tras la sección anterior que contenía la descripción de los tres protocolos de la familia *All-Path* a analizar, es fácil ver que Flow-Path posee una capacidad de balanceo de carga

nativa mayor dado que crea diversos caminos diferentes por sistema final, seguido por ARP-Path que genera un camino por host y finalmente Path-Bridge, que de media construye menos de un camino por dispositivo puesto que las rutas se comparten por grupos de hosts. Sin embargo, el coste de almacenamiento es también mucho mayor para Flow-Path, seguido por ARP-Path y el más bajo para Bridge-Path, siendo éste un parámetro crucial para la escalabilidad de la red e inversamente proporcional al anterior. Por consiguiente, en esta sección analizaremos la idoneidad de cada uno de los protocolos para diferentes topologías de manera que se garantice la combinación óptima de balanceo de carga y tamaño de las tablas o escalabilidad de la red.

A. Estudio de balanceo de carga

Aunque de manera intuitiva es fácil suponer que los protocolos de la familia *All-Path* balancean muy adecuadamente la carga, dado que los caminos que se generan son siempre de mínima latencia y esta forma de selección hace que se tienda a escoger los recursos menos utilizados, en la práctica es complicado realizar un estudio analítico del balanceo de carga puesto que son muchos los factores a tener en cuenta, entre ellos el estado de la red en cada momento y el tipo de tráfico. En cualquier caso, de manera empírica se han probado las bondades de ARP-Path en cuanto a balanceo de carga con diferentes simuladores e implementaciones hardware [9], demostrando que efectivamente esta familia de protocolos tiende a utilizar todos los recursos disponibles de la red.

En el caso del análisis del presente documento, tomaremos como referencia de calidad de balanceo de carga el número de caminos independientes teóricos que puede construir cada protocolo, para poder realizar posteriormente una comparativa entre ellos y frente al tamaño de tablas requerido en cada caso.

Así pues, el número de caminos bidireccionales independientes teóricos que pueden crear de media Flow-Path, ARP-Path y Bridge-Path, y que denominaremos P_{FP}, P_{AP} y P_{BP} respectivamente, son:

$$P_{FP} = F_B = H*(H-1)/2 \quad (1)$$

$$P_{AP} = H/2 \quad (2)$$

$$P_{BP} = B_E/2 \quad (3)$$

Siendo F_B: número medio de flujos bidireccionales en la red, H: número medio de hosts o sistemas finales activos, B_E: número medio de puentes frontera activos ($B_E \leq H$, puesto que un puente frontera siempre dispondrá de un grupo de hosts conectados a él). Nótese que se trata de caminos bidireccionales, es decir, recursos utilizados en ambos sentidos de la comunicación. Si un camino hacia un sistema A va por un camino y hacia B vuelve por otro, en la práctica es un único camino bidireccional y no dos en términos de recursos utilizados.

Según las ecuaciones, y como era de esperar, el número de caminos que puede generar Flow-Path es el mayor, seguido de ARP-Path y finalmente Bridge-Path. Para analizar el balanceo de carga habrá que comparar este valor teórico con el valor actual de caminos disponibles que posee la topología, puesto que quizás el número de caminos teórico puede ser mayor para un protocolo que para otro, pero si en la práctica no existe ese número de caminos disponibles, el balanceo de carga quizás es el mismo para ambos.

B. Estudio de escalabilidad

En el caso del estudio sobre escalabilidad, tomaremos como referencia el número de entradas de tabla generadas en toda la red, puesto que es la única diferencia entre los protocolos respecto a este parámetro.

Así pues, el número de entradas de tabla totales en la red que generarán de media Flow-Path, ARP-Path y Bridge-Path, y que denominaremos T_{FP}, T_{AP} y T_{BP} respectivamente, son:

$$T_{FP} = F_U * b = H*(H-1) * b \quad (4)$$

$$T_{AP} = H * (b+Le) \quad (5)$$

$$T_{BP} = B_E * (b+Le) \quad (6)$$

Siendo F_U: número medio de flujos unidireccionales en la red ($F_U = 2*F_B$, dado que se considera un flujo en cada sentido y cada sentido es una entrada de tabla), H: número medio de hosts o sistemas finales activos, B_E: número medio de puentes frontera activos ($B_E \leq H$, y además B_E siempre será una fracción de H), b: número de puentes que forman el camino medio, Le: número de puentes extra que también comparten el camino con otros destinos.

Nótese que, igual que en el caso del número de caminos generados, *Flow-Path* genera más entradas de tabla que *ARP-Path* y éste último más que *Bridge-Path*, siendo los valores resultantes proporción del cuadrado de H, de H y de una fracción de H, respectivamente. Como segunda parte de la operación, las tres ecuaciones contienen b, número de puentes que forman el camino medio, dado que si un camino atraviesa n puentes, eso significará n entradas (una entrada por puerto) en cada sentido de la comunicación. Finalmente, el valor Le, no aplicado en Flow-Path, es el número de puentes medio que forman ramificaciones del camino. Esto último se debe a que ARP-Path y Bridge-Path generan árboles de acceso a cierto sistema o conjunto de sistemas, es decir, generan un camino para un destino (host o puente) y diversas ramificaciones para el resto de destinos, compartiendo todas ellas cierta parte del camino principal, lo que no sucede en Flow-Path puesto que el camino es único para cada comunicación establecida.

Si mostramos los valores anteriores como una razón para comparar las proporciones, obtenemos las siguientes ecuaciones:

$$R_{FA} = \frac{T_{FP}}{T_{AP}} = \frac{H*(H-1)*b}{H*(b+Le)} = (H-1)*\frac{b}{b+Le} \quad (7)$$

$$R_{AB} = \frac{T_{AP}}{T_{BP}} = \frac{H*(b+Le)}{B_E*(b+Le)} = \frac{H}{B_E} \geq 1 \quad (8)$$

Como muestra la Ec. 7, la ratio del número de entradas de Flow-Path y ARP-Path R_{FA} no depende sólo del número de hosts activos (al ser el número de flujos normalmente un cuadrado de dicho valor), sino también del tipo de topología empleada: si la topología es muy ancha, por ejemplo, el valor Le aumentará y la razón disminuirá. Mientras que la Ec. 8 muestra como la relación entre ARP-Path y Bridge-Path R_{AB} será mayor o igual que 1.

IV. Análisis de Escalabilidad VS Balanceo de Carga

Para poner en práctica los dos estudios anteriores, utilizaremos un par de topologías (con nodos y enlaces idénticos) de ejemplo para analizar qué protocolo tendría las mejores características para ser aplicado en el encaminamiento de la red.

A. *Análisis en topología mallada simple*

Primero analizaremos la topología mallada que se muestra en la Fig. 7. Se trata de una malla con cuatro puentes frontera y de tamaño cuadrado *n* x *n*, donde n en la figura tiene valor 3. El análisis será del número de entradas de tabla y del número de caminos en función del tamaño de la topología *n*, que a su vez afectará a los parámetros *b* y *Le*, y en función del número medio de hosts activos en la topología *H*, parámetros de los que derivan las ecuaciones anteriores.

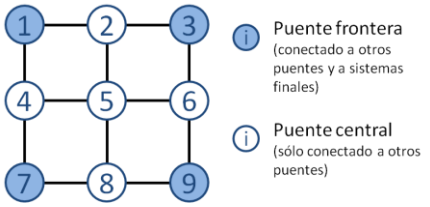


Fig. 7. Topología mallada simple *n* x *n*, con n = 3

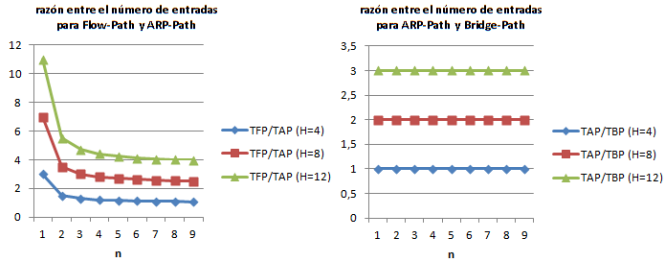


Fig. 8. Razón entre el número de entradas de tabla de Flow-Path y ARP-Path, y de ARP-Path y Bridge-Path, en función de *n* y *H*

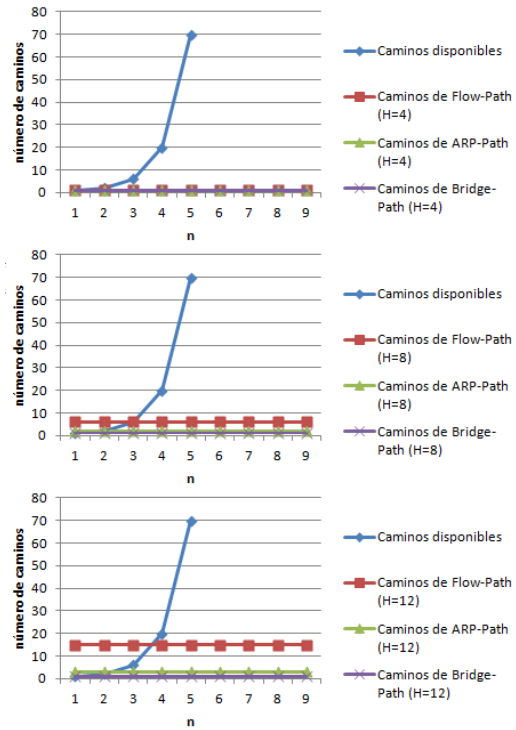


Fig. 9. Caminos disponibles en la red mallada simple frente a los caminos ofrecidos por Flow-Path, ARP-Path y Bridge-Path, en función de *n* y *H*

Como puede observarse en la Fig. 8, la razón del número de entradas entre Flow-Path y ARP-Path disminuye según la topología crece y se hace más ancha. Así pues, en el caso por ejemplo de *H*=12 (tres hosts activos de media por cada uno de los cuatro puentes frontera), la razón no es casi 12 veces mayor como pensaríamos intuitivamente, sino que llega a valores menores de 4 según crece la topología. La relación entre ARP-Path y Bridge-Path es 1, 2 y 3 respectivamente, que coincide con la proporción del número de hosts por puente frontera.

Para analizar los caminos, se han tenido en cuenta los caminos entre dos extremos de la red, ya sean los nodos 1 y 9, o 3 y 7 (Fig. 7). En el caso de los caminos disponibles se han considerado sólo los caminos mínimos. En este tipo de topologías, para *n*=2 habría 2 caminos mínimos (de 3 puentes), para *n*=3 habría 6 (de 5 puentes), para *n*=4 habría 20 y aumenta exponencialmente. Según las gráficas, podemos ver que según aumenta *H*, es más interesante utilizar Flow-Path, sobre todo si *n* es grande, dado que aumenta la utilización de la red unas 10 veces más respecto a ARP-Path o Bridge-Path y sólo por tamaños de tabla 4 veces mayores. Mientras que para *H* y *n* pequeños, lo más interesante es utilizar Bridge-Path, con coste mucho menor.

B. *Análisis en topología mallada cruzada*

A continuación analizaremos un caso similar al anterior, en el que añadimos enlaces cruzados en diagonal entre los puentes tal y como se muestra en la Fig. 10.

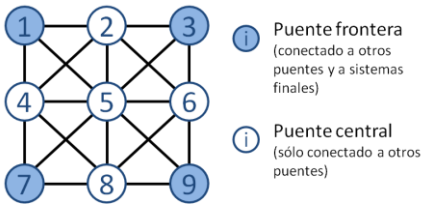


Fig. 10. Topología mallada cruzada *n* x *n*, con n = 3

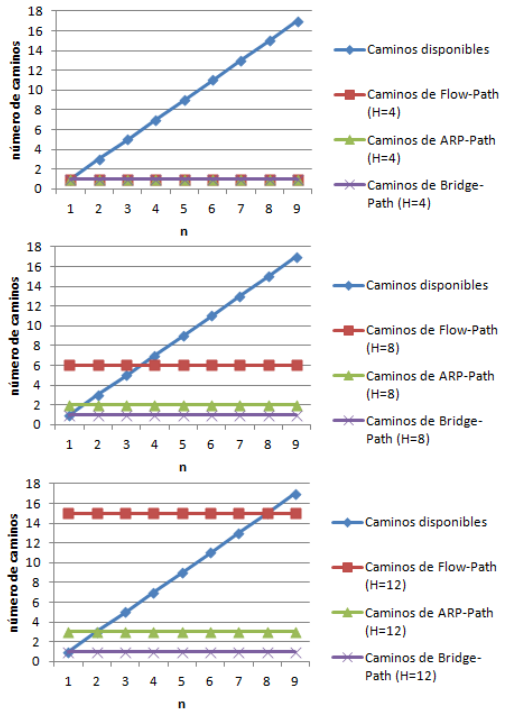


Fig. 11. Caminos disponibles en la red mallada cruzada frente a los caminos ofrecidos por Flow-Path, ARP-Path y Bridge-Path, en función de *n* y *H*

La peculiaridad de esta topología frente a la anterior es que sólo existe esta vez un camino mínimo, que es el que recorre los puentes de extremo a extremo por la diagonal central, mientras que la razón entre el número de entradas se conserva. Si tomamos como caminos disponibles el mínimo y los que tienen un salto más que el mínimo (excluimos el resto porque consideramos que será más compleja su selección, aunque no imposible si estos primeros están muy cargados), obtenemos los resultados mostrados en la Fig. 11. Esta figura nos muestra que hay casos en los que Flow-Path no es tan necesario, al ser mayor su número de caminos generados que los caminos disponibles en la topología y podemos ahorrar entradas y repartir adecuadamente simplemente usando ARP-Path por ejemplo.

V. Conclusiones

La familia *All-Path* tiene diferentes y variadas soluciones para redes de conmutadores teniendo en cuenta como parámetros el balanceo de carga y la escalabilidad, y obteniendo las ventajas nativas de no necesidad de configuración, generación de caminos de mínima latencia, buen rendimiento y utilización de todos los recursos de la red. ARP-Path es el protocolo base, mientras que Flow-Path ofrece incluso mayor balanceo de carga, a costa de un mayor número de entradas de tabla, y Bridge-Path mayor escalabilidad.

Se demuestra la capacidad de ajuste fino de esta familia según los requerimientos de la red y del proveedor, frente a alternativas como SPB y TRILL, que distribuyen el tráfico de manera aleatoria, sin tener en cuenta el estado de la red en cada momento y además requieren una complejidad mayor de instalación, dado que el protocolo de estado que utilizan necesita una configuración inicial. Por ejemplo, ARP-Path tiene muy buen balanceo de carga, pero Flow-Path puede superarlo cuando los caminos mínimos son múltiples (como es el caso de la primera red estudiada) y más incluso si uno de los sistemas es un punto caliente o *hot spot*; mientras que Bridge-Path disminuye drásticamente el número de entradas especialmente cuando la proporción de puentes frontera es alta respecto al total de la red y estos tienen múltiples sistemas conectados (como es el caso de las redes de centros de datos).

Actualmente el grupo GIST-Netserv dispone de diversas implementaciones (simulador y hardware) que además confirman los anteriores resultados y continúa estudiando mejoras de la familia de protocolos *All-Path*.

Agradecimientos

Este trabajo ha sido financiado en parte gracias al proyecto MEDIANET-CM (S-2009/TIC¬1468) y CMACs (UAH2011/EXP-016) otorgados por la Comunidad de Madrid y la Universidad de Alcalá respectivamente.

Referencias

[1] IEEE 802.1aq – Shortest Path Bridging: http://www.ieee802.org/1/pages/802.1aq.html
[2] RFC 6325 – Routing Bridges (RBridges): Base Protocol Specification: http://tools.ietf.org/html/rfc6325
[3] IEEE 802.1D-2004 - MAC Bridges: http://www.ieee802.org/1/pages/802.1D-2003.html
[4] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, A. Vahdat. "Hedera: Dynamic flow scheduling for data center networks". En actas de Usenix NSDI 2010.
[5] G. Ibáñez et al. "ARP-Path: ARP-based Shortest Path Bridges". IEEE Communication Letters. Julio 2011
[6] G. Ibáñez et al. "Path-Moose: A Scalable All-Path Bridging Protocol". IEICE Transactions Vol.E96-B No.3 pp. 756-763, 2013.
[7] M. Scott, A. Moore, J. Crowcroft. "Addressing the Scalability of Ethernet with MOOSE": http://www.cl.cam.ac.uk/~mas90/
[8] Grupo de Ingeniería de Servicios Telemáticos de la Universidad de Alcalá: http://www.it.aut.uah.es/ist
[9] G. Ibáñez et al. "Evaluating Native Load Distribution of ARP-Path Bridging Protocol in Mesh and Data Center". En actas de IEEE ICC 2013.

Mejora del rendimiento de TCP en redes malladas inalámbricas con técnicas multi-camino: MPTCP

Pablo Garrido[1],David Gómez[2], Ramón Agüero[2] y Luis Muñoz[2]
Universidad de Cantabria, Santander, España
[1]{**pablo.garrido**}**@alumnos.unican.es**
[2]{**dgomez,ramon,luis**}**@tlmat.unican.es**

***Resumen*—Las últimas tendencias en el mundo de las comunicaciones, donde cada vez es más corriente que los terminales posean diferentes interfaces con los que acceder a Internet, cuestiona el paradigma clásico de mantener una única ruta por conexión, impuesto por el protocolo de transporte más utilizado en la actualidad, TCP. En este trabajo se evalúa el comportamiento del protocolo MPTCP, el cual permite la división transparente de una sesión a nivel de transporte en múltiples flujos simultáneos, mejorando el rendimiento e incrementando la robustez frente a posibles fallos en alguna de las rutas. A través de una extensa campaña de simulación sobre `ns-3` se han observado mejoras, en términos de throughput, de hasta un 48 % en comparación con TCP.**

***Index Terms*—MPTCP, Redes malladas inalámbricas, Transmisiones multi-camino, Algoritmos de control de la congestión**

I. Introducción

Desde sus inicios, el mundo de Internet ha visto como uno de sus protocolos más importantes, TCP (y sus sucesivas modificaciones), se ha convertido con pleno derecho en la solución de nivel de transporte más empleada, por encima de otras alternativas, como UDP, SCTP, DCCP, etc. Sin embargo, en la época en la que fue propuesto (principios de los años 70), la tecnología estaba marcada por el dominio de redes y dispositivos cableados, existiendo una única opción a la hora de acceder a la red por parte de los terminales. Con el paso del tiempo, esta tendencia ha ido evolucionando gradualmente y actualmente el paradigma empleado para definir las comunicaciones es completamente diferente.

Gran parte de la culpa de este cambio la tiene el enorme crecimiento, tanto en términos de tecnologías disponibles como de despliegue y popularidad, de los dispositivos inalámbricos, cuyo impacto ha volteado el concepto tradicional de red de acceso impuesto en los orígenes de Internet. Además, la inmensa mayoría de este tipo de terminales cuenta a día de hoy con múltiples interfaces pertenecientes a diferentes tecnologías de acceso radio (e.g. IEEE 802.11, Bluetooth, redes de acceso celular UMTS/LTE, etc.)[1], abriendo la puerta a la posibilidad de que en un futuro todos ellos puedan coexistir y trabajar simultánea y eficientemente.

Todo esto ha suscitado un gran interés en la comunidad investigadora, que está aunando sus esfuerzos en la búsqueda de un modo adecuado para proporcionar conexiones fiables a partir de las nuevas posibilidades aparecidas con estas nuevas tendencias. Uno de sus frutos más destacables aparece con el protocolo MultiPath TCP (MPTCP), surgido a raíz de la creación de un grupo de trabajo propio en el IETF. Esta especificación puede ser definida como una evolución natural de TCP que permite la transmisión de la información de manera simultánea a través de múltiples caminos (o subflujos) dentro de una única conexión TCP. Los mecanismos de control de flujo distribuyen la carga disponible entre los subflujos presentes y activos, que estarán estrechamente ligados a las direcciones IP definidas en los nodos. A través de esta idea (aparentemente) tan sencilla, las aplicaciones podrán beneficiarse de un rendimiento más alto en términos de throughput y de una mayor robustez frente a los posibles fallos producidos durante la transmisión.

Aunque la mayor parte de los análisis de las soluciones multi-camino propuestas en la literatura están enfocadas a topologías cableadas, existe un reducido número de contribuciones que tratan de estudiar el comportamiento de este tipo de transmisiones multipath sobre redes malladas inalámbricas. Este tipo de escenarios despierta un gran interés, ya que es bien conocido que la naturaleza intrínseca de los medios inalámbricos deteriora notablemente el rendimiento de los protocolos de nivel de transporte orientados a la conexión, cuyo principal exponente es TCP.

Para la realización de este trabajo se ha portado un esquema completamente funcional del protocolo MPTCP, cumpliendo con los requerimientos impuestos en los RFCs que lo definen (que serán detallados más adelante), permitiendo dividir una única sesión TCP en varios subflujos (que serán negociados durante el establecimiento de la propia conexión y que dependerán del número de direcciones IP válidas de los terminales). En un extenso proceso de simulación, se caracterizarán algunos de los algoritmos de control de congestión, independiente para cada uno de los subflujos creados. Además, se demostrará que el rendimiento obtenido a través del protocolo MPTCP en redes inalámbricas multicanal es netamente superior al devuelto por el esquema tradicional de un único camino que usa TCP.

El documento se ha dividido como se muestra a continuación: la Sección II resume las principales contribuciones relativas al empleo de técnicas multi-camino como alternativa al TCP tradicional, centrándose en aquellas que tratan de caracterizar su comportamiento sobre enlaces inalámbricos. La Sección III describe las características más relevantes del protocolo MPTCP, implementadas en el marco del simulador utilizado para el análisis. A continuación, las Secciones IV y V muestran la platafoma de simulación que ha sido desarrollada para caracterizar el comportamiento de MPTCP y los principales resultados obtenidos, respectivamente. Por último, la Sección VI cierra el documento, extrayendo las principales

[1]Del mismo modo, muchos de estos equipos, como los ordenadores portátiles o los cada vez más populares todo-en-uno portables, incluyen un puerto Ethernet con el que conectarse a la red de una manera cableada.

conclusiones obtenidas y planteando aquellas cuestiones que deberán ser tratadas en el futuro.

II. Trabajo previo

La tendencia a ofrecer diferentes puntos de acceso hacia el exterior en los nodos actuales (e.g. los servidores presentan un buen número de puertos de acceso a Internet a través de diferentes ISPs, los grandes centros de datos cuentan con rutas replicadas que se activan en caso de errores, los dispositivos portátiles incorporan múltiples interfaces asociados a diferentes tecnologías inalámbricas, etc.) dan lugar al planteamiento de un nuevo esquema de funcionamiento en el que el tráfico pueda dividirse y transportarse al mismo tiempo por caminos distintos. Muestra de este creciente interés, el IETF crea un grupo de trabajo (llamado explícitamente *Multipath TCP Working Group*) que centra sus intereses en la creación de una solución que permita multiplexar el tráfico de una única sesión TCP a través de diferentes rutas. Los cimientos de este protocolo se encuentran en [1], que a su vez se apoya en una serie de extensiones ([2], [3]), que definen la base de la arquitectura propuesta y un esquema para controlar la congestión entre los diferentes subflujos, respectivamente. Además, el impacto que han generado las comunicaciones inalámbricas ha originado otra extensión, [4], aún no aprobada, que propone una serie de modificaciones para implementar correctamente el protocolo sobre este tipo de canales.

MPTCP no es la única solución que trata de romper las barreras impuestas por TCP, donde las conexiones estaban restringidas a un único flujo. Antes incluso de su creación, el IETF, a través del grupo de trabajo SIGTRAN (SIGnalling TRANsport), sentó las bases de las comunicaciones multi-camino definiendo el protocolo Stream Control Transmission Protocol (SCTP) [5]. Ambos esquemas guardan ciertas similitudes, como la posibilidad de utilizar múltiples direcciones en los nodos terminales, permitiendo conexiones multipath; no obstante, las diferencias entre ambas especificaciones son notables: en MPTCP el objetivo claro es el de mejorar las prestaciones (throughput y robustez) de TCP mediante la transmisión simultánea, mientras que SCTP trata de proporcionar un factor de redundancia y movilidad a nodos multihomed, pero sin poder paralelizar el tráfico en más de un camino al mismo tiempo (es cierto que existen extensiones que tratan de habilitar esta posibilidad, pero aún están lejos de ser incorporadas al protocolo principal).

Es posible encontrar en la literatura trabajos que, al igual que en este documento, analizan el comportamiento de MPTCP sobre enlaces inalámbricos. Basándose en la implementación pública disponible para el Kernel de Linux [6], Maxine Lim y Josh Valdez [7] demuestran la mejora introducida con una transmisión MPTCP comparada con el rendimiento de TCP en una combinación de canales Ethernet, IEEE 802.11 y 3G, comprobando también la capacidad de mantener una sesión durante la realización de un traspaso vertical sin corromperse. Mientras que su campaña de medidas se basa en canales emulados configurados con unas tasas de error de paquete fijas (0 % en Ethernet, 2 % en 3G y 3 % en IEEE 802.11), los autores comparan sus resultados con los obtenidos a través de medidas sobre canales reales en [8], concluyendo que a través de este nuevo esquema se consigue mejorar significativamente el rendimiento del sistema, aunque no inducen condiciones adversas sobre el escenario que permitan evaluar las virtudes del protocolo MPTCP en mayor profundidad. Por otro lado, en [9] se utiliza otra implementación del protocolo y se evalúa el rendimiento instantáneo y la distribución de la carga entre subflujos en escenarios que mezclan tecnologías Ethernet, IEEE 802.11 y 3G. En este caso los resultados obtenidos no son tan alentadores, ya que cuando se mezclan dos canales físicos diferentes, el rendimiento obtenido es inferior al que obtiene TCP utilizando el mejor camino posible. Los autores achacan este pobre bagaje al impacto negativo que supone una reordenación poco eficiente en subflujos de diferentes características, pero no mencionan qué tipo de mecanismo utilizan para sus análisis.

Debe mencionarse también la contribución llevada a cabo por Chihani et al. [10], responsables de la implementación de MPTCP en la arquitectura del simulador `ns-3`, concretamente para su versión *6*. Para ello utilizan como base las recomendaciones de los RFCs del grupo de trabajo de MPTCP ya mencionadas. La piedra angular de su trabajo describe el funcionamiento de los cuatro algoritmos para el control de congestión tratados en este documento (cuyo comportamiento es estudiado con mayor profundidad en [11]). En relación a los resultados mostrados, los autores comparan el rendimiento de dos algoritmos de reordenación diferentes en una transmisión FTP entre un cliente y un servidor conectados a través de dos enlaces cableados punto a punto, estudiando el comportamiento de las ventanas de congestión asociadas a cada uno de los subflujos.

III. Implementación del protocolo MPTCP en el marco del simulador ns-3

MPTCP nace como una versión modificada del protocolo TCP [12], proponiendo una serie de extensiones que permiten particionar una sesión de nivel de transporte en múltiples flujos, que transportarán la información de manera simultánea. El protocolo MPTCP será el encargado de distribuir la carga a través de las distintas “subconexiones”, que recorrerán caminos potencialmente disjuntos, pudiendo emplear incluso tecnologías diferentes. En primera instancia el protocolo ha sido diseñado para trabajar en esquemas multi-camino extremo a extremo, donde uno (o ambos) equipos terminales deberán disponer de más de una dirección IP.

Otra de las características fundamentales de MPTCP es la imposición, desde sus bocetos iniciales, a mostrar una compatibilidad hacia atrás con su protocolo raíz, TCP (o cualquiera de sus derivados), factor que permitiría un despliegue menos agresivo. De este modo, para cualquier aplicación no compatible, una conexión MPTCP será a todos los efectos indistinguible de una realizada con TCP.

Los siguientes tres objetivos representan el comportamiento deseable de un esquema muti-camino, para pasar a ser un candidato para sustituir al esquema TCP más tradicional:

1. *Aumentar el throughput*: El rendimiento obtenido a través de un esquema MPTCP debe ser, como mínimo, no inferior al resultante de TCP cuando éste emplee la mejor ruta disponible.
2. *No perjudicar*: Un subflujo MPTCP no debe consumir más recursos que los que TCP necesitaría utilizando únicamente uno de los caminos.

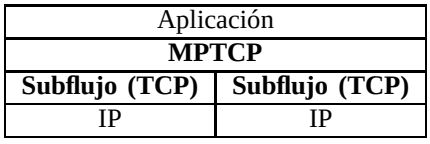


Figura 1: Arquitectura del protocolo MPTCP

3. *Nivelar la congestión*: Ante una situación de congestión, los algoritmos de control de flujo deberán derivar la mayor cantidad de recursos posible a aquellos subflujos que se encuentren menos congestionados (respetando obviamente los dos primeros objetivos).

III-A. Descripción de la arquitectura MPTCP

Como se muestra en la Figura 1, el protocolo MPTCP actúa en el nivel de transporte, supliendo todo el rango de tareas soportado por TCP. Su operación se ha dividido en dos partes con funcionalidades claramente diferenciadas:

1. El subnivel superior será el encargado de realizar las funciones orientadas a la aplicación: inicialización/finalización de las sesiones, establecimiento de los subflujos, detección y uso de múltiples caminos, etc.
2. La subcapa inferior, enfocada a las tareas orientadas hacia la red, se encargará de gestionar cada uno de los subflujos que se haya creado durante la fase de inicialización de la conexión. Para ello, se dividirá la operación de control en tantas entidades como subflujos haya presentes en la conexión.

Por debajo, cada uno de los subflujos estará asociado a un interfaz IP diferente (merece la pena recordar que al menos uno de los nodos terminales deberá tener más de un interfaz IP). Como ya ha sido comentado, esta arquitectura permite una operación transparente, tanto hacia las capa superiores como a las inferiores, mostrando un comportamiento equivalente a una conexión TCP.

A continuación se resumirán, a grandes rasgos, las principales funcionalidades llevadas a cabo por el subnivel superior:

Establecimiento de la conexión. Con el fin de respetar la compatibilidad hacia atrás impuesta en los patrones de diseño del protocolo, una sesión MPTCP se inicializará con el saludo a tres vías (*three-way-handshaking*) típico de TCP. En una segunda etapa, en el caso de que sea posible la utilización de más de un camino (se interpretará la presencia de múltiples direcciones IP en los nodos terminales como un factor que posibilita la creación de una conexión multipath), se establecerán diferentes sesiones TCP, donde las combinaciones de las posibles direcciones IP equivalen potencialmente a subflujos adicionales.

Números de secuencia. Respetando de nuevo el patrón utilizado, el protocolo MPTCP conservará el esquema de secuenciamiento empleado por TCP, aunque será específico e independiente para cada subflujo. Adicionalmente, para permitir la reordenación de los datos de aplicación en el receptor, será necesario un espacio de numeración adicional que permita recomponer las piezas de información recibidas a través de los diferentes subflujos. Para ello deberá realizarse, tanto a la hora de transmitir como de recibir, un mapeo entre los números de secuencia de datos y los números de secuencia de los subflujos, cuya información será transportada en un campo opcional de la cabecera MPTCP conocido como Data Sequence Number (DSN).

Reordenación de los paquetes. El hecho de fragmentar la conexión en varios subflujos que, a su vez, recorren diferentes caminos, fomenta la posibilidad de que los segmentos de información lleguen al destino en un orden no predecible. Por ello es imprescindible disponer de esquemas que permitan recuperar la información de una forma eficiente, introduciendo la menor cantidad posible de retransmisiones. Aunque existen numerosas alternativas a la hora de acometer dicha labor, en este trabajo se hace uso del mecanismo *DSACK* [13], una extensión del algoritmo Selective Acknowledgement (SACK), que permite el reconocimiento y retransmisión selectiva de aquellos fragmentos de información necesarios, evitando la retransmisión de bloques enteros de datos.

Distribución de paquetes. Por otra parte, se necesitará utilizar un mecanismo que se encargue de distribuir los paquetes por los subflujos MPTCP. Por razones de simplicidad, la solución elegida en la implementación se basa en la utilización de una técnica tradicional, *Round Robin (RR)*, que reparte equitativamente los segmentos de datos a través de los subpaths habilitados en la conexión. Concretamente, el subnivel superior enviará alternativamente un paquete a cada uno de los subflujos, repitiéndose el proceso mientras el buffer de transmisión del subnivel superior disponga de paquetes esperando a ser enviados.

Junto con todas las funcionalidades presentadas, es preciso destacar que MPTCP mantiene intactos algunos de los mecanismos más utilizados de TCP, como por ejemplo *slow start*, *fast retransmit* o *fast recovery*.

Una vez detalladas las funciones relacionadas con la conectividad y su interacción con el nivel de aplicación, es necesario establecer unos mecanismos que sean capaces de distribuir convenientemente el tráfico a través de los diferentes subflujos establecidos. Para ello, un interfaz situado entre los dos subniveles MPTCP deberá gestionar el paso de información entre ambos, distribuyendo los recursos convenientemente a través de las diferentes conexiones establecidas. En este punto es importante elegir aquellos mecanismos de control de congestión que sean capaces de asegurar el correcto cumplimiento de los tres objetivos descritos anteriormente. Para ello, deberá efectuarse una correcta gestión de los recursos (en [14] se conoce como *resource pooling*, donde se presenta una solución para gestionar todos los recursos disponibles en la red como si se trataran de un único recurso global).

El criterio elegido en este protocolo es el de dotar a cada uno de los subflujos una ventana de congestión diferente. Para lograr un correcto *resource pooling*, es necesario que la evolución de las ventanas de congestión no sea independiente, sino que deberá presentar un cierto factor de acoplamiento.

A continuación, se describen los cuatro algoritmos para el control de la congestión soportados por el esquema de MPTCP implementado en el simulador. De aquí en adelante, se utilizará la notación w_i para referirse al tamaño de la ventana de congestión del subflujo i-ésimo, siendo la variable w la encargada de calcular el tamaño acumulado de todas las ventanas: $w = \sum_i w_i$, donde $i = 1, \ldots, N$, siendo N el número de subflujos.

- **Uncoupled subflows**: Como primera opción se incorpo-

ra un algoritmo básico, donde cada una de las ventanas de congestión adaptadas a cada subflujo se controla de manera completamente aislada, comportándose como conexiones TCP independientes.

$$w_i = \begin{cases} w_i + \frac{1}{w_i}, & \text{si Additive Increase (AI)} \\ \frac{w_i}{2}, & \text{si Multiplicative Decrease (MD)} \end{cases}$$

- **Fully coupled**: A través de este algoritmo, en el que el comportamiento de las ventanas de congestión se encuentra estrechamente ligado, cuando uno de los subflujos experimenta una tasa de error ligeramente superior al otro, el protocolo MPTCP interpretará una situación de congestión y tratará de aliviarla asignando una carga mayor al nodo menos saturado (**Objetivo 3**). El problema del mecanismo surge cuando se pierden tramas en un subflujo de manera continuada, llegando a tener una ventana mínima ($w_i \approx 0$), situación que mantiene durante un intervalo de tiempo. Para volver a una situación estable, el otro subflujo deberá sufrir un número mucho mayor de pérdidas hasta hacer que las tasas queden niveladas. A este efecto que puede resultar tan nocivo se le conoce como "*flappiness*".

$$w_i = \begin{cases} w_i + \frac{1}{w}, & \text{si AI} \\ max(w_i - \frac{w}{2}, 1), & \text{si MD} \end{cases}$$

- **Linked increases**: Para reducir el efecto "flappiness" observado en el caso anterior, Raiciu et al. [11] proponen una solución que, a costa de sacrificar la eficiencia en la gestión de recursos, evita, en la mayor medida posible, el reparto poco equitativo entre los subflujos. En la expresión siguiente se observa la presencia de un parámetro nuevo, α, que marcará el factor de crecimiento de la ventana de congestión.

$$w_i = \begin{cases} w_i + \frac{\alpha}{w}, & \text{si AI} \\ \frac{w_i}{2}, & \text{si MD} \end{cases}$$

- **RTT compensator**: El último de los algoritmos se trata de una ligera modificación del anterior, pensado para ser utilizado en escenarios cuyos caminos están caracterizados por presentar valores de Round Trip Time (RTT) muy diferentes (e.g. diferentes tecnologías físicas, cuellos de botella en algún enlace concreto, mayor carga de tráfico, etc.). Al igual que para el mecanismo *Linked increases*, la tasa de crecimiento de la ventana de congestión está controlada por el parámetro α.

$$w_i = \begin{cases} w_i + min(\frac{\alpha}{w}, \frac{1}{w_i}), & \text{si AI} \\ \frac{w_i}{2}, & \text{si MD} \end{cases}$$

Como se ha visto en los dos últimos algoritmos, el factor de crecimiento de la ventana de congestión viene dado por la presencia de un nuevo factor, α, conocido también como *factor de agresividad*, que responde a la expresión expuesta en (1).

$$\alpha = w \cdot \frac{max(\frac{w_i}{RTT_i^2})}{(\sum_i \frac{w_i}{RTT_i})^2} \quad (1)$$

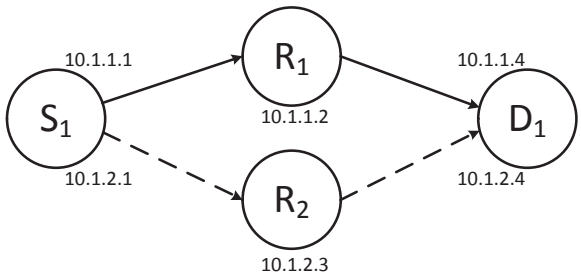


Figura 2: Topología canónica empleada para mostrar los beneficios de las técnicas multi-camino sobre el esquema tradicional de un solo flujo

A través de este parámetro se trata de acomodar el ancho de banda agregado del sistema de tal manera que se cumplan los **Objetivos 1** y **2**. No obstante, este parámetro no es capaz de satisfacer completamente el **Objetivo 3**, ya que no permite reducir la carga de tráfico en aquellos subflujos que se encuentren más congestionados, gestionando de una forma no óptima los recursos disponibles en la red.

IV. Plataforma de simulación

Para evaluar el rendimiento del protocolo MPTCP se ha realizado una completa campaña de medidas sobre el simulador de redes `ns-3`, que está llamado a ser unos de los entornos de simulación más populares en los próximos años, gracias, entre otras virtudes, a su flexibilidad, su carácter abierto y, quizás característica más importante, su amplia y activa comunidad de usuarios.

El proceso seguido para llevar a cabo las simulaciones se describe en la Figura 2, cuyos puntos principales se resumen a continuación:

- El nodo S_1 envía un fichero de 20 MBytes al destino correspondiente, D_1. Dado que este último no se encuentra dentro del radio de cobertura del transmisor, será necesario apoyarse en los nodos intermedios R_1 y R_2, que serán los encargados de reenviar los paquetes recibidos hacia D_1.
- Como se define en [1], un requerimiento básico para el correcto funcionamiento del protocolo MPTCP consiste en que los terminales dispongan de múltiples direcciones IP. Para la realización de este experimento, cada nodo contará con dos interfaces IEEE 802.11, cada uno de ellos asociado a una subred IPv4 diferente, como se muestra en la Figura 2.
- Se establecen unos umbrales superiores de rendimiento para diferentes configuraciones en el nivel de transporte. Para tal fin, se recreará un canal saturado, donde el nodo transmisor tenga siempre al menos una trama esperando ser transmitida (comportamiento habitual del tráfico elástico y el protocolo TCP). Además, se comparará el comportamiento de los cuatro algoritmos para el control de la congestión descritos en la Sección III.
- Los enlaces han sido configurados según las especificaciones del estándar IEEE 802.11b; el número total de transmisiones por trama se limita a cuatro intentos, tras los que se descarta definitivamente.
- Además, para analizar el impacto de los errores de transmisión, cada enlace podrá estar caracterizado por

una tasa de error o Frame Error Rate (FER), permitiendo analizar el rendimiento de la capa de transporte bajo condiciones adversas.

El objetivo principal de este trabajo consiste en demostrar que la utilización del protocolo MPTCP realmente mejora al TCP tradicional, explotando el potencial que traen consigo aquellos dispositivos con más de un interfaz sobre escenarios inalámbricos. Para ello, se compararán las prestaciones obtenidas a través de tres configuraciones diferentes:

1. La primera de ellas corresponde al caso de una transmisión TCP clásica (concretamente, la versión utilizada es la *New Reno*), donde únicamente habrá un flujo de datos. Por defecto (ya que el esquema de encaminamiento empleado se basa en tablas estáticas), la ruta seguida por los segmentos de datos es la siguiente: $S_1 \rightarrow R_1 \rightarrow D_1$.
2. El segundo caso implementa MPTCP como solución de transporte, creando para ello dos subflujos independientes sobre el escenario ($S_1 \rightarrow R_1 \rightarrow D_1$ y $S_1 \dashrightarrow R_2 \dashrightarrow D_1$, configurados sobre un único interfaz inalámbrico que tendrá asignadas dos direcciones IP), por lo que ambas transmisiones utilizarán el mismo canal. Dada la naturaleza broadcast del medio inalámbrico, los envíos pertenecientes a ambos subflujos interferirán entre sí, incrementando el número de estaciones que contienden por el acceso al canal, así como las potenciales colisiones, factores que afectarán negativamente al rendimiento global del sistema.
3. Finalmente, y partiendo de la base de la configuración anterior, se emulará la posibilidad de utilizar interfaces independientes, trabajando en dos canales ortogonales de la banda de 2 GHz. Este cambio evita la contención entre nodos pertenecientes a diferentes caminos, incrementando notablemente el rendimiento final.

V. Resultados

A lo largo de esta sección se mostrarán los resultados más representativos obtenidos durante la campaña de simulación descrita anteriormente. Para ello se presentarán en tres etapas claramente diferenciadas: en primer lugar, se estudiará el comportamiento de los diferentes algoritmos de control de la congestión en un escenario sin errores; posteriormente se comparará el rendimiento de diferentes configuraciones en el nivel de transporte en un canal más realista, en el que se produce cierta pérdida de paquetes. Por último, se evaluará la capacidad de balancear la carga hacia aquellos subflujos menos congestionados, reaccionando ante diversas variaciones en la configuración de los canales.

V-A. Comparación de los mecanismos de control de flujo en un escenario ideal

El primer grupo de resultados se obtiene sobre un escenario ideal, en el que la pérdida de tramas, debido a los efectos adversos de la propagación inalámbrica, puede considerarse despreciable; por lo tanto, en este caso, la única forma de perder información estará asociada a las colisiones producidas durante la comunicación. En la Figura 3 se puede observar el throughput instantáneo a lo largo del tiempo de simulación de una medida arbitraria (y representativa) para algunas de las diferentes configuraciones estudiadas con anterioridad: en primer lugar, la Figura 3a muestra el rendimiento obtenido utilizando el protocolo TCP clásico a través de un único flujo, que mantiene una tasa estable de $\sim$2.5 Mbps. Este valor es importante, ya que el **Objetivo 2** de MPTCP busca que ninguno de los subflujos emplee más recursos de los utilizados por TCP, por lo que se podrá tomar como referencia. Por otra parte, la Figura 3b refleja el comportamiento de una configuración MPTCP cuando sólo se emplea un único interfaz inalámbrico, ilustrando el throughput instantáneo individual de cada uno de los subflujos, así como la suma de ambos y el valor promedio de la simulación. Puede extraerse que, a pesar de que la carga está repartida equitativamente entre cada uno de ellos, el rendimiento agregado es claramente inferior al obtenido con TCP, debido principalmente a la penalización que supone que ambas subredes estén compartiendo el mismo canal de transmisión (factor que deriva en e.g. tiempos de contención más largos, aumento del número de colisiones, etc.).

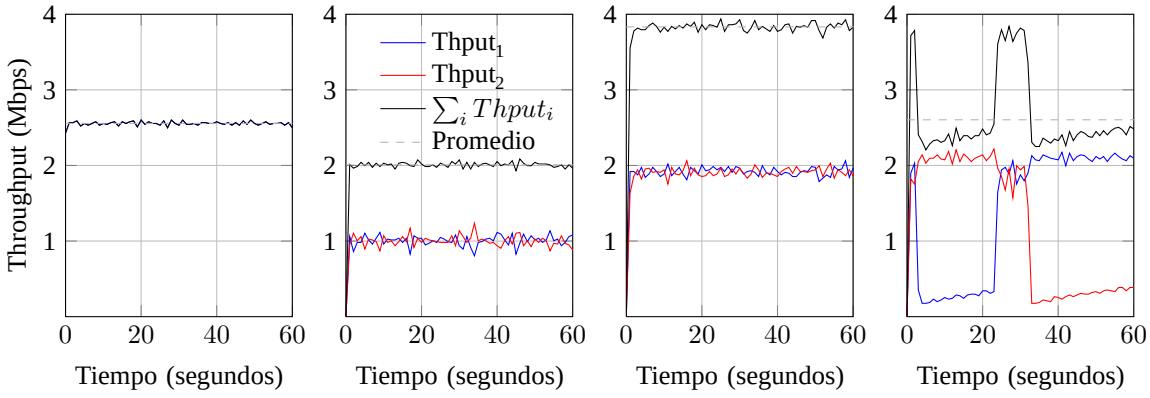
Para la caracterización de MPTCP sobre dos interfaces, la Figura 3c refleja el comportamiento del algoritmo *Uncoupled*[2], donde tras una breve fase inicial transitoria correspondiente con el mecanismo *Slow Start* de TCP, el throughput de ambos subflujos muestra un reparto equitativo y estable, y cuyo valor agregado supera con creces (en torno a un 48 %) al obtenido a través de TCP. Es importante destacar que ninguno de los subflujos toma valores de rendimiento superiores a TCP, cumpliendo de esta manera el **Objetivo 2**. Finalmente, la Figura 3d muestra el impacto del efecto *flappiness* descrito anteriormente, observado principalmente en el algoritmo *Fully Coupled* cuando las tasas de error de los subflujos son similares (debe recordarse que los errores son producidos por las colisiones). Puede comprobarse la alternancia de throughput entre ambas conexiones, donde es uno de los subflujos el encargado de cargar con la mayor parte del tráfico, reduciendo considerablemente la carga del otro subflujo. En el momento en el que el primero de éstos acumula una cierta cantidad de errores, la tendencia se invertirá y será el segundo de ellos el que pase a ser el flujo "dominante". Todo esto repercutirá enormemente en el ancho de banda agregado ofrecido al nivel de aplicación, que se verá gravemente perjudicado en comparación con el obtenido a través de un algoritmo que no presente este comportamiento (concretamente, el throughput total es un $\sim$47 % más bajo).

V-B. Rendimiento en un escenario con errores

En este segundo caso, la probabilidad de perder un paquete en los enlaces entre los nodos ya no es despreciable, con lo que el rendimiento global del sistema se verá afectado en gran medida. Concretamente, sólo los enlaces dirigidos $S_1 \rightarrow R_1$ y $S_1 \rightarrow R_2$ generarán errores de transmisión[3]. La Figura 4 muestra la evolución del throughput global percibido en el nivel de aplicación a medida que las condiciones del canal van empeorando. Después de analizar el comportamiento de los diferentes algoritmos de control de congestión, en este punto se utilizará el *Linked increases*, ya que es capaz de repartir

[2]Este algoritmo muestra una gran similitud con los mecanismos *Linked increases* y *RTT compensator* cuando la tasa de errores producidos durante la propagación es despreciable, por lo que no se hace necesaria su representación en este apartado.

[3]Por razones de simplicidad, el flujo inverso de reconocimientos TCP no se verá afectado por las pérdidas del canal.



(a) TCP original (b) MPTCP (1 interfaz) (c) Uncoupled (MPTCP 2 interfaces) (d) Fully coupled (MPTCP 2 interfaces)

Figura 3: Comparación del throughput instantáneo de los diferentes algoritmos en un escenario ideal

eficientemente la carga entre los dos subflujos sin provocar el efecto "flappiness". En ella se representa el valor medio y el intervalo de confianza del 95 % de un experimento de 50 simulaciones para cada uno de los puntos dibujados. Es evidente que el valor más pobre corresponde a una transmisión MPTCP basada en un único canal inalámbrico (a través de un único interfaz), como resultado de las razones comentadas con anterioridad: en primer lugar, el control de flujo de cada uno de los subflujos limita la tasa de envío, es decir el crecimiento de la ventana de congestión con el fin de no sobrepasar al que se obtendría con TCP, respetando el **Objetivo 2**; por otra parte, ya que todos los nodos están compartiendo el mismo canal inalámbrico, cada nodo que intente transmitir una trama deberá contender con el resto de estaciones por el acceso; cuantos más nodos traten de enviar información, mayor será el tiempo de espera promedio[4]. En un punto intermedio se encuentra el rendimiento alcanzado por las transmisiones TCP a través de un único flujo.

Finalmente, se observa que la aplicación de MPTCP sobre mútiples interfaces (pertenecientes a canales ortogonales) mejora significativamente el rendimiento mostrado por TCP (aproximadamente un $48\,\%$) en un escenario con condiciones ideales, manteniendo en todo momento un amplio margen de mejora en el resto de configuraciones.

V-C. Prueba del balanceo de carga

En esta última parte se analizará la capacidad del protocolo de balancear la carga entre los subflujos bajo diversas configuraciones del canal, con el fin de comprobar si los diferentes algoritmos de control de congestión son capaces de compensar el deterioro de rendimiento producido cuando alguno de ellos presenta unas condiciones más hostiles (**Objetivo 3**). La Figura 5 muestra el throughput medio de cada uno de los subflujos y el intervalo de confianza del 95 % de un total de 50 realizaciones por cada configuración. Además, se puede observar el ancho de banda agregado (puntos cuadrados) y su correspondiente intervalo de confianza. Por último, una línea horizontal discontinua refleja el throughput medio obtenido a través de las transmisiones de TCP en un escenario sin

[4]Además, mayor será la probabilidad de colisión o transmisiones simultáneas.

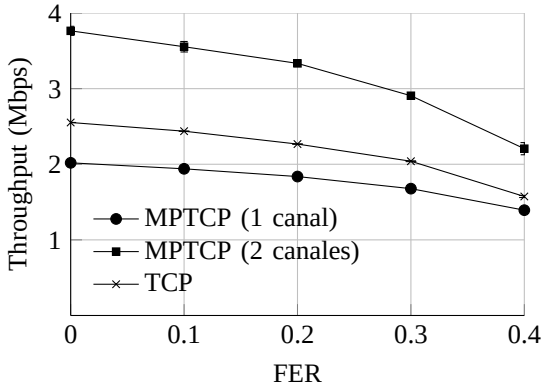
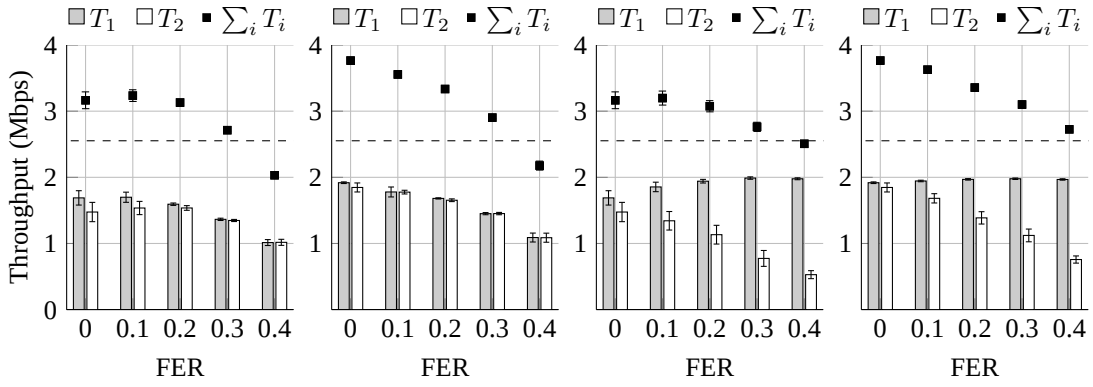


Figura 4: Evolución del throughput en un canal con errores

errores, umbral que será utilizado como margen superior de rendimiento, y que no deberá ser sobrepasado por ningún subflujo MPTCP (**Objetivo 2**).

Las Figuras 5a y 5b muestran el reparto de ancho de banda ofrecido por los algoritmos *Fully Coupled* y *Linked increases*, respectivamente, cuando las pérdidas en el canal afectan de igual modo a ambos caminos (esta configuración será conocida como *simétrica*). Si bien ambos mecanismos evidencian un reparto equitativo entre los dos subflujos, se observa en el primero de los casos una mayor variabilidad en los resultados, debida a la falta de estabilidad asociada al propio algoritmo (como ya se observó en la Figura 3d, donde el hecho de tener en un momento puntual una tasa de error más alta en uno de los subflujos, implica que el otro se apodera de la mayor parte de los recursos), que en un gran porcentaje de los casos conduce a situaciones dominadas por el efecto *flappiness*. Se puede concluir que este algoritmo es inestable cuando las ventanas de congestión de ambos subflujos son similares ($w_1 \sim w_2$), ya que un ligero cambio en una de ellas inducirá una situación de descompensación extrema entre la carga aportada a cada subflujo.

Finalmente, se ha modificado ligeramente la configuración de los errores de propagación, creando en el escenario una situación "asimétrica": mientras que el camino superior ($S_1 \rightarrow R_1$) no presenta pérdidas en el canal, el inferior



(a) Fully coupled (b) Linked increases (c) Fully coupled (d) RTT compensator

Figura 5: Reparto del ancho de banda entre subflujos en un canal con errores. (a) y (b) configuración simétrica. (c) y (d) configuración asimétrica

($S_1 \rightarrow R_2$) se configura para que la probabilidad de que una trama no alcance su destino no sea nula. A través de este simple cambio, se evaluará si la implementación realizada del protocolo MPTCP es capaz de compensar la congestión[5] producida en el segundo subflujo, incrementando la carga de tráfico en el primero. La Figura 5c muestra los resultados obtenidos utilizando el *Fully Coupled* como algoritmo de control de la congestión, poniendo de manifiesto una variabilidad más elevada y un rendimiento global inferior que el *RTT compensator* (ver Figura 5d), el cual será la elección más adecuada, ya que adaptará el crecimiento de las ventanas de contención al valor de RTT estimado en cada uno de los subflujos. La principal diferencia radica en el "flappiness" característico del primero de los mecanismos, efecto que conduce a la infrautilización de los recursos, produciendo como resultado un throughput agregado más bajo en estos casos. Sin embargo, puede apreciarse en ambos mecanismos que, a medida que la tasa de error en el enlace $S_1 \rightarrow R_2$ sube, la carga soportada por el primero de los subflujos crece gradualmente (sin sobrepasar al valor de TCP), demostrando que una parte del tráfico que supuestamente iría destinado al segundo de los caminos es traspasado satisfactoriamente al subflujo menos congestionado, compensando (parcialmente) la pérdida provocada por el canal más hostil.

VI. Conclusiones y líneas futuras

En este trabajo se ha portado el protocolo MPTCP (inicialmente implementado por Chihani et al. [10]) a una versión más completa y estable del simulador `ns-3` (concretamente, `ns-3.13`). El software desarrollado presenta una estructura completamente funcional que sigue las especificaciones definidas en las descripciones de la arquitectura, cuya recomendación principal es [1]. Sus principales características se basan en una completa transparencia para los niveles superiores, que no verán más que una conexión TCP a nivel de tranporte, aunque de manera subyacente se creen múltiples subflujos independientes, regidos por el cumplimiento de los tres grandes objetivos del protocolo MPTCP: *aumentar el throughput, no perjudicar* y *balancear la congestión*.

[5]Debe tenerse en cuenta que MPTCP, al igual que TCP, no es capaz de distinguir una pérdida ocasionada por la congestión de una debida a la propagación a través del medio.

A pesar de que la gran mayoría de los trabajos existentes centran su atención en la evaluación de las técnicas multicamino en topologías cableadas, en este trabajo se ha optado por estudiar el comportamiento de una solución concreta, MPTCP, sobre una red mallada inalámbrica. La columna vertebral del protocolo hereda las características fundamentales de las especificaciones de TCP, compartiendo del mismo modo todas sus debilidades exhibidas cuando las transmisiones son realizadas a través de un medio inalámbrico.

Durante la realización de este trabajo se ha llevado a cabo una completa caracterización del comportamiento de MPTCP sobre redes inalámbricas a través del simulador `ns-3`. En primer lugar, se ha comparado la respuesta de cuatro de los algoritmos de control de congestión soportados por la arquitectura en un escenario sin errores. Mientras que los mecanismos *Uncoupled*, *Linked increases* y *RTT compensator* presentan unos resultados ciertamente parejos, repartiendo equitativamente el ancho de banda entre los dos subflujos, el esquema *Fully coupled* evidencia un efecto conocido como "flappiness", donde uno de los flujos (el que presenta la tasa de pérdidas más reducida) "captura" la mayor parte de los recursos, viéndose el otro relegado a tasas muy inferiores. En consecuencia, el throughput agregado del sistema se ve severamente dañado.

En una segunda etapa, se han introducido pérdidas de paquetes entre los nodos, producidas a causa de una baja calidad del canal inalámbrico, comparando el rendimiento del TCP clásico con dos configuraciones diferentes del protocolo MPTCP: mientras la primera utiliza el mismo interfaz inalámbrico para transmitir los dos subflujos (que, por tanto, comparten el medio), la segunda emula una red multicanal libre de interferencias entre los dos tráficos. Tras analizar los resultados obtenidos, se ha observado que MPTCP introduce una mejora de throughput respecto a TCP del 48 % en el caso en el que los flujos sean ortogonales y la pérdida de paquetes debida al canal se mantenga despreciable.

Por último, se ha estudiado la capacidad de MPTCP para balancear la carga entre los subflujos propuesta en las recomendaciones. Para ello, se ha analizado el comportamiento de diferentes algoritmos de control de congestión bajo diferentes condiciones. Mientras el tráfico de los dos subflujos se reparte

de manera justa cuando las pérdidas afectan por igual a los dos caminos, en el momento en el que uno de ellos sufre una FER superior, se verá cómo la carga del subflujo menos congestionado aumenta en proporción a la disminución del camino menos eficiente, paliando el efecto negativo producido por los errores en la propagación a través de un canal deficiente.

Tras la realización del trabajo, todavía quedan pendientes una serie de cuestiones y líneas abiertas que deberán ser tratadas con profundidad en trabajos futuros. De entre todas ellas, se citan a continuación algunas de las más importantes:

1. Dada la simpleza del algoritmo utilizado para repartir los segmentos procedentes de los niveles superiores (Round Robin), sería posible plantear la implementación de técnicas más complejas, como *Weighted Round Robin*, que permitan redistribuir la carga entre los subflujos en función de la capacidad del canal en un instante dado. De este modo, el cumplimiento del **Objetivo 3** se vería optimizado en canales donde los subflujos presenten rendimientos dispares.
2. Evaluar el impacto de modelos de canal inalámbrico realistas sobre el rendimiento del protocolo MPTCP, ya que los utilizados más frecuentemente en el simulador no reflejan con la fidelidad suficiente el comportamiento con memoria que muestran las transmisiones sobre enlaces inalámbricos reales. El rasgo más característico de este tipo de canal se basa en la correlación mostrada entre recepciones consecutivas, induciendo a la aparición de ráfagas de tramas erróneas, que producirán un empeoramiento significativo en el rendimiento global del sistema, especialmente en protocolos de transporte orientados a la conexión, como TCP y MPTCP. Este fenómeno ha sido analizado en un gran número de trabajos, como por ejemplo [15], [16].
3. Por otra parte, está prevista la aplicación de las técnicas multi-camino en escenarios más realistas, en los que el despliegue de los nodos sea puramente aleatorio. En este caso, como paso anterior al establecimiento de las conexiones MPTCP, será necesaria la ejecución de algoritmos de búsqueda de rutas que permitan al nodo transmisor comunicarse con el destino deseado.
4. Del mismo modo, sería interesante añadir movilidad a los nodos, permitiendo estudiar nuevas métricas relativas al rendimiento del protocolo en una red mallada más dinámica (e.g. durabilidad de las rutas, estabilidad de las mismas, etc.), mientras los usuarios se mueven.

Para terminar, es conveniente destacar que la implementación del protocolo MPTCP realizada a lo largo de este trabajo se ha regido respetando la normativa Generic Public License (GPL) y puede encontrarse en [17], estando a total disposición para su utilización y modificación.

Agradecimientos

Los autores querían expresar su agradecimiento al Gobierno de España por su financiación en los proyectos "*Comunicaciones Cognitivas y Cooperativas sobre Entornos Heterogéneos*", C3SEM (TEC2009-14598-C02-01) y "*Connectivity as a Service: Access for the Internet of the Future*", COSAIF (TEC2012-38574-C02-02).

Referencias

[1] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, " TCP Extensions for Multipath Operation with Multiple Addresses," *RFC*, no. 6824, January 2013. [Online]. Available: http://www.ietf.org/rfc/rfc6824.txt

[2] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar, "Architectural Guidelines for Multipath TCP Development," RFC 6182 (Informational), Internet Engineering Task Force, Mar. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6182.txt

[3] C. Raiciu and M. H. D. Wischik, "Coupled Congestion Control for Multipath Transport Protocols," *RFC*, no. 6356, January 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6356.txt

[4] G. Hampel and T. Klein, " Enhancements to Improve the Applicability of Multipath TCP to Wireless Access Networks," individual, IETF Internet Draft – work in progress 00, June 2011. [Online]. Available: http://tools.ietf.org/html/draft-hampel-mptcp-applicability-wireless-networks-00

[5] R. Stewart, "Stream Control Transmission Protocol," RFC 4960 (Proposed Standard), Internet Engineering Task Force, Sep. 2007, updated by RFC 6096. [Online]. Available: http://www.ietf.org/rfc/rfc4960.txt

[6] "MPTCP - Linux Kernel implementation," http://mptcp.info.ucl.ac.be/pmwiki.php?n=Main.HomePage.

[7] M. Lim and J. Valdez, "MPTCP Wireless performance," http://reproducingnetworkresearch.wordpress.com/2012/06/06/mptcp-wireless-performance-draft/.

[8] C. Raiciu, C. Paasch, S. Barre, A. Ford, M. Honda, F. Duchene, O. Bonaventure, and M. Handley, "How hard can it be? designing and implementing a deployable multipath TCP," in *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, ser. NSDI'12. Berkeley, CA, USA: USENIX Association, 2012, pp. 29–29. [Online]. Available: http://dl.acm.org/citation.cfm?id=2228298.2228338

[9] S. C. Nguyen and T. M. T. Nguyen, "Evaluation of multipath TCP load sharing with coupled congestion control option in heterogeneous networks," in *Global Information Infrastructure Symposium (GIIS), 2011*, 2011, pp. 1–5.

[10] B. Chihani and D. Collange, "A multipath TCP model for ns-3 simulator," *CoRR*, vol. abs/1112.1932, 2011.

[11] C. Raiciu, D. Wischik, and M. Handley, "Practical congestion control for multipath transport protocols," *UCL Technical Report*, no. 6824, January 2009.

[12] J. Postel, "Transmission Control Protocol," RFC 793 (Standard), Internet Engineering Task Force, Sep. 1981, updated by RFCs 1122, 3168, 6093. [Online]. Available: http://www.ietf.org/rfc/rfc793.txt

[13] S. Floyd, J. Mahdavi, M. Mathis, and M. Podolsky, "An Extension to the Selective Acknowledgement (SACK) Option for TCP," RFC 2883 (Proposed Standard), Internet Engineering Task Force, Jul. 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2883.txt

[14] D. Wischik, M. Handley, and M. B. Braun, "The resource pooling principle," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 5, pp. 47–52, Sep. 2008. [Online]. Available: http://doi.acm.org/10.1145/1452335.1452342

[15] R. Agüero, M. García-Arranz, and L. Muñoz, "Accurate simulation of 802.11 indoor links: a bursty channel model based on real measurements," *EURASIP J. Wirel. Commun. Netw.*, vol. 2010, pp. 16:1–16:12, April 2010.

[16] M. Zorzi, A. Chockalingam, and R. Rao, "Throughput analysis of TCP on channels with memory," *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 7, pp. 1289–1300, 2000.

[17] "Source code and documentation of the MPTCP implementation (ns-3.13)," https://github.com/dgomezunican/multipath-ns3.13.

Algoritmos y técnicas multi-camino para la mejora del rendimiento de TCP sobre redes malladas inalámbricas

Carlos Rabadán[1],Pablo Garrido[1],David Gómez[2], Ramón Agüero[2]
Universidad de Cantabria, Santander, España
[1]{**carlos.rabadan,pablo.garrido**}**@alumnos.unican.es**
[2]{**dgomez,ramon**}**@tlmat.unican.es**

***Resumen*—El incremento en las ventas de dispositivos inalámbricos, unido al abaratamiento de las tecnologías implicadas en su fabricación, permiten que un porcentaje cada vez mayor de este tipo de terminales dispongan de más de un interfaz para acceder a la red a través de diferentes tecnologías de acceso radio. Esto ha acrecentado el interés de la comunidad investigadora en buscar soluciones que permitan explotar las posibilidades de realizar transmisiones simultáneas a través de varios interfaces. En este trabajo se evalúan tres tipos de algoritmos (*Link Disjoint, Node Disjoint* y *Zone Disjoint*) que tratan de encontrar la mejor configuración de caminos disjuntos en una red mallada inalámbrica. Además, tras los resultados obtenidos se evaluará, mediante una campaña de simulación, el rendimiento del protocolo MPTCP, que permite el envío de tráfico simultáneo a través de diferentes caminos, demostrando que su rendimiento es significativamente superior al del comportamiento tradicional de TCP basado en un único flujo.**

***Index Terms*—Redes malladas inalámbricas, Algoritmos de enrutamiento, MPTCP, Redes multi-canal, Estrategias multi-camino**

I. Introducción

Las tecnologías inalámbricas son las que posiblemente han adquirido una mayor relevancia en las comunicaciones actuales. Junto con los dispositivos más clásicos que hacen uso de ellas (e.g. teléfonos móviles, ordenadores portátiles, etc.), ha aparecido un elenco de nuevos terminales, como los tablets o smartphones, que vienen a demostrar el enorme potencial de este tipo de comunicaciones. Hoy en día viene siendo habitual el hecho de que un usuario medio posea más de un dispositivo que cuente con al menos un interfaz inalámbrico, creando a su alrededor redes de área personal, incluso participando en federaciones de redes.

Algunos de estos equipos serán capaces de interconectarse formando redes malladas inalámbricas, en las que es necesario realizar varios saltos para alcanzar el destino, apoyándose en nodos intermedios. Para poder establecer de manera eficiente una (o varias) rutas, es imprescindible la utilización de protocolos de encaminamiento que proporcionen el conjunto de caminos potenciales para comunicar dos nodos. Existen dos grandes grupos de mecanismos, el reactivo y el proactivo. Los pertenecientes al primero sólo intercambian mensajes de descubrimiento o mantenimiento de rutas en caso de necesidad, mientras que en el segundo tipo se actualizan las tablas de rutas de manera periódica, introduciendo una considerable sobrecarga.

Del mismo modo, la predisposición de los fabricantes a incluir múltiples interfaces en sus dispositivos es una realidad cada vez más habitual en el ámbito de la electrónica de consumo. Gracias a este fenómeno, cada vez se está haciendo más habitual la tendencia a desarrollar nuevos protocolos que posibiliten la utilización simultánea de todos los recursos disponibles en los diferentes "puntos de acceso". Aunque existen multitud de soluciones que tratan de hacer frente a este nuevo tipo de desafíos, el protocolo MultiPath TCP (MPTCP) [1] es una de las apuestas más importantes, contando incluso con un grupo de trabajo en el IETF dedicado exclusivamente a su especificación, así como de un conjunto de extensiones que ayudan a mejorar sus prestaciones. MPTCP es en sí una evolución de TCP (con el que comparte la mayor parte de su arquitectura), que permite dividir la carga entre varios interfaces (siempre y cuando los nodos terminales tengan más de una dirección IP configurada) y consigue mejorar notablemente el rendimiento observado en TCP. La realización de este trabajo se presenta en dos partes claramente diferenciadas: por un lado, se evaluarán las prestaciones de los algoritmos *Link Disjoint (LD)*, *Node Disjoint (ND)* y *Zone Disjoint (ZD)* [2] para encontrar la combinación óptima de caminos disjuntos sobre una red mallada inalámbrica; posteriormente, con la información obtenida se procederá a simular, con `ns-3`, el rendimiento del protocolo MPTCP en este tipo de despliegues, comprobando si es capaz de mejorar las prestaciones del esquema tradicional de TCP. La estructura de este documento se organiza como se detalla a continuación: la Sección II resume las principales contribuciones encontradas en la literatura en los temas aquí tratados, la Sección III introduce los tres algoritmos de búsqueda de rutas que van a ser utilizados para la posterior caracterización del protocolo MPTCP, que será presentado en la Sección IV. La Sección V presenta los principales resultados obtenidos y discute las ventajas e inconvenientes de la aplicación de las técnicas utilizadas. Por último, la Sección VI concluye el documento y anticipa las posibles líneas de investigación que deberán tratarse en el futuro para completar el trabajo aquí presentado.

II. Trabajo previo

En este trabajo se propone la utilización de diferentes algoritmos de encaminamiento, para el posterior empleo de estrategias multi-camino que permitan explotar las ventajas de este tipo de transmisiones sobre redes malladas inalámbricas. Entre sus premisas básicas, se puede decir que ofrecerán

un mayor rendimiento, ya que el ancho de banda agregado entre todas las subconexiones será, como mínimo, igual que el obtenido con, por ejemplo, el protocolo TCP. Además, aportarán una mayor robustez a la conexión, modificando dinámicamente la carga en los subflujos, en función de las condiciones de saturación que presentan.

La clasificación de los algoritmos o protocolos de encaminamiento se divide en dos grandes tipos que, partiendo de bases opuestas, tratan de establecer los mecanismos para descubrir y mantener las rutas en redes multi-salto. Por un lado se encuentran los protocolos proactivos (siendo su principal representante *Optimized Link State Routing - OLSR* [3]), que mantienen la información de las rutas inundando periódicamente la red, factor que introduce una notable sobrecarga en la misma. Por otra parte, los protocolos reactivos o bajo demanda (*Ad hoc On-demand Distance Vector routing - AODV* [4]) tratan de reducir al máximo el intercambio de mensajes de control, recurriendo a ellos sólo cuando sea imprescindible.

La primera generación de protocolos de encaminamiento fue pensada para trabajar con estrategias "single-path", donde un caso de avería/sobrecarga en la ruta establecida provoca que un nodo transmisor tenga que volver a iniciar un mecanismo de descubrimiento para encontrar caminos alternativos con los que poder alcanzar al destino. Debido al crecimiento de las soluciones multi-camino que han ido apareciendo en los últimos tiempos, se hace necesaria la implementación de nuevos protocolos que hagan frente a las demandas impuestas por esta tendencia. La mayor parte de las soluciones encontradas son modificaciones de los protocolos *single-path*, pudiendo clasificarse según el criterio que utilizan para obtener las alternativas al camino más corto: *LD*, que excluye únicamente los enlaces de las rutas calculadas previamente (e.g. *Ad hoc On-demand Multipath Distance Vector - AODVM* [5]), *ND*, que no permite que los nodos intermedios estén presentes en dos rutas diferentes (e.g. *Geographic Multipath routing Protocol - GMP* [6]) y, por último, *ZD*, que inhíbe la participación, tanto de los nodos como de sus vecinos (e.g. *Zone Disjoint Multipath extension of the Dynamic Source Routing - ZD-MPDSR* [7]).

Entre los trabajos más destacados en esta línea se encuentran los realizados por Meghanathan ([8], [2]) que, apoyándose en la teoría de grafos, elabora un completo análisis de las prestaciones de los algoritmos *Link*, *Node* y *Zone Disjoint* en esquemas multi-camino sobre una red mallada inalámbrica con nodos móviles, donde caracteriza exhaustivamente, a través de simulaciones, las diferentes métricas de rendimiento que caracterizan el comportamiento de los algoritmos analizados (e.g. número medio de rutas encontradas, número medio de saltos, tiempo medio entre solicitudes de descubrimiento de rutas, etc.). Por otra parte, Waharte et al. [9] llevan a cabo un estudio alternativo que se centra en los algoritmos LD y ND, prestando especial atención a las posibles interferencias producidas entre los diferentes subflujos (que comparten el mismo canal inalámbrico), estimando el throughput en función del rango de cobertura de los nodos y su posición en el escenario. A diferencia de las contribuciones de Meghanathan, que centra exclusivamente en los algoritmos de encaminamiento, en este caso se aplica tráfico del nivel de aplicación para comparar el rendimiento de los algoritmos de encaminamiento multi-camino con el obtenido con un esquema *single-path*, aunque en ambos casos el protocolo de nivel de transporte utilizado es UDP.

Una vez obtenido el conjunto de caminos disjuntos con el que un nodo transmisor puede enviar información a cualquier otro nodo de la red, aparece la necesidad inmediata de desarrollar algún tipo de solución que pueda particionar una única conexión en diferentes subflujos. Las técnicas más habituales tratan de modificar las funcionalidades del protocolo TCP, permitiendo utilizar estrategias multi-camino (e.g. *mTCP* [10], *R-MTP* [11], *pTCP* [12]). Además, la presencia de grandes organizaciones estandarizadoras, como el IETF, es una garantía del potencial que conlleva este nuevo paradigma de transmisión. Se han creado sendos grupos de trabajo dedicados en exclusiva al diseño e implementación de, posiblemente, las dos alternativas más importantes en lo que se refiere a este tipo de transporte multipath: Stream Control Transmission Protocol (SCTP) [13] y MPTCP [1]. El primero de ellos establece múltiples rutas para proporcionar un factor de redundancia ante errores en algún punto de la red, o facilitar la movilidad entre redes sin necesidad de interrumpir la sesión (nivel de transporte), pero no contempla la utilización simultánea de los diferentes caminos conectados; por el contrario, MPTCP se centra en la mejora de las prestaciones ofrecidas por TCP, aprovechándose de la posibilidad de multiplexar la carga a través de recursos potencialmente ortogonales.

En relación a los trabajos que estudian el comportamiento del protocolo MPTCP en escenarios inalámbricos, se puede encontrar en [14], [15], [16] diferentes estudios del comportamiento de este protocolo, llevados a cabo de diferentes formas, ya sean implementaciones en sistemas reales o canales emulados a través de la implementación en el Kernel de Linux, donde se observa una clara mejoría con respecto a la utilización de TCP, aunque en [16] los autores encuentran un problema cuando los atributos físicos de las tecnologías que constituyen los subflujos son muy diferentes (e.g. IEEE 802.11 y 3G), debido a la sobrecarga introducida por los algoritmos de reordenación de paquetes. Un denominador común de todos estos trabajos es que las topologías objeto de análisis son muy sencillas, consistiendo básicamente en transmisiones de uno o, a lo sumo, dos saltos.

Por último, destacar la contribución realizada por Chihani et al. en [17], que describe una implementación del protocolo MPTCP para el simulador `ns-3` (`ns-3.6`), que sirvió como base para la realización del empleado en este trabajo. En él se presentan un conjunto de algoritmos de control de congestión [18], comparando el comportamiento de las ventanas de congestión de los diferentes subflujos en una transferencia FTP sobre una topología cableada simple, basada en dos terminales conectados directamente a través de dos enlaces punto a punto.

III. Algoritmos de búsqueda de rutas para esquemas multi-camino

El objetivo que persiguen los diferentes algoritmos de encaminamiento multi-camino es el de encontrar una configuración óptima de rutas disjuntas, de tal manera que permitan obtener las mejores prestaciones a la hora de transportar tráfico de manera simultánea a través de los múltiples subflujos (como

se conocerá cada una de las subconexiones en el protocolo MPTCP, objeto de estudio de este trabajo) en un escenario basado en una red mallada inalámbrica.

Para describir el comportamiento de cada uno de los algoritmos utilizados (LD, ND y ZD) se utilizará la notación empleada en la teoría de grafos, tal y como se resume a continuación.

Sea G (V,E) el grafo que representa el escenario sobre el que se requiere obtener el conjunto de rutas (ya sean a través del algoritmo LD, ND o ZD)[1] entre el nodo origen s y el nodo destino d. El conjunto V representa al grupo de nodos desplegados sobre el escenario, mientras que E es el conjunto de enlaces presentes en la red. Se considerará un enlace entre dos nodos si la distancia entre ellos es inferior al rango de transmisión de los dispositivos. En este trabajo se asumirá la utilización de nodos homogéneos, con el rango de transmisión.

El primer paso para obtener el conjunto de caminos a través de los diferentes mecanismos es común: se utilizará el algoritmo de *Dijkstra* [19] para determinar el camino más corto que conduce desde el nodo origen s hasta el destino d. Si existe, al menos, una ruta en el grafo G, será incluida en el conjunto correspondiente (P_L, P_N o P_Z, según corresponda a los algoritmos LD, ND o ZD, respectivamente), procediendo posteriormente a actualizar el grafo según el criterio marcado por el algoritmo, que en este caso sí será diferente. A continuación se muestra el proceso seguido por cada una de las soluciones analizadas:

- **Link Disjoint**. En primer lugar, para determinar el conjunto de rutas LD, después de obtener el camino más corto (Dijkstra), se eliminarán del grafo G todos aquellos *enlaces* que hayan formado parte de la ruta obtenida, dando lugar a un nuevo grafo G' (V, E^L). El proceso se repetirá mientras haya rutas disponibles entre el origen y el destino (que volverán a ser calculadas a través del algoritmo Dijkstra), para añadirlas al conjunto P_L. Una vez terminadas las iteraciones, se dirá que P_L posee el conjunto de caminos *link-disjoint* del grafo original en el instante de tiempo dado.
- **Node disjoint**. En este caso, el criterio de modificación del grafo se centra en la eliminación de todos aquellos *nodos* que han pertenecido a la ruta seleccionada (evidentemente, el borrado de un nodo conlleva a la desaparición de todos los enlaces asociados al mismo). Por lo tanto, tras la conclusión de un ciclo, se obtendrá una nueva ruta a añadir al conjunto *node-disjoint* P_N y un grafo modificado G'(V^N, E^N). De nuevo, el proceso se repetirá mientras s pueda establecer una conexión con d, obteniendo al final el conjunto P_D.
- **Zone disjoint**. Por último, se emplea el algoritmo más restrictivo, el que más penaliza al grafo entre sucesivas iteraciones, eliminándose todos los *nodos* pertenecientes a la ruta devuelta por Dijkstra, así como sus *vecinos adyacentes*, pasando del grafo original G al modificado G' (V^Z, E^Z). Al terminar el bucle, el algoritmo devolverá el conjunto de rutas P_Z.

En un esquema real, los tres algoritmos pueden ser implementados de manera distribuida en una red mallada inalámbrica. El criterio elegido para seleccionar la mejor ruta disponible se basará en aquella que necesite un menor número de saltos; el proceso se repetirá hasta que el transmisor no pueda alcanzar al receptor.

En este trabajo las tareas de elección de rutas se han llevado a cabo en un marco ajeno a la implementación del protocolo MPTCP (y la simulación correspondiente), empleando para ello un código propietario en C++, donde en primera instancia se ha generado un despliegue aleatorio de nodos, dando lugar al grafo G (V,E). Posteriormente, la obtención de los diferentes caminos se ha realizado a través de un único proceso.

Dado que el objetivo de este trabajo es el de utilizar el protocolo de nivel de transporte MPTCP para transmitir información a través de múltiples caminos, solamente se considerarán aceptables aquellos conjuntos de rutas (P_L, P_N o P_Z) que contengan más de un camino que comunique el origen s con el destino d.

IV. El protocolo MPTCP como solución de nivel de transporte

MPTCP nace como una evolución del protocolo TCP que, aún a día de hoy, sigue siendo la solución más utilizada a nivel de transporte, a pesar de que sus prestaciones han sido puestas en entredicho en más de una ocasión. El motivo de su creación viene asociado con el hecho, cada vez más común, de que los dispositivos incorporan múltiples interfaces[2], a través de los cuales será posible comunicarse con el exterior.

El principio básico del protocolo MPTCP es en sí muy simple: si los terminales tienen múltiples puntos de interconexión, se podrían explotar las posibilidades que ello conlleva, dividiendo el tráfico enviado de manera simultánea a través de las diferentes conexiones. Con la utilización de estos esquemas multi-camino se pueden conseguir notables mejoras en el rendimiento global del sistema, así como aumentar la resistencia frente a posibles fallos, pudiendo incluso redirigir la carga completa de un subflujo a otro en caso de que se rompa la conexión en alguno de sus enlaces.

Con el fin de facilitar una compatibilidad hacia atrás con TCP, la recomendación [1] establece que cualquier implementación de MPTCP emplee un esquema que permita una correcta operación en aplicaciones no pensadas para trabajar con este protocolo; en estos casos, no serán capaces de distinguir entre una sesión TCP y una MPTCP. Por este motivo MPTCP será, en esencia, una versión modificada de TCP, por lo que compartirá gran parte de la estructura utilizada para éste, añadiendo extensiones en aquellos puntos que se consideren diferenciales.

Otro de los requerimientos definidos en la recomendación base de MPTCP consiste en que para el establecimiento de una sesión multi-camino será condición necesaria que al menos uno de los equipos terminales, disponga de más de una dirección IP (ya sea configurando varias sobre el mismo interfaz o, para obtener mejores resultados, utilizando dispositivos *multi-homed*).

Para ello, y tras la definir las bases del protocolo en [1], el gran reto de MPTCP puede resumirse en la persecución de los siguientes tres objetivos:

[1] En este trabajo, dado que los nodos permanecen inmóviles, la topología del escenario va a permanecer invariante a lo largo del tiempo.

[2] En la literatura se emplea el concepto de dispositivos *multi-homed*.

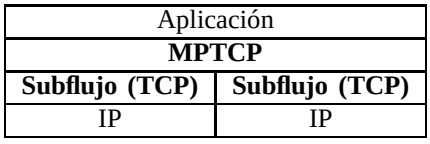


Figura 1: Arquitectura del protocolo MPTCP

1. *Aumentar el throughput*: El rendimiento obtenido a través de un esquema MPTCP debe ser, como mínimo, no inferior al resultante de TCP cuando éste emplee la mejor ruta disponible.
2. *No perjudicar*: Un subflujo MPTCP no debe consumir más recursos que los que TCP necesitaría utilizando únicamente uno de los caminos.
3. *Nivelar la congestión*: Ante una situación de congestión, los algoritmos de control de flujo deberán derivar la mayor cantidad de recursos posible a aquellos subflujos que se encuentren menos congestionados (respetando obviamente los dos primeros objetivos).

Una vez resumidas las funcionalidades generales del protocolo MPTCP, así como los objetivos que persigue, se describe en la Figura 1 la arquitectura que lo define dentro del modelo TCP/IP. Como puede apreciarse, se sitúa en el nivel de transporte y se divide, a su vez, en dos subcapas: mientras la primera de ellas será la encargada de las tareas orientadas a la aplicación (inicialización/finalización de las sesiones, descubrimiento/establecimiento de los subflujos, etc.), el subnivel inferior tendrá una instancia para cada uno de los subflujos creados durante la negociación de la conexión TCP. Asimismo, cada uno de estos tendrá ligada una entidad IP diferente, a través de las que se enviarán los segmentos de información hacia los niveles inferiores.

El mayor desafío al que tiene que enfrentarse el protocolo MPTCP consiste en la distribución correcta de los recursos (conocido en la literatura como "resource pooling" [20]). Para poder conseguir esta meta y, al mismo tiempo, cumplir los objetivos expuestos en la definición del protocolo, será esencial la implementación de un algoritmo de control de congestión en el que el comportamiento de los subflujos esté acoplado de alguna manera. El criterio elegido, a pesar de que el protocolo soporta varias soluciones, consiste en que cada subflujo maneja una ventana de congestión independiente[3]. En el subnivel superior se vinculará un controlador de la congestión, que tratará de mantener un nivel de throughput agregado que, como mínimo, sea igual al que obtendría el TCP tradicional sobre el mejor camino disponible (**Objetivo 1**), sin requerir más recursos de los necesarios (**Objetivo 2**) y llevando, siempre que sea posible, la carga hacia aquellos caminos que se encuentren menos congestionados (**Objetivo 3**). Para estimar el ancho de banda de un flujo TCP simple, la entidad de control estima las tasas de pérdidas y los Round Trip Times (RTTs), devolviendo el nuevo valor de la ventana de congestión correspondiente a cada flujo. Este mecanismo presenta tal magnitud que el IETF ha especificado una recomendación completa para abordarlo [21].

[3]Merece la pena mencionar que, mientras las expresiones para incrementar la ventana de congestión (*additive increase*) tras la llegada de un ACK son específicas de MPTCP, utiliza los mecanismos estándar de TCP en caso de la pérdida de un segmento (*multiplicative decrease*).

V. Simulación y resultados

En esta sección se resumirán las principales características de las campañas realizadas para la obtención de los resultados, presentando aquellos que se han considerado más relevantes. Éstas han sido divididas en dos partes claramente diferenciadas: primeramente, se estudia y compara el comportamiento de las tres técnicas de búsqueda de rutas presentadas en la Sección III; por otro lado, tras la elección de los dos caminos óptimos, se llevará a cabo una simulación en la que se analizará el rendimiento del protocolo MPTCP, para demostrar que puede mejorar la prestaciones ofrecidas por TCP.

V-A. Obtención de las rutas para la aplicación del protocolo MPTCP

En primer lugar, y como paso previo a la caracterización del protocolo MPTCP, se ha implementado un software propietario que, tras la introducción de los parámetros de entrada (área del escenario, número de nodos y rango de cobertura), será capaz de: (1-) desplegar los nodos sobre la superficie, (2-) ejecutar los tres algoritmos de búsqueda de rutas y (3-) generar los ficheros que serán utilizados en `ns-3` para llevar a cabo las simulaciones pertinentes.

Concretamente, para la realización de este trabajo se ha optado por establecer las siguientes condiciones y/o restricciones en esta etapa:

- Los nodos estarán ubicados dentro de un área cuadrada de 100x100 metros.
- Inicialmente se descartarán aquellos despliegues que originen un grafo no conexo.
- En este trabajo no se analiza el comportamiento de los nodos cuando se mueven; por lo tanto, permanecerán estáticos durante todo el tiempo de simulación.
- El rango de cobertura de los nodos será una circunferencia perfecta de 20 metros de radio.
- Para fijar una cierta consistencia a la hora de elegir cuál será la pareja de nodos origen-destino, evitando que puedan ser incluso nodos adyacentes, se ha establecido la siguiente restricción: el nodo más cercano al punto de coordenadas $(20, 50)$ será elegido como transmisor, mientras que el más próximo al $(80, 50)$ ejercerá el papel de receptor, tal y como puede verse en la Figura 2.

A modo de ejemplo, en la Figura 2 se muestra un despliegue completamente aleatorio de 16 nodos elegido arbitrariamente entre todas las realizaciones. En esta topología en concreto se observa que el nodo 8 es el elegido para hacer las veces de transmisor, mientras que el nodo 3 será el destinatario de los mensajes. En lo relativo a las rutas elegidas, los tres algoritmos proporcionarán el mismo resultado: mientras que el camino óptimo estará formado por la secuencia $8 \rightarrow 13 \rightarrow 15 \rightarrow 3$, la segunda opción sigue el orden $8 \rightarrow 11 \rightarrow 10 \rightarrow 12 \rightarrow 3$.

En términos absolutos, la Figura 3 resume el porcentaje de escenarios "realizables" para implementar un esquema multicamino en función del número total de nodos desplegados en el escenario[4]. Un algoritmo será considerado como apto si, al menos, devuelve dos rutas diferentes, para poder dividir el tráfico gracias al protocolo MPTCP. La tendencia observada es

[4]El experimento realizado ha constado de 1000 realizaciones.

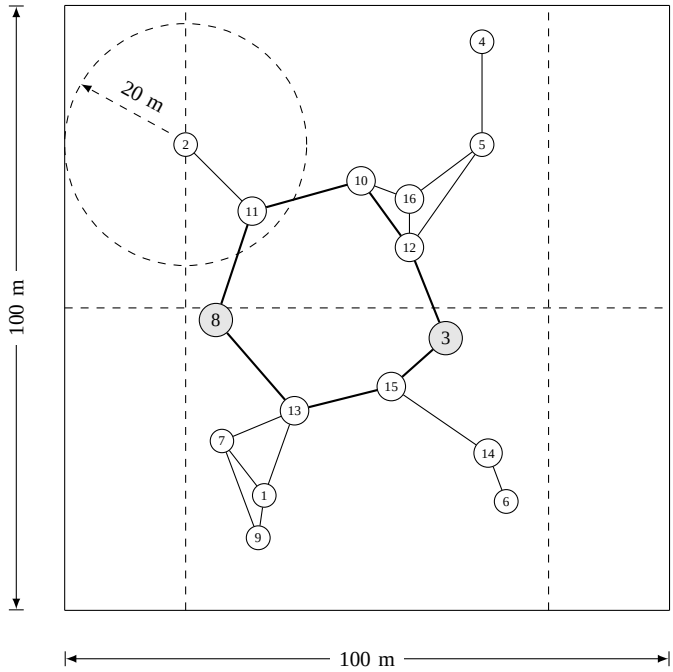


Figura 2: Despliegue aleatorio de 16 nodos en un escenario cuadrado de 100x100 metros

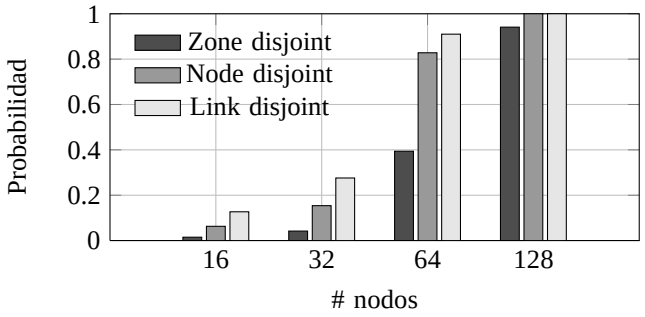
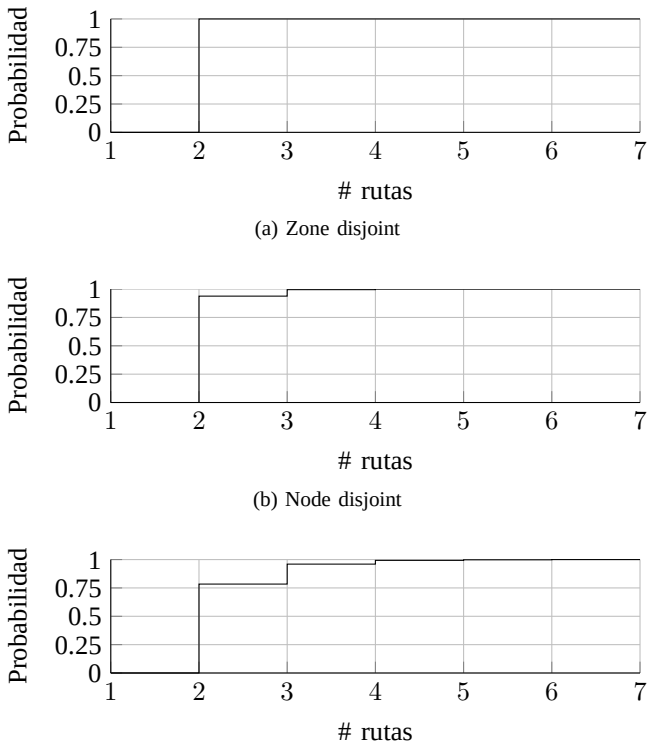


Figura 3: Probabilidad de encontrar una solución multicamino de los diferentes algoritmos de búsqueda

una superioridad generalizada del algoritmo *LD*, seguido por *ND*, que muestran porcentajes muy superiores a los ofrecidos por *ZD*, que aparece como la alternativa más restrictiva.

Tras la comparación efectuada con anterioridad, para la obtención de los siguientes estadísticos se ha añadido una nueva restricción, que permite que los nuevos escenarios generados puedan ser aplicados en las simulaciones de `ns-3`: sólo se darán por válidas aquellas configuraciones que presenten al menos dos rutas en los tres algoritmos estudiados. Además, se ha fijado el número de nodos desplegados a 32. Para tener un número lo suficientemente elevado de muestras, se han obtenido un total de 1000 escenarios que cumplen estos requerimientos. Merece la pena mencionar que para conseguir un número tan elevado de despliegues han tenido que desecharse un número elevado de escenarios, ya que, como se observó en la Figura 3, sólo un 4.2 % de los escenarios de 32 nodos generados presenta las condiciones necesarias para encontrar dos caminos con *ZD*.

En primer lugar, en la Figura 4 se expone la función



(a) Zone disjoint

(b) Node disjoint

(c) Link disjoint

Figura 4: Función de distribución del número de rutas encontradas por los diferentes algoritmos

de distribución acumulada (*cdf*) del número total de rutas encontradas por cada uno de los algoritmos. Tal y como era de esperar, *LD* es el que más posibilidades proporciona, debido a que es el que menos penaliza a los grafos entre las sucesivas iteraciones del algoritmo. *ND* es la solución intermedia, con una probabilidad de que existan escenarios capaces de dividir el tráfico por tres caminos disjuntos. Por último, las restricciones impuestas por *ZD*, no permite encontrar despliegues con más de dos caminos alternativos.

Otro parámetro estadístico de gran interés es la *cdf* del número de saltos encontrados en las dos primeras iteraciones, como se muestra en la Figura 5. Como es predecible, la primera iteración es común para todos, por lo que la longitud del camino más corto no depende del algoritmo empleado. Para el segundo, se repite nuevamente el orden de los parámetros visto anteriormente: como *LD* es el algoritmo que menos modifica el grafo entre rutas, encontrará (en la segunda iteración) los caminos más cortos; por su parte, *ND* se muestra como la opción intermedia, siendo *ZD* otra vez el esquema que presenta peores resultados. El número de saltos tendrá una gran influencia en el ancho de banda agregado del sistema, ya que cuanto mayor sea la longitud de las rutas más se penalizará el throughput del subflujo afectado.

V-B. Rendimiento del protocolo MPTCP en redes malladas inalámbricas

Tras el análisis efectuado para caracterizar y comparar los tres algoritmos en despliegues aleatorios de 32 nodos inalámbricos, se procederá a la simulación de los escenarios resultantes en el simulador `ns-3` [22], utilizando la tecnología

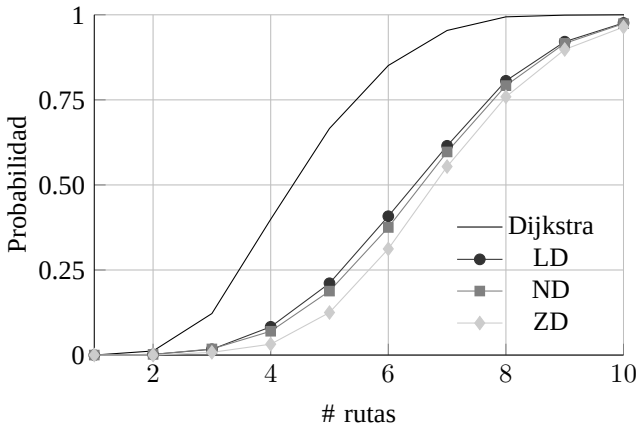


Figura 5: Función de distribución del número de saltos para las dos rutas preferentes

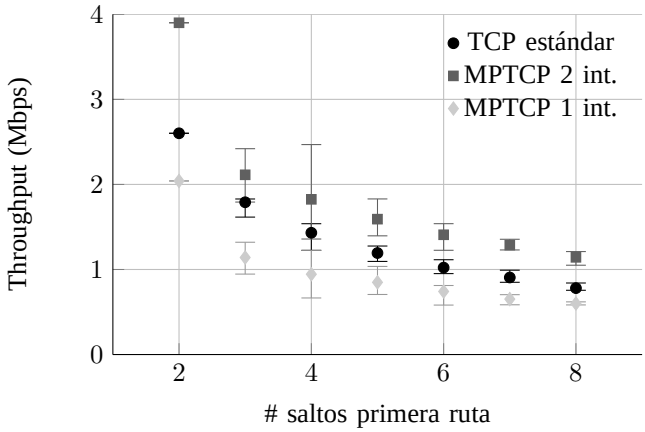


Figura 6: Throughput medio en función del número de saltos de la primera ruta

IEEE 802.11. Es preciso recordar que todos los despliegues aquí analizados presentan, al menos, dos rutas, para los tres algoritmos vistos anteriormente. Por lo tanto, el punto de partida en esta etapa serán los resultados obtenidos en la anterior, que constan de diversos ficheros que proporcionan: (1-) la localización de cada uno de los nodos desplegados, (2-) la secuencia de nodos elegida por cada uno de los algoritmos en las diferentes rutas.

Una vez generados los escenarios, se procederá a simular el comportamiento de diferentes soluciones de nivel de transporte, con el fin de caracterizar su rendimiento:

1. TCP sobre un único flujo. Se corresponde con la configuración más clásica, donde el camino elegido es el más corto (común a los tres algoritmos).
2. MPTCP en dispositivos con un único interfaz, que deberá compartir dos direcciones IP. Con este esquema, el rendimiento se ve enormemente afectado, ya que los dos subflujos comparten el mismo canal inalámbrico, por lo que tanto el número de estaciones contendiendo por el acceso al medio como el número de colisiones serán más elevados.
3. MPTCP en dispositivos con dos interfaces heterogéneos. Se asignará una dirección IP a cada uno de ellos, y estarán asociados a canales diferentes, por lo que no habrá ningún tipo de interferencia entre los subflujos.

Para el análisis del protocolo MPTCP, se ha portado a la versión `ns-3.13` del simulador el trabajo realizado en [17][5], que trata de respetar las indicaciones propuestas en las recomendaciones del IETF [1], [23], [21]. Los esquemas elegidos para el control de la congestión y el reordenamiento de paquetes son *Linked increases* y *DSACK*, respectivamente (para más información acerca de estos algoritmos, consultar [17], donde se detalla su operación). La arquitectura implementada se instalará en cada nodo según convenga en la configuración escogida (1 ó 2 interfaces), distribuyendo la carga a través de los dos subflujos.

Además, es preciso mencionar una serie de puntos utilizados a la hora de generar el entorno de simulación:

1. El nodo transmisor envía un fichero de 20MB al receptor (tráfico *unicast*). Como el objetivo es el de comprobar las capacidades máximas en cada una de las configuraciones, siempre habrá al menos un paquete esperando a ser transmitido en el buffer del equipo transmisor. Con esto se asegura un canal saturado en el que el medio inalámbrico será el auténtico cuello de botella del sistema.
2. El canal inalámbrico elegido estará formado por enlaces basados en la recomendación IEEE 802.11b, fijando el número máximo de transmisiones por trama a 4.
3. Ya que se utilizarán los caminos obtenidos de manera independiente a través de los algoritmos *LD*, *ND* y *ZD*, el esquema de encaminamiento configurado estará basado en rutas estáticas.
4. La única fuente de pérdidas en la transmisión estará ligada a las posibles colisiones, siendo la presencia de errores debidos a la propagación a través del medio inalámbrico despreciable.

Por razones de espacio, solamente se presentan en este documento los valores obtenido con el algoritmo *LD*, que se corresponden con los que presentan un mayor rendimiento (como se ha deducido anteriormente a partir de la *cdf* del número de saltos del segundo camino).

Los resultados obtenidos con las tres configuraciones se exponen en la Figura 6, que muestra el throughput medio, así como los valores máximo y mínimo observados en función del número de saltos requeridos en la ruta más corta. Puede observarse la gran mejora que introduce la utilización del protocolo MPTCP utilizando dos interfaces, consiguiendo en la inmensa mayoría de las situaciones un rendimiento agregado superior a TCP (solamente en casos muy contados, cuando la segunda ruta escogida requiere un número mucho mayor de saltos que la primera se obtienen resultados inferiores), llegando a alcanzar tasas hasta un 50 % superiores en escenarios de dos saltos. Por otro lado, se demuestra el efecto negativo de utilizar la solución multi-camino sobre un único interfaz, ya que la contención causada por el elevado número de nodos accediendo al canal produce unos largos tiempos de espera y un gran porcentaje de colisiones, que tienen como consecuencia unos rendimientos muy inferiores a los vistos en TCP.

[5]Fue desarrollado para la versión 3.6.

V-C. Rutas libres de interferencias

Los resultados vistos hasta este momento han mostrado una clara inferioridad del algoritmo de *ZD* respecto a *LD* y *ZD* en todos los aspectos estudiados: debido al carácter restrictivo que presenta el algoritmo entre las sucesivas iteraciones, donde se elimina la zona de influencia de cada uno de los nodos, no es posible, en la mayor parte de los escenarios, encontrar tan siquiera dos rutas diferentes con las que utilizar técnicas multi-camino. Por si fuera poco, en aquellas topologías en la que sí se obtienen dos caminos, el número de saltos necesarios en la segunda ruta utilizada es mayor, factor que, evidentemente, penaliza el ancho de banda agregado en una conexión MPTCP.

No obstante, existe una posibilidad en la que *ZD* puede presentar unas prestaciones superiores a las alternativas *LD* y *ND*. En aquellos dispositivos que únicamente cuenten con un interfaz inalámbrico[6]. Una escenario ilustrativo de este caso particular se expone en la Figura 7, donde se representa otro despliegue aleatorio de 16 nodos en un área de 100x100 metros.

Como ya ha sido comentado, el primero de los caminos es idéntico para los tres algoritmos, y se corresponde con la secuencia $15 \rightarrow 11 \rightarrow 2 \rightarrow 5$. A continuación se presentan los resultados devueltos para la segunda ruta: $15 \rightarrow 3 \rightarrow 2 \rightarrow 16 \rightarrow 5$ para *LD*, $15 \rightarrow 3 \rightarrow 8 \rightarrow 16 \rightarrow 5$ para *ND* y por último, $15 \rightarrow 14 \rightarrow 10 \rightarrow 13 \rightarrow 5$ para *ZD*. En la figura se aprecia cómo los caminos obtenidos con *LD* y *ND* se encuentran realmente próximos en el espacio, por lo que parece lógico que el efecto de la contención y las colisiones sea elevado, ya que un gran número de nodos tratará de acceder al canal de manera simultánea, siendo el propio medio inalámbrico el auténtico cuello de botella. Por el contrario, gracias a que *ZD* separa "espacialmente" los caminos, conseguirá reducir el "efecto embudo" visto tanto en *LD* como en *ND*. Tras los resultados obtenidos realizando un total de 10 simulaciones con cada uno de los algoritmos, se ha observado un incremento de más de un 5 % en términos de throughput, valor que demuestra que, a pesar de que aparentemente es un algoritmo poco aprovechable en técnicas multi-path, *ZD* es capaz de mejorar las prestaciones obtenidas con los otros dos algoritmos en circunstancias particulares.

VI. Conclusión y líneas futuras

En este trabajo se han presentado tres algoritmos diferentes (*Link Disjoint*, *Node Disjoint* y *Zone Disjoint*) para la obtención de rutas en despliegues genéricos, aunque en este caso han sido aplicados a la utilización de protocolos multi-camino en redes malladas inalámbricas. Han sido sujeto de estudio y se han comparado en términos de utilidad (calculando el porcentaje de realizaciones en los que se obtienen dos o más rutas), número de rutas encontradas y número de saltos necesarios para alcanzar el destino en los dos caminos más cortos. A tenor de los resultados obtenidos, el algoritmo ZD parece una técnica poco conveniente en la búsqueda de rutas para soluciones multipath, aunque es posible que, cuando encuentra múltiples caminos, obtenga un rendimiento mayor en la transmisión, ya que sus condiciones altamente restrictivas buscan alejar las rutas en la mayor medida posible, reduciendo el impacto producido por las interferencias entre diferentes subflujos (e.g. colisiones, contención por el canal, etc.)

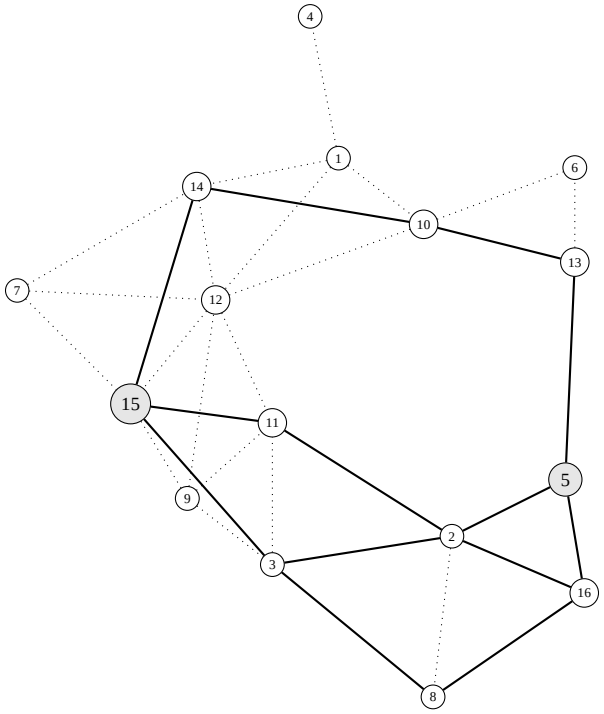


Figura 7: Escenario aleatorio de 16 nodos donde el rendimiento obtenido con las rutas zone-disjoint mejora al observado a través de los algoritmos ND y ZD

Por otra parte, se han utilizado los escenarios y los conjuntos de rutas generados en la etapa de caracterización de los algoritmos de encaminamiento para comparar el rendimiento del protocolo MPTCP con el de TCP, a través de simulaciones en `ns-3`, obteniéndose mejoras que se sitúan alrededor del 50 % en algunos de los casos.

Durante el desarrollo de este trabajo han ido surgiendo una serie de cuestiones que invitan a proseguir expandiendo el análisis de las técnicas multi-camino en redes malladas heterogéneas. A continuación se muestran algunos de los puntos que serán tratados en el futuro:

- Utilizar otros esquemas de encaminamiento, caracterizando sus prestaciones a la hora de encontrar diferentes caminos, potencialmente disjuntos, que exploten la diversidad espacial subyacente a las transmisiones inalámbricas.
- Profundizar en el estudio del rendimiento del protocolo MPTCP en redes malladas inalámbricas, añadiendo un comportamiento más acorde con topologías reales, donde las transmisiones estarán sujetas a errores producidos por la propagación a través del canal inalámbrico.
- Introducir movilidad en los dispositivos emulando el comportamiento dinámico de los nodos como terminales móviles. Con este cambio, los cambios de posición producidos interrumpirán las conexiones entre los elementos, por lo que será necesario calcular de nuevo el esquema de encaminamiento.

[6]En el caso de poder disponer de más de uno, la elección es indiferente, ya que no se presentan interferencias entre las transmisiones de los diferentes subflujos.

Por último, pero no menos importante, es preciso destacar que todo el material relacionado con la implementación del protocolo MPTCP en el marco del simulador `ns-3` tiene un carácter público y puede encontrarse en [24], quedando a total disposición de la comunidad científica.

Acknowledgements

Los autores querían expresar su agradecimiento al Gobierno de España por su financiación en los proyectos "*Comunicaciones Cognitivas y Cooperativas sobre Entornos Heterogéneos*", C3SEM (TEC2009-14598-C02-01) y "*Connectivity as a Service: Access for the Internet of the Future*", COSAIF (TEC2012-38574-C02-02).

Referencias

[1] A. Ford, C. Raiciu, M. Handley, y O. Bonaventure, " TCP Extensions for Multipath Operation with Multiple Addresses," *RFC*, no. 6824, January 2013. [Online]. Available: http://www.ietf.org/rfc/rfc6824.txt

[2] N. Meghanathan, "Performance comparison of link, node and zone disjoint multi-path routing strategies and minimum hop single path routing for mobile ad hoc networks," *CoRR*, vol. abs/1011.5021, 2010.

[3] T. Clausen y P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626 (Experimental), Internet Engineering Task Force, Oct. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[4] C. Perkins, E. Belding-Royer, y S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (Experimental), Internet Engineering Task Force, Jul. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[5] Z. Ye, S. Krishnamurthy, y S. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 1, 2003, pp. 270–280 vol.1.

[6] V. Loscri y S. Marano, "A new geographic multipath protocol for ad hoc networks to reduce the route coupling phenomenon," in *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*, vol. 3, 2006, pp. 1102–1106.

[7] N. T. Javan y M. Dehghan, "Reducing end-to-end delay in multi-path routing algorithms for mobile ad hoc networks," in *Proceedings of the 3rd international conference on Mobile ad-hoc and sensor networks*, ser. MSN'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 715–724. [Online]. Available: http://dl.acm.org/citation.cfm?id=1781974.1782046

[8] N. Meghanathan, "Stability and hop count of node-disjoint and link-disjoint multi-path routes in ad hoc networks," in *Wireless and Mobile Computing, Networking and Communications, 2007. WiMOB 2007. Third IEEE International Conference on*, 2007, pp. 42–42.

[9] S. Waharte y R. Boutaba, "Totally disjoint multipath routing in multihop wireless networks," in *Communications, 2006. ICC '06. IEEE International Conference on*, vol. 12, 2006, pp. 5576–5581.

[10] M. Zhang, J. Lai, A. Krishnamurthy, L. Peterson, y R. Wang, "A transport layer approach for improving end-to-end performance and robustness using redundant paths," in *Proceedings of the annual conference on USENIX Annual Technical Conference*, ser. ATEC '04. Berkeley, CA, USA: USENIX Association, 2004, pp. 8–8. [Online]. Available: http://dl.acm.org/citation.cfm?id=1247415.1247423

[11] L. Magalhaes y R. H. Kravets, "Transport level mechanisms for bandwidth aggregation on mobile hosts," in *Network Protocols, 2001. Ninth International Conference on*, Nov. 2001, pp. 165–171.

[12] H.-Y. Hsieh y R. Sivakumar, "A transport layer approach for achieving aggregate bandwidths on multi-homed mobile hosts," in *Proceedings of the 8th annual international conference on Mobile computing and networking*, ser. MobiCom '02. New York, NY, USA: ACM, 2002, pp. 83–94. [Online]. Available: http://doi.acm.org/10.1145/570645.570656

[13] R. Stewart, "Stream Control Transmission Protocol," RFC 4960 (Proposed Standard), Internet Engineering Task Force, Sep. 2007, updated by RFC 6096. [Online]. Available: http://www.ietf.org/rfc/rfc4960.txt

[14] M. Lim y J. Valdez, "MPTCP Wireless performance," http://reproducingnetworkresearch.wordpress.com/2012/06/06/mptcp-wireless-performance-draft/.

[15] C. Raiciu, C. Paasch, S. Barre, A. Ford, M. Honda, F. Duchene, O. Bonaventure, y M. Handley, "How hard can it be? designing and implementing a deployable multipath TCP," in *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, ser. NSDI'12. Berkeley, CA, USA: USENIX Association, 2012, pp. 29–29. [Online]. Available: http://dl.acm.org/citation.cfm?id=2228298.2228338

[16] S. C. Nguyen y T. M. T. Nguyen, "Evaluation of multipath TCP load sharing with coupled congestion control option in heterogeneous networks," in *Global Information Infrastructure Symposium (GIIS), 2011*, 2011, pp. 1–5.

[17] B. Chihani y D. Collange, "A multipath TCP model for ns-3 simulator," *CoRR*, vol. abs/1112.1932, 2011.

[18] C. Raiciu, D. Wischik, y M. Handley, "Practical congestion control for multipath transport protocols," *UCL Technical Report*, no. 6824, January 2009.

[19] E. W. Dijkstra, "A note on two problems in connexion with graphs," *NUMERISCHE MATHEMATIK*, vol. 1, no. 1, pp. 269–271, 1959.

[20] D. Wischik, M. Handley, y M. B. Braun, "The resource pooling principle," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 5, pp. 47–52, Sep. 2008. [Online]. Available: http://doi.acm.org/10.1145/1452335.1452342

[21] C. Raiciu y M. H. D. Wischik, "Coupled Congestion Control for Multipath Transport Protocols," *RFC*, no. 6356, January 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6356.txt

[22] "The ns-3 network simulator," http://www.nsnam.org/.

[23] A. Ford, C. Raiciu, M. Handley, S. Barre, y J. Iyengar, "Architectural Guidelines for Multipath TCP Development," RFC 6182 (Informational), Internet Engineering Task Force, Mar. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6182.txt

[24] "Implementación del protocolo MPTCP en el marco del simulador ns-3 (versión 13)," https://github.com/dgomezunican/multipath-ns3.13.

Optimized Path Selection in a Game-Theoretic Routing Protocol for Video-Streaming Services over MANETs

Ahmad Mohamad Mezher, Carolina Tripp-Barba, Luis Urquiza Aguiar, Mónica Aguilar Igartua,
Isabel Martín Faus, Luis J. de la Cruz, Emilio Sanvicente
Department of Telematic Engineering.
Universitat Politècnica de Catalunya (UPC)
Jordi Girona street 1-3, 08034 Barcelona, Spain.
[ahmad.mezher, ctripp, maguilar, isabelm, ljcruz, e.sanvicente]@entel.upc.edu, luisfelipe@lfurquiza.com

***Abstract*—Mobile ad hoc networks (MANETs) are infrastructureless networks formed by wireless mobile devices. Recently, the demand over multimedia services such as video streaming has increased specially since the number of mobile end users is growing as well. MPEG-2 VBR is one of the most fitting video coding techniques for MANETs which improves the distribution of video streams specially when it is used with a proper multipath routing scheme. In this article, we aimed to design a routing scheme to dynamically select the forwarding paths using a game-theoretic approach over a multipath routing protocol. Our proposal seeks to describe an equation of the probability p of sending video frames through the best available path. p depends on network parameters that vary throughout time. The aim is that the most important video frames (I+P) will be sent through the best path with a certain probability p and will be sent through the second best path with a probability $1-p$. To achieve that, we carried out simulations done with fixed values of p and after that we applied a lineal regression method to obtain the coefficients of the equation for p. Simulations have been done to show the benefits of our proposal where interfering traffic and mobility of the nodes are present.**

***Keywords*—Mobile ad hoc networks, adaptive multipath routing, game theory, video-streaming services.**

I. INTRODUCTION

A Mobile Ad hoc NETwok (MANET) is a group of wireless mobile nodes (MNs) able to communicate with each other. MANETs are self-organized networks that operate without the need of any fixed network infrastructure or centralized administrative support. MANETs suffer from link breakages and frequent changes of network topology due to nodes that move and have a limited battery life. In addition, the transmission range in such mobile devices is limited, so each node will operate both as a terminal host and as a forwarding node. MANETs should adapt dynamically to be able to maintain communications despite all these issues [1].

MANETs have attracted much attention from the research community over the last years and important technical advances have risen. Recently, these multi-hop networks are considered as an important kind of next generation network access, where multimedia services will be demanded by end users. Two main reasons seem to ensure the success of these networks: firstly, the increasing number of multimedia devices capable of maintaining wireless communications; secondly, the growing number of users who require these multimedia services from their mobile devices. Nowadays, video-streaming services are demanded by users using their mobile terminals from everywhere. In many situations and areas, these demanding users may spontaneously form an infrastructureless ad hoc network to share their resources and their contents.

Multimedia services require Quality of Service (QoS) provision. The special characteristics of MANETs, such as mobility, dynamic network topology, energy constraints, infrastructureless and variable link capacity, make the QoS provision over these networks an important target. That is, instead of using fixed network configuration parameters, a better solution is to adjust the framework according to current environmental parameters.

Our research focuses on the design of a QoS-aware self-configured dynamic framework able to offer video-streaming services over MANETs. In this work, we aimed to design a dynamic selection of the forwarding paths using a game-theoretic approach plus a multipath multimedia routing protocol (MMDSR). This contribution seeks to further enhance the overall performance of the service.

The rest of the paper is structured as follows. Section II presents the basics of our framework. In section III we explain the features of our multipath routing protocol. Section IV gives a brief explanation of the game-theoretic proposal. Simulation results are shown and analyzed in section V. Finally, conclusion and future work are given in section VI.

II. BASICS OF THE FRAMEWORK

We used a framework which provides video-streaming services over IEEE 802.11e [8] MANETs. The multipath routing scheme used in this work is based on the DSR (Dynamic Source Routing) protocol [9]. Video is distributed using RTP/RTCP (Real-time Transport Protocol/RTP Control Protocol) [10] over UDP as a transport protocol. Next, we will summarize the main ideas of the video coding and the IEEE 802.11e standard that we used in our framework.

Our system uses a layered MPEG-2 VBR coding of the video flow, which is formed by sets of frames, usually 4 to 20 frames, called GoP (Groups of Pictures). A GoP has three types of frames: I, P and B, and has a unique frame-pattern in a video repeated in each GoP. I (Intra) frames encode spatial redundancy. They are the base layer and provide a basic video quality. They carry the most important information for the

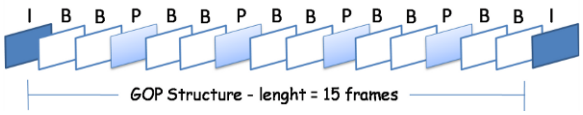


Fig. 1. MPEG-2 GoP structure.

decoding process at the receiving side. The whole GoP would be lost if the corresponding I frame were not available at decoding time. P (Predicted) and B (Bi-directional) frames carry differential information from preceding (for P) or preceding and posterior (for B) frames, respectively. Considering these characteristics, different priorities could be assigned to the video frames according to their importance within the video flow. Therefore, I frames should have the highest priority, P frames a medium one and B frames the lowest one. The structure of a GoP is shown in figure 1, where we can see the relationship between frames at decoding time.

In the MAC (Media Access Control) layer, we used the IEEE 802.11e [8] standard, which provides QoS support to services such as video-streaming. It consists of four different Access Categories (AC). Each packet from the higher layer arrives at the MAC layer with a specific priority value and it is mapped into the proper AC. We defined the mapping of the different packets into each one of the four access categories of the IEEE 802.11e MAC as follows:

- AC0: signaling.
- AC1: high priority packets (I frames).
- AC2: medium priority packets (P frames).
- AC3: low priority packets (B frames + other best effort traffic).

III. Multipath Multimedia Dynamic Source Routing (MMDSR)

In this section we will give a brief summary of the main features of the framework, whose complete description was presented in [2], [3]. In those previous works we presented the MMDSR routing protocol, which here is just summarized very briefly. In this present article we further improve the game-theoretical routing scheme by designing an equation for p that depends on some network parameters. This way, the framework is able to dynamically adapt to the changing network conditions inherent in MANETs.

A. Multipath routing scheme

MMDSR is a multipath routing protocol that uses the standard DSR as base to search for available paths. MMDSR uses up to three paths where the three types of video frames will be sent. As figure 2 shows, the most important video frames (I frames) should be sent through the best path available; P frames through the second best path (medium path) and B frames through the third (worst one). Nonetheless, a different way to send I, P and B frames could be used. In both [5] and [6], they proved that arranging more than three paths simultaneously in a multipath scheme will not give a big improvement benefit while an increasing excessive overhead will be detected .

The user requirements are considered using QoS parameters knowing their threshold values to provide the negotiated image quality. We use the following parameters: minimum

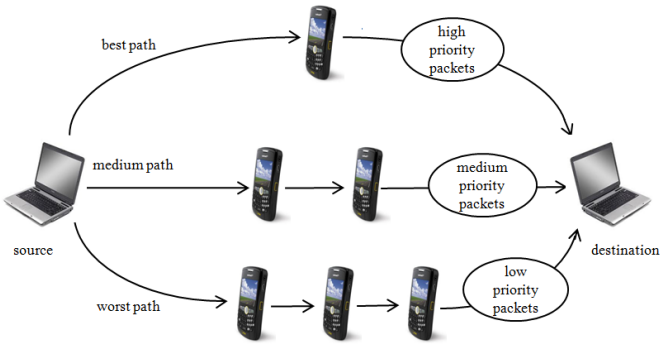


Fig. 2. Multipath routing scheme using three paths.

expected bandwidth (BW_{min}), the maximum percentage of data losses (L_{max}), the maximum delay (D_{max}) and the maximum delay jitter (J_{max})

$$customer\_req \equiv \{BW_{min}, L_{max}, D_{max}, J_{max}\} \quad (1)$$

B. MMDSR control packets

All decisions such as the path selection or the tunning of configuration parameters are operated from the source.

MMDSR periodically discovers D available paths between source and destination by sending monitoring *Probe Message* (PM) packets. After that, a *Probe Message Reply* (PMR) packet is generated at destination to carry the collected information about the quality of the available paths. Notice that the reduced size of theses packets and the low frequency of sending them makes the incurred overhead almost negligible. Figure 3 shows the PM and PMR packets which are periodically interchanged between source and destination.

Finally, a score is given to each one of the paths after analyzing the feedback information at the source node, which classifies them accordingly. Actually, the quality parameters of the paths will be compared to certain thresholds and then the source selects three paths to compose the multipath scheme. The details of the score process can be seen in [2]. *path-state* is a vector that has all quality parameters calculated for each one of the available paths:

$$path - state_k^i \equiv \{BW, L, D, J, H, RM, MM\}_k^i \quad (2)$$

where i is the iteration number of the algorithm and k refers to each one of the paths (with $k \leq D$). The other parameters are: end-to-end available bandwidth (BW_k^i), percentage of losses (L_k^i), delay (D_k^i), delay jitter (J_k^i), hop distance (H_k^i), reliability Metric (RM_k^i) calculated from the SNR (Signal to Noise Ratio) of the links involved in each path, and Mobility Metric MM_k^i calculated from the relative mobility of the neighboring nodes within each path.

To refresh the paths, this process is repeated periodically due to the topology of MANETs that vary and can produce link breakages. This routing period depends on the network state, as it is shown in section III-D.

C. Path classification

Once we have selected a set of paths that fulfil the requirements (see equation (1)), the classification of those paths is done by checking sequentially the qualifications of the QoS parameters as seen in the following list:

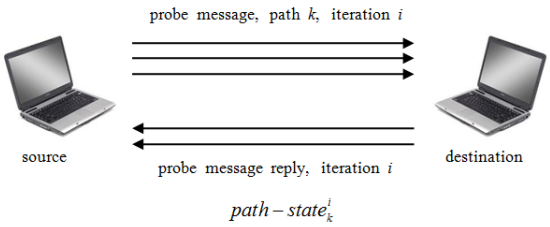


Fig. 3. PM and PMR packets.

1) $RM_k^i + MM_k^i$
2) H_k^i
3) BW_k^i
4) $L_k^i + J_k^i$
5) D_k^i.

First of all, the two metrics RM and MM are used to classify paths since the most reliable and stable paths should be a priority for the correct distribution of video-streaming services over MANETs. In case of draw, the decision is taken depending on the hopcount metric which decide the shortest path. In case of another draw, we consider bandwidth, losses, delay jitter and delay to break the draw, knowing that they are not so decisive metrics in such scenarios. Finally, the source selects k paths (with $k \leq D$) required to compose the multipath routing scheme. In our case, k=3 paths. Notice that if only two paths were available, we still could differentiate both paths (i.e., the better and the worst), but if only one was available then all the packets would be sent through that single path.

D. MANET self-configuration

Here, we will just point out the basics of the self-configuration operation. For further details please see [2], [3]. Due to the network topology of MANETs which is highly variable, any proposed solution should be dynamic. Having this in mind, we designed a self-configured proposal named a-MMDSR (adaptive-MMDSR) [2], [3].

Our framework monitors the current state of the network and in case of changes, the algorithm modifies some configuration parameters, e.g. the routing period of the algorithm and the thresholds to classify paths. We apply some tuning functions to adjust those parameters dynamically depending on a new parameter called *NState*, which has information about the global network state and is updated by the algorithm iteration by iteration. *NState* is computed as follows

$$\begin{aligned} NState^i &= w_{RM} \cdot \overline{RM^i} + w_{MM} \cdot \overline{MM^i} + \\ & w_{BW} \cdot \overline{BW^i} + w_L \cdot \overline{L^i} + \\ & w_D \cdot \overline{D^i} + w_J \cdot \overline{J^i} + w_H \cdot \overline{H^i}. \end{aligned} \quad (3)$$

In equation (3) upper bars denote averages and the *w*s are appropriate weights that sum one. When the source receives the feedback from the network by means of PMR packets, it calculates the *NState* using equation (3).

As *NState*, the routing period ($T_{routing}$) to refresh the multipah scheme also varies dynamically and is calculated according to

$$T_{routing}^{i+1} = 10 \cdot NState^i + 3. \quad (4)$$

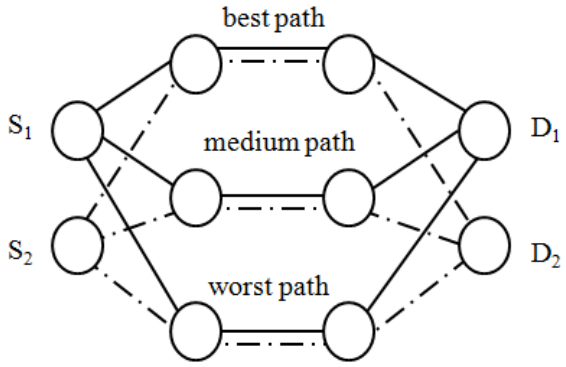


Fig. 4. Fixed strategy to allocate resources.

To reach to the previous equation, a high number of simulations were conducted under a wide range of situations where the network performance was good, normal and bad. The goal was to make it lineal (simple) because it will be computed by light mobile devices.

Till now, we have presented the basics of a QoS-aware adaptive multipath routing protocol. Next, we introduce a game-theoretic routing scheme to further improve the performance of video streaming services over MANETs.

IV. Game Theory in MANETs

Game theory is a branch of applied mathematics that has been used basically in economics to model competition between companies. During the last years, game theory has also been applied to networking, generally to solve routing and resource allocation problems in a competitive environment. MANET nodes make decentralized decisions, and resource management mechanisms can help these nodes to behave in such a way that is constructive to the network as a whole [11]. We applied Game Theory in our multipath routing protocol to develop the present proposal. Each source node has a set of video frames (I, P and B) of a video flow to be transported and has three paths through which those frames could be sent. Nodes *play* a *routing game* to distribute the video flows trying to reach their own best performance. The *players* of the game are the MANET nodes and the *action* of the game is to select the proper route to forward their video-streams. In the following section, we will introduce the game-theoretic proposal included in the multipath routing scheme.

A. A game-theoretic routing protocol

Figure 4 shows the proposed architecture. A complete description of the framework can be found in a previous work [4]. For simplicity of comprehension, we assume two connections (S_1-D_1, S_2-D_2) and three paths. However, it is possible to apply this proposed architecture to any MANET independently from the number of connections, nodes and paths.

By default, nodes always try to send the most important video frames through the best available path discovered by the multipath routing protocol. This means that I frames, which are the bigger ones, will be sent through the best path, whereas the least important frames (i.e., B frames) will be sent through the worst one. Nevertheless, if each node prefers to send the

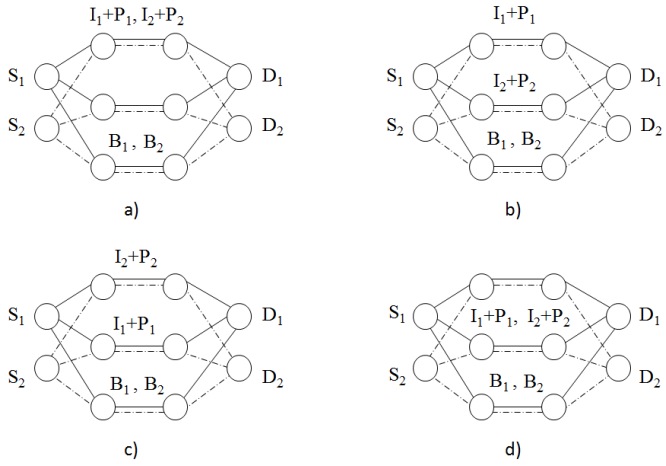


Fig. 5. Four possible allocation situations after playing the game.

most important frames through the best path, this path could got congested. As a consequence, that best path could suffer more losses than the others, which would lead to classify it as a worse path. This behavior could provoke an oscillatory performance that might affect the video experience of users if it happened frequently.

To cope with this issue, users could *play a game* such that the best two paths (best, medium) could be selected by each player to transmit the most important video frames. That is, each user will prefer to send sometimes the most important frames through the second best path. Just for simplicity, B frames are considered always to be sent through the third path, which is the worst one. Also, I and P frames belonging to the same video stream are going to be sent through the same path to make more evident the inconveniences of sharing the same path, since there are more P frames than I frames per flow.

In our game, in each iteration users select paths for their respective video flows. As shown in figure 5, we have four possible situations. I+P frames will be sent through the best path by each user with certain probability p. That is, p is the probability according with users to send their I+P frames through the best available path, where $1 - p$ is the probability that users send their I+P frames through the second best available path. It is important to remember that without playing the game, both users would always send the important frames through the best path (figure 5a). Alternatively, they could play our routing game so that three additional situations would exist as it is depicted in figure 5b, 5c and 5d. In cases b) and c), the user who sends I+P frames through the best path notices a considerable improvement, whereas the other user detects an improvement as well even if it is not so much noticeable. Therefore, cases b) and c) outperform case a). Nonetheless, case d) is worse than a) for both users since they are sending their frames together through the worst path. Notice that players (users) must decide their choices simultaneously and without communicating with each other. A best response; taking other players strategies as given, is a strategy that gives the most favorable outcome for a player. A Nash Equilibrium [7] is a solution where each player plays a best response to the strategies of other players. As an assumption, each player knows the strategies of the other players, and no player will get more benefits to a unilaterally change of their current strategy while the other players keep theirs unchanged.

B. Our new proposal to compute p

Each user plays the routing game to select the forwarding path at each round of the game. So I+P frames are sent through the best path with a certain probability p, which is computed by each source node at each round using equation (5). As we will see, in our approach p is updated over time and it adapts to the changing conditions of the network basically measured in terms of losses. Without the game, I+P frames would always be sent through the best available path (i.e., $p = 1$).

For each video transmission between two nodes, the average packet losses, average end-to-end packet delay and jitter were measured for a different number N of video flows (2 to 5), with and without using our game-theoretic scheme in our MMDSR routing protocol.

The proposal to compute p consists on finding an equation that depends on some network parameters, such as the packet losses and the number of users. This way, the probability p of sending I+P frames through the best path will adapt to the changing networks conditions throughout time. To do this, we conducted a high number of simulations varying the probability p and the number of players (users) N. N varies from 2 till 5 players and p varies from 0.5 till 0.9. In each simulation, we measured the average packet losses as the QoS parameter considered to calculate the coefficients of an equation for p. The equation for p has the following form

$$p(N, Losses) = \beta_0 + \beta_1 \cdot N + \beta_2 \cdot Losses \qquad (5)$$

where

- p = Probability of sending (I+P) frames through the best path.
- N = 2, 3..., N_p where N_p is the number of players.
- $Losses$ = Packet losses from source till destination, i.e.

$$Losses = \left(\frac{packets_{sent} - packets_{received}}{packets_{sent}} \right) \cdot 100 \qquad (6)$$

- β_0, β_1 and β_2 are constants to be calculated.

It is important to mention that in each *Hello Message* (HM), a new field is added to indicate if the node which sent the HM is a video source sender or not. In this way, each node can know how many video source senders are among its neighbours. Then the node can estimate, assuming homogeneity, the total number of video source senders N in the MANET given that the area is known. Finally, the node will be able to compute the value of p using (5).

V. Simulation Results

Our proposal was implemented in the open source network simulator ns-2 (v2.27) [12] where we conducted simulations to evaluate the benefits of our approach. The MANET scenario was generated with the Bonnmotion tool [13]. Interfering CBR traffic was generated to constrain the paths. The simulation settings of the scenario are shown in table I.

The scenario used to test the proposal consists of a set of 50 motion nodes distributed in a MANET of 520x520 m. The

Table I
SIMULATION SETTINGS SCENARIO.

Area	520x520m
Number of nodes	50
Average node speed	2 m/s
Transmission range	120m
Mobility Pattern	Random Waypoint
MAC specification	IEEE 802.11e, EDCF
Nominal bandwidth	11 Mbps
Simulation time	200s
Video codification	MPEG-2 VBR
Video bit rate	150 Kbps
Video sources	2 to 5
Video	Blade Runner
Routing protocol	Game Theoretic algorithm + MMDSR
Transport protocol	RTP/RTCP/UDP
Maximum packet size	1500 Bytes
Multipath scheme	K=3 paths
Weighting values (equation (3))	1/7
Queue sizes	50 packets
Interfering CBR traffic	300 Kbps
Channel noise	-92 dBm
Mobility generator	Bonnmotion

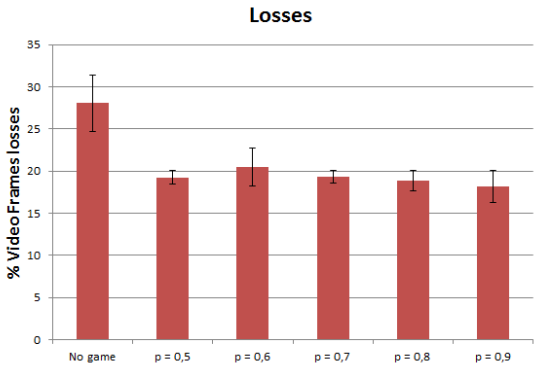
transmission range of the nodes is 120 m. Nodes move with a speed up to 2 m/s. Video flows are transmitted from node S_1 to D_1, S_2 to D_2 till S_N to D_N, where N is the number of players (users). The paths discovered by the MMDSR routing protocol are the same for all sources and are equally classified for all the users using the MMDSR path classification described in section III-C. Each source decides the path to route packets according to the routing game presented in section IV-A and depicted in figure 5.

After multiple simulations, we found the optimal probability p^* that produced lower losses for N= 2, 3, 4 and 5 players. After that, we used lineal regression to obtain the coefficients of the p expression shown in equation (5). The obtained values of the coefficients were: $\beta_0 = 1.2390$, $\beta_1 = -0.1806$ and $\beta_2 = 0.004298$. As the following figures depict, using equation (5) simulations show clear benefits when a variable p is used, compared to the case of using a fixed p value. After we found the values of β_0, β_1 and β_2, we test the results of the output p using (5) by giving the values of losses and N as an inputs. Results of p values are almost the same as shown in table II. This test makes our equation validated.

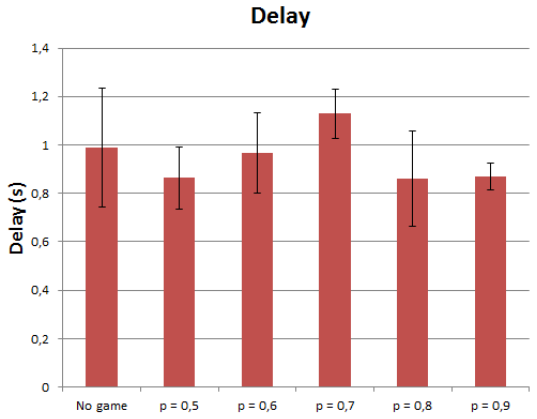
All the figures present confidence intervals (CI) of 90% obtained from five simulation per point. In the following, results of losses, average jitter delay and average end-to-end delay are shown for the case of using the game-theoretic routing versus the case of non using it. We vary the number of users (players) N= 2, 3, 4 and 5. When we use a fixed p, the probability p of choosing the best path to transmit I+P video frames varies from 0.5 till 0.9.

A. For N = 2 players

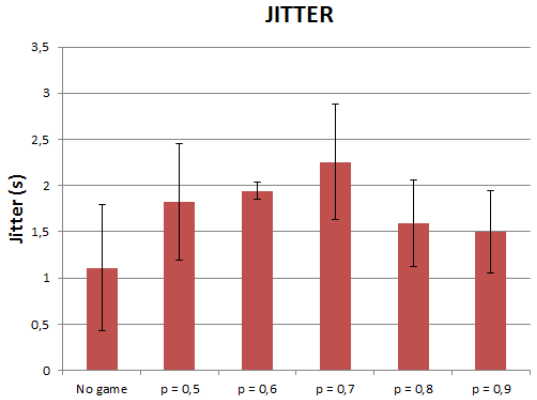
Figure 6(a) shows the average percentage of frame losses when using the game-theoretic scheme for a fixed p value from 0.5 till 0.9 versus the case of non using any game-theoretic scheme (*No game*). We can clearly notice how including the game-theoretic routing scheme, the average video frame losses are reduced from 28% to around 20% depending on the p value. We obtain the lowest value for losses, which is 18,1553% for p^* = 0.9. That is, when 90%



(a) Average packet losses



(b) Average delay

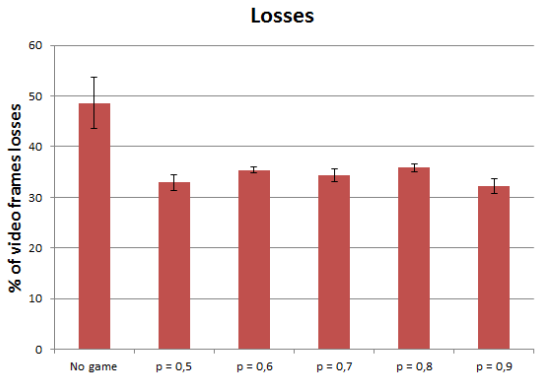


(c) Average delay jitter

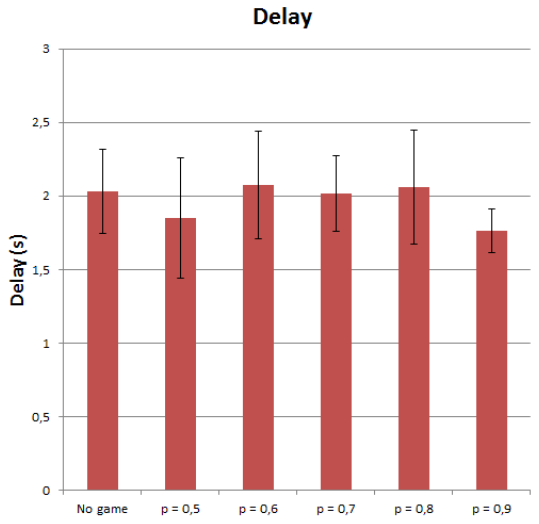
Fig. 6. Losses, delay and jitter delay for N = 2 players

of the time users choose the best path to transmit I+P video frames and 10% of the time they choose the worst path. Notice that without using the game-theoretic approach losses were 28%. This result is due to our routing game that spreads the load among the two best paths so that network resources are used more efficiently and losses decrease.

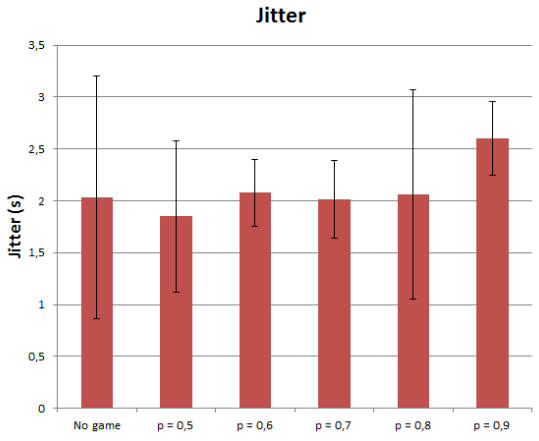
Figure 6(b) shows the average end-to-end packet delay. We see that the delay using the game-theoretic scheme for p = 0.8 or 0.9 shows a better value compared to the *No game* case. Figure 6(c) shows the average delay jitter suffered by the packets. The jitter using the game-theoretic scheme does not show a better result unless for p^* = 0.9, which has a slightly higher value than for the *No game* case.



(a) Average packet losses



(b) Average delay



(c) Average delay jitter

Fig. 7. Losses, delay and jitter delay for N = 3 players

In a previous work [4] we presented a 2-player game-theoretical routing scheme for MANETs where we obtained p^* analytically, although only for the case $N = 2$ players. Our goal as future work is to develop a general game-theoretical routing model for any number of players N. Basically, the MOS (Mean Opinion Score) in each available path was estimated from the packet losses reported in RTP packets using equation (7). Then, the optimum p^* was computed applying equations (7) and (8) in (9). Please, refer [4] to see the whole explanation of the proposal. From figure 6(a) for $N = 2$ we see that the optimum p value is $p^* = 0.9$, whereas in [4] it was $p^* = 0.75$. The reason is that in [4], the average MOS in the best path and in the second best path were $\mu_1 = 4$, $\mu_2 = 2$, respectively. Here, in our scenario these averaged values were $\mu_1 = 5$ and $\mu_2 = 1$. Substituting the MOS values in equation (8) and (9), we obtain $A(\mu_1, \mu_2) = 2$ and p^*=0.75 in [4] and $A(\mu_1, \mu_2) = 1.2$ and $p^* = 0.9$ in this present work. Notice that $p^* = 0.9$ is the same value obtained in our experiments. This comparison leads to the conclusion that depending on the network characteristics we can get one or another optimal p^*.

$$MOS_i = \mu_i \simeq \lfloor 5 \cdot e^{-12 \cdot Losses_i} \rfloor \tag{7}$$

$$A(\mu_1, \mu_2) = 1 + 4 \cdot \frac{\mu_2}{(\mu_1 - \mu_2) \cdot \mu_1} \tag{8}$$

$$p^* = \frac{1}{2}\left(1 + \frac{1}{A(\mu_1, \mu_2)}\right), 0.5 \leq \{p^*\} < 1 \tag{9}$$

B. For N = 3 players

Figure 7(a) shows the average percentage of video frame losses with and without including the proposed routing game.

Again, we notice how including the game-theoretic routing scheme, the average video frame losses are reduced. We obtain the best value for losses with p^* = 0.9. Figure 7(b) shows the average end-to-end delay with and without the game-theoretic scheme. The game-theoretic scheme for p^* = 0.9 shows the lowest delay. Figure 7(c) shows the delay jitter, which is between 2 and 2.5 sec.

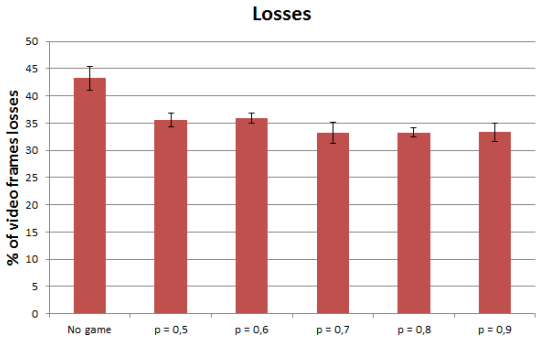
C. For N = 4 players

Figure 8(a) shows the average percentage of video frame losses with and without the proposed routing game. Here, we obtain the lowest value for losses with p^* = 0.7. Figure 8(b) depicts the average end-to-end packet delay. In this case, delay values do not vary a lot, showing values from 0.8 sec to 1.2 sec. Figure 8(c) represents the delay jitter. In this case, we see how the jitter is better when p is greater than 0.5, reaching negligible values.

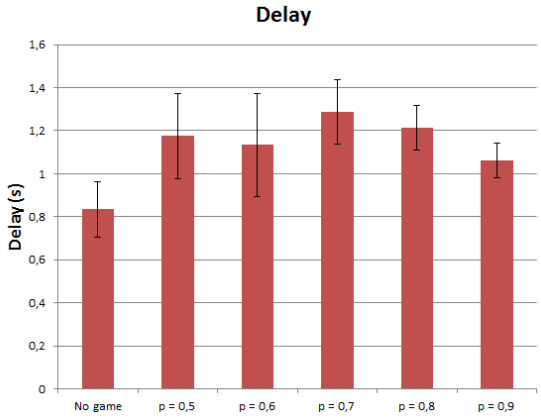
D. For N = 5 players

Figure 9(a) shows the average percentage of video frame losses with and without including the proposed routing game. Again, including the game-theoretic routing scheme, the average video frame losses decrease. We obtain the lowest value for losses with p^* = 0.5. Figure 9(b) shows the average end-to-end delay. We obtain the best value for p^* = 0.5 too. Figure 9(c) shows the delay jitter. In this case, we obtain the best value for p^* = 0.5 as well.

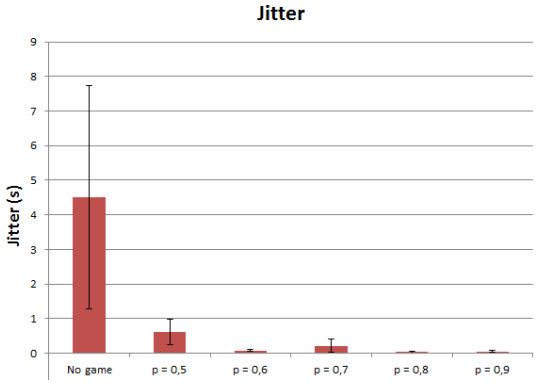
After seeing the previous results, we can see that for $N = 2$ and $N = 3$ players, the optimal value of p that offers the lowest losses is $p^* = 0.9$. For $N = 4$, we obtain $p^* = 0.7$ and for $N = 5$ the optimal value of p is $p^* = 0.5$. These results are resumed in table II. We can see that as the number of players N increases, the optimal value for p decreases tending to 0.5. This has sense, because as N grows, the traffic increases and the paths get loaded, so the best strategy is to choose



(a) Average packet losses

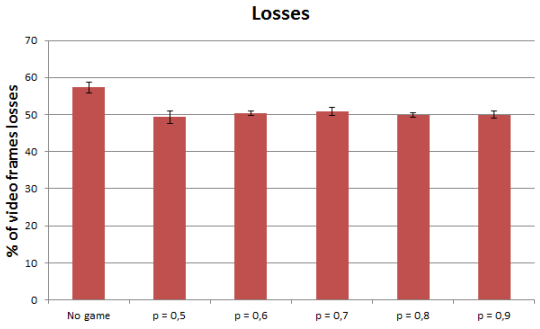


(b) Average delay

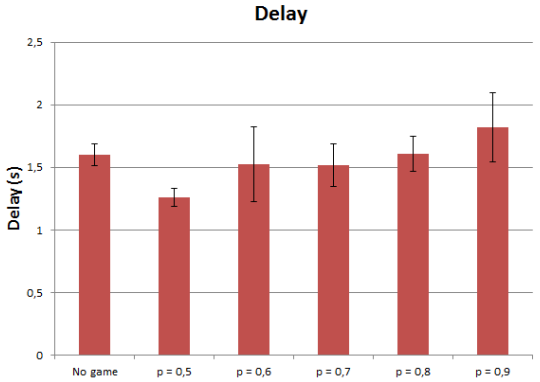


(c) Average delay jitter

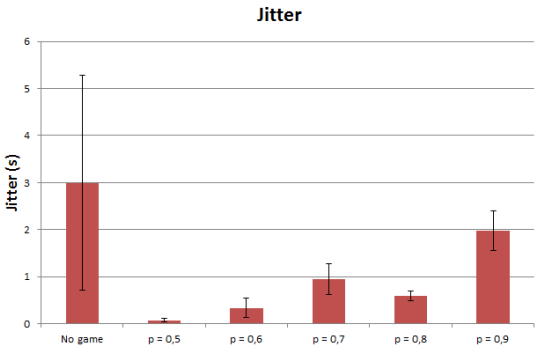
Fig. 8. Losses, delay and jitter delay for $N = 4$ players



(a) Average packet losses



(b) Average delay



(c) Average delay jitter

Fig. 9. Losses, delay and jitter delay for $N = 5$ players

Table II
RESULTS OF THE OPTIMAL $p*$ VALUE.

N	% Losses	Optimal p^*
2	18.1553	0.9
3	32.2535	0.9
4	33.2469	0.7
5	49.3450	0.5

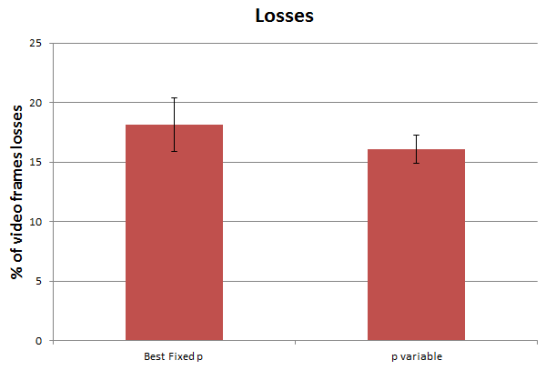
them quite randomly. The load balancing produced by the game-theoretic routing scheme alleviates packet losses. From these results we applied a lineal regression and found the coefficients needed in equation (5).

Now, we will show a performance evaluation obtained with our game-theoretic routing scheme but applying equation (5) to compute p dynamically throughout time instead of using a fixed p value (in particular, the optimal p^*). We will see the results in the scenario for $N = 2$ players.

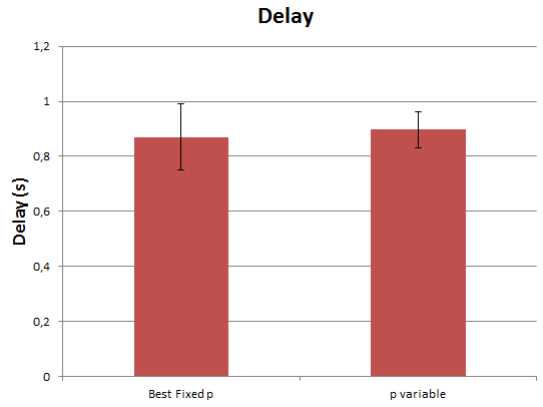
As we can clearly see in figure 10(a), using the variable p losses are lower in comparison to using the best optimal fixed value $p*$. Using our equation for p the probability of choosing the best path to transmit I+P frames depends on the instantaneous characteristics of the network which produces a better behavior.

Figure 10(b) shows the delay which is almost the same in both cases, while the jitter delay shown in figure 10(c) using our new equation to compute p gets a better result.

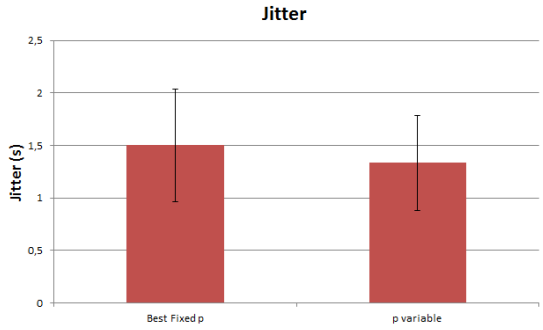
Our multipath routing protocol MMDSR plus our game-theoretic scheme have shown how the global benefits of the users improve if the framework adapts dynamically to the changing network conditions. Our game-theoretical scheme produces lower video frame losses and thus a higher received



(a) Average packet losses



(b) Average delay



(c) Average delay jitter

Fig. 10. Performance for $N = 2$ players, with fixed p^* vs. variable p

video quality. In addition, the network resources are used more efficiently.

VI. Conclusions and Future Work

The inherent dynamic features of MANETs makes providing video-streaming services over wireless mobile ad hoc networks a difficult task. In this paper we have derived from diverse simulations an equation which makes the probability p of sending the most important video frames (i.e., I+P) through the best available path vary depending on some network characteristics. This means, instead of sending I+P video frames always through the best available path, users play a strategic routing game where these frames will be sent through one of the two best paths according to a certain probability p. First, we found by simulation the optimal probabilities p^* which produce the best result. After that, we applied a lineal regression to find the coefficients of the proposed equation (5).

Simulation results show the benefits of our proposal, first outperforming the results compared to the case of non using our game-theoretical routing; and second improving the case of using the game-theoretical routing with a variable value of p over the case of using the fixed value of p^*. Our proposal makes the network more efficient as well as achieves a higher degree of satisfaction of the users.

As a future work, we are planning to develop an analytical approach to compute p in the game-theoretical routing for a general number N of players. In a previous work [4] we solved this for $N = 2$ users, based on a 2-player routing game. Now, we plan to design a N-player routing game. Also, we would like to implement this framework in vehicular ad hoc networks (VANETs), where video-streaming services are taking an important attention. Our proposal could be a solution to improve the routing operation for multimedia data over VANETs.

Acknowledgements

This work was partly supported by the Spanish Government through the projects CONSEQUENCE (TEC2010-20572-C02-02), TAMESIS (TEC2011-22746) and SERVET (TEC2011-26452). Ahmad Mezher is the recipient of a FI-AGAUR grant, from the Government of Catalonia. Carolina is granted by the Autonomous University of Sinaloa (Mexico). Luis Urquiza is the recipient of a grant from Secretaria Nacional de Educación Superior, Ciencia y Tecnología SENESCYT and the Escuela Politécnica Nacional (Ecuador).

References

[1] Azzedine Boukerche, “Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks”, *Wiley-IEEE Press*, 2008.
[2] V. Carrascal, G. Díaz, A. Zavala, M. Aguilar, “Dynamic cross-layer framework to provide QoS for video-streaming services over Ad Hoc networks”, *ACM QShine*, Hong Kong, 2008.
[3] V. Carrascal Frías, G. Díaz Delgado, M. Aguilar Igartua, “Multipath Routing with Layered Coded Video to Provide QoS for Video-streaming applications over MANETs”, *14th IEEE International Conference on Communication Networks* (ICON), 2006.
[4] Mónica Aguilar Igartua, Luis J. de la Cruz Llopis, Víctor Carrascal Frías, Emilio Sanvicente Gargallo, “A game-theoretic multipath routing for video-streaming services over mobile Ad Hoc networks”, Computer Networks, ISSN: 1389-1286, Vol. 55, Iss. 13, pp. 2985-3000, 15th September 2011, DOI: 10.1016/j.comnet.2011.06.007.
[5] V. Carrascal Frías, G. Díaz Delgado, M. Aguilar Igartua, “Multipath Routing with Layered Coded Video to Provide QoS for Videostreaming applications over MANETs”, 14th IEEE International Conference on Communication Networks (ICON), 2006.
[6] V. Loscri, F. De Rango, S. Marano, “Performance evaluation of ondemand multipath distance vector routing protocol over two MAC layers in mobile ad hoc networks”, 1st International Symposium on Wireless Communication Systems, 2004.
[7] J.F. Nash, Non-cooperative games, Annals of Mathematics, 1951.
[8] IEEE 802.11e standard with Quality of Service enhancenments, *http://standards.ieee.org/getieee802/download/802.11e-2005.pdf*.
[9] RFC 4728, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4”, 2007.
[10] RFC 3550, “RTP: A Transport Protocol for Real-Time Applications”, *http://www.ietf.org/rfc/rfc3550.txt*, 2003.
[11] M. Nasarien, K. Tepe, “Game theoretic approach in routing protocols for wireless ad hoc networks”, *Elsevier Ad Hoc Networks*, Vol. 7, pp: 569-578, 2009.
[12] The Network Simulator, ns-2, *http://nsnam.isi.edu/nsnam/*.
[13] BonnMotion, A mobility scenario generation and analysis tool, *http://web.informatik.uni-bonn.de/IV/Mitarbeiter/dewaal/BonnMotion/*, 2005.

Medición de la Privacidad de Perfiles de Usuario mediante un Add-on de Navegador

José Estrada-Jiménez, Ana Rodríguez, Javier Parra-Arnau, Jordi Forné, David Rebollo-Monedero
Departamento de Ingeniería Telemática
Universidad Politécnica de Catalunya (UPC)
C. Jordi Girona 1-3, 08034 Barcelona, España
{jose.estrada, ana.rodriguez, javier.parra, jforne, david.rebollo}@entel.upc.edu

***Resumen*- Actualmente, la monitorización de los usuarios en Internet es permanente, y la información obtenida en este proceso es de enorme interés para grandes compañías de publicidad e incluso gobiernos. Además, la gran cantidad de datos susceptibles de recopilarse por los sistemas de información personalizados representa un grave riesgo para la privacidad del usuario en Internet. Quizá aún más crítico es que muchos usuarios no son conscientes de este riesgo, ya que éste no es tan manifiesto como en el mundo físico.**

En este artículo presentamos un *add-on* de navegador que estima el riesgo de privacidad del perfil de un usuario, quien por sus hábitos de navegación, está expuesto a mecanismos de *profiling* en Internet. El nivel de riesgo se muestra, de manera comprensible y accesible en la interfaz gráfica del navegador y se calcula tomando en cuenta diferentes modelos de adversario.

***Palabras Clave*- perfil de usuario, métricas de privacidad, entropía de Shannon, divergencia de Kullback-Leibler, extensión de navegador, *add-on de navegador*.**

I. INTRODUCCIÓN

Actualmente en Internet, y gracias a los evidentes avances en las técnicas de análisis de datos, el *profiling* y la clasificación de usuarios son una práctica común, llevada a cabo por sistemas de personalización de contenido que se alimentan de toda la información que entrega el usuario aunque éste, en la mayoría de casos, no sea consciente de su magnitud.

La creación de perfiles de usuario, a partir sus patrones de navegación, permite la recomendación personalizada de contenido y, especialmente, de publicidad, pero a un precio bastante alto: la privacidad del usuario. Los rastros que deja un usuario, aunque sean dispersos o incluso perturbados, combinados con otros de distintas fuentes, podrían revelar información potencialmente sensible relacionada con preferencias personales [1], [2].

La información sujeta a análisis va desde el contenido de las páginas visitadas, el tiempo consumido en un sitio web, el número de clics, las consultas a un motor de búsqueda, los datos entregados en formularios, y las cookies, hasta la configuración particular del navegador [17].

En ese entorno existe, por lo tanto, una amplia gama de posibles atacantes: motores de búsqueda, sistemas de recomendación, redes sociales, sistemas de etiquetado, etc. Sin embargo, los proveedores de servicios de Internet son entidades que tienen acceso a toda esa información sobre la actividad del usuario y, en muchos casos, ésta es también comercializada con compañías de publicidad o directamente utilizada para alimentar una plataforma de anuncios, sin considerar la privacidad de los dueños de esos datos [3].

Existe mucha presión sobre estas empresas que manejan información personal ([4] y [5]) para que apliquen fuertes políticas de privacidad, con el fin de proteger los datos sensibles. Parece, sin embargo, que la presión externa (desde gobiernos por ejemplo) por revelar este rastro digital puede resultar mayor.

Además, las políticas de privacidad que aplican los proveedores de servicios se comunican de una manera tan deficiente que los usuarios apenas las leen y difícilmente las comprenden, por lo que las aceptan rápidamente sin reflexionar, con el único fin de hacer uso inmediato de algún servicio "gratuito".

Esto demuestra que existe una generalizada falta de consciencia respecto a los riesgos a los que están expuestos los usuarios en Internet y de la consecuente vulneración de su derecho a la privacidad.

Estos intereses económicos y políticos sobre la información en la Web y las prácticas inadecuadas respecto a la privacidad de los usuarios no parece que vayan a cambiar con el tiempo. Sin embargo, el comportamiento del usuario respecto a su información sí puede modificarse, si se logra evidenciar las debilidades de su conducta. El problema radica en que no existen herramientas que informen al usuario sobre su nivel de privacidad. Existen herramientas que implementan medidas de ofuscación o bloqueo, pero ninguna que permita al menos determinar su efectividad. Es que el nivel de privacidad (o riesgo de privacidad) puede ser relativo al entorno del usuario (la población) y, por lo tanto, las medidas de protección podrían depender incluso de sus intereses individuales.

A nuestro juicio, es imprescindible medir el nivel de privacidad para aplicar, en función de éste, un mecanismo de protección que se ajuste a las necesidades del usuario, especialmente cuando el enorme éxito de la publicidad dirigida incentiva a todos los proveedores de contenido a aplicar avanzadas técnicas de elaboración de perfiles para modelar el comportamiento de los usuarios.

A. Contribución

Considerando el riesgo para la privacidad que representan las actividades de *profiling*, y la inexistencia de mecanismos para poder evidenciarlo, proponemos la implementación de un *add-on* para el navegador Mozilla Firefox que permite medir la privacidad del usuario a partir de su perfil, que se obtiene de las consultas a motores de búsqueda, del contenido de las páginas web desplegadas, del número de clics sobre las páginas y del tiempo que el usuario permanece

en ellas. Este *add-on* captura todo este rastro dejado por el usuario y en base a éste último muestra, de una manera comprensible, varias mediciones de su privacidad, teniendo en cuenta distintos modelos de adversario.

El conocimiento y la interpretación de estas medidas de privacidad podrían ayudar a los usuarios a tomar una decisión informada respecto de su actividad en la Web y permitirían evaluar tecnologías de mejoramiento de la privacidad para determinar su utilidad real. Esto facilitaría, además, la comparación y la optimización de estas tecnologías.

Nuestro *add-on* reutiliza el módulo de *profiling* de otro *add-on* de Mozilla Firefox llamado Adnostic [5]. En concreto, dicho módulo nos permite obtener un perfil de usuario en base al cual determinamos varios niveles de riesgo de privacidad, mediante la utilización de métricas justificadas en conceptos de teoría de la información.

B. Organización

El artículo se ha organizado de la siguiente manera. La Sec. II explora algunas de las herramientas y mecanismos existentes orientados a la protección de privacidad. La Sec. III resume los modelos de atacante y las métricas utilizadas para determinar los niveles de riesgo de privacidad. La Sec. IV describe la arquitectura y los módulos de nuestro *add-on*. Finalmente en la Sec. V se mencionan las conclusiones.

II. ESTADO DEL ARTE

Actualmente existen algunas herramientas que tratan de proteger la privacidad del usuario en Internet, esencialmente mediante el bloqueo de funciones que facilitan la entrega de información personal. Estos mecanismos, generalmente basados en la heurística, no miden el riesgo de privacidad del usuario ni evalúan el nivel de protección que ofrecen.

Adnostic [6] es un *add-on* desarrollado para Mozilla Firefox que implementa una arquitectura para desplegar publicidad personalizada, sin comprometer la privacidad del usuario, ya que se decide en el navegador qué anuncios mostrar, en función de un perfil calculado localmente. Este perfil se obtiene a partir de un procesamiento de las consultas que realiza el usuario y del contenido de las páginas que visita. Luego, esta información es clasificada utilizando procesamiento natural de lenguaje dentro del navegador. Los anuncios, parte de un conjunto previamente descargado, se despliegan dependiendo de los intereses del usuario.

REPRIV [7] es otro sistema propuesto para trabajar en el navegador que ofrece una personalización mejorada de contenido y un mecanismo de control del usuario sobre la información que entrega a terceros. Usa la información de navegación del usuario para descubrir cuáles son sus intereses, y comunicarlos a terceros para que estos últimos puedan ajustar el contenido en base a esas preferencias. Propone interfaces para sitios web de terceros para los protocolos de comunicación de información personal que funcionan sobre HTTP. Promete una mejora importante en la provisión de contenido a medida, gracias al gran detalle de la información del navegador, pero el control de privacidad podría verse afectado por la falta de usabilidad de las políticas de protección que se implementen y que un usuario promedio tendría que gestionar. Además, no implementa ninguna métrica que indique al usuario el nivel de privacidad que posee.

En relación específica con la medición de privacidad, existen un par de estudios ([8] y [9]) sobre herramientas para redes sociales (Facebook en los dos casos) que determinan el riesgo de privacidad del usuario en función de la cantidad de información que de éste se puede inferir a partir de sus relaciones con otros usuarios. También implementan acciones de protección de privacidad bloqueando estos usuarios, analizando la configuración de privacidad de la cuenta o detectando y eliminando aplicaciones que poseen demasiados permisos.

TrackMeNot [10] es otra herramienta para protección de privacidad a nivel de navegador que propone ofuscar el flujo de consultas del usuario a motores de búsqueda mediante la generación de consultas falsas. Ha recibido muchas críticas respecto de su eficacia, aunque no se han propuesto muchos mecanismos para evaluar sus bondades. En [11] se muestra que estas consultas falsas podrían ser identificadas con relativa facilidad utilizando clasificadores basados en inteligencia artificial. Sin duda, la falta de una herramienta de medida de privacidad le impide al usuario valorar su condición de riesgo antes y después de aplicar una estrategia de protección como ésta.

Google Sharing [20] es otra herramienta que implementa un mecanismo de protección de privacidad al prevenir el rastreo del usuario realizado por Google mediante las consultas al motor de búsqueda. El mecanismo consiste en que el usuario envía sus peticiones a un proxy externo que gestiona un grupo de identidades asociadas a *cookies*. Estas *cookies* reemplazan las *cookies* de las peticiones, enmascarando la identidad del usuario, y luego son reenviadas con la petición original a Google. Aun cuando permite enviar peticiones cifradas desde el usuario, su privacidad puede comprometerse si hay colusión entre Google y el servidor proxy.

Ghostery y *Collusion* son *add-ons* que enfrentan el problema de privacidad del usuario mediante la identificación de *trackers* o entidades que rastrean los movimientos del usuario, generalmente a través de una *cookie* de terceros. *Ghostery*, en especial, es muy completa ya que detecta y muestra información sobre estos *trackers*, y además bloquea los elementos de ejecución dinámica no confiables que se cargan en el navegador, mediante los cuales es posible este rastreo. Estas herramientas dejan de lado, sin embargo, la información que el usuario entrega en Internet y que podría fácilmente revelar su identidad.

El modo de "navegación privada" es también una opción de protección de privacidad en los navegadores más conocidos. Ésta opción deshabilita el almacenamiento local de información (historial, imágenes, videos, *cookies*, etc.) durante la navegación web. Esto complica significativamente el acceso del usuario a muchos sitios en Internet, por lo que quienes usan este modo lo hacen durante intervalos de tiempo muy cortos. El nivel de protección se limita al ámbito local pues externamente existen otros mecanismos para identificar y clasificar al perfil del usuario.

El bloqueo o desactivación de ciertas características del navegador web es una medida común implementada por varias soluciones en forma de *plug-ins* de navegador (NoScript [18], AdBlock Plus [17], DoNotTrackMe [21]), y evitan que se libere información que pueda usarse para identificar al usuario.

Sin embargo, ninguna de estas herramientas o mecanismos evalúa el nivel de privacidad del usuario. Se considera como posibles adversarios únicamente a los anunciantes o a los servicios de redes sociales pero no a los proveedores de servicios de Internet (ISP, *Internet Service Provider*) que son las entidades que más información poseen sobre los usuarios, tomando en cuenta que es muy habitual que los usuarios naveguen utilizando conexiones sin cifrar (sin usar HTTPS). Con base a la última consideración, el ISP tiene acceso a mucha información, y el gran detalle de la misma representa un enorme incentivo para su comercialización, por lo que además existen muchos potenciales compradores.

En [22], [23], [24] y [25] se abordan en detalle algunos mecanismos que podrían emplearse para la protección de la privacidad del usuario en entornos donde éste hace consultas o etiqueta contenido; considerando también el costo de estas estrategias que se refleja en la pérdida de utilidad de los datos, la pérdida de funcionalidad de un servicio o el consumo adicional de recursos. Se incluye entre estos mecanismos la falsificación de consultas o la supresión de etiquetas con el fin de mostrar una versión distorsionada del perfil del usuario que el atacante no pueda explotar. La optimización de estos mecanismos así como su impacto son también sujetos de estudio.

III. Modelos de Atacante y Métricas de Privacidad

En esta sección presentamos los dos modelos de atacante considerados en este artículo, así como las dos métricas que nos permiten evaluar el nivel de privacidad de un usuario. Los modelos y métricas de usuario son ampliamente justificados en [12].

A. Modelos de Atacante

Los criterios de privacidad se plantean inicialmente asumiendo que el perfil del usuario es modelado como una función de masa de probabilidad o un histograma de frecuencias relativas de datos de usuario a lo largo de un conjunto preestablecido de categorías de interés. Este modelo supone una representación muy habitual en los servicios de información personalizada.

El modelo de adversario permite definir las propiedades del atacante, considerando como tal a cualquier entidad capaz de tener acceso a información de usuario con el objetivo de obtener su perfil, con el riesgo a la privacidad que esto implica.

Conocer al adversario es importante ya que la privacidad del usuario se mide respecto a éste. En función de las propiedades del adversario, el usuario podría implementar medidas de protección de su privacidad que, por ejemplo, modificasen su perfil de intereses.

Esencialmente, se contemplan dos objetivos del atacante, en función de sus capacidades y que definen el modelo de adversario; *identificación* y *clasificación*.

- *Identificación*, cuando el atacante intenta distinguir al usuario del resto de la población, detectando desviaciones de sus intereses respecto del perfil promedio de la población.

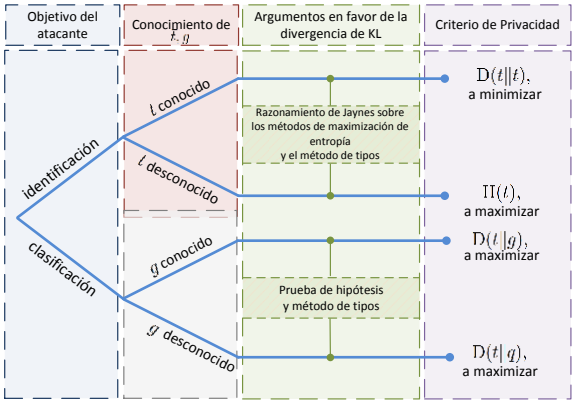


Fig. 1. Resumen de las interpretaciones de la entropía de Shannon y de la divergencia de KL (entropía relativa) como métricas de privacidad, de acuerdo con la justificación presentada en [12].

- *Clasificación*, cuando el atacante intenta clasificar al usuario en un grupo de población, comparando el perfil del usuario con el perfil representativo del grupo.

B. Métricas de Privacidad

En [12] se justifica la entropía de Shannon y la divergencia de Kullback-Leibler [28] (conocida también como divergencia de KL o entropía relativa) como medidas de privacidad. Las interpretaciones de estas medidas dependerán de las hipótesis que se hagan, fundamentalmente respecto del modelo de adversario.

Otra métrica más general, no limitada a la privacidad de perfiles, es la propuesta en [26]. En este trabajo, los autores proponen medir la privacidad como el error de estimación de un adversario, e interpretan, mediante argumentos de teoría de la información y teoría de decisión Bayesiana, otras métricas del estado del arte como casos particulares de la suya.

Para facilitar la comprensión, además, se resume a continuación las principales definiciones propuestas para la justificación de estas métricas de privacidad. Se revisa además la interpretación de estas dos cantidades de teoría de la información como métricas de privacidad de perfiles de usuario.

El símbolo H denotará la entropía de Shannon y D denotará la divergencia de KL. La entropía $H(p)$ de una variable aleatoria discreta X con distribución de probabilidad p es una medida de su incertidumbre, definida como

$$H(X) = -E \log p(X) = -\sum_x p(x) \log p(x).$$

La divergencia de KL o entropía relativa D ($p \parallel q$) entre dos distribuciones de probabilidad $p(x)$ y $q(x)$ sobre el mismo alfabeto se define como

$$D(p \parallel q) = E_p \log \frac{p(X)}{q(X)} = \sum_x p(x) \log \frac{p(x)}{q(x)}.$$

La divergencia de KL es una medida de discrepancia entre distribuciones de probabilidad, garantizando que $D(p \parallel q) \geq 0$, con igualdad si, y sólo si, $p=q$. Consecuentemente se deduce que la entropía $H(p)$ alcanza su valor máximo en $H(u)=\log n$, siendo n la cardinalidad del alfabeto finito sobre el que se calcula $D(p \parallel u)$, para una distribución uniforme u:

$$D(p \parallel u) = \log n - H(p) .$$

En concreto, acorde con el análisis en [12] tenemos que la maximización de la entropía resulta ser un caso especial de la

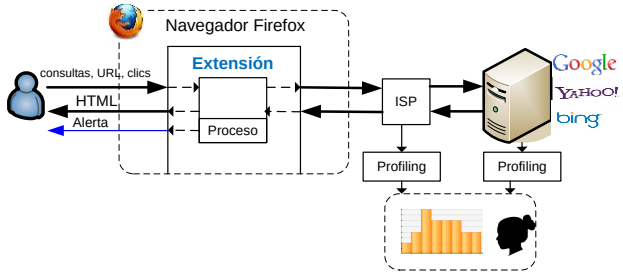


Fig. 2. Esquema de navegador y un *add-on* como intermediarios entre usuario y servicios de Internet (motores de búsqueda y proveedor de servicios) y el inherente riesgo de *profiling*.

minimización de la divergencia, alcanzada idealmente cuando la distribución a optimizar es idéntica a la de referencia.

Sea q el perfil de interés de un usuario, t una versión perturbada o modificada del mismo y $\bar{t}$ la distribución del perfil de la población. En la Fig. 1 se muestran las interpretaciones de la entropía de Shannon y de la divergencia de KL como medidas de privacidad. Éstas se explican a continuación, de acuerdo al objetivo del atacante.

- *Métricas contra identificación*

En caso de que el objetivo del atacante sea identificar al usuario, el razonamiento de Jaynes acerca de los métodos de maximización de la entropía permite justificar la divergencia y la entropía como medidas de privacidad.

La entropía del perfil aparente del usuario, que es el perfil observado por el atacante, es justificada en [12] como una medida de la probabilidad de este perfil perturbado, en el sentido de frecuencia de aparición de dicho perfil en la población de usuarios. Considerando esta probabilidad del perfil de usuario como una medida razonable de su anonimato (o privacidad), en [12] se justifica también la entropía como una métrica de privacidad. En concreto, mientras mayor sea la entropía de este perfil, mayor es su probabilidad, y por tanto mayor es el número de usuarios que se comportan de acuerdo con este perfil, haciéndolo más privado.

Además, como se puede observar en la primera rama de la Fig. 1, si la distribución del perfil de la población $\bar{t}$ es conocida, se utiliza la divergencia entre el perfil del usuario t y el perfil de la población como métrica de privacidad, de manera que, cuanto más pequeña sea esa divergencia, más privado se puede considerar el perfil.

En definitiva, la elección de perfiles aparentes que conduzcan a la minimización de la divergencia de KL mejora el anonimato. En términos más simples, una menor divergencia corresponde a una mayor frecuencia de ocurrencia de dicho perfil, permitiendo al usuario pasar más desapercibido. En el caso de un perfil de referencia de la población uniforme, esto equivale a la maximización de la entropía de Shannon.

- *Métricas contra clasificación*

Si el objetivo del atacante es clasificar al usuario como miembro de un grupo en particular, se utiliza la divergencia como métrica de privacidad, de acuerdo al análisis realizado en [12], a partir del *test* de hipótesis y el método de tipos. Como se indica en la Fig. 1, en la segunda rama, si el perfil del grupo g es desconocido en el lado del usuario, la opción es maximizar la divergencia entre el perfil real q y el perfil observado (aparente) t, con el fin de evitar ser clasificado de acuerdo a su perfil original.

Nótese que en el problema de clasificación, al contrario de lo que ocurre en el problema de identificación, buscamos maximizar la divergencia de KL, en lugar de minimizarla. La intuición subyacente al análisis citado es que se desea agrandar la distancia entre el perfil aparente del usuario y el perfil real, o el representativo del grupo en el que deseamos evitar la categorización.

IV. Medición de la privacidad en el navegador

En este artículo presentamos un *add-on* para el navegador Mozilla Firefox, que mide la privacidad del usuario en términos de riesgo o ganancia de privacidad.

Tal como se mencionó en la Sec. II, casi no existen herramientas que muestren, en tiempo real, el estado de privacidad del usuario. Desde un principio, por tanto, el usuario no es realmente consciente del peligro que representa para su privacidad todo el rastro digital que va dejando en los distintos servicios que utiliza en Internet. Esto constituye ya un grave problema, pues una percepción clara del riesgo al que se enfrenta el usuario derivaría en sospecha y ésta, muy probablemente, conduciría a un comportamiento más activo (i.e. defensivo) respecto al manejo de la información [13].

En este trabajo, proponemos una herramienta que presenta información comprensible al usuario, referente a sus niveles de privacidad, que le permiten asimilar el riesgo y probablemente, desde su perspectiva e interés, tomar una decisión para protegerse.

La información relativa a los niveles de privacidad, como se mencionó previamente, se determina en base a los conceptos de teoría de la información que se resumen en la Sec. III y consta, básicamente, de una alerta de riesgo de identificación y el resultado de la clasificación del perfil del usuario entre varios grupos definidos.

A. *Consideraciones de Diseño*

Partimos de la premisa de que el usuario no confía en ningún agente externo distinto de su dispositivo local de comunicación por lo que no está interesado en ceder información de su perfil.

Adicionalmente, consideramos dos atacantes posibles cuyas actividades de *profiling* podrían representar un grave riesgo a la privacidad, dada la gran cantidad de información a la que tienen acceso. Estos atacantes son, como se muestra en la Fig. 2, los motores de búsqueda y el proveedor de servicios de Internet. Los motores de búsqueda pueden recopilar todas las consultas que realizan sus usuarios y en las que se revela información detallada de sus intereses. Los ISPs tienen acceso a la mayor parte del contenido que el usuario genera desde su navegador; es decir, tiene acceso a contenido de sitios web, clics sobre enlaces, tiempo de permanencia en páginas web (dependiendo del sitio web) y también las consultas realizadas a motores de búsqueda. Esta afirmación se cumple siempre y cuando la conexión del usuario no esté cifrada (sin utilizar HTTPS); de manera que si la conexión está cifrada, el ISP dispondrá solamente de información sobre qué sitios visita el usuario y no de los contenidos de las páginas. Muy pocos sitios implementan mecanismos de cifrado.

El patrón de navegación formado por la información descrita podría permitir a los atacantes obtener un perfil muy detallado de los usuarios. Obtener este perfil es también crucial para el usuario para que pueda comprender el riesgo al

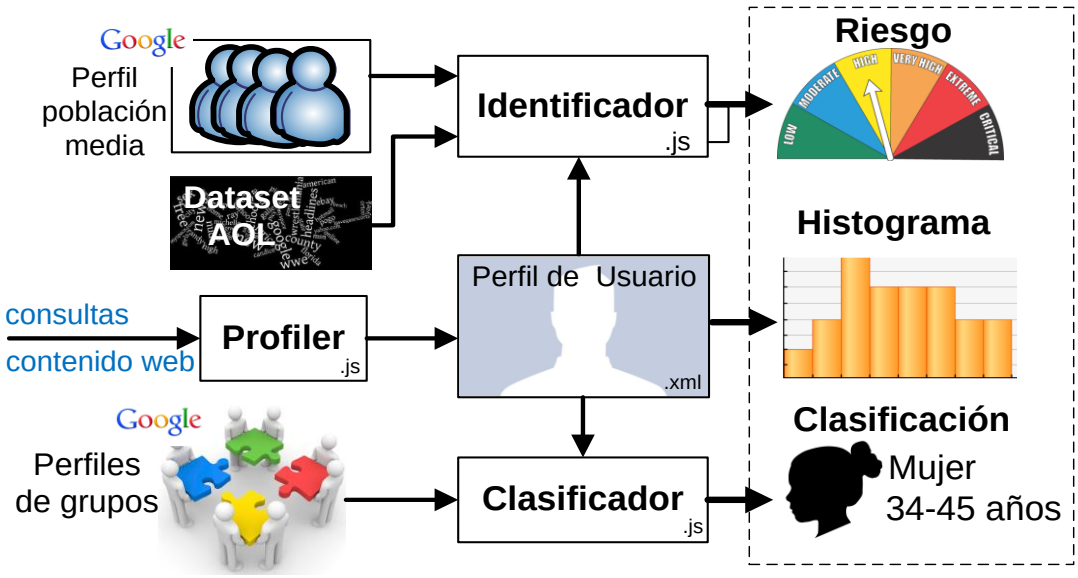


Fig. 3. Arquitectura para el cálculo del nivel de privacidad.

que se enfrenta cuando navega en Internet. Este perfil es también importante para generar las alertas que le ayuden a tomar una decisión respecto de su privacidad.

El navegador web se adapta muy bien a estas premisas, pues, dado que actúa como un intermediario entre el usuario e Internet (Fig. 2), es el encargado de gestionar todas las peticiones que el usuario realiza y todas las respuestas que recibe de Internet, y que se despliegan generalmente como páginas web. La información de la actividad del usuario, obtenida a partir del navegador, es muy detallada y por lo tanto muy útil para obtener su perfil, tal como lo modelarían los atacantes mencionados.

Con el fin de considerar el entorno del usuario en el proceso de evaluación de su privacidad, especialmente cuando se intenta clasificarlo, se requiere la información de los perfiles de varios grupos de población.

Finalmente, cumpliendo con el antecedente de un usuario que no confía en terceros, la información del perfil de usuario, como el resultado de su procesamiento se mantendrá siempre en el ámbito local del navegador.

B. Arquitectura

En esta sección se explica el funcionamiento de los componentes principales de la arquitectura para la medición de la ganancia y riesgo de privacidad del usuario. La estructura se ilustra en la Fig. 3, en donde se refleja el flujo de procesos y los resultados obtenidos por cada módulo funcional.

Navegador web. En este caso el navegador Mozilla Firefox, es el encargado de recibir las órdenes de navegación del usuario, generalmente en forma de palabras, recogidas mediante formularios que se traducen en peticiones HTTP hacia servidores web o motores de búsqueda. Están disponibles varias interfaces necesarias para acceder a gran parte de la información que envía y recibe el navegador en nombre del usuario, mediante los *add-ons*. El uso de Firefox en este trabajo se justifica en el aprovechamiento que se da de la extensión *Adnostic*, también desarrollada para este navegador, de la que se reutiliza el módulo de *profiling* para construir el perfil de usuario cuya privacidad se mide en nuestra herramienta. Sin embargo, este proceso de medición de privacidad puede implementarse en otros navegadores como Chrome o Internet Explorer, por ejemplo. Dado que estos ofrecen distintas interfaces de desarrollo, nuestra herramienta debería ser adaptada para que use los componentes de la interfaz de los distintos navegadores a los que se desea portarla.

Profiler. El proceso de *profiling* o establecimiento del perfil del usuario consiste en obtener una tabla de frecuencias de un conjunto de categorías pre-establecido. La "puntuación" de cada categoría irá incrementándose conforme se vayan revelando las preferencias del usuario a través de sus consultas y la información que recibe de los servidores web.

Histograma. Es nuestro modelo de perfil de usuario. Está formado por barras cuyo tamaño representa la popularidad de cada categoría en este perfil. El esquema de categorización, que heredamos de Adnostic, y que se basa en la representación que hacía[1] *Google Ad Preferences*, usa 3 niveles de categorías con 602 categorías en total. El primer nivel de la jerarquía se compone de 27 categorías. En el histograma se muestran las 8 categorías más representativas de este primer nivel de jerarquía. Esta representación gráfica le da al usuario una impresión básica de su perfil.

Identificador. Tal como se muestra en la Fig. 4, este módulo determina el nivel de privacidad del usuario ante un ataque de identificación. Este nivel se muestra de 3 maneras distintas, tal como se explicó en la Sec. III.

La primera forma en que mostramos al usuario su nivel de privacidad es mediante la entropía de su perfil, que sirve como una métrica de anonimidad o ganancia de privacidad.

La segunda forma está relacionada con la misma entropía del perfil de usuario, pero ahora usando como referencia los

[1] Actualmente *Google Ad Preferences* utiliza un número mayor de categorías.

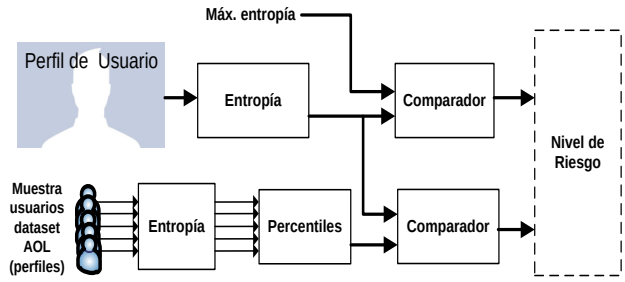


Fig. 4. Arquitectura del proceso de Identificación.

valores de entropía de una población real. Los perfiles de esta población de referencia se obtienen a partir de un subconjunto de un *dataset* de consultas de AOL liberado hace varios años.

Además, y dado que se dispone de una distribución aproximada del perfil de la población media (obtenido de la herramienta Ad Planner de Google [14]), tenemos una tercera forma de mostrar el nivel privacidad dada por la divergencia de KL del perfil de usuario relativo al perfil de la población media. Un valor de divergencia de KL de 0 indicaría una distribución del perfil de usuario equivalente a la de la población media, lo que representaría el nivel más bajo de riesgo de privacidad. Sin embargo, este valor no se puede normalizar respecto de un máximo, para determinar otros niveles de riesgo, pues este máximo no está acotado superiormente. Posteriormente este valor podría ser utilizado para medir la ganancia de privacidad, luego de aplicar alguna medida de protección.

Clasificador. Este módulo emplea la divergencia de KL entre la distribución del perfil de usuario y la del perfil de varios grupos predefinidos (ver Fig. 5). Se intenta recrear el ataque que haría un adversario con la intención de clasificar al usuario como parte de un grupo. Con ese objetivo, se calcula la divergencia de KL entre la distribución del perfil de usuario y la promedio de cada grupo de población en los que Google clasifica a sus usuarios de acuerdo a sus preferencias (datos obtenidos de la herramienta Ad Planner de Google).

El menor valor de divergencia es el que identifica al grupo con el cual el perfil del usuario tiene la menor discrepancia y, por lo tanto, el grupo al que el usuario tiene mayor probabilidad de pertenecer.

Desde el punto de vista del usuario, ésta es información muy ilustrativa ya que le da una idea bastante clara de lo previsible que es su perfil en Internet y, especialmente, lo mucho que se puede inferir a partir de su rastro digital.

Este método de clasificación es consistente con la métrica y el ataque correspondientes en la Sección III.B, resumidos en la Fig. 1, en el que el perfil representativo del grupo se escoge como el promedio de los perfiles pertenecientes.

Como nota marginal, cualquier método de clasificación supervisada, pongamos por ejemplo máquinas de vectores de soporte, podría ser utilizado por el atacante o la arquitectura para clasificar un perfil en uno de los subgrupos de población predeterminados. El método elegido en esta arquitectura es conceptual y computacionalmente simple, además de consistente con la métrica de privacidad propuesta en [12]. Una observación adicional es que la divergencia de KL es un caso particular de divergencia de Bregman, y por ello el promedio de un grupo es su centroide. Así, el método empleado corresponde al establecimiento de celdas de Voronoi en cuantificación con divergencias de Bregman [27].

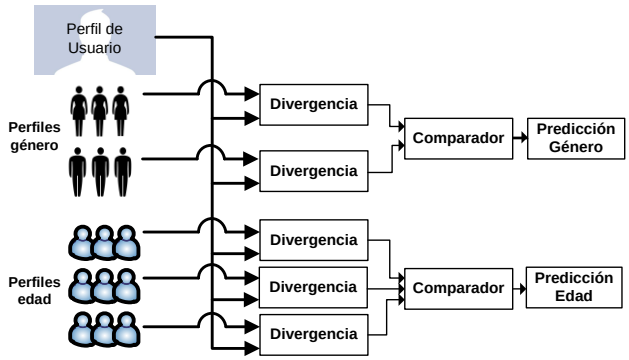


Fig. 5. Arquitectura del proceso de Clasificación.

C. Aspectos relevantes de la implementación

Este *add-on* para el navegador Firefox se ha programado utilizando los lenguajes Javascript y XUL.

Profiling. El perfil de usuario se obtiene mediante el módulo *profiler*, tomado del *add-on* Adnostic. Aquí se detectan los eventos de despliegue de las páginas Web en Firefox cuando el usuario navega y, al hacerlo, se recupera la información del usuario que da forma a su perfil. Esta información se reduce a: las consultas realizadas en motores de búsqueda, las *keywords* del código html perteneciente a las páginas que el usuario visita, los clics sobre estas páginas y el tiempo que permanece en ellas. Estos elementos permiten una clasificación bajo el esquema de 602 categorías utilizado por *Google Ad Preferences* y conforme a los resultados de la clasificación se actualizan los "puntajes" de las categorías en el perfil. Esta información tabulada de categorías es utilizada luego por nuestros módulos para evaluar el nivel de privacidad del usuario.

Modificamos este módulo para que el puntaje absoluto de cada categoría en el perfil del usuario no estuviese limitado a un valor de 500. Del mismo modo, realizamos cambios para que permitiese el *profiling* cuando el usuario se conecta a sitios con https.

Recolección de datos de población. Para obtener las métricas de privacidad relacionadas con la divergencia de KL, especialmente cuando el objetivo es clasificar al usuario en un grupo de varios predefinidos, es necesario disponer de la información del perfil de cada uno de estos grupos. Para poder comparar los distintos perfiles, desde luego, deben basarse en el mismo alfabeto de categorías.

Ventajosamente, Google posee una herramienta de publicidad en línea llamada Ad Planner [14] que dispone de mucha información sobre la distribución de los intereses de usuarios, clasificados utilizando la misma jerarquía que se utiliza para definir las preferencias de los usuarios de Google y Gmail. Esta información está tabulada de diversas formas: geográficamente, por grupos de edad y por grupos de género.

En números absolutos, en esta herramienta de análisis de intereses, se indica la cantidad de personas que estarían interesadas en cada una de las categorías tomadas como referencia para la clasificación.

Los datos recopilados para el proceso de clasificación del perfil del usuario pertenecen a los siguientes grupos;

edad (en años):

- 18 a 24,
- 25 a 34,

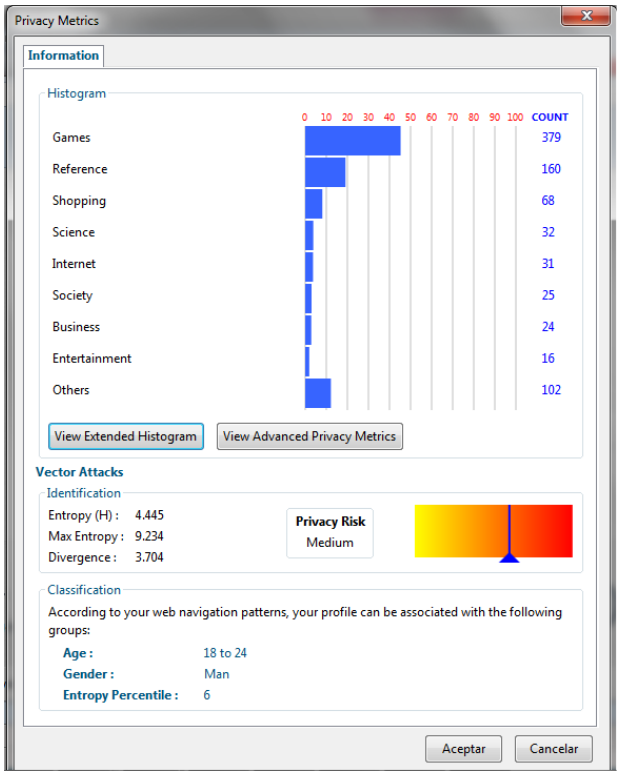


Fig. 7. Ventana de Información de métricas de privacidad (riesgo de privacidad) para el usuario.

- 35 a 44,
- 45 a 54,
- 55 a 64,
- 65 y más,

y género.

Estos datos, agrupados en correspondientes archivos, se incluyen en el *add-on* para recuperarse el momento de calcular la divergencia del perfil del usuario.

Training de datos de AOL. Se utilizó un conjunto de datos de consultas de usuarios liberado por AOL en 2006 [15] para encontrar la distribución de los valores de entropía en una población real.
Este *conjunto* está formado por cerca de 20 millones de consultas Web realizadas por alrededor de 650.000 usuarios, en un período de 3 meses.

La cantidad de consultas por usuario oscila entre 1 y varios cientos de miles. Con el fin de obtener una muestra de usuarios con una cantidad de consultas suficiente para obtener perfiles representativos, seleccionamos los usuarios con 501 a 1000 consultas, dando un total de 6674 usuarios.

Modificamos el módulo de *profiling* de Adnostic para que recibiera las consultas realizadas por los 6674 usuarios del grupo seleccionado y que por cada uno de ellos creara un perfil distinto. Luego, calculamos los valores de entropías de cada perfil, obteniendo una distribución que se puede observar en la Fig. 8.

Finalmente, en esta distribución se calcularon los percentiles de manera que podamos ubicar la entropía del perfil de usuario en alguno de los intervalos, para determinar su nivel de riesgo de privacidad. El *add-on* únicamente incluye estos valores de percentiles.

Interfaz gráfica. Para la creación de ventanas que muestren las distintas métricas que se han descrito utilizamos XUL, un lenguaje implementado como dialecto de XML orientado al desarrollo de interfaces de usuario.

En la ventana principal del navegador Firefox, el primer indicador de riesgo de privacidad que se muestra se ubica en la barra de complementos en la parte inferior. Tal como se observa en la Fig. 6, se detallan 3 elementos que le dan al usuario una idea rápida de su condición de privacidad: una escala de nivel que ilustra el riesgo de privacidad del usuario, el valor de la entropía del perfil de usuario y la última categoría en la que el usuario se ha clasificado. El nivel de riesgo se dibuja en función del percentil al que pertenece la entropía del usuario.

Fig. 6. Barra de información de privacidad del usuario ubicada en la parte inferior del navegador.

Adicionalmente, en el menú de herramientas del navegador se crea una opción para abrir una ventana en la que se muestran las distintas métricas que se han calculado en base al perfil de usuario y el de los distintos grupos poblacionales. En la Fig. 7 se puede observar esta información (usando los dos modelos de atacante mencionados): el histograma de categorías de interés, la entropía del perfil de usuario, un indicador de riesgo de privacidad y los grupos de edad y género en los que se ha clasificado al usuario.
Mediante dos botones, en esta ventana, se pueden abrir dos cuadros de diálogo adicionales. Uno para desplegar un histograma extendido con la información de hasta 19 categorías, y otro para mostrar una ventana con información un poco más detallada sobre las métricas de privacidad.

Esta última ventana incluye, además, los valores de las divergencias del perfil de usuario respecto de cada uno de los grupos de población. Dicha discrepancia se muestra también en una regla de nivel para fácil interpretación.

Importación de historial. Como parte de la implementación, se incorpora también un mecanismo para que el usuario, una vez que ha instalado el *add-on*, pueda alimentar su perfil, utilizando la información disponible en el historial de su navegador. Para eso se agrega otro elemento en el menú Herramientas que da acceso al proceso de categorización y *profiling* de los registros del historial de Firefox. En este caso, se utilizan como entradas al módulo de *profiling* los títulos de las páginas y las palabras ingresadas mediante formularios.

V. Conclusiones

Considerando el gran riesgo al que se enfrentan los usuarios cuando navegan en Internet debido a los agresivos mecanismos de *profiling* empleados por los principales sistemas de acceso a la Web (por ejemplo motores de búsqueda o ISPs) y la escasez de herramientas que evalúen este compromiso de seguridad, hemos propuesto un *addon* para Mozilla Firefox capaz de medir la ganancia y el riesgo de privacidad, poniendo estas magnitudes en un contexto determinado por los intereses del usuario y su entorno.

Una gran cantidad de usuarios se sienten anónimos en Internet y otros muchos apenas advierten la gravedad de las

amenazas contra su intimidad en el mundo digital. Por ello necesitan información accesible al respecto y fácil de interpretar. Con este *add-on* proveemos métricas interpretables como niveles de privacidad y un modelo de clasificación basado en conceptos justificados en la teoría de la información y el test de hipótesis, que el usuario puede emplear para tomar una decisión adecuada.

Estamos seguros de que la percepción que tiene el usuario respecto al riesgo puede ser un aporte muy valioso. Quién mejor que el usuario para escoger los intereses o los datos que debe proteger, dependiendo de su situación particular.

Del mismo modo, esta herramienta de medición e interpretación de la privacidad podría ser empleada para determinar la efectividad de otras herramientas que implementan mecanismos de protección (por ejemplo TrackMeNot [16]), así como también para comparar la utilidad entre ellas. El entorno de desarrollo para Firefox ofrece muchas facilidades para la implementación de esta herramienta para medir la privacidad (en especial la disponibilidad de la extensión *Adnostic* de la que se reutiliza el mecanismo de *profiling*), pero sería también conveniente portarla a Chrome o Internet Explorer, considerando la gran cantidad de usuarios que tienen estos navegadores actualmente. Aunque se debería tomar en cuenta que, con respecto a la privacidad, ahora se tiene muchas reservas respecto de Google y Microsoft, creadores de Chrome e Internet Explorer, respectivamente.

Aunque no se ha validado la utilidad real de la extensión con usuarios, se intuye que la misma va a depender mucho de la situación particular de cada usuario (intereses, valores, preocupaciones, actitudes, etc.) y por tanto de la visión individual que tenga cada usuario con respecto a su privacidad.

Finalmente, la estructura de categorías podría modificarse para incluir algunas categorías no tomadas en cuenta por *Google Ad Preferences* relacionadas con raza, religión, orientación sexual, o salud para disponer de un perfil de usuario mucho más completo.

AGRADECIMIENTOS

Este trabajo fue apoyado en parte por el Gobierno español a través de los proyectos Consolider Ingenio 2010 CSD2007-00004 “ARES”, TEC2010-20572-C02-02 Consequence y por el Gobierno de Catalunya a través de la subvención 2009 SGR 1362. Del mismo modo, se recibió el apoyo del Gobierno ecuatoriano a través de la Secretaría Nacional de Ciencia y Tecnología – SENESCYT, mediante la beca de estudios otorgada a Ana Rodríguez y José Estrada. D. Rebollo-Monedero disfruta de una beca postdoctoral Juan de la Cierva, ref. JCI-2009-05259, otorgada por el Ministerio de Ciencia e Innovación español.

REFERENCIAS

[1] Arvind Narayanan y Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets". En Security and Privacy, 2008. SP 2008. IEEE Symposium on, C1, 2008.

[2] Michael Barbaro y Tom Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749". En The New York Times, Technology, URL http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all, Agosto 2006.

[3] Eric Pfanner, "Internet Providers in Deal for Tailored Ads". En The New York Times, Technology, URL http://www.nytimes.com/2008/02/18/technology/18target.html?_r=2&oref=slogin&, Feb. 2008.

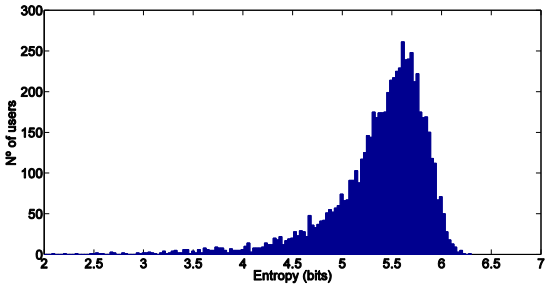


Fig. 8. Distribución de entropía de usuarios con 500 a 1000 consultas del *dataset* de consultas de AOL.

[4] Katy Hafner, “Google Resists U.S. Subpoena of Search Data”. En The New York Times, Technology, URL http://www.nytimes.com /2006/01/20/technology/20google.html?_r=1, Enero 2006.

[5] Russia Today, “Google se enfrenta al FBI para no revelar datos privados de los usuarios”, Abril 2013.

[6] V. Toubiana, D. Boneh, H. Nissenbaum, and S. Barocas, “Adnostic: Privacy Preserving Targeted Advertising ∗”. En Proceedings of the 17th Annual Network and Distributed System Security Symposium (NDSS), 2009.

[7] S. Vi-a, G. News, S. Vi-b, I. Browsing, and I. Explorer, “R E P RIV : Re-Envisioning In-Browser Privacy.”

[8] J. Becker y H. Chen, “Measuring Privacy Risk in Online Social Networks”. En Proceedings of W2SP 2009: Web 2.0 Security and Privacy, 2009.

[9] M. Fire, D. Kagan, A. Elishar, and Y. Elovici, “Social Privacy Protector - Protecting User' Privacy in Social Networks”.

[10] D. Howe and H. Nissenbaum. “TrackMeNot: resisting surveillance in web search”, 2006. mrl. nyu.edu/˜dhowe/trackmenot/.

[11] S. Teja Peddinti y N. Saxena, “On the Privacy of Web Search Based on Query Obfuscation: A Case Study of TrackMeNot”. En 10th International Symposium, PETS, 2010.

[12] J. Parra-Arnau, D. Rebollo-Monedero, J. Forné, “Measuring the Privacy of User Profiles in Personalized Information Systems”. En Future Generation Computer Systems, 2013.

[13] J. Drennan,G. Sullivan and J. Previte, “Privacy, Risk Perception, and Expert Online Behavior: An Exploratory Study of Household End Users”. En Journal of Organizational and End User Computing (JOEUC), 18(1), 1-22, 2006.

[14] Google Ad Planner, URL https://www.google.com/adplanner/ #audienceBuilder.

[15] G. Pass, A. Chowdhury, C. Torgeson, "A Picture of Search". En The First International Conference on Scalable Information Systems, Hong Kong, June, 2006.

[16] TrackMeNot, URL http://cs.nyu.edu/trackmenot/.

[17] Peter Eckersley, “How Unique Is Your Web Browser?”.

[18] Palant, Wladimir: Adblock Plus: Save your time and traffic, http://adblockplus.org/.

[19] Maone, Giorgio. NoScript. Online: http://noscript.net, 2009.

[20] Google Sharing, URL https://addons.mozilla.org/en-us/firefox/addon/googlesharing/

[21] DoNotTrackMe, URL https://addons.mozilla.org/en-US/firefox/addon/donottrackplus/?

[22] David Rebollo-Monedero, Jordi Forné, y Josep Domingo-Ferrer, “Query Profile Obfuscation by Means of Optimal Query Exchange between Users”. En IEEE Trans. Depend., Secure Comput., 2012.

[23] J. Parra-Arnau, D. Rebollo-Monedero and J. Forné, “A Privacy-Preserving Architecture for the Semantic Web based on Tag Suppression”. En Proc. Int. Conf. Trust, Priv., Secur., Digit. Bus., Bilbao, España, pp. 58-68, 2010.

[24] J. Parra-Arnau, D. Rebollo-Monedero, J. Forné, J. L. Muñoz y O. Esparza, “Optimal tag suppression for privacy protection in the semantic Web”. En Data, Knowl. Eng., vol. 81-82, pp. 46-66, 2012.

[25] J. Parra-Arnau, A. Perego, E. Ferrari, J. Forné and D. Rebollo-Monedero, “Privacy-Preserving Enhanced Collaborative Tagging”. En IEEE Trans. Knowl. Data Eng., 2012.

[26] D. Rebollo-Monedero, J. Parra-Arnau, Claudia Diaz and J. Forné, “On the Measurement of Privacy as an Attacker's Estimation Error”. En Springer, International Journal of Information Security, vol. 12, n. 2, pp. 129-149, 2013.

[27] D. Rebollo-Monedero, "Quantization and transforms for distributed source coding," Ph.D. dissertation, Stanford Univ., Dec. 2007.

[28] Wikipedia, “Divergencia de Kullback Leibler”, URL http://es.wikipedia.org/wiki/ Divergencia_ de_Kullback-Leibler

Protección de la propiedad intelectual mediante mapas auto-organizados

A. Ortiz, A. Peinado, G. Cotrina
Departamento Ingeniería de Comunicaciones
Universidad de Málaga
E.T.S. Ingeniería de Telecomunicación, Campus de Teatinos, Málaga
aortiz@ic.uma.es, apeinado@ic.uma.es

***Resumen*- En este trabajo se propone la aplicación de mapas auto-organizados (SOM) para la autenticación del propietario de una imagen. El sistema propuesto corresponde a la categoría de sistemas de autenticación robusta basada en contenido. En consecuencia, el sistema permite autenticar el origen de una imagen aunque haya sufrido modificaciones. La utilización de los mapas auto-organizados y de las trayectorias definidas sobre el mismo supone una alternativa a los sistemas basados en marcas de agua. La propuesta se presenta como aplicación para el control de la autoría de las imágenes descargadas de Internet.**

***Palabras Clave*- Autenticación de imagen, hash, SOM, derechos de autor.**

I. INTRODUCCIÓN

La rápida y continua evolución de las comunicaciones digitales y de los sistemas de almacenamiento de información ha favorecido el auge de la transmisión de contenidos multimedia a través de redes inseguras, como Internet. Con el fin de proporcionar un servicio de autenticación a las imágenes transferidas por la red, se han desarrollado numerosos sistemas de autenticación de imagen, que incluyen técnicas criptográficas convencionales, marcas de agua y esquemas de firma digital basados en contenido [1].

Las técnicas criptográficas convencionales proporcionan autenticación utilizando fundamentalmente funciones hash de uso general, como el MD5 o SHA-1[2], en las que la modificación de un solo bit en el mensaje de entrada genera salidas completamente diferentes. Este esquema aplicado a imágenes implica que una imagen I' que difiera en un solo pixel de la imagen original I sea considerada distinta, cuando desde un punto de vista perceptual son exactamente iguales. Esta aproximación a la autenticación de imágenes se conoce como autenticación estricta y puede ser útil en casos muy concretos como las imágenes médicas o militares.

Por lo tanto, se requiere una aproximación perceptual a la autenticación de las imágenes, de forma que dos versiones diferentes de una imagen sean reconocidas como la misma siempre que perceptualmente lo sean. En este sentido, han aparecido numerosas propuestas basadas en la inserción de marcas de agua ocultas en las imágenes que se desean autenticar [3, 4]. Si estas marcas de agua son frágiles, los sistemas permiten la detección de cualquier modificación sufrida por la imagen. Es decir, la permanencia de la marca es lo que determina la autenticidad de la imagen y cualquier modificación que sufra hará que la marca no se pueda recuperar. Este tipo de marcas se utilizan para la autenticación estricta, al igual que las técnicas criptográficas tradicionales. En cambio, las marcas de agua semi-frágiles permiten un cierto margen en las modificaciones que pueden sufrir las imágenes, distinguiéndose dos tipos de variaciones: las que preservan el contenido de la imagen, como las que se pueden producir por errores de transmisión, cambios de formato, transformaciones geométricas o filtrados para mejorar la calidad de la imagen; y aquellas que alteran claramente el contenido de la imagen, como el borrado o incorporación de objetos, cambios de color o de textura, cambios de posición de algún objeto, etc. Estos sistemas, se utilizan para distinguir las imágenes auténticas de aquellas que han sido manipuladas con el fin de alterar su contenido. A este tipo de autenticación se la conoce como autenticación selectiva.

Por último, existen marcas de agua robustas, cuyo objetivo consiste en resistir todo tipo de modificaciones con el fin de autenticar al propietario de la imagen. Este tipo de sistemas se aplica a la protección de contenidos multimedia para detectar las copias realizadas de forma ilegal. La robustez de estos sistemas está generalmente limitada por la calidad subjetiva de las copias manipuladas, de tal forma que las manipulaciones que se deben aplicar a la imagen original para eliminar la marca conviertan a la imagen en una copia de muy mala calidad, y en consecuencia el atacante no obtenga beneficio.

En este artículo se presenta una aproximación inicial al uso de mapas auto-organizados (SOM: *self-organizing maps*) [5] para la implementación de sistemas de autenticación robusta, como alternativa a las marcas de agua. El sistema de autenticación resultante se presenta como una posible solución para identificar de forma automática las copias distribuidas a través de bancos de imágenes y comprobar si se cumple con los derechos que el autor ha concedido, como las licencias Creative Commons [6] que permiten el uso y en algunos casos la modificación de las imágenes descargadas.

En la siguiente sección se describe el esquema general de funcionamiento del sistema propuesto, que sigue el modelo de los esquemas basados en contenido, así como las características de la imagen que se han seleccionado para describirlo. En la sección III se describen los SOM y el modo en que se utilizan en el esquema propuesto. La sección IV trata sobre la fase de codificación del hash que servirá para la posterior verificación. Los resultados experimentales se presentan en la sección V, y las conclusiones en la sección VI.

II. Esquema general del sistema de autenticación

El esquema de autenticación propuesto en este trabajo es un esquema basado en contenido [7] y, en consecuencia, estará compuesto de una fase de extracción de características, una fase de procesado de tales características, que en este caso se realizan utilizando un SOM, y una fase final de codificación del hash que se utilizará como elemento principal en la verificación. El resultado de cada una de estas fases dependerá de una clave *k*, de tal modo que el hash resultante dependa no solo de la imagen sino también del autor de la misma (ver Fig. 1).

En general, como se describe en [8], el propietario de una imagen *I*, generará un hash $h = H_k(I)$, siendo *k* una clave secreta elegida por él mismo y *H* la función que implementa el esquema de autenticación presentado en este trabajo.

Dada una imagen $I' \neq I$, el hash *h'* correspondiente a *I'* será $h' = H_{k'}(I')$, de tal modo que si *I'* es una versión modificada de la imagen original *I*, se debe cumplir que

$$d(h,h') \leq \varepsilon \tag{1}$$

siendo *d* el operador distancia calculado entre los dos valores de hash correspondiente a sendas imágenes, y ε el umbral que determina la diferencia máxima que pueden tener dos versiones de la misma imagen. En la sección IV se describe el cálculo de la distancia empleado en el sistema propuesto.

III. Extracción de las características de la imagen

El contenido de la imagen quedará determinado por una serie de características que han de extraerse al comienzo del proceso. Dicha extracción se aplica sobre cada uno de los bloques de 25 x 25 pixels en que se divide la imagen una vez normalizada a un tamaño fijo de 150 x 150 pixels. Por tanto, todas las características extraídas son características locales a cada uno de estos bloques.

El tamaño elegido para los bloques permite extraer propiedades sobre la textura y sobre momentos invariantes que proporcionan robustez frente a los efectos de rotaciones y escalado. Las características elegidas para este sistema de autenticación se pueden agrupar en tres categorías.

Gradientes locales. Esta característica consiste en el cálculo de las dos direcciones principales de máxima variación de la intensidad. Se calcula por medio de gradientes de intensidad locales, calculando las derivadas parciales de la imagen en las direcciones *x* e *y*. Considerando *I*(*x*,*y*) la intensidad de una imagen *I*, la dirección de máxima variación se puede calcular a partir de las variaciones de los pixeles contiguos como:

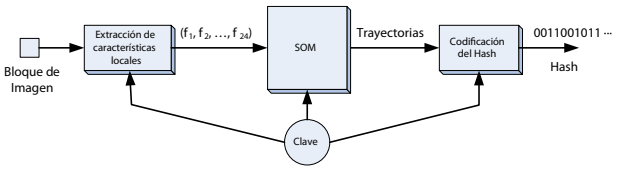


Fig. 1. Diagrama general del algoritmo de autenticación.

$$\frac{\partial I(x,y)}{\partial x} = \left(\frac{I(x+1,y) - I(x-1,y)}{\partial x} \right) \tag{2}$$

$$\frac{\partial I(x,y)}{\partial y} = \left(\frac{I(x,y+1) - I(x,y-1)}{\partial y} \right) \tag{3}$$

La dirección de máxima variación obtenida en cada bloque se puede representar mediante una magnitud y una fase.

Momentos invariantes. El segundo grupo de características proporcionan información invariante con respecto a la traslación, escalado y rotación. Esta información se obtiene calculando los momentos HU [9, 10] calculados para cada bloque.

Histograma. La característica histograma describe la distribución de niveles de gris en cada bloque. En este caso, la media, la varianza, la curtosis y la entropía son las características elegidas para describir la información proporcionada por el histograma sobre el contenido de la imagen. Considerando l_i, $1 \leq i \leq N$ los niveles de gris representados en el histograma se tiene:

$$\mu = \frac{1}{N} \sum_{i=1}^{N} l_i \tag{4}$$

$$\sigma^2 = \frac{1}{N} \sum_{i=1}^{N} (l_i - \mu)^2 \tag{5}$$

$$Kurtosis = \frac{\sum_{i=1}^{N} (l_i - \mu)^4}{(N-1)\sigma^4} \tag{6}$$

$$Entropy = -\sum_{i=1}^{N} l_i \log_2(l_i) \tag{7}$$

Las características extraídas de cada bloque conforman el vector en entrada al SOM.

IV. Aplicación del SOM

Los SOM o redes de Kohonen [5] son unos de los modelos de redes neuronales artificiales más utilizados para aprendizaje no supervisado basados en el comportamiento animal. El principal objetivo del SOM es analizar datos en muchas dimensiones y presentarlos de manera más sencilla a través de una visualización de dimensión menor, generalmente dimensión 2. Los SOM preservan la topología, es decir, que las instancias de datos que sean muy diferentes aparecerán alejadas en el mapa de salida, mientras que las que sean similares aparecerán agrupadas.

Un SOM consiste en un conjunto de nodos o neuronas dispuestos generalmente en forma de malla de dos dimensiones con distribución ortogonal o hexagonal. Cada neurona de la malla tiene asociado un vector de las mismas dimensiones que el espacio de entrada, que se denomina vector de pesos de la neurona.

Durante la fase de entrenamiento se miden las distancias entre los vectores de entrada y los pesos de las neuronas (también llamadas unidades), para obtener la unidad más cercana, la que más se le parece. Cada entrada determina entonces una unidad ganadora (BMU) y sus pesos se actualizan así como el de las unidades vecinas. Para asegurar la convergencia del procedimiento los pesos no se modifican de forma significativa en las iteraciones de la fase de entrenamiento.

Una vez concluida la fase de entrenamiento, el SOM responderá ante cualquier entrada generando una BMU en un lugar determinado del mapa de salida.

Así pues, en el sistema de autenticación que se propone en este trabajo, las entradas al SOM son vectores compuestos por todas las características que se han extraído de la imagen en la etapa previa, descrita en la sección II.A. En total son 24 características: 2 del gradiente local, 18 de los momentos invariantes y 4 del histograma.

Dado que las características se extraen de cada uno de los bloques, se dispone de 36 vectores de características, puesto que 36 son los bloques en que se divide cada imagen. En consecuencia, el SOM proporcionará 36 BMU por cada imagen que se procesa, representando cada BMU en el mapa de salida que está compuesto por una malla hexagonal de 10 x 10 unidades.

A. *Agrupamiento en el SOM*

El SOM se puede considerar como un método de agrupamiento (*clustering*) puesto que cuantifica el espacio de entrada, en este caso el espacio de las características de la imagen, utilizando un número determinado de prototipos. Es decir, cada prototipo puede considerarse como el vector más representativo de una clase. De esta manera, cualquier entrada que se introduzca en el mapa será representada por el prototipo que mejor la represente [11].

Por otro lado, los prototipos se proyectan sobre una superficie de dos dimensiones preservando la topología y cada unidad del mapa de salida actúa como un *cluster*, puesto que está agrupando a todos los vectores de entrada que quedan representados por un determinado prototipo.

Sin embargo, considerar que cada unidad es un *cluster* no aprovecha toda la información que puede proporcionar el SOM. En realidad, el SOM ofrece ventajas sobre los algoritmos clásicos de clustering si mas de una unidad se utiliza para representar a una misma clase, y por tanto, un conjunto de unidades puede actuar como BMU para un subconjunto de datos. En consecuencia, se hace necesario agrupar las unidades del mapa para definir claramente los *clusters* [12]. Aunque se han definido algoritmos específicos para dividir el SOM en *clusters* [13], en este trabajo se utiliza el algoritmo *k*-means debido a su simplicidad [14]. El algoritmo consiste en definir *k* centroides y colocar cada valor en la clase del centroide más cercano. A continuación, se recalcula el centroide de cada grupo y se vuelven a distribuir todos los valores. El proceso se repite hasta que no hay cambios.

En la Fig 2. se observan los tres *clusters* en que se divide el mapa que se utiliza para la autenticación al aplicar el algoritmo *k*-means.

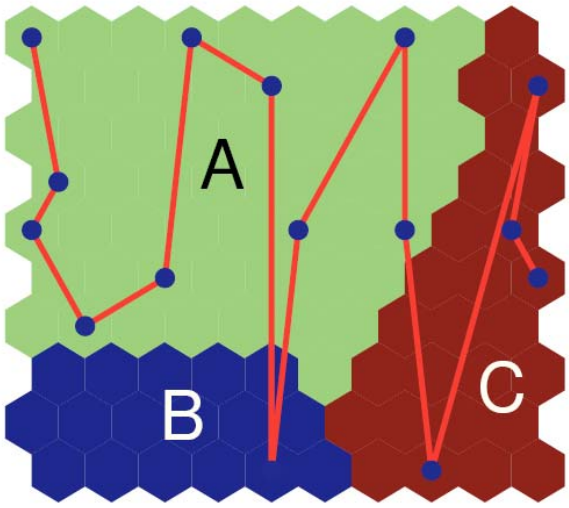


Fig. 2. Trayectorias sobre el mapa de salida dividido en tres clusters.

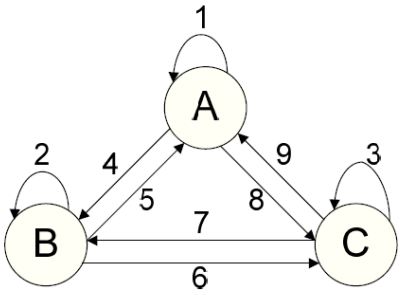


Fig. 3. Diagrama de estados para el cálculo del hash a partir de las trayectorias..

B. *Calculo de las trayectorias*

Como ya se ha mencionado, cada imagen se divide en 36 bloques, cuyas características conforman los vectores de entrada al SOM. Por tanto, se define una secuencia de 36 vectores de entrada para cada imagen que generarán 36 BMU en el mapa de salida. Esta secuencia de BMU constituye una trayectoria sobre el mapa, que representa una proyección de la secuencia de entrada (la secuencia de características) sobre un mapa de dimensión dos. Esta reducción de dimensión (de 24 a 2) supone siempre una pérdida de información.

Para mitigar este problema se pueden considerar grupos de BMU en lugar de las BMU individuales. Estos grupos serán los clusters calculados mediante el algoritmo k-means, de manera que la secuencia de salida no sean las BMU sino los clusters a los que pertenecen estas BMU.

La Fig. 2 muestra un mapa de salida en el que aparece trazada la trayectoria de las BMUs correspondiente a los primeros 15 bloques de una imagen. La división del mapa en tres *clusters* permite que la secuencia final de salida sea AAAAAAABAAACCCC...

V. CODIFICACIÓN DEL HASH

Esta etapa transforma los datos que ofrece el SOM a la salida en un valor hash que se utilizará posteriormente para verificar la propiedad de la imagen.

Una vez que el SOM ha sido entrenado, se aplica el algoritmo k-means para dividir las unidades en tres *clusters*. Estos *clusters* son identificados como A, B y C (ver Fig. 2).

El cálculo del hash se realiza a partir de la secuencia definida por los *clusters* a los que pertenecen las BMU (AAAAABAAACCC ...), considerando las transiciones entre *clusters*. Para ello se define el diagrama de estados de la Fig. 3 en el que se identifican todas las transiciones posibles entre los 3 estados o *clusters*. La secuencia de transiciones se codifica finalmente en binario asignando 4 bits a cada elemento.

Como ejemplo, la secuencia ACBAABBBAAAAABBB de 16 *clusters* se transforma en la secuencia 875142251111422 de 15 transiciones que corresponde a la secuencia binaria 1000 0111 0101 0001 0100 0010 0010 0101 0001 0001 0001 0001 0100 0010 0010.

VI. Aplicación de la Clave de Usuario

Tal como se ha definido en la sección II, el hash calculado depende de una clave *k* elegida por el propietario de la imagen. La Fig. 1 muestra que dicha clave es tenida en cuenta en las tres fases principales del proceso: extracción de características, el SOM y la codificación del hash.

En la fase de extracción de características se genera un vector de 24 componentes por cada bloque que será la entrada del SOM. En lugar de introducir directamente el vector de características generado, se aplica una permutación al vector y a continuación se introduce en el SOM. Con esta operación se consigue que las trayectorias generadas sobre el mapa de salida dependan fuertemente de la *k*. Esta permutación afecta directamente al propio SOM ya que se debe aplicar igualmente durante la fase de entrenamiento.

Dado que se utilizan 24 características, se pueden seleccionar 24! permutaciones distintas. En consecuencia, la clave k que determina la permutación tendrá una longitud de $log_2(24!) \approx 79$ bits.

Por otra parte, la aplicación de la clave *k* a la fase de generación del hash consiste en permutar los identificadores asociados a las transiciones en el diagrama de estados de la Fig. 3. Como se utilizan tres *clusters*, existen 9 transiciones diferentes. En consecuencia, existen 9! formas diferentes de asignar los valores, lo que determina que se necesitan $log_2(9!) \approx 18$ bits.

En definitiva, la clave *k* tendrá una longitud de 97 bits como resultado de la concatenación de los bits necesarios para definir ambas permutaciones. La longitud de la clave se puede incrementar si se aumenta el número de características elegidas para describir el contenido de la imagen.

VII. Resultados experimentales

Se han llevado a cabo pruebas experimentales sobre tres de las imágenes más representativas de la base de datos USC-SIPI [15] (Fig. 4) con el fin de comprobar la estabilidad y la robustez del método propuesto.

En todas las pruebas realizadas se ha utilizado un SOM de 10 x 10 unidades distribuidas en una malla hexagonal.

La robustez del sistema se ha comprobado utilizando dos tipos de transformación a la imagen: el escalado y el recorte. En el primer caso, siguiendo los criterios de [7] se han comparado las imágenes con sus correspondientes versiones escaladas al 2%, 5%, 20% y 30% de su tamaño. La comparación se ha realizado midiendo la distancia *edit* o *Levenshtein* entre las cadenas hash generadas.

La Fig. 5 muestra el resultado de la comparación de las versiones escaladas de las tres imágenes con cada una de las imágenes de referencia. Así, la distancia entre las versiones escaladas de una imagen con respecto a su original es 0 en todos los casos, mientras que la distancia con respecto a las otras imágenes de referencia es mayor que 0. Esto permite diferenciar claramente una imagen de las demás, y en consecuencia, identificarla en un conjunto determinado de

Fig. 4. Imágenes utilizadas en las pruebas experimentales. (a) Baboon, (b) Lena, (c) Pepper.

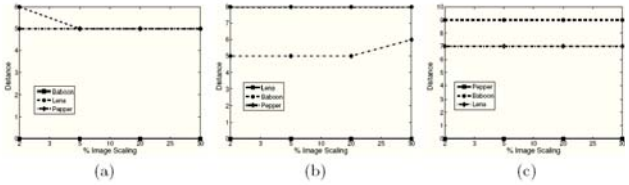


Fig. 5. Distancia entre el hash de las imágenes escaladas (a) Baboon, (b) Lena, (c) Pepper.

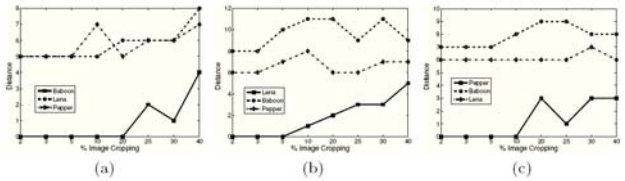


Fig. 6. Distancia entre el hash de las imágenes recortadas (a) Baboon, (b) Lena, (c) Pepper.

imágenes. Por tanto, la transformación escalado no afecta al hash calculado. Es decir, una imagen y sus versiones escaladas generarán la misma cadena hash.

La transformación de recorte es aplicada eliminado la zona exterior de la imagen correspondiente al 2%, 3%, 5%, 10%, 20%, 25%, 30% y 40% del tamaño original. Esta transformación es una de las más agresivas con el contenido de la imagen puesto que se pueden perder determinados elementos significativos.

La Fig. 6 muestra el resultado de la comparación de las cadenas de hash calculadas sobre las versiones recortadas de las tres imágenes con respecto a cada una de las imágenes de referencia. Se aprecia que la distancia permite discriminar las versiones que proceden de la imagen de referencia considerada con respecto a todas las demás.

Esta transformación determina ciertas limitaciones en la aplicación del hash propuesto en este trabajo, debido a que la cadena hash generada para una versión recortada no es idéntica a la obtenida en la imagen original. Como se aprecia en la Fig. 6, a medida que el factor de recorte aumenta, disminuye la diferencia entre las cadenas hash generadas por las distintas imágenes.

VIII. CONCLUSIONES

En este trabajo se presenta una primera aproximación de la utilización de un SOM como elemento fundamental para autenticar al propietario de una imagen. El método presentado presenta un buen comportamiento sobre los experimentos realizados, puesto que permite relacionar las imágenes modificadas con la imagen original de la que proceden y diferenciarlas del resto.

El algoritmo propuesto se aplica sobre las imágenes normalizadas a un tamaño fijo con el fin de proporcionar resistencia ante las posibles modificaciones de la imagen mediante transformaciones de escalado. Este planteamiento se ha demostrado efectivo en las pruebas realizadas que se muestran en la Fig. 5.

Por otra parte, se han extraído 24 características de la imagen de forma que el espacio transformado permita la diferenciación de las cadenas hash generadas. Un número muy pequeño agruparía imágenes perceptualmente distintas bajo la misma clase, mientras que un número demasiado alto complicaría en exceso el procedimiento de extracción y procesado.

Se necesita realizar más pruebas sobre más imágenes y considerar un mayor número de transformaciones para poder estimar con precisión la robustez del sistema propuesto.

En cualquier caso, el sistema presentado genera un valor hash compuesto de 140 bits utilizando una clave de unos 97 bits. Esto permite al propietario de las imágenes realizar búsquedas en la red de su propias imágenes para verificar de forma automática si se cumple con los derechos de uso que hayan establecido, que pueden ser de prohibición total de su utilización, de uso sin modificación o de uso y modificación, como ocurre con algunas licencias del tipo Creative Commons.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el proyecto TIN2011-25452 "TUERI: Technologies for secUre and Efficient wiReless networks within the Intenert of things with applications in transport and logistics" del MICINN.

REFERENCIAS

[1] A. Haouzia, R. Noumeir “Methods for image authentication: a survey”, Multimedia Tools and Applications (2008) 39:1–46

[2] A. Menezes, P. Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC Press, 2001.

[3] S. Katzenbeisser, F. Petitcolas. Information Hiding. TEchniques for steganography and digital watermarking. Artech House 2000.

[4] A. Hanjalic, G. Langelaar, P. van Roosmalen, J. Biemond, R. Lagendijk. Image and video databases: restoration, watermarking and retrieval. Elsevier 2000.

[5] T. Kohonen. Self-Organizing Maps. Springer, 2001.

[6] Creative Commons International. http://wiki.creativecommons.org/ CC_Affiliate_Network

[7] S.H. Han, H.C. Chu, "Content-based image authentication: current status, issues and challenges". International Journal of Information Security, 9:19–32, 2010.

[8] D. Tonien, R. Safavi-Naini, P. Nickolas, Y. Desmedt, "Unconditionally Secure Approximate Message Authentication", IWCC 2009, LNCS 5557, pp 233-247, 2009.

[9] Ming-Kuei Hu, "Visual pattern recognition by moment invariants". IRE Transactions on Information Theory, 8(2):179–187, 1962.

[10] Z. Huang, J. Leng, "Analysis of hu’s moment invariants on image scaling and rotation", In Proc. 2nd Int Computer Engineering and Technology (ICCET) Conf, volume 7, 2010.

[11] P. Somervuo, T. Kohonen, "Self-organizing maps and learning vector quantization for feature sequences", Neural Processing Letters, 10:151–159, 1999.

[12] A. Ortiz, J.M. Górriz, J. Ramírez, D. Salas-González, J.M. Llamas-Elvira, "Two fully-unsupervised methods for mr brain segmentation using som-based strategies", Applied Soft Computing, 2012.

[13] K. Tasdemir, P. Milenov, B. Tapsall, "Topology-based hierarchical clustering of self-organizing maps", IEEE Transactions on Neural Networks, 22(3):474–485, 2011.

[14] S. Theodoridis, K. Koutroumbas. Pattern Recognition. Academic Press, 2009.

[15] USC-SIPI. Signal & image processing institute: The usc-sipi image database. university of southern california, 2007.

Plataforma de votación segura para la evaluación de la QoE

J. L. Tornos, J. L. Salazar, J. J. Piles, L. Casadesus, J. Ruiz-Mas y J. Fernández-Navajas
Grupo de Tecnologías de las Comunicaciones – Instituto de Investigación en Ingeniería de Aragón
Dpt. IEC. Centro Politécnico Superior Universidad de Zaragoza
Edif. Ada Byron, 50018, Zaragoza
{jltornos, jsalazar, jpiles, luis.casadesus, jruiz, navajas}@unizar.es

***Resumen*- Los sistemas de votación electrónica llevan mucho tiempo siendo empleados como medio de recolección de información. Muchos de estos sistemas de votación no incluyen medidas de seguridad, algo necesario en numerosos procesos de este tipo. En este artículo se describe la implementación de un sistema seguro de eVoting basado en firmas en anillo. Gracias a una serie de características, como la enlazabilidad, el sistema es muy atractivo para ser empleado como herramienta de recogida de información de QoE. Esta característica permite que los distintos votos de un usuario sean enlazados y, manteniendo el anonimato, observar las tendencias de los usuarios de una manera individual. Para participar en el proceso de votación los usuarios emplean el navegador web. Este posibilita que dentro del mismo formulario, o evaluación de QoE, esté incluido el contenido multimedia, protocolo o aplicación a evaluar facilitando el proceso de votación.**

***Palabras Clave*- Votaciones seguras, firmas en anillo, QoE**

I. INTRODUCCIÓN

Los mecanismos de votación electrónica (eVoting) han sido una constante desde mediados del siglo pasado. Los primeros mecanismos empleados se valían de papeletas perforadas o lectores ópticos para registrar el voto. Este tipo de votación electrónica empleaba medios electrónicos para realizar el conteo o escrutinio de los votos. Sin embargo, el voto no era registrado de manera electrónica.

Más adelante, se empezaron a emplear dispositivos con distintos tipos de interfaz que servían como urnas electrónicas, sistemas de voto electrónico de registro directo (DRE) [1]. Estos sistemas permiten que el voto quede automáticamente registrado después de ser emitido, sin necesidad de un procesado posterior para realizar su escrutinio. Estas urnas electrónicas se ubicaban en los centros de votación donde los votantes acudían para participar en el proceso de votación. Aunque los DRE pueden facilitar el posterior escrutinio de los votos, existen diferencias entre el método tradicional de votación y las votaciones que emplean DRE [2].

Conforme el uso de las TIC, y en especial internet, fue extendiéndose, se desarrollaron mecanismos de votación electrónica en los que no era preciso que el votante acudiera al centro de votación. El votante empleaba su propio ordenador para llevar a cabo la votación empleando las aplicaciones o herramientas desarrolladas a tal efecto.

Hoy en día, es posible participar en una gran variedad de procesos de votación empleando internet sin necesidad siquiera de emplear una red segura. Dentro de estos mecanismos de votación, encontramos una gran variedad de posibilidades con distintas características y requisitos que hacen que no todos los sistemas se puedan emplear en las múltiples situaciones en las que se requiere de un proceso de votación.

Un primer caso de las votaciones realizadas por internet es el de las encuestas que se muestran en las páginas web. Las cuestiones pueden ser de cualquier índole y normalmente el proceso es tan sencillo como que el usuario/votante seleccione una de las opciones que el sistema le muestra. Se suelen emplear preguntas de respuesta cerrada ya que el objetivo final es obtener unos resultados cuantitativos. De esta manera, después de votar se suele mostrar el resultado de la votación hasta ese momento.

Un paso más allá se da en las votaciones en las que se requiere que el usuario esté registrado en el sistema para participar en el proceso de votación. Esto es necesario en las encuestas o votaciones que se realizan en los foros o redes sociales. En este caso, los usuarios primero se identifican en la plataforma en la que se desarrolla la votación; acceden al área de votación; y seleccionan una de las opciones propuestas, en caso de ser una votación cerrada, o responden a la pregunta en un campo libre si la pregunta es abierta.

Los sistemas anteriores no cumplen con todos los requisitos de seguridad necesarios para realizar una votación segura [3-5]. Es por esto que se desarrollaron sistemas de votación electrónica seguros basados en uno de los siguientes principios, que sí cumplen los requisitos de seguridad: firmas ciegas [6, 7], mix-nets [8, 9], cifrado homomórfico [10, 11] o firmas en anillo [12]. Estos sistemas permiten realizar la votación de una manera anónima empleando mecanismos para o bien dotar al usuario de anonimato o bien imposibilitando relacionar a un votante y su voto emitido, empleando una red de servidores que impide esta relación.

Un paso más se puede dar cuando se quiere buscar la tendencia en los votos de los usuarios, sus cambios de opinión u opción. Para poder llevar esto a cabo es necesario que se pueda realizar algún tipo de enlace entre los votos de los usuarios. Esta característica la cumple el sistema descrito en [13]. Mediante el uso de firmas cortas, espontáneas y enlazables [14] se consigue, sin perder el anonimato del usuario, enlazar los votos de un mismo usuario mediante un valor llamado *linking tag*. Este valor permite conocer los distintos votos emitidos por un usuario durante una o diversas rondas de una votación y así poder realizar estudios individualizados de sus valoraciones.

Este mecanismo es uno de los pilares en los que se basa un sistema democrático emergente, e-Cognocracia [15], que emplea las nuevas tecnologías para buscar una participación

activa de los ciudadanos en la toma de decisiones del gobierno. Este sistema requiere además poder realizar un seguimiento de opiniones y la creación de grupos con distintos pesos. Al poder llevar un control sobre las votaciones, u opiniones, emitidas por los usuarios, también es un mecanismo muy eficiente para la realización de encuestas seguras y con fuentes de información de calidad en el ámbito del marketing o en la recogida de información relacionada con la QoE.

Dentro de este último campo, esta herramienta es muy útil para realizar controles de calidad externos. Se dota a los usuarios de un mecanismo para aportar ideas de un modo seguro, manteniendo en todo momento su anonimato y permitiendo realizar un estudio en profundidad de sus distintas decisiones o elecciones. Todas estas características se adecúan de una manera perfecta a una herramienta para recoger de una manera confiable la información sobre QoE de los usuarios de un determinado producto, sistema o protocolo. Mediante el uso de un sistema de votación que garantiza el anonimato conseguiremos que los usuarios no se sientan coaccionados en sus valoraciones y, gracias al enlazado, seremos capaces de diferenciar las valoraciones de cada usuario de manera individual.

Para poder implantar un sistema adecuado a las necesidades específicas del protocolo descrito en [13], es necesario el desarrollo tanto de la parte de gestión del sistema como la parte con la que trabajará el usuario. En este artículo se detalla la implementación de un sistema completo de votación con las características previamente descritas presentando dos herramientas diferenciadas que interactúan entre ellas. En el lado del servidor se implantarán las herramientas de gestión adecuadas mientras que para la parte del usuario se instalará una extensión en el navegador (Firefox) que permitirá el acceso a las votaciones y realizar una votación de manera segura empleando firmas en anillo.

El uso del navegador como herramienta para efectuar la votación se basa en la usabilidad. Los usuarios están acostumbrados a emplear el navegador y de esta manera se facilita el empleo del sistema de votación segura. El único cambio que verá el usuario se dará en el momento de realizar la firma cuando se le solicite el password con el que protege su clave privada. Además, el empleo de un navegador como medio de recogida de información sobre QoE es muy útil, ya que permite introducir contenido multimedia en el propio formulario de recogida de información para que sea evaluado.

En la Sección II se introducen los conceptos de votación electrónica segura. La Sección III muestra la implementación de nuestro sistema de votación segura basado en firmas en anillo. En la Sección IV se explican los detalles de los procesos de distribución de claves, elección y tratamiento de la información. En la Sección V se analiza la relevancia que puede tener este sistema de votación en relación con la obtención de valoraciones de la QoE y la prueba piloto que se desarrolló en el laboratorio. En la Sección VI se dan las conclusiones.

II. Sistemas de eVoting Seguro

Los mecanismos para la recogida de información o votación más empleados en internet son las encuestas, formularios que encontramos en multitud de páginas web y foros. Este tipo de votaciones podemos diferenciarlas por el mecanismo de registro de los votantes. En el primer caso el registro se realiza de manera anónima. Mediante el registro en la plataforma, el usuario accede al sistema con un perfil en el que se le identificará con un pseudónimo o nick. Este mecanismo no permite relacionar la identidad real del usuario con su identidad digital.

Un segundo caso se da en los foros o plataformas en los que es necesario realizar una autenticación de la identidad frente a la autoridad que organiza el foro. En caso de que los responsables no puedan hacerse cargo del proceso de autenticación se puede delegar en un tercero de confianza (TTP). En estos casos, los usuarios, una vez identificados, tienen acceso al sistema mediante un perfil en el que se le puede identificar o bien mediante un nick o bien mediante su identificación en la vida real, normalmente nombre, función o cargo.

Los dos sistemas anteriores tienen un uso muy amplio hoy en día en internet. Los mecanismos que no necesitan una autenticación de usuario son empleados en la gran mayoría de foros y redes sociales. Los sistemas en los que se emplea una autenticación de la identidad de los usuarios se suelen dar en instituciones como las universidades y también en empresas privadas.

El empleo de estos mecanismos conlleva una serie de restricciones a la hora de realizar consultas o votaciones. El primero de ellos se da en los sistemas que no se realiza una autenticación de la identidad. En estos casos, los usuarios pueden participar y votar, cuantas veces quieran en los procesos de consulta. El segundo, común a los dos mecanismos de identificación, con y sin autenticación, es que el administrador del sistema que gestiona la votación puede saber qué ha votado cada uno de los usuarios. Esto se debe a que la identificación del usuario se realiza de manera directa y por tanto puede vincular la identidad del usuario con el voto emitido.

Para evitar los problemas de seguridad de los métodos anteriores, se han desarrollado sistemas de votación seguros. Estos sistemas emplean mecanismos, basados en TTPs, que dotan a los usuarios de unas claves o certificados que después emplean para identificarse en el sistema. De esta manera se evitan los problemas que aparecen en los sistemas anteriores, en los que no existe un proceso de autenticación de usuarios, como son el voto por duplicado o el control de la votación por la entidad organizadora.

El cambio de mentalidad que se exige a los ciudadanos para que depositen su confianza en un sistema de votación electrónica es inmenso. Convencer a un ciudadano de que todos los derechos que tiene en una votación física se mantienen en la votación electrónica no es sencillo. Es por esto que se han definido una serie de requisitos que los sistemas de votación electrónica deben cumplir [3-5]. Algunos de estos requisitos son incluso más restrictivos que los que se imponen para un sistema de votación presencial, como se muestra más adelante. En [3] se muestran los requerimientos para las votaciones electrónicas separadas en dos grupos, básicos y extendidos:

Requisitos básicos: Privacidad, Completitud, Firmeza, No reusable, Elegibilidad, y Rectitud.

Requisitos extendidos: Robustez, Verificabilidad universal, Sin necesidad de recibo y No coercitivo.

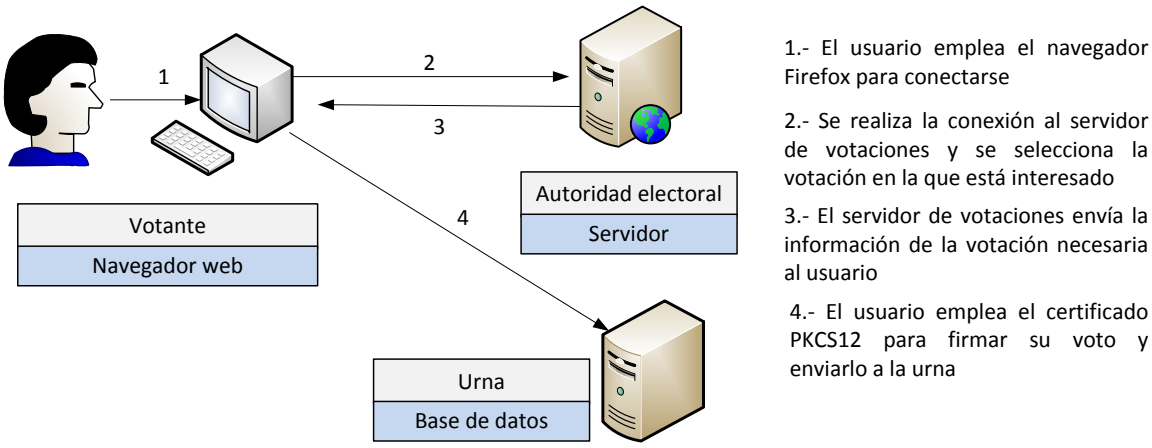


Fig. 1. Proceso de adquisición de clave de firma y de eVoting con dos TTP

Los requerimientos básicos resultan de la aplicación directa de los métodos tradicionales de votación. Tan solo los usuarios censados pueden votar, *Elegibilidad (*Elegibility); los votantes solo podrán emitir un voto válido, *No reusable* (Unreusability); los votos inválidos deben ser detectados y no hay que tenerlos en cuenta en la votación, *Firmeza* (Soundness); los votos son secretos, *Privacidad* (Privacy); la votación no se tiene que ver afectada, *Rectitud* (Fairness) y los votos correctamente emitidos deben formar parte del recuento final, *Completitud* (Completeness).

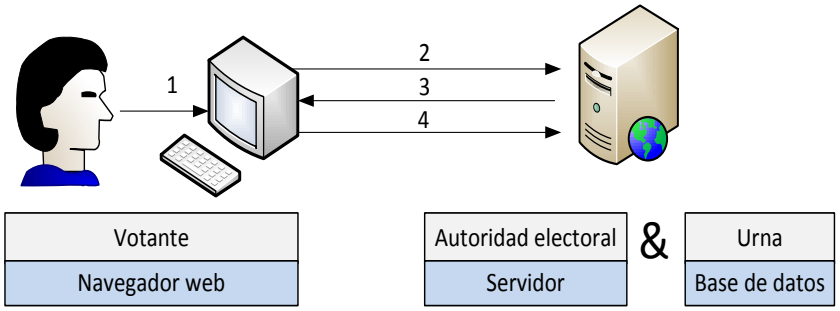
Los requerimientos extendidos van más allá de los básicos. Se pueden interpretar como mecanismos para dotar de mayor seguridad a los sistemas de votación electrónica debido a las necesidades del mecanismo de votación y también como mecanismos de promoción de los sistemas de votación electrónica. En primer lugar encontramos el requerimiento de *Robustez* (Robustness), que implica que debemos aislar las distintas partes que conforman el sistema de votación electrónica de manera que el fallo de una de las partes no impida el correcto funcionamiento de todo el sistema. El requisito de *Verificabilidad Universal* (Universal verifiability) es un valor añadido a las votaciones electrónicas. En los sistemas tradicionales de votación existe un grupo de personas encargadas de llevar a cabo el recuento de los votos; en los sistemas de votación electrónica, una vez publicados los votos, cualquiera debe ser capaz de poder realizar el recuento. Mediante un sistema *Sin necesidad de recibo* (Receipt-freeness) se logra que un votante no reciba ningún tipo de ticket o testigo que revele el sentido de su voto. La última característica extendida trata al sistema como *No coercitivo*(Incoercibility), lo que implica que un votante no puede ser coaccionado en el momento de la votación.

Los sistemas de eVoting seguro se pueden clasificar en 4 grupos atendiendo al método mediante el cual dotan al sistema de la seguridad necesaria:

- **Firmas ciegas** [6, 7]: el proceso de firmas ciegas emplea un administrador de la votación al que cada votante envía su voto ofuscado. El administrador verifica que el votante tiene permiso para participar en el proceso de votación y, si es así, firma el voto. El votante recibe de vuelta su voto firmado por el administrador, elimina la ofuscación del voto y, acompañándolo de la firma del administrador, lo envía a la urna. La urna verifica que la firma que acompaña al voto es correcta y añade el voto a la votación.
- **Mix-nets** [8, 9]: el mecanismo que emplea el proceso mix-nets para anonimizar los votos se compone de una red de servidores. Estos servidores, denominados mixes, reciben un lote de votos y realizan una permutación sobre ellos de manera que a un observador no le sea posible relacionar las entradas con las salidas.
- **Cifrado Homomórfico** [10, 11]: Se suele emplear para votaciones de conteo, como pueden ser los referéndums. Consiste en operar los votos cifrados para finalmente obtener el resultado cifrado de la votación. Luego éste se descifra y se hace público. De esta manera, se puede identificar al votante cuando emite su voto cifrado, ya que éste sabe que nunca se descifrará. El cifrado homomórfico está muy limitado a operaciones muy básicas como puede ser la suma y la resta, ya que la función de cifrado E ha de ser un homomorfismo y cumplir que $E(x+y)=E(x)+E(y)$. Por eso su uso es muy apropiado para referendums.
- **Firmas en anillo** [12]: Las firmas en anillo son una evolución de las firmas en grupo [16]. Más adelante surgieron las firmas enlazables en anillo [17] que permiten enlazar dos firmas de un mismo votante. El punto débil de este tipo de firmas es que su tamaño aumenta linealmente con el número de participantes en el anillo. En [14] se soluciona el problema del aumento de tamaño consiguiendo mantener inalterable el tamaño de la firma independientemente del número de participantes en el anillo.

Las firmas en anillo en las que se basan los sistemas de eVoting tienen las características de ser espontáneas, cortas y enlazables. La principal característica que tienen es que permiten realizar la firma de manera que al firmante se le identifique como perteneciente a un grupo pero sin revelar su identidad. Además, gracias a la característica de enlazabilidad, permiten realizar un control sobre los usuarios que ya han votado, evitando así que un votante emita dos votos. Al ser espontáneas, no necesitan de un manager que realice la gestión de las claves ni pueda revocar el anonimato de los votantes.

El esquema principal de los sistemas de votación seguro se observa en la Figura 1. Dependiendo del sistema de eVoting empleado será necesario que la autoridad electoral esté separada de la urna, como en los métodos basados en firmas ciegas, o podría no ser necesario que estuviesen separadas, como en los sistemas basados en firmas en anillo. Este útimo sistema permite unificar recursos ya que el



1.- El usuario emplea el navegador Firefox para conectarse

2.- Se conecta al servidor de votaciones y selecciona la votación en la que está interesado

3.- El servidor de votaciones envía toda la información necesaria al usuario

4.- El usuario emplea el certificado PKCS12 para firmar su voto y enviarlo a la urna

Fig. 2.- Proceso de votación con una sola TTP

anonimato requiere tan solo una TTP frente a las dos requeridas en otros sistemas. En este caso, los recursos necesarios para implementar el sistema de votación y los pasos a seguir para completar el proceso, se muestran en la Figura 2.

III. Implementación del sistema de votación segura

El sistema de votación segura implementado [13] emplea firmas cortas, enlazables en anillo [14]. Para realizar la implementación real del sistema de eVoting se han desarrollado distintos módulos que combinados permiten su correcto funcionamiento. Por un lado se emplea una PKI [18] para realizar la gestión de los certificados; también se ha desarrollado la parte de gestión de votaciones y votantes; y por último el programa que permite a los votantes realizar la votación de manera segura, a través de una herramienta conocida ampliamente como es un navegador. Todos estos bloques emplean software libre: Firefox para el navegador, Apache para el servidor de votaciones y MySQL para gestionar la base de datos.

A. Despliegue de la PKI

Existen numerosos requisitos para llevar a cabo la implementación de un sistema de votación seguro. Además, si se requiere de un tipo específico de claves no estandarizadas, como es nuestro caso, la creación de una PKI ad hoc se vuelve necesaria.

Las claves que se emplean en el sistema de votación descrito en [13] tienen las siguientes características:

- Las operaciones se realizan módulo n, con n = pq = (2p' +1) (2q' +1) de λ bits, siendo p, q, p', q' números primos.
- Las claves privadas (e_1, e_2) son dos primos distintos del intervalo ($2^l - 2^\mu$, $2^l + 2^\mu$), donde l y μ son parámetros de seguridad del protocolo
- Clave pública: ($2e_1e_2 + 1$), el cual es primo.

Al no existir unos certificados estándar para este tipo de claves y necesitar que las claves estuviesen en certificados que luego pudiesen ser manejados por los navegadores, se hace necesario emplear campos extendidos de los certificados estándar para claves RSA [19] para almacenar los parámetros necesarios para la firma. Para crear el certificado digital [20] de la clave pública no hay ningún problema ya que se almacena el valor del módulo n=pq en el campo destinado al módulo y en el campo destinado al exponente público RSA se almacena el valor $2e_1e_2 + 1$. Al crear la clave privada debemos almacenar los valores de n, e_1 y e_2. Para almacenarlos nos valemos del campo módulo para almacenar n; en el exponente público almacenamos $2e_1e_2 + 1$; para almacenar el valor de e_1 usamos el campo del exponente privado; y el campo primo1 para el valor e_2.

El hecho de emplear certificados estándar válidos para almacenar la información y no desarrollar otros específicos para nuestra firma se debe a que facilitan su uso en el navegador. De esta manera se pueden emplear las funciones criptográficas de Firefox y así no tener que modificar su código.

Una vez emitidos el certificado de clave pública y la clave privada, se crea el certificado PKCS12 [21] para el votante. De esta manera se consigue obtener un certificado de usuario con las características requeridas para nuestro sistema de votación y que son admitidos por los navegadores.

Para poder implantar una PKI se debe dotar a los usuarios de los certificados realizando una correcta gestión y control de manera que la PKI sea confiable. Se debe efectuar de manera correcta el proceso de identificación y autenticación de usuarios y realizar una correcta entrega de los certificados. También se deben desarrollar los mecanismos para revocar los certificados que hayan dejado de ser confiables para el sistema.

B. Servidor de votaciones/Autoridad Electoral

El servidor de votaciones es la parte del sistema encargada de realizar la gestión, administración y elaboración de las votaciones, así como de llevar el control y gestión de los votantes. El lenguaje de programación empleado es Java y se emplea MySQL para realizar la gestión de las bases de datos.

Dentro del apartado de gestión podemos diferenciar dos grandes apartados. El primero de ellos será la gestión de usuarios y el segundo la gestión de votaciones y sus resultados. La gestión de usuarios se realiza en varias etapas. La primera de ellas se encarga de dar de alta o baja a los usuarios dentro el sistema. Para que un usuario pueda ser dado de alta debe disponer de un certificado válido. Los administradores cargan el certificado en el sistema y es la propia aplicación la encargada de verificar el certificado y extraer los campos significativos que en él se almacenan. El

certificado también será almacenado en su totalidad ya que será empleado para que el resto de usuarios carguen valores del sistema y puedan verificar el censo, uno de los parámetros de la votación. La gestión de la caducidad de los certificados se realiza de manera automática y ningún certificado se emplea fuera de los márgenes temporales para los que está autorizado.

La parte de gestión de votaciones se realiza mediante una interfaz en la que el administrador carga los parámetros necesarios para el proceso de votación: censo; número de rondas de la votación; márgenes temporales de las distintas rondas; y la pregunta o votación. También indica si existen diversos pesos para los votantes, de manera que se pueda subdividir a los votantes en distintos grupos, algo necesario para las votaciones ponderadas.

Mientras que los valores correspondientes a los parámetros de la votación son campos prefijados, en cantidad que no en valor, y el censo se elabora mediante un listado con los nombres o certificados de los usuarios registrados que pueden participar, las opciones para plantear la pregunta/cuestión son más amplias y pueden realizarse ad-hoc para cada votación.

Para incluir la pregunta en el sistema se permite a los administradores o creadores de la encuesta que desarrollen un entorno o escenario a su medida. La única condición que se impone a la hora de elaborar la pregunta es que la respuesta u opción a firmar sea un *string*. Esto se consigue mediante el empleo de la función *voteBallot*() que transforma la respuesta en un *string* ya sea rellenando la posible respuesta hasta alcanzar un determinado tamaño o mediante alguna técnica de compresión, hash, en el caso de que la opción elegida tenga un tamaño mayor que aquel que se debe firmar. De esta manera, el sistema permite que la pregunta sea completamente personalizable permitiendo, entre otras: preguntas abiertas; cerradas; empleo de las opciones como los *radio button*, listas de opciones, respuestas múltiples usando *checkboxes*, etc.

C. *Extensión de Firefox en el cliente*

Para facilitar la usabilidad del sistema y facilitar al usuario el testeo del sistema de votación, se ha desarrollado el programa del cliente como una extensión de Firefox. Los usuarios descargan la extensión, disponible en la misma página de votaciones, y la instalan en su navegador. El programa cliente está diseñado para que sea compatible con el navegador Firefox y con los sistemas operativos basados en Linux (Ubuntu 10.04.4 LTS) y para Windows desde XP en adelante.

Esta extensión es la encargada de realizar la gestión de los certificados PKCS12 diseñados para el correcto funcionamiento del sistema de votación. También realiza el intercambio de información necesaria para obtener los parámetros de la votación y gestiona el proceso de firma del votante. Ha sido diseñado de tal manera que su empleo sea transparente para el usuario excepto en el proceso de votación. Será en ese momento cuando se solicite al usuario el password con el que protege su clave privada. Para crear una mayor sensación de seguridad en el sistema de votación, se muestra al finalizar el proceso una ventana indicando que el voto ha sido emitido y contabilizado de forma correcta así como el valor de la firma final.

Fig. 3 a.- Selección de votación. b.- Página de votación

IV. Proceso de elección, firma y Gestión de la información

La interacción del usuario con el sistema de votación se realiza según se muestra en la Figura 3. El usuario accede al sistema de votación y selecciona la votación en la que quiere tomar parte. El servidor le mostrará la pantalla de votación y el usuario seleccionará su opción o bien dará una opinión si es una pregunta abierta. Cuando la selección haya finalizado se iniciará el proceso de firma. El programa instalado en el cliente le solicitará al votante la ubicación del certificado PKCS12 en el que se almacena su clave privada y también el password que desbloquea el acceso a la clave privada. Una vez que se ha aprobado el acceso se inicia el proceso de firma, se solicitan al servidor los parámetros necesarios para realizar la firma, en caso de que sea necesario se realiza un hash de la respuesta, y se procede a la firma de la opción seleccionada. Una vez firmado el mensaje se cifra con la clave pública de la urna y se envía al servidor acompañado de la firma.

Durante todo el proceso se muestran diversas ventanas de aviso e información al usuario. Se le indica la opción seleccionada para realizar la votación (que deberá ser verificada), el usuario que va a realizar la firma y el valor de la firma del mensaje.

Una vez que ha pasado el plazo permitido para realizar la votación, se cierra el proceso y se procede al escrutinio. La urna es la encargada de descifrar los votos empleando su clave privada. Es en ese momento cuando se realiza la verificación de las firmas asociadas a cada voto. Las firmas que no sean verificadas serán descartadas junto con sus votos. Una vez obtenidos los votos válidos, se procederá a descartar los votos provenientes de un mismo usuario, identificados mediante el *linking tag*. Este caso se puede dar

ya que el sistema permite que los votantes cambien de opinión mientras el periodo de votación se encuentre abierto. El voto válido será el último emitido dentro del plazo de votación, esta característica se puede modificar para cada votación indicando qué voto será el válido: el primero, el último o la media de los votos.

Al emplear un sistema de votación basado en firmas en anillo, no se podrá publicar un listado con los usuarios que han participado en la votación, pero sí que se podrá publicar un listado con el *linking tag* asociado a cada uno de los votos. Al permitir el sistema la división de los usuarios en grupos, se pueden realizar escrutinios por separado y después ponderar los resultados parciales para obtener el resultado final.

El sistema permite que una votación se componga de diversas rondas de votación, cada una con un periodo de tiempo prefijado. De esta manera, se podrá realizar un análisis de la evolución de las opiniones emitidas por los votantes ya que los distintos votos se podrán enlazar mediante el valor del *linking tag* asociado. Es gracias a esta característica que el empleo de este sistema de votación es de gran valor para realizar consulta de QoE. No sólo tendremos un mecanismo seguro de votación sino que además podremos realizar un seguimiento en la evolución de sus valoraciones con distintos mecanismos y en distintos momentos de tiempo.

V. QoE y Experiencia de Laboratorio

El sistema de eVoting propuesto tiene diversas características que lo hacen muy interesante para su empleo en la valoración de la QoE. El primero de ellos es el hecho de emplear el navegador web como medio para llevar a cabo la votación. De esta manera la usabilidad que se consigue es muy alta al no tener el votante que aprender el manejo de una aplicación específica. Además, el navegador web nos permite una gran maniobrabilidad para poder diseñar la votación de manera que se le facilite al máximo al usuario el proceso y realizar una presentación compacta tanto del contenido a evaluar (video, imagen, sonido, etc.) como del proceso de evaluación.

La segunda característica que hace que el sistema de eVoting propuesto otorgue un valor añadido para quienes realizan la evaluación es que, garantizando siempre el anonimato de los usuarios, se puede realizar un seguimiento de las respuestas de los votantes de manera individual. Esta característica nos permitirá analizar las respuestas de los votantes y poder realizar filtrados si se observan patrones de respuesta contradictoria.

Gracias a esta última característica y dada la relación entre QoE y QoS [22, 23], se podrá realizar un análisis sobre las variaciones en la valoración de la QoE por parte de los usuarios para unas medidas de QoS fijadas. De esta manera se podrá efectuar un seguimiento de los votantes cuyas respuestas sigan la tendencia marcada por la relación QoE-QoS y dar un mayor peso a estas votaciones respecto a las de otros usuarios cuyas votaciones no se ajusten a la relación establecida o en los que se observen respuestas aleatorias.

Empleando otra de las posibilidades del sistema, como es la de realizar diversas rondas para una misma votación, se podrá llevar a cabo un seguimiento temporal y relacionar las respuestas y sus variaciones en diferentes momentos. Todos estos valores darán a los evaluadores una mayor

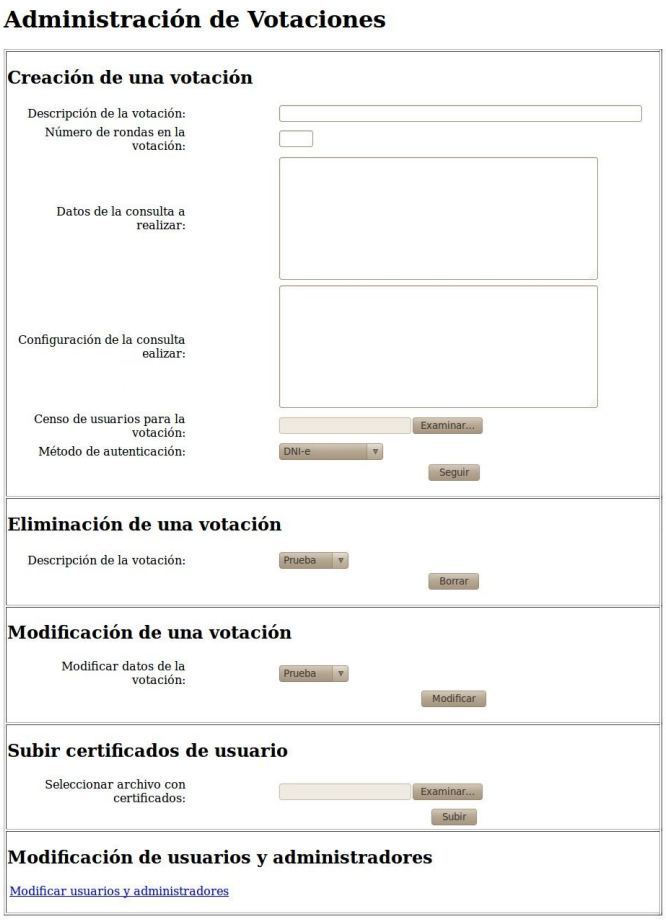


Fig. 4.- Administración de votaciones

cantidad de información al poder ligar los momentos de las distintas rondas de votación con momentos temporales determinados.

Para probar el correcto funcionamiento del sistema se realizó una prueba en el que se planteaba una pregunta relacionada con el diseño de la página web del departamento. En la Figura 4 se muestra la interfaz mediante la que el administrador del sistema introduce en el sistema los parámetros necesarios para realizar nuevas votaciones y la manera de gestionar votaciones ya existentes. El campo libre del formulario "*Datos de la consulta a realizar"* es el lugar donde se carga la pregunta. Este campo permite introducir código html de manera que tanto la manera de presentar como de realizar la pregunta es muy versátil pudiendo implementar las preguntas de manera ad-hoc para cada votación.

Para que la experiencia fuese lo más cercana a la realidad posible se obtuvieron unas nuevas claves para repartir entre los participantes en la votación. Se realizó el reparto de las claves y se realizó el censo añadiendo a todos los participantes en la votación. Adicionalmente se añadieron también más certificados con claves que no iban a ser empleadas en la votación para manejar un censo más amplio. La única condición que se impuso en la votación fue la elección del sistema operativo. De esta manera se consiguió que se empleasen sistemas operativos Windows y Linux en sus versiones de 32 y 64 bits y así realizar un mayor testeo del sistema en la parte del cliente.

A la vez que se repartían las claves se realizó un seguimiento individualizado para comprobar si existía algún

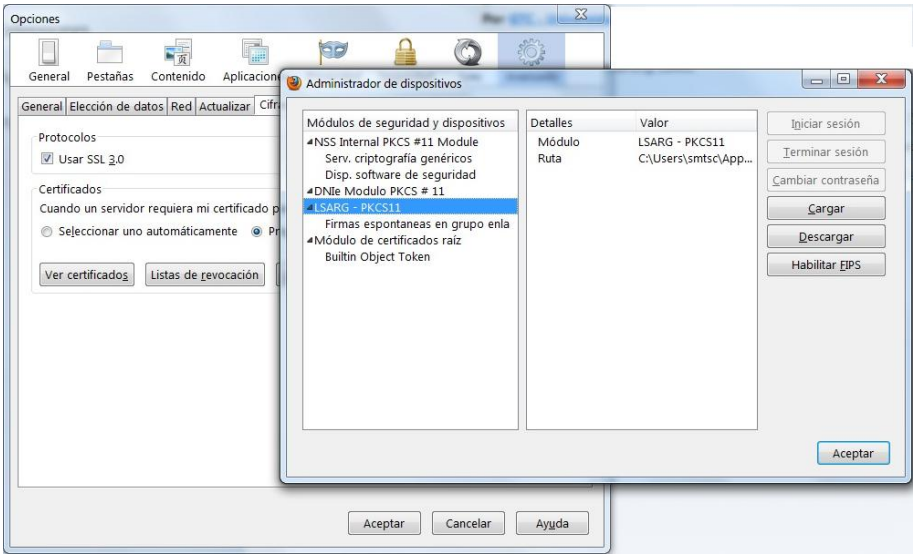


Fig. 5.- Extensión de gestión de las firmas enlazables en anillo instalada en el ordenador

problema para cargar el certificado PKCS12 en los distintos ordenadores. Alguno de los participantes almacenaba primero el certificado y después instalaban la extensión necesaria para realizar la gestión de los certificados y el proceso de firma. Otros usuarios instalaban primero la extensión en el navegador y después cargaban el certificado. Se pudo comprobar que no hubo ningún problema independientemente del orden ni del sistema operativo empleado.

Una vez cargada la extensión en el navegador del cliente se puede observar como se ha instalado una nueva extensión que va a ser la encargada de trabajar con las firmas en anillo empleadas para realizar las operaciones de verificación y firma necesarias por el sistema de votación. Además, si se abre la ventana del navegador correspondiente a la administración de dispositivos seguros, se observa que se ha instalado la extensión y que esta va a ser la encargada de gestionar las firmas espontáneas enlazables en anillo, Figura 5.

Para realizar la prueba de laboratorio se realizó una votación, con una pregunta y una única ronda, en la que se daba la opción de indicar el color que se creía más adecuado para emplear como fondo en la página inicial del departamento. La opción preferida debía indicarse mediante la selección del color con un *radio button* diseñado a tal efecto. A petición nuestra, varios de los votantes votaron más de una vez para probar si se realizaba una correcta detección de los votos de un mismo usuario.

Al finalizar el tiempo permitido para realizar las votaciones se procedió al escrutinio de los votos. Se realizaron las verificaciones necesarias y además se realizó una comprobación con todos los participantes para comprobar que los resultados obtenidos se correspondían con la realidad. Al realizar el escrutinio final se detectaron los votos emitidos por un mismo usuario comprobando el *linking tag* que acompaña al voto y siendo válido únicamente para el escrutinio final el último de los votos emitidos.

El procesado de los votos emitidos se realizó de manera "manual" debido a que el número de votos no era muy elevado y que las posibilidades de respuesta se reducían a dos. De todas maneras, la información, con los votos en claro y las firmas que lo acompañan, es fácilmente manejable ya que se puede trabajar o volcar la información almacenada y diseñar programas para realizar una gestión automática de los votos. Esta gestión de los resultados de la votación, al igual que la presentación de la consulta, se realiza *ad hoc* para cada votación. De esta manera se consigue una mayor versatilidad para la plataforma.

VI. CONCLUSIONES

El empleo de un sistema de votación segura permite la recogida de información fiable y de calidad. Estos sistemas cumplen una serie de requisitos que los equiparan a los procesos de votación presenciales, e incluso pueden llegar a aumentar las prestaciones para los votantes al facilitar una verificación universal de los resultados.

La aplicación más inmediata de los sistema de votación electrónico es la sustitución o complementación de los actuales procesos de votación presencial, servir de base a nuevos sistemas de gestión de la democracia (eCognocracia) o para llevar a cabo la recogida de información de una manera segura y fiable en encuestas de marketing y en especial en sistemas de recogida de información para la evaluación de la QoE de un protocolo o sistema.

La implementación de un sistema de votación segura requiere cumplir una serie de características de seguridad de manera que el proceso teórico no se vea afectado por los mecanismos desarrollados para su implantación. En este artículo se ha mostrado una implementación real de un sistema de votación segura empleando firmas en anillo y desarrollada en su totalidad mediante software libre y verificable por el usuario.

El sistema presenta unas características que lo hace muy propicio para realizar medidas de QoE en entornos seguros. El protocolo empleado garantiza el anonimato de los participantes y a la vez permite enlazar los distintos votos emitidos durante el proceso y así analizar la evolución de la valoración de la QoE de un usuario.

Como línea futura de trabajo se quiere realizar un estudio más extenso sobre la usabilidad del sistema mediante su

empleo en encuestas con un mayor número de participantes y dificultad técnica que las realizadas hasta el momento en el entorno de pruebas de laboratorio. Además, se trabajará sobre los datos recogidos para realizar un estudio sobre la evaluación de la QoE basadas en diversas experiencias multimedia, como el análisis de video con distinta QoS y así poder realizar un estudio que ligue la evaluación subjetiva QoE con los parámetros objetivos de QoS.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente subvencionado por el proyecto CPUFLIPI (MICINN TIN2010-17298) del Gobierno de España, Cátedra Telefónica-Universidad de Zaragoza y el Fondo Social Europeo en colaboración con el Gobierno de Aragón.

REFERENCIAS

[1] T. Kohno, A . Stubblefield, A.D. Rubin and D.S. Wallach: “Analysis of an electronic voting system”. In: IEEE Symposium on Security and Privacy. IEEE Computer Society Press, Los Alamitos (2004)

[2] S. P. Everett, K. K. Greene, M.D. Byrne, D.S. Wallach, K. Derr, D. Sandler and T. Torous: “Electronic voting machines versus traditional methods: improved preference, similar performance”. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08). 2008, pp. 883 - 892. DOI=10.1145/1357054.1357195

[3] B. Lee and K. Kim.: “Receipt-free electronic voting scheme with a tamper resistant randomizer”. In Proceedings of the 5th international conference on Information security and cryptology (ICISC'02), pp. 389 - 406.

[4] J. Benaloh and D. Tuinstra.: “Receipt-free secret-ballot elections”. Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of computing (STOC'94), 1994, 544–553.

[5] L.F. Cranor, R.K. Cytron.: “Design and Implementation of a Practical Security-Conscious Electronic Polling System”, Technical Report WUCS-96-02, Washington University, 1996.

[6] Z. Xia and S. Schneider: “A New Receipt-Free E-Voting Scheme Based on Blind Signature” In: WOTE: Workshop on Trustworthy Elections, 2006, pp. 14 – 28.

[7] D. Chaum. Blind signatures for untraceable payments. In Advances in Cryptology – Crypto ’82, pages 199–203. Plenum Press, 1983.

[8] M. Jakobsson, A. Juels, and R. L. Rivest: “Making mix nets robust for electronic voting by randomized partial checking”. In Proceedings of the 11th USENIX Security Symposium (USENIX ’02), 2002, pp 339 – 353

[9] M. Michels and P. Horster. “Some remarks on a receipt-free and universally verifiable mix-type voting scheme”. In ASIACRYPT ’94, pages 125–132. Springer-Verlag, LNCS 1163, 1996.

[10] A. Acquisti: “Receipt-free homomorphic elections and write-in ballots.” Cryptology ePrint Archive, Report 2004/105 (2004)

[11] I. Damgård, M. Jurik: “A Generalisation, a Simplification and Some Applications of Paillier’s Probabilistic Public-Key System”. In: PKC 2001. LNCS, (vol. 1992), 2001, pp. 119–136.

[12] R.L. Rivest, A. Shamir and Y. Tauman: “How to leak a secret. “in Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), 2001 , pp. 552-565.

[13] J.L. Salazar, J. Piles, J. Ruiz and J.M. Moreno-Jiménez: “Security approaches in e-cognocracy”. Computer Standards and Interfaces, 32 (5–6), 2010, pp. 256–265.

[14] P. P. Tsang and V. K. Wei: “Short linkable ring signatures for e-voting, e-cash and attestation”. In Proceedings of the First international conference on Information Security Practice and Experience (ISPEC'05), 2005, pp. 48 - 60. DOI=10.1007/978-3-540-31979-5_5

[15] J.L. Salazar, J. Piles, J. Ruiz and J.M.Moreno-Jiménez: “E-cognocracy and its voting process”, Computer Standards and Interfaces, 2008, pp 124–131.

[16] D. Chaum and E. Van Heyst: “Group signatures”. In Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques (EUROCRYPT'91), 1991, pp. 257 - 265.

[17] J. Liu, V. Wei, D. Wong: “Linkable spontaneous anonymous group signature for ad hoc groups”, in:, ACISP 2004. LNCS, (3108), 2004, pp. 325–335.

[18] C. Adams and S. Lloyd: “Understanding Public-Key Infrastructure – Concepts, Standards, and Deployment Considerations”. Macmillan, Indianapolis (1999)

[19] R. L. Rivest, A. Shamir and L. Adleman: “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, (v.21 n.2), 1978 , pp.120-126. DOI:10.1145/359340.359342

[20] S. Brands: “Rethinking Public Key Infrastructure and Digital Certificates - Building in Privacy”. PhD thesis, Eindhoven Institute of Technology, Eindhoven, The Netherlands, 1999.

[21] PKCS #12: Personal Information Exchange Syntax Standard. http://www.rsa.com/rsalabs/node.asp?id=2138. Revised 01/04/2013

[22] H. J. Kim, D. H. Lee, J. M. Lee, K. H. Lee, W. Lyu and S. G. Choi: "The QoE Evaluation Method through the QoS-QoE Correlation Model," Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference on , vol.2, no., pp.719-725, 2-4 Sept. 2008 doi: 10.1109/NCM.2008.202

[23] H. J. Kim and S. G. Choi: "A study on a QoS/QoE correlation model for QoE evaluation on IPTV service" Advanced Communication Technology (ICACT), 2010 The 12th International Conference on , vol.2, no., pp.1377-1382, 7-10 Feb. 2010

INDECT Lawful Interception Platform: Overview of ILIP Decoding and Analysis Station

Raquel Aparicio, Manuel Urueña, Alfonso Muñoz, Gerson Rodríguez, Sergio Morcuende
Telematics Engineering Department
Universidad Carlos III de Madrid
Avda. Universidad 30, 28911 Leganés (Madrid) Spain
{raparici, muruenya, ammunoz, gsantos, smorcuen}@it.uc3m.es

***Abstract*- The INDECT Lawful Interception Platform (ILIP) will enable European Police forces to capture and analyze the data communications of suspects under the auspices of a Digital Wiretap Warrant. This paper provides an overview of the ILIP Decoding and Analysis Station that will help Police analysts to process in a cost-effective manner the huge amount of information that may be seized even from a single suspect. It features advanced capabilities such as VoIP-to-text transcription, content annotation and classification, an enhanced access control based on smart cards and digital certificates, as well as a flexible plug-in architecture that enables the automatic pre-classification of contents. Its modular architecture has been designed to easily integrate other analysis tools and services developed by INDECT, such as the LINK relationship analyzer or the INACT image cataloguing tool.**

***Keywords*- INDECT Lawful Interception Platform (ILIP), Law Enforcement Agency (LEA), Digital Wiretap Warrant (DWW), Voice over IP (VoIP), Content pre-classification, Smart Card (SC).**

I. INTRODUCTION

Nowadays criminals are increasingly employing Internet and other communications networks to both coordinate crimes in the real world and even commit crimes directly over the Internet. Therefore, the Lawful Interception (LI) of data communications will become an indispensable tool for Police forces to investigate crime organizations.

This paper introduces the INDECT Lawful Interception Platform (ILIP), which is being developed within the INDECT project [1] and whose general objective is the development of solutions and tools for European Police forces. ILIP has been designed to be compliant with current ETSI Lawful Interception standards, and even enhances them regarding privacy and civil rights protection. A key element of ILIP is the so-called Digital Wiretap Warrant (DWW) [2], which guarantees by technical means that all ILIP wiretaps have been approved by a judge or senior officer, and thus conform to the national and European legal frameworks. Moreover, ILIP has been designed with a number of security and privacy mechanisms that enable the seized communications to be used as digital evidences in a court of justice.

Moreover, ILIP provides European Police forces with a tool capable of automating some of the repetitive tasks that agents have to perform during criminal investigations: it captures a subject's communications, decodes them to obtain the exchanged information, and even performs some data pre-classification to filter irrelevant traffic and thus helps Police analysts to focus on important contents first. However, it must be stressed that this automatic pre-classification is just the first step of the whole content classification process, since the final classification decision always lies at the hands of the Police analysts. The ILIP platform is composed by two main entities (Fig. 1):

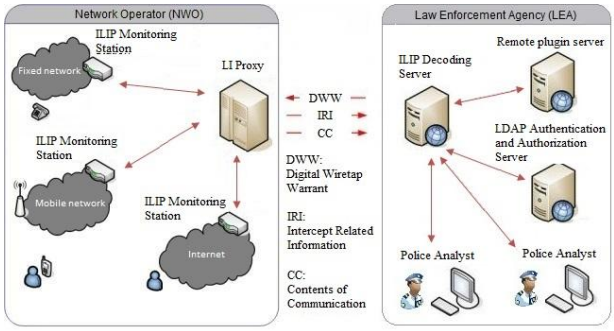


Fig. 1. Main components of the INDECT Lawful Interception Platform (ILIP)

- **ILIP Capture Stations**. These probes are placed at the Point of Presence (PoP) of an Internet Service Provider (ISP) or Network Operator (NOW) and capture all the traffic from the clients of the ISP covered by a valid DWW. Seized data traffic is digitally signed, time-stamped, compressed, and encrypted before being sent to the decoding server assigned to the case.
- **ILIP Decoding and Analysis Server**. It is located in the premises of a Lawful Enforcement Agency (LEA). Each investigation case has an associated Decoding Server that reconstructs the communication flows from the packets captured by the monitoring stations and decodes the contents being exchanged by the suspects under investigation. The decoded contents are indexed and stored in a database to ease its access by the authorized Police analysts assigned to that case.

This paper is focused on the ILIP Decoding and Analysis Server that is employed by the Police analysts to process the contents captured by the ILIP Monitoring Stations. The ILIP Decoding and Analysis Server is based on Xplico network forensic tool [7], although it has been extended in multiple ways to enhance its security, decoding and analysis features. In particular a speech-to-text module for Voice over IP (VoIP) communications has been developed to help in the transcription process, and thus it now enables indexing and searching VoIP communications. In order to handle the huge amount of information that may be captured, even from a

single suspect, the ILIP Decoding and Analysis Server features a novel plug-in architecture for content pre-classification. This architecture greatly simplifies the integration of smart data analysis tools and services that may either run locally or be accessed remotely by means of a web service interface. A novel illegal content identification plug-in [10] has been developed to validate the feasibility of this architecture. Unlike other content identification tools, it is based on fuzzy hashing which even allows identification of illegal contents (i.e. child porn, terrorist manuals) that have been modified by the suspects to evade detection. The ability to integrate other tools being developed in the INDECT project will further increase the analysis capabilities of ILIP. For instance the VoIP and e-mail communications of the suspects can be easily exported to the LINK relationship analysis and visualization tool [11] to identify communication patterns and understand the structure of the criminal organization they belong to.

The organization of this paper is as follows: Section 2 provides a brief overview of ETSI Lawful Interception standards. Section 3 explains in detail the ILIP Decoding and Analysis Server, including all developed modules and pre-classification plug-ins, as well as its integration with other INDECT tools. Section 4 details how ILIP is integrated into the INDECT Security Architecture. Finally, Section 5 concludes the paper and presents the future of the ILIP platform.

II. State of the art: ETSI lawful interception standards

The European Telecommunication Standards Institute (ETSI) is the organization that specifies Lawful Interception (LI) standards for the European Union and other countries. In particular the ETSI has a Technical Committee for Lawful Interception. This section provides an overview of the main ETSI LI standards:

- Requirements from a Lawful Enforcement Agency's point of view: TS 101 331 [3].
- Requirements from a Network Operator's point of view: ES 201 158 [4].
- Handover Interface description: TS 101 671 [5], ES 201 158, TR 101 943 [6].

It is important to take into account that much of the information in these documents is subject to national law and international treaties and therefore has to be interpreted in accordance with applicable national regulations in its particular context and implemented if required.

A. Requirements from a Lawful Enforcement Agency's point of view

The particular requirements and results of the interception of a certain subject are specified in a lawful authorization (a.k.a. wiretap warrant), which is handed over to the Network Operator (NWO) of the suspect, so that it must cooperate immediately upon its reception. Besides, results from different investigations on the same subject are to be kept completely separated (e.g. different LEAs investigating the same person). The interception results are composed of two kinds of information: the Contents of Communication (CC) themselves and Intercept Related Information (IRI), which consists of any other metadata such as connection attempts (e.g. missed calls), service, state, location information, etc.

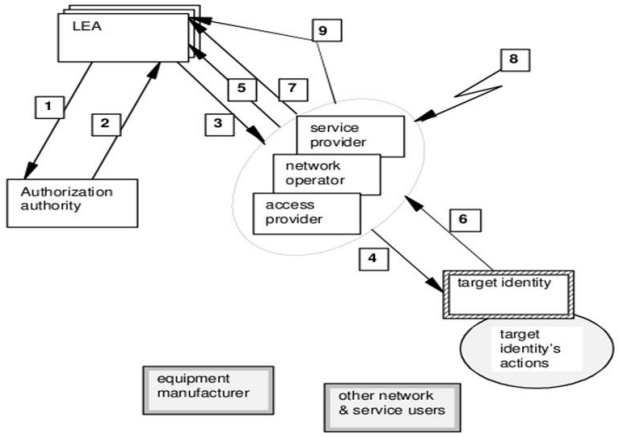


Fig. 2. ETSI functional role model of Lawful Interception [4].

B. Requirements from the Network Operators' point of view

Due to the fact that the actual interception is performed by the suspect's communications operator, which can be either a Network Operator (NWO), Access Provider (AP) or Service Provider (SvP), ES 201 158 [4] deals mainly with the process to be performed to initiate a lawful interception. The functional role model shown in Fig. 2 describes the typical procedural operation of lawful interception:

1. The Lawful Enforcement Agency (LEA) requests a lawful authorization from an authorization authority, which may be a court of law.
2. The authorization authority issues a lawful authorization to the LEA.
3. The LEA hands over the lawful authorization to the operator, which determines the relevant target identities from the information given in the lawful authorization.
4. The operator configures interception facilities to be applied to the relevant target identities.
5. The operator informs the LEA that the lawful authorization has been received and acted upon. Additional information may be passed to the LEA relating to the target identities and the target identification.
6. IRI and CC from the suspect's communications are monitored by the operator.
7. IRI and CC are then passed from the operator to the LEA.
8. Either on request from the LEA, or when the period of authority of the lawful authorization has expired, the operator will cease the interception arrangements.
9. The operator announces this cessation to the LEA.

C. Handover Interface description

The ETSI LI standards define a generic Handover Interface (HI) that can be applied to any telecommunication system. This interface is divided into three ports, depending on the type of information that is transmitted through them:

- Handover Interface port 1 (HI1) is the LI administrative interface and works in both directions: lawful authorizations, acknowledgments, state reports and alarms are sent through this interface.

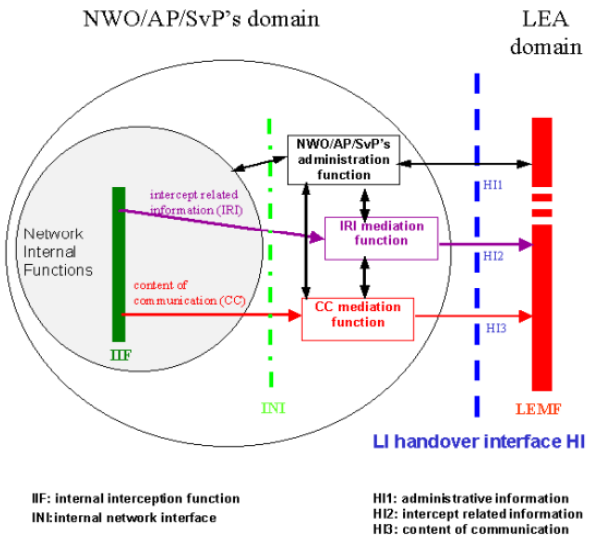


Fig. 3. Functional block diagram of ETSI Handover Interface [5].

- Handover Interface port 2 (HI2) transports the Interception Related Information (IRI) from the operator to LEA premises.

- Handover Interface port 3 (HI3) transports the Contents of Communication (CC) from the operator to LEA premises.

These three ports can be clearly distinguished in Fig. 3, which shows the internal structure of the Handover Interface on the operator side. The outer circle represents the operator domain with respect to Lawful Interception. It contains the network internal functions (inner circle) such as switching, routing and handling of communication processes, where data are intercepted by the Internal Interception Functions (IIF), and three new elements: the Internal Network Interface (INI), the Administration Function and two Mediation Functions (for IRI and CC), which can be integrated into just one Mediation Function. The purpose of these Mediation Functions is to completely isolate the operator and LEA domains.

ILIP has been designed to fulfil all the requirements defined by the ETSI LI Technical Committee. In particular the Digital Wiretap Warrant (DWW) [2] is the interception authorization mandated by the ETSI, with the special feature that it is not just an administrative document but it enforces the security and privacy of lawful interceptions by technical means. The ILIP Monitoring Stations implement the Network Internal Functions defined by the ETSI. That is, capturing all IP traffic exchanged by the suspect and sending it, after being compressed, encrypted and digitally signed, to the Mediation Function of the network operator. This information, still in encrypted form, will be sent to the LEA Mediation function in order to be processed by the ILIP Decoding and Analysis Server.

III. ILIP DECODING AND ANALYSIS SERVER

The ILIP Decoding and Analysis Server is based on the Xplico network forensic tool [7], able to extract the application data contained in captured IP traffic. Several new modules have been developed to be integrated with Xplico, so as to be applicable to Lawful Interception, and thus serving as the basis to the ILIP Decoding and Analysis Server. The main modules that have been developed are listed below:

- **VoIP transcription module [8]:** It performs an automatic text transcription of the suspect's VoIP conversations.
- **Content distribution module [9]**: It acts as an intermediary between Xplico and the pre-classification plug-ins, making it possible to process multiple contents in parallel.
- **Content pre-classification plug-ins [9]:** They are smart analysis applications or services capable of processing the seized contents and obtaining their pre-classification importance values, which are then analyzed in detail by Police analysts.
- **Illegal content identification plug-in [10]:** This content pre-classification plug-in assigns the maximum importance to known illegal contents from a back list. It is based on fuzzy hashing, which enables it to identify illegal contents, even if they have been modified to avoid its detection by using traditional hashing techniques.
- **Integration with LINK application [11]**: E-mail and VoIP communications can be exported in order to visualize the relationships of the suspects using the LINK application, which has been developed by AGH University, also within the INDECT project.

The ILIP Decoding and Analysis Server also provides a graphical web interface, both to configure its modules and plug-ins, as well as to analyze all seized data. Access to the application has been further protected by means of X.509 digital certificates stored in Smart Cards or USB Tokens, and performing user authentication and authorization against an LDAP directory.

A. Modular Architecture

Xplico [7] is an open source, network forensic tool that has been used as a base for the ILIP Decoding and Analysis Server. It has been heavily modified in order to be applicable to lawful interception, as well as to be integrated with other INDECT tools in order to increase the system overall functionality. The traffic decoding phase is performed by the so-called dissectors, which are specialized components that assemble application-level information from the captured IP datagrams. Xplico implements 44 dissectors, in different development stages, that support the most popular Internet protocols including HTTP, FTP, SMTP, POP, IMAP, Telnet, SIP, H.323 and RTP.

Captured traffic can be provided to Xplico in .pcap files or by performing a live capture. In the case of the INDECT Lawful Interception Platform (ILIP), it only makes use of the capture file decoding functionality since the traffic filtering and interception is performed by the ILIP Monitoring Stations, which supply time-stamped, encrypted and digitally signed files that the ILIP Decoding and Analysis Server must check and decrypt in order to obtain the raw .pcap file for Xplico. Decoded contents (e-mail messages, visited web pages, downloaded images, video, files, etc.) are stored in separate files, as well as in database entries that contain some meta-information about the captured content. For example, the capture and decoding times, the size of the content, the IP

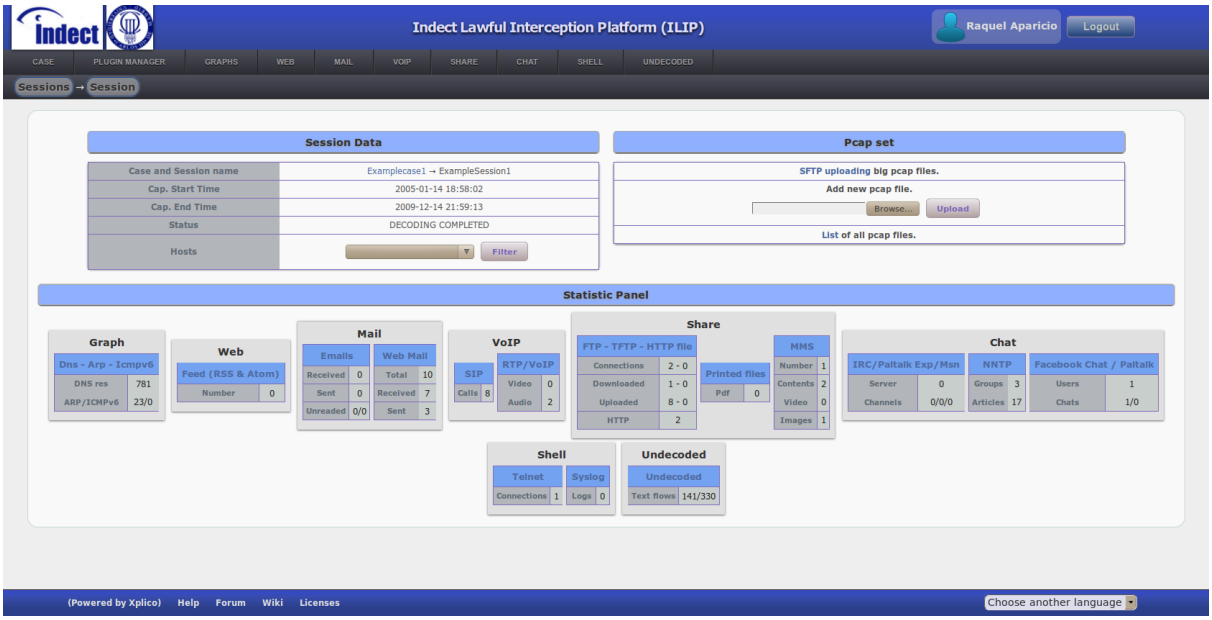


Fig. 4. Screenshot of ILIP Decoding and Analysis Station web interface.

address of a Telnet server the suspect connected to, or the SIP addresses of those involved in a VoIP conversation with the suspect. The captured information is further organised in cases and sessions. A Xplico case relates to a Police's investigation case, and corresponds to one criminal category (e.g. terrorism, drug or human trafficking). It is then divided in sessions that contain the different capture files. This structure helps the Police analysts to organize the data for example by date or location, letting each session to correspond to a different day and/or to a different communication channel of the suspect. Once a case and a session have been created, capture files are processed one by one by Xplico dissectors and other modules until the application-level contents are obtained as files and stored in the local file system and the associated meta-data is keep in a local SQLite database.

The integration with other analysis tools is performed after contents are obtained. Basically, all contents are sent to the content distributing module that checks if there is any pre-classifying plug-in able to process that type of content. In the particular case of audio contents coming from VoIP conversations, they are previously processed by the VoIP transcription module in order to obtain text files which can be further processed by other text pre-classification plugins. Both modules will be described in more depth in the following sections. Once their content processing has finished, modules call Xplico back, which has been modified to update the database with these results and, in the case of VoIP contents, to also send the newly obtained transcription files to the content distributing module for their processing.

The platform offers access to the decoded contents through its web interface, which is organized by type of content as shown in Fig. 4. Most of the main screen space contains data about the number of decoded contents, organized by type. Above it, the status of the decoding process is shown and, on the top of the page, there is a menu bar that provides access to visualize the decoded information by content type and to configure the plugin manager.

This web interface has been heavily modified and integrates the new interfaces of both the Content Distribution and Pre-Classification module and the VoIP module, in order to simplify the access and configuration of the platform. The details about the developed modules are given in the following subsections.

B. VoIP Transcription Module

The VoIP Transcription Module [8] is based on the Sphinx-4 [13] voice recognizing engine. This software was selected because it is the only opensource one that provides acoustic models adapted to telephone conversations, including VoIP. The module uses the HUB4 language model, which contains 64,000 English words and it is the largest and offers a theoretical error rate of 20%. Cmudict.0.6.d is employed as the dictionary, because it is the largest available one in Sphinx-4.

When the RTP flows of a VoIP conversation are decoded, each audio is then processed with Sphinx-4 using a generic acoustic model by default, although specific acoustic models can be employed for the suspect and other involved peers that appear repeatedly in the captured conversations. After the transcription is done, the VoIP database table is updated with the audio of the different peers and their text transcriptions, which are then passed to the Content Distribution module for further analysis (e.g. flagging certain keywords).

In our tests, the accuracy of the transcription process with the generic acoustic model is quite low (i.e. less than a 40%). Therefore the automatic transcription may be then edited manually, splitting the whole conversation in phrases (both in text and audio) and thus helping the Police to locate the erroneous words and rewrite them after listening the audio associated to those phrases. Moreover, once the whole transcription has been corrected, the user may train the system with that audio and text, which creates new acoustic models for that particular users (identified by their SIP addresses), or improves the existing ones. The transcriptions using the user's specific acoustic model feature a significant accuracy improvement (i.e. up to a 60%) if the model is trained with corrected transcriptions. It is worth noting that the transcription accuracy solely depends on the selected speech-to-text library, not the ILIP module itself, which may

be easily adapted to support other libraries, such as Google Voice, for instance.

C. Content Distribution Module

The Content Distribution module receives the decoded contents from Xplico and distributes them, according to their MIME (Multipurpose Internet Mail Extensions) type, among the respective plug-ins, which in turn perform a pre-classification of the contents and return an importance value in the form of an integer between 0 and 5, as well as a textual description of such classification. A returned value of 0 means that the plug-in was not able to classify it (e.g. it does not appear in the illegal contents black list). A value between 1 and 5 defines the content importance, where 1 means that the content is not important at all (e.g. a spam message), and 5 that the content is of the utmost importance (e.g. a known illegal content). The usage of the Content Distribution module as an intermediary step in the decoding process provides three important benefits:

1. The decoding code does not need to be modified every time a new analysis plug-in is inserted into the system. This module takes care of new plug-ins in runtime.
2. It performs a pre-processing of the data received from the dissectors, and generates other common meta-data necessary for plug-ins, such as the content size, its MIME Type, and a MD5 hash of the content to uniquely identify it.
3. It allows processing multiple contents in parallel, by running each analysis process in a separate thread

The first feature is enabled by keeping information about the plug-ins in the system database. Every time it receives a content, the Content Distribution module reads the database to obtain the list of available plug-ins that are able to analyze that type of content. This makes the dynamic insertion and removal of plug-ins as easy as updating the database. Each plug-in must specify its location (i.e. how to call it), its priority and the content types it can process, and a short description explaining its purpose. The supported content types are specified using a syntax similar to that of MIME types. For instance, for analysing a web page, a `text/html` plug-in is preferred, rather than a `text/*` plug-in or the generic `*` one. Since there may be multiple plug-ins for the same content type, the order in which they are called is specified by using the priority attribute. Once the list of available plug-ins is sorted by type and priority, the plug-ins are called in order until any of them returns a pre-classification value (1 to 5) or all plug-ins return an unknown (0) value. Thus, this simple syntax enables a fairly flexible rule-based mechanism for content analysis.

Contents are processed in parallel by means of a thread pool, which limits the number of threads that can execute at the same time on the system, to prevent overloading it. Each content is processed by its own thread, which is obtained from the thread pool for the first plug-in that processes the content, and reused by the following ones until a pre-classification value is obtained.

D. Pre-classification plug-ins

Pre-classification plug-ins can execute either locally, on the same machine than the Content Distribution module, and thus are called *local* plug-ins, or remotely, as a web service running in a different server, and thus are called *remote* plug-ins. The first kind of plug-in is adequate for simple classifications that do not require a large knowledge database and have a low CPU usage. On the other hand, remote plug-ins are intended for those with high CPU or memory requirements, and complex analysis tools that manage its own set of data, so keeping them in a centralized server simplifies its maintenance and leverages the common knowledge among all ILIP Analysis Servers that consult it.

Plug-in developers have to implement only two operations: *Analysis* and *Training*. The *Analysis* operation is executed when the Content Distribution module asks the plug-in to provide a pre-classification value for a given content. In order to let the Police analysts understand why a given pre-classification value was assigned, a textual description is also returned (e.g. specifying the specific illegal content the content is similar to). However, if the Police analysts consider that the assigned importance is wrong (either too low or too high), they can change it and *train* the plug-in with the correct importance value for that content, by using the *training* operation.

1. Local plug-ins

Local plug-ins are those which operate on the local ILIP Decoding and Analysis Server. They are executed as separate processes to prevent crashing the Content Distribution module itself. Therefore, any executable program, developed with any programming language, can be employed as a local plug-in as long as it returns the content importance as its exit value, and prints the textual description though the standard output. The location of the content to be analyzed and the additional meta-data is passed as an argument to the plug-in executable. This allows existing programs to be easily employed as local pre-classification plug-ins (i.e. using `spamassassin` to assign the lowest importance to spam messages) just by developing a small input/output wrapper.

2. Remote plug-ins

Remote plug-ins are those executing on a server other than the ILIP Decoding and Analysis Server, but probably located in the same LEA datacenter. They are executed as web services using a simple SOAP interface. Therefore they can also be developed with any programming language featuring web service libraries. We have developed a small Java package to develop plug-ins that can be executed both locally and remotely. By executing in a separate dedicated server, remote plug-ins can be as sophisticated as desired, with the additional benefit that an intelligent content analysis service (e.g. Natural Language Processing) can be shared among multiple Analysis Stations, and thus leveraging the common knowledge base and the training performed by all Police analysts handling cases from the same criminal category.

To increase the overall performance of the pre-classification process, both the Content Distribution module and the remote plug-ins developed with our Java-based development framework implement caching, so known contents are not processed multiple times but its importance value is returned immediately.

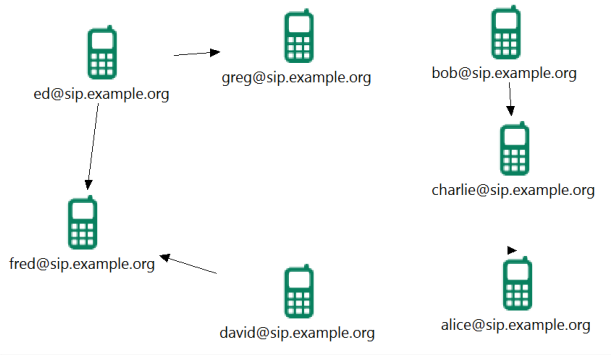


Fig. 5. LINK graph of captured VoIP conversations

E. Integration with other INDECT tools

Apart from integrating analysis modules directly into the ILIP Decoding and Analysis Server, it is also possible to extend the platform to export captured information that can serve as input for other analysis applications. For instance a simple module has been developed to export a summary of VoIP and e-mail communications for the LINK tool [11]. LINK, which is also being developed by the INDECT project, consists of a set of tools to integrate, process and visualize data from several sources such as telephone bills, bank statements or address books. It has been further extended to support e-mails and VoIP conversations captured by ILIP.

In particular a list with the selected VoIP or e-mail communications of the suspect could be exported to a CSV (Comma-Separated Values) file. Each communication record includes the users involved in the communication, where the origin is the sender of the e-mail or the SIP user that initiated the VoIP call. The length of the conversation or the size of the e-mail is also provided to indicate the importance of that communication. Fig. 5 shows a sample graph obtained by LINK after processing a list of VoIP calls supplied by ILIP.

F. Advanced Security

Given the strict security requirements of Law Enforcement Agencies, and in order to protect the privacy of the suspects and the Police analysts investigating them, the ILIP Decoding and Analysis Server has been integrated into the INDECT Security Architecture [14], and can only be accessed by means of HTTPS. Therefore, the ILIP Decoding and Analysis Station employs a X.509 certificate from the INDECT Public Key Infrastructure (PKI) to prevent man-in-the-middle attacks. The INDECT PKI will issue certificates for all INDECT subsystems (from the INDECT Devices CA) and users (from the INDECT Users CA), featuring 2048 bits-long RSA keys and signatures based on SHA256 message digests. INDECT users will also have a X.509 certificate that is employed for authentication purposes, by means of the User ID (`uid`) extension field that uniquely identifies each INDECT user. Users' certificates will be securely stored in Smart Cards or USB Tokens, as the ones shown in Fig. 6.

The underlying Apache web server of the ILIP Decoding and Analysis Server has been configured to perform mutual authentication in the underlying SSL/TLS session. This means that the users connecting to the ILIP platform must first provide a valid INDECT user certificate. However not all INDECT users may access the ILIP platform even if they have a valid INDECT certificate. After authenticating a user, the ILIP Decoding and Analysis Server checks the INDECT LDAP User Directory to check whether such user is allowed to access the ILIP platform, and to obtain her authorization attributes.

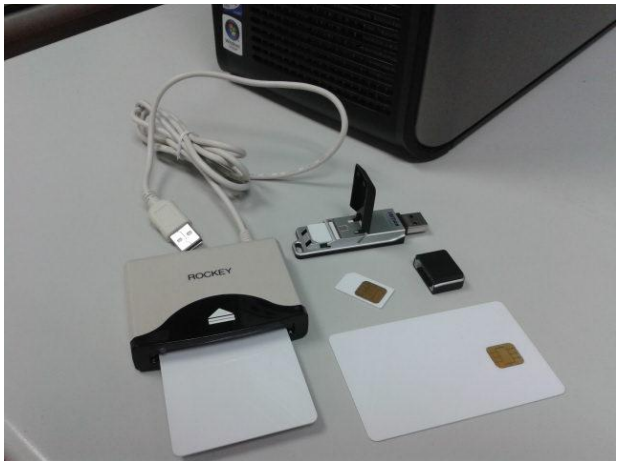


Fig. 6. Security devices employed to access the ILIP platform

The INDECT LDAP User Directory is organized around two main groups of objects: modelling applications and users. The information about all INDECT applications and subsystems is stored as `application` objects, identified by its unique application Id (`aid`); unsurprisingly, the application ID of the ILIP platform is "`aid=ilip`". In order to be compatible with current LEA IT systems, the information about INDECT users is stored in standard `inetOrgperson` objects, identified by the User ID (`uid`) field that must correspond with the certificate extension field of the same name and OID. The authorization attributes of the user are stored as sub-objects, identified with the corresponding application ID. If there is no object under the user for a particular application, the user is not allowed to access the application at all. There are multiple types of `appPermisison` objects in order to be able to represents different sets of attributes for each application (e.g. a `ilipAppPermission` class) although, for complex authorization rules, it is also possible that each application stores the authorization attributes of its users locally, and thus only employs the INDECT LDAP User Directory for authentication purposes.

Moreover a multi-factor authentication mechanism has been implemented for users with special roles, such as the ILIP administrator, who is able to manage (create/delete) cases. After being authenticated using its X.509 certificate, the administrator has to provide an additional password (the login is the UID of her certificate), which is also securely stored in the LDAP User Directory.

IV. Conclusions

The INDECT Lawful Interception Platform (ILIP) is a next generation Lawful Interception platform for IP-based communications that has been specially tailored for European Law Enforcement Agencies. Therefore it fulfils all requirements [3-6] specified by the ETSI LI Technical Committee and includes advanced features such as state-of the-art security and civil rights protection by means of the so-called Digital Wiretap Warrant (DWW) [2].

This paper has presented in detail the ILIP Decoding and Analysis Server that has been designed to help Police analysts to process the huge amount of information that may be seized from suspects covered by valid DWWs. In particular, the Xplico network forensics tool has been employed as the base of the ILIP Decoding and Analysis Servers since it implements more than 44 dissectors, which are able to decode the most popular Internet protocols nowadays. Furthermore, Xplico has been extended in several ways in order to be employed for Lawful Interception. In particular, this paper has presented the main extension modules that have been developed in the INDECT project.

The VoIP transcription module employs the open source Sphinx-4 library to provide an automatic speech-to-text transcription of VoIP calls. The accuracy of the standard English acoustic model is still low, but the module allows correcting the transcriptions manually and the train the acoustic model of the suspect in order to increase the accuracy of following transcriptions.

Without any doubt, the automatic processing and analysis tools of the ILIP platform are the most critical features for Police analysts. Therefore, the ILIP Decoding and Analysis Server features a novel content analysis architecture based in pre-classification plug-ins. The Content Distribution module is able to load new plug-ins in runtime, and has a simple but powerful rule-based mechanism to choose which plug-ins are applied to captured contents based on their MIME types. The pre-classification plug-ins can be run either locally or remotely. Local plug-ins execute in the ILIP Decoding and Analysis Server as separate processes, and thus can be implemented using any programming language. Only simple classification tools should be executed as local plug-ins in order to do not interfere with the ILIP server itself. Complex content analysis applications requiring a large knowledge base or having greater processing and memory requirements can be also employed by ILIP as remote plug-ins. In order to do so, these applications may run in a dedicated server as web services. The Content Distribution module is able to access such remote plug-ins by using a simple SOAP interface with only two operations: analyze and train. By means of training Police analysts are able to adapt the classification behaviour of plug-ins (either remote or local) by specifying the importance that a plug-in should assign to given contents.

Apart from pre-classification plug-ins, the ILIP platform has been integrated with other analysis tools developed within the INDECT project. For instance the LINK relationship analysis and visualization application can be employed to study the VoIP and e-mail communication patterns of the subject. As a future work we are looking into integrating the INDECT Advance Image Catalog Tool (INACT) [12] image processing tool into the ILIP Decoding and Analysis Server.

It is also worth noting that ILIP has been the first INDECT subsystem that has been integrated into the recently proposed INDECT Security Architecture [14]. In this sense, the ILIP web interface can only be accessed by means of HTTPS, featuring mutual user-server authentication. Both ILIP servers and INDECT users have X.509 certificates issued by the INDECT Public Key Infrastructure (PKI). ILIP implements a multi-factor user authentication, where INDECT user certificates are stored in Smart Cards or USB tokens, and access to ILIP can be further protected by password, which is securely stored in the INDECT LDAP User Directory. This LDAP directory is also employed to store user information, as well as the different authorization attributes each user has for the applications she is allowed to access.

ACKNOWLEDGEMENTS

This work has been funded by the EU Project INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) — grant agreement number: 218086 — and the Spanish project CRAMNET — TEC-2012-38362-C03-01.

REFERENCES

[1] INDECT Project website: http://www.indect-project.eu/. Accessed: 27 November 2012.

[2] Alfonso Muñoz, Manuel Urueña, Raquel Aparicio and Gerson Rodríguez. “Digital Wiretap Warrant: Guaranteeing Civil Liberties in ETSI Lawful Interception”. Submitted to the Computers & Security Journal. 22 of October 2012.

[3] ETRI TS 101 331: Lawful Interception (LI); Requirementes of Law Enforcement Agencies. Versión 1.3.1. October 2009.

[4] ETRI ES 201 158: Telecommunications security; Lawful Interception (LI); Requirements for network functions. Versión 1.2.1. April 2002.

[5] ETRI TS 101 671: Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic. Versión 3.10.1. June 2012.

[6] ETRI TR 101 943: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture. Versión 2.2.1. November 2006.

[7] Xplico website: http://xplico.org/. Accessed: 27 November 2012.

[8] Jesús Vallinot. “Módulo de transcripción VoIP-texto”. Technical Report, Universidad Carlos III de Madrid. February 2012.

[9] Rubén Mena. “Módulo de distribución y pre-clasificación de contenidos”. Technical Report, Universidad Carlos III de Madrid. July 2011.

[10] Roberto Sánchez. “Módulo de clasificación de contenidos basado en hashes difusos”. Technical Report, Universidad Carlos III de Madrid. April 2012.

[11] LINK website: https://link.iisg.agh.edu.pl/. Accessed: 27 November 2012.

[12] Michał Grega, Damian Bryk, Maciej Napora and Marcin Gusta. “INACT - INDECT Advance Image Catalog Tool”. 4th Multimedia Communications, Services and Security (MCSS’11), Krakow, Poland, June 2-3, 2011.

[13] Shinx-4 website: http://cmusphinx.sourceforge.net/sphinx4/. Accessed: 1 February 2013.

[14] INDECT Consortium. “INDECT D8.7 – Definition of mechanisms and procedures for the security and privacy of the exchanged information”. January 2013.

Nuevo Sistema de Emisión de CRLs para la Red KAD

Juan Caubet, Carlos Gañán, Oscar Esparza, Jose L. Muñoz
Departamento de Ingeniería Telemática (ENTEL)
Universitat Politècnica de Catalunya (UPC)
C/ Jordi Girona 1-3, Campus Nord, Edificio C3, 08034, Barcelona, España
{juan.caubet, carlos.ganan, oscar.esparza, jose.munoz}@entel.upc.edu

***Resumen*—Muchas overlays P2P requieren ciertos servicios de seguridad para poder ser utilizadas como aplicaciones comerciales, y una simple Infraestructura de Clave Pública (PKI) podría solucionar el problema. Sin embargo, estas infraestructuras tienen que estar vinculadas a un sistema de revocación, como por ejemplo las Listas de Certificados Revocados (CRLs). Un sistema con una estructura cliente/servidor, donde una Autoridad de Certificación (CA) juega el papel de servidor central. Por lo tanto, propenso a sufrir problemas en grandes redes por el hecho de tener un único punto de fallo. Y si además tenemos en cuenta que los usuarios de muchas redes P2P pueden cambiar de identidad, o incluso disponer de más de una, los problemas crecen. El tamaño de las CRLs crecerá exponencialmente con el número de usuarios y deberemos actualizarlas con mucha frecuencia para garantizar la frescura de la información que contienen. Nosotros proponemos un nuevo sistema de revocación distribuido para la red KAD. La distribución de las CRLs se lleva a cabo utilizando la propia overlay, y para no comprometer la capacidad de almacenamiento de los nodos, las CRLs son divididas en segmentos. Este mecanismo mejora la accesibilidad de la información de revocación, incrementa la disponibilidad de los segmentos, y garantiza la frescura de la información mediante la emisión de los segmentos de forma independiente.**

***Palabras Clave*—Lista de Certificados Revocados (CRL), Overlay P2P Estructurada, Red KAD**

I. Introducción

Los sistemas P2P emergieron como un incipiente paradigma de las comunicaciones, permitiendo compartir recursos sin la necesidad de utilizar servidores centralizados. Hoy en día estas redes tienen un gran éxito gracias a la disponibilidad de un considerable ancho de banda a bajo coste y al gran incremento en el número de dispositivos compartiendo recursos y servicios. Sin embargo, la mayoría de redes de este tipo tienen problemas de seguridad por falta de una autoridad centralizada y la asunción de que los nodos siempre tienen un comportamiento honesto [1]. Por estas razones, y otras como la privacidad [2], [3], estas redes no están siendo ampliamente utilizadas por aplicaciones comerciales. Por lo tanto, desplegando una Infraestructura de Clave Pública (PKI) dentro de una overlay permitiríamos que los nodos pudieran comunicarse y compartir información de forma segura. Serían capaces de realizar transacciones (pagos electrónicos) o incluso de firmar contratos de forma digital sin poner en riesgo información confidencial.

Las PKIs fueron desarrolladas para cumplir con los principales requisitos de seguridad propuestos para entornos de Internet, adoptando la idea de clave pública y empleando el concepto de certificado digital para vincular los datos de una entidad con la clave pública correspondiente. Pero utilizar certificados digitales implica la necesidad de validarlos [4]. Cuando un usuario quiere acceder a un recurso, éste no sólo necesita encontrar una cadena de certificados que lo una al proveedor, sino que también necesita comprobar cada uno de esos certificados intermedios para determinar que la cadena es válida. Sin embargo, el proveedor sólo necesita ser capaz de rechazar los nodos conflictivos. Los certificados digitales pueden ser revocados por varias razones. Por ejemplo, un certificado será revocado si la clave privada vinculada a éste ha sido comprometida o la afiliación del propietario ha cambiado, ya que en ambos casos el certificado ya no es válido. Hasta día de hoy se han propuesto muchos sistemas diferentes de revocación, pero la solución tradicional y más utilizada está basada en Listas de Certificados Revocados (CRLs) [4].

Las CRLs son listas negras, emitidas periódicamente por las Autoridades de Certificación (CAs), que enumeran certificados revocados junto con su fecha de revocación, y opcionalmente con la razón de la revocación. Otros mecanismos convencionales están basados en realizar peticiones a un servidor que es capaz de verificar el estado de revocación de un certificado, por ejemplo el Protocolo de Estado de Certificados Online (OCSP) [5]. Estos sistemas de revocación, y otros menos populares, tienen diferentes características en términos de sobrecarga de la red, carga en los servidores que proporcionan la información de revocación, frescura de esta información e idoneidad para su uso *offline*. Pero la mayoría son estructuras cliente/servidor, donde una CA juega el rol de servidor central y sufre los típicos problemas de un único posible punto de fallo. Además, si únicamente unas pocas CAs (o una sola) distribuyen una CRL a todos los usuarios de una red aparece un cuello de botella.

En el contexto de las overlays, si sólo unas pocas CAs son las encargadas de distribuir las CRLs a todos los nodos de una red, seguro que sufrirán sobrecarga; ya que una overlay P2P estructurada puede tener cientos de miles de usuarios, o incluso millones. Y si tenemos en cuenta que los usuarios pueden cambiar de identidad dentro de la red, siempre con un certificado asociado, el problema se acentúa; ya que el tamaño de la CRL[1] crece exponencialmente con el número de usuarios. Además, si la red tiene muchos usuarios y cada usuario tiene un conjunto de certificados, se espera que la tasa de revocación de certificados sea muy elevada. Por lo tanto, la CRL debe ser actualizada con más frecuencia porque en caso contrario la información no será lo suficientemente fresca. Así que las políticas de actualización tradicionales no

[1]Nótese que en este artículo nos referimos al tamaño de una CRL, o segmento, para referirnos al número de certificados que están almacenados en esa lista

son adecuadas para asegurar la disponibilidad y la frescura de la información de revocación en estas redes.

Por otro parte hay gente dentro de la comunidad investigadora reacia a aceptar el uso de cualquier clase de servicio centralizado en una overlay P2P estructurada, ya que se supone que estas redes son redes P2P puras[2]. Por lo tanto, en este tipo de redes no es suficiente con replicar el servidor que emite las CRLs para evitar cuellos de botella.

Para resolver los problemas anteriormente mencionados, nosotros proponemos un nuevo sistema distribuido de revocación para una overlay P2P particular, la red KAD. Este sistema distribuye las CRLs utilizando la propia overlay, y para no comprometer la capacidad de almacenamiento de los nodos, las CRLs son divididas en varios segmentos. Lo cual nos permite emitir la CRL por partes y de forma independiente, afectando menos el rendimiento de la red y evitando cuellos de botella.

En nuestra propuesta, la CA es otro nodo más dentro de la red, pero la responsable de publicar y almacenar todos los nuevos segmentos de CRL. Sin embargo, a diferencia de en otros métodos tradicionales, el resto de nodos no sólo se descargan los segmentos de CRL de la CA, o de otros nodos, sino que se convierten en proveedores de esos segmentos en el mismo momento en que empiezan una descarga. De esta forma el número de propietarios de segmentos de CRL que pueden proporcionar información de revocación crece exponencialmente, por lo que su disponibilidad crece. Además, esta nueva forma de distribuir segmentos de CRL nos permite mejorar la política de actualización de las CRLs, pero manteniendo todas las propiedades de seguridad de los sistemas tradicionales. Ahora los segmentos de CRL pueden ser actualizados de forma independiente, cosa que mejora la frescura de sus datos consumiendo menos ancho de banda.

El resto del artículo está organizado de la siguiente forma: en la siguiente Sección encontramos un breve estado del arte. La Sección III presenta una breve descripción sobre la red KAD. La Sección IV describe el funcionamiento de nuestro sistema. La Sección V analiza su rendimiento. Y en la Sección VI tenemos las conclusiones.

II. Estado del Arte

Ying y Jiang [7] proponen un nuevo sistema de revocación de certificados basado en la red Chord [8], y el uso de un "filtro de bloom" para evitar cuellos de botella. Su sistema se basa en difundir el vector del "filtro de bloom" de un cierto segmento de CRL por toda la red. De esta forma los autores consiguen utilizar menos ancho de banda y espacio de almacenamiento, sin embargo estos filtros pueden dar falsos positivos, la cual cosa complica el proceso de validación de los certificados.

En [9] los autores proponen un método basado en "Super Nodos" para mejorar la estructura de distribución, y gracias a la incorporación de esta jerarquía consiguen minimizar los requisitos de almacenamiento en los nodos/servidores. Los nodos actúan tanto de clientes como de servidores, y los "Super Nodos" como autoridades. El proceso de distribución se basa en un mecanismo de *pulling*.

[2]Las redes puramente descentralizadas utilizan mecanismos P2P en todos y cada uno de sus procesos, y de ningún modo existe un servidor central. Un típico ejemplo de este tipo de redes es la red Gnutella [6].

Morogan y Mutfic describen un sistema distribuido de revocación de certificados basado únicamente en el uso de una red P2P [10]. De esta forma consiguen un buen rendimiento ante periodos de desconexión y mejoran la disponibilidad de los servidores.

En [11], sus autores proponen una nueva infraestructura de confianza distribuida, basada en la red Chord, y con ella presentan un nuevo sistema de revocación. Ellos utilizan a los nodos de la red para almacenar la información de revocación directamente, es decir, no utilizan CRLs. Cada nodo es responsable de almacenar un conjunto de certificados, y si un certificado esta revocado el mismo nodo añade una etiqueta para indicarlo.

Por otra parte, la confianza (*trust*) también se puede utilizar como una alternativa muy válida para controlar/limitar el acceso a las redes P2P. El nivel de confianza refleja la responsabilidad, el buen hacer, y la satisfacción de un nodo; por este motivo los modelos de confianza pueden incrementar el número de relaciones exitosas. Además, su implantación es más simple y mejora la escalabilidad del sistema. Por ejemplo, el modelo BBK [12] describe una confianza cuantificada y dividida en dos tipos: confianza directa y confianza referenciada. Sin embargo, en este modelo la confianza positiva y la negativa son escaladas en la misma medida, lo cual puede dar pie a referencias maliciosas. En [13], los autores presentan un modelo de confianza distribuido para la plataforma JXTA [14]. Aquí la confianza se calcula en base a los intereses y palabras clave de los usuarios, pero ello precisa de una tabla por grupo de nodos, la cual cosa puede resultar ineficiente en redes P2P muy densas. Los autores de [15] describen diferentes tipos de confianza, y la relación que existe entre los valores de confianza y los roles en un modelo de control de acceso. Sin embargo, ellos no determinan como trabaja el modelo de control de acceso basado en roles con una red basada en relaciones de confianza.

III. La red KAD

KAD es una de las implementaciones más populares de una overlay P2P estructurada, a día de hoy se estima que estén conectados a ella alrededor de 4 millones de usuarios. Se trata de una red basada en el uso de la Tabla de Hash Distribuida (DHT) Kademlia [16], e implementada por aplicaciones de compartición de ficheros como eMule [17] and aMule [18], ambas de código abierto. Cada nodo de la red KAD dispone de un identificador *KADID* de 128 bits que indica su posición dentro del espacio virtual de la overlay, y la distancia entre dos puntos (nodos o recursos) es el número entero resultante de realizar la operación exclusive-or (XOR) entre esos dos puntos. De esta forma, los nodos dentro de la red KAD son tratados como hojas de un árbol binario, donde el prefijo único más corto de su *KADID* determina su posición. Los nodos agrupan sus contactos en *buckets* y almacenan estas listas como tablas de enrutamiento. Cada nodo registra un máximo de k contactos por nivel i, donde esos contactos son una distancia, entre 2^{128-i} y 2^{127-i}, a contar desde el *KADID* del nodo. Cuánto más cerca se encuentre el contacto del punto objetivo, mayor conocimiento tendrá de esa parte de la DHT; lo cual llega a proporcionar un enrutamiento de orden $O(logn)$. El enrutamiento hacia un *KADID* se realiza de forma

iterativa, los mensajes son enviados a n contactos cercanos al objetivo y cada nodo en la ruta devuelve el siguiente salto.

Al igual que en otras muchas overlays, el propósito de la DHT es relacionar ficheros con palabras clave (*keywords*). Para compartir un fichero, los datos y las palabras clave deben ser procesados por separado usando la función MD5, y después publicados en la red varias veces (al menos 10 veces). KAD sólo publica referencias (metadatos y fuentes), y estas referencias se almacenan en nodos cercanos a los identificadores de las palabras clave (*keywordIDS*) y las fuentes (*sourceIDs*) respectivamente. La distancia que determina si la cercanía es suficiente se llama zona de tolerancia de un *KADID*, y se calcula utilizando los 8 bits más significativos del identificador. Además, para mejorar la disponibilidad, los recursos se republican periódicamente: los *sourceIDs* cada 5 horas y los *keywordIDs* cada 24 horas. Análogamente, el nodo donde fue publicado un *sourceIDs* o *keywordIDs*, lo eliminará pasadas 5 o 24 horas respectivamente. El proceso de republicación es idéntico al de publicación.

IV. Sistema de Distribución de CRLs

En una overlay P2P con cientos de miles de usuarios, o quizás algún que otro millón, si cada usuario dispone de un conjunto de seudónimos, el número de certificados emitidos por una CA puede llegar a ser de decenas de millones. Por esta razón surgen dos problemáticas que los sistemas de revocación tradicionales no tienen en cuenta. Por una parte el tamaño de las CRLs es mucho mayor, la cual cosa dificulta su distribución. Y por otra parte existe un compromiso entre mantener la frescura de la información y la sobrecarga de la red producida por la distribución de las CRLs. Por lo tanto, es necesario definir un nuevo sistema de distribución de CRLs adaptado a las características de estas redes. Necesitamos mejorar la disponibilidad de la información de revocación y mantener la información lo más fresca posible.

A. Requisitos del Sistema

1) **Escalabilidad:** El coste de validar el estado de los certificados debe ser el menor posible, ya que estas redes pueden involucrar a decenas de CAs y unos cuantos millones de usuarios, todos ellos llevando a cabo decenas de transacciones.
2) **Balanceo de la Carga:** El coste de almacenar y distribuir CRLs debe ser distribuido entre todos los nodos de la red.
3) **Tolerancia a Cambios Frecuentes:** El sistema debe saber adaptarse a las constantes entradas y salidas de nodos en la red, ya que las redes P2P se caracterizan por su falta de estabilidad.
4) **Alto Rendimiento:** El sistema debe ser eficiente, pero sin requerir un excesivo coste computacional ni demasiado ancho de banda.
5) **Seguridad:** Ningún nodo debería ser capaz de generar información de revocación válida de forma fraudulenta.

B. Descripción General

Nuestra propuesta divide las CRLs en varios segmentos para evitar que se conviertan en listas poco manejables debido a su tamaño. Los segmentos se almacenan y dividen de forma distribuida, mejorando así su disponibilidad y previniendo que las CAs se conviertan en cuellos de botella.

Ahora todos los nodos son servidores potenciales de los segmentos de CRL, y las CAs actúan como cualquier otro nodo de la overlay. Sin embargo, las CAs siguen siendo las responsables de emitir e introducir los segmentos en la red. Esta introducción se realiza mediante un mecanismo de *pulling*, es decir, las CAs envían los segmentos de CRL a los nodos que los demandan. Obviamente, las CAs también son las responsables de dividir las CRLs en los diferentes segmentos, y de evitar que los nodos puedan falsificarlos; para ello firman cada segmento de la misma forma que se hace con las CRLs.

Los nodos comparten los segmentos de CRL desde el primer momento en que se han descargado un solo *chunk*[3], de esta forma se convierten en servidores de un segmento sin disponer todavía de él. Gracias a ello, las CAs no se convierten en cuellos de botella; incluso si el número de peticiones en un corto periodo de tiempo es muy elevado. Cuando una CA actualiza un segmento de CRL, el proceso empieza de nuevo; la CA es la única poseedora del mismo y los nodos deben pedir un segmento para poder empezar a compartirlo.

A continuación describimos el funcionamiento del sistema desde el punto de vista de un nodo, A, por medio de un ejemplo práctico, el cual se ilustra en la Figura 1. Vamos a suponer que A quiere verificar si el certificado c es válido, y para ello, primero de todo debe calcular el número del segmento i en el que estaría incluido el número de serie del certificado c, en caso de estar revocado. Una vez A conoce el número de dicho segmento, comprueba si dispone del segmento o necesita obtenerlo de la red. En caso de tenerlo almacenado en local, consulta si el número de serie de c está en la lista y acaba el proceso. En caso contrario, A envía una petición a la overlay para descargase el segmento i. Esta petición llega hasta un nodo, B, el cual responde a A indicándole que el nodo C tiene el segmento i. Finalmente, el nodo A se descarga el segmento del nodo C y comprueba si el número de serie de c está en esta lista. Obviamente, si el número de serie está en la lista c no es válido, si no lo está sí que lo es.

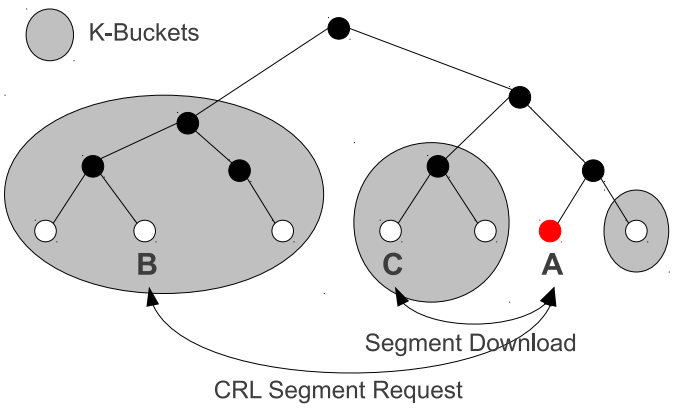


Fig. 1. Ejemplo de búsqueda en la red KAD.

Cabe destacar que el funcionamiento de la red KAD es un

[3]Los *chunks* son los fragmentos de información más pequeños que manejan los sistemas P2P.

poco más complejo que lo que muestra el ejemplo, y que el número de nodos que responderían a A sería considerable, así como el número de nodos que dispondrían del segmento. También es lógico pensar que normalmente no se encuentra un nodo servidor del contenido que se busca en un sólo salto; lo normal es que en las primeras respuestas recibamos punteros a nodos que pueden saber quién tiene el contenido, pero los nodos que contestan no disponen de él.

En cuanto a la posible implementación de este sistema en otras overlays P2P, tales como BitTorrent [19] o P2PStream, es necesario tener en cuenta una serie de características para garantizar su buen rendimiento. Los ficheros deben ser almacenados por los propietarios de los mismos y por todo aquel que se los haya descargado, pero los punteros o referencias a ellos deben ser almacenados por la overlay. La red Chord [8] es un ejemplo de red donde no se cumplen estas características, ya que los propietarios no almacenan sus contenidos. Además, es importante que la red replique los punteros o referencias en un número considerable de nodos. De esta forma las búsquedas son más rápidas y las respuestas se distribuyen mejor. Y por último, destacar que el proceso de búsqueda y la forma en que se identifican los recursos dentro de la red no deberían ser un problema; el sistema se podría adaptar fácilmente.

C. Segmentación de las CRLs

Nosotros proponemos dividir las CRLs en 2^k segmentos, donde k es la longitud del resultado de la función utilizada para asignar los certificados a un segmento en concreto. Las CAs utilizan una función de hash, $h(\cdot)$, la cual, dado el número de serie de un certificado devuelve el número del segmento donde debería estar almacenado ese certificado en caso de estar revocado. De esta forma, la CA que debe revocar un certificado, primero calcula el hash del número de serie del mismo y lo almacena en el segmento de CRL indicado por la salida de la función. De forma inversa, los nodos calculan la función de hash del número de serie del certificado que quieren verificar y obtienen el número del segmento que deben consultar.

Cabe destacar que este funcionamiento sería válido para cualquier CA utilizada, ya que es independiente de la longitud del número de serie de los certificados; cada CA puede utilizar un número de bits diferente para identificar los certificados [4]. Por lo tanto, el número de segmentos sería el mismo independientemente de la longitud de los números de serie.

La función de hash más simple y que cumple con los requisitos comentados anteriormente es la función de hash modular; $h(c) = c \ mod \ 2^k$, donde c es el número de serie del certificado. De esta forma conseguimos que el tamaño potencial de los segmentos sea limitado e igual en todos ellos. Teniendo en cuenta que el número de certificados emitidos puede ser como máximo 2^n, cada segmento almacenaría como máximo 2^{n-k} certificados revocados. Y gracias a la simplicidad de esta función, la sobrecarga computacional introducida en las CAs y en los nodos es mínima.

Para crear los diferentes segmentos, o calcular un número de segmento concreto, no es necesario conocer el tamaño real de la CRL. Las CAs y los nodos sólo necesitan saber cuál es el tamaño máximo que podría tener la CRL entera. Por lo tanto, el número de segmentos en que se divide una CRL es independiente de su tamaño. Así que k debe ser elegido cuando se dimensiona el sistema. Si se espera tener CRLs muy grandes, k deberá ser un número elevado, y vice versa. De esta forma conseguiremos mejorar el rendimiento del sistema.

Cabe destacar que en muchos casos puede haber segmentos de CRL vacíos, pero incluso en estos casos es necesario que sean publicados. Los nodos deben poder comprobar que el certificado que quieren validar no se encuentra en el segmento donde debería estar, y éste está firmado por la CA correspondiente. Por razones de seguridad, el hecho de que un nodo no encuentre un segmento de CRL en la red no debe considerarse como que el segmento se encuentra vacío.

La Figura 2 muestra un ejemplo simplificado de división de una CRL en 128 segmentos, ya que la CRL sólo contiene los números de serie de los certificados, única información necesaria para realizar la segmentación.

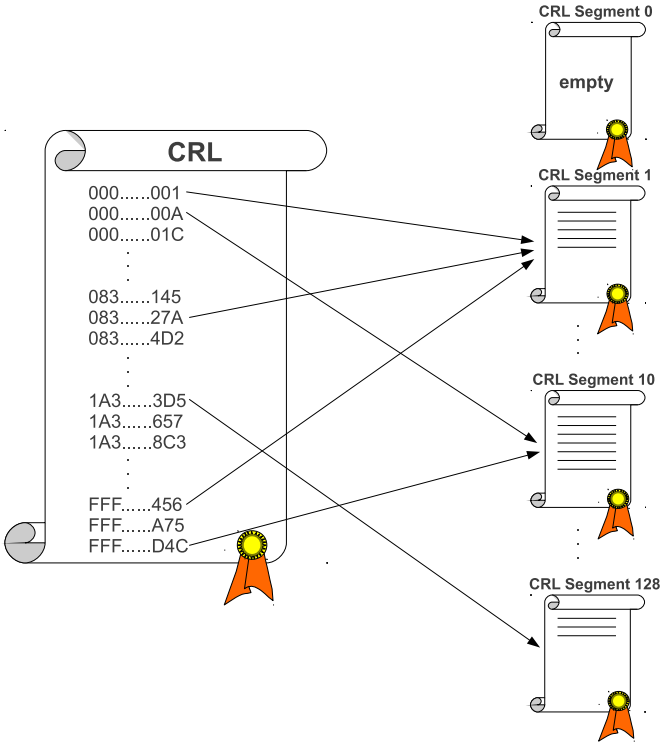


Fig. 2. Segmentación de una CRL.

D. Compartición de los Segmentos de CRL

Los segmentos de CRL se comparten en la red KAD de la misma forma que cualquier otro recurso. Como hemos dicho antes, cada segmento de CRL tiene un número que lo identifica y hace posible que los nodos encuentren los que necesitan. El formato de los nombres es de la forma *"CRL Segment xxx"*, donde *xxx* representa el número de segmento (con una longitud de m bits), por ejemplo *CRL Segment 10*. Por otra parte, los punteros o referencias a los segmentos se encuentran duplicados dentro de la overlay y asociados a tres palabras clave; *CRL*, *Segment* y al número del segmento (*xxx*).

Como ya explicamos en la Sección III, los recursos dentro de la red KAD se buscan a través de sus `keywordIDs` y `souceIDs` ($hash(keyword)$ y $hash(file)$ respectivamente). Por lo tanto, cuando un nodo quiere descargar un nuevo segmento de CRL realiza una búsqueda de una o más palabras

clave, la cual proporciona punteros a múltiples fuentes que contestan con una lista de los nodos que tienen el segmento en cuestión. En ese momento el nodo empieza la descarga, y en cuanto dispone de al menos un *chunk* realiza la publicación del segmento. Para ello publica dos tipos de referencias, metadatos y fuentes, las cuales son enviadas a los nodos que se encuentran en su zona de tolerancia. Las palabras clave son metadatos distribuidos que referencian a las fuentes. Las fuentes son directamente la información de localización de los nodos que contienen copias de ese segmento. En KAD, todos los metadatos y las fuentes se replican en decenas de nodos dentro de la red, y así las búsquedas son más rápidas y devuelven más resultados. Cabe destacar que en el caso de los segmentos de CRL se utilizan tres palabras clave para publicar los metadatos y las fuentes. Sin embargo, sólo una de esas palabras clave diferencia un segmento de otro. Las otras dos se utilizan para diferenciar la información de revocación del resto de recursos compartidos por la red.

Continuando con el ejemplo de la Figura 2, ahora vamos a considerar que un nodo necesita verificar la validez de un certificado con número de serie "FFF.....D4C". Primero de todo, el nodo calcula el hash de dicho número de serie y obtiene, por ejemplo, el número 10; número del segmento a buscar. Acto seguido realiza la búsqueda de *CRL Segment 10*, obtiene una lista de posibles servidores, y se empieza a descargar el segmento de la red. A partir de este momento él se convierte en servidor del segmento 10. Notar que inicialmente sólo la CA disponía de este segmento, en ese caso el nodo se descargaría el segmento de la CA sí o sí.

E. Emisión de los Segmentos de CRL

A medida que pasa el tiempo, la CA que ha emitido una CRL tiene que ir actualizándola; así los nuevos certificados revocados son añadidos a la lista y los que han caducado son eliminados.

En la mayoría de sistemas de revocación que utilizan CRLs, éstas son emitidas de forma periódica, cada 24 horas normalmente. Por lo tanto, cada vez que se emite una nueva CRL, todos los nodos que necesitan validar un certificado también necesitarán descargarse la CRL otra vez. Sin embargo, realizar actualizaciones periódicas sin tener en cuenta la tasa de revocación de certificados, o la actividad de la red puede provocar problemas con la frescura de la información de revocación. Si la actividad en la overlay es elevada y muchos certificados son revocados cada hora, un nodo que utilice una CRL emitida hace 12 horas estará consultando información desactualizada, lo que puede suponer un grave problema de seguridad.

Por esta razón, en nuestra propuesta las CRLs no se emiten periódicamente. Las CAs sólo emiten un nuevo segmento de CRL cuando tienen suficiente información que actualizar, o ese segmento lleva un tiempo considerable sin ser actualizado. Además, nosotros también tenemos en cuenta que cuando se va a emitir una nueva CRL no todos los segmentos que la compondrían habrían sufrido cambios. Por lo tanto, es más eficiente emitir cada segmento por separado y únicamente cuando sea necesario. De esta forma los diferentes segmentos de CRL son gestionados y emitidos como si de CRLs independientes se tratase. Las CAs añaden y eliminan los certificados de los diferentes segmentos, y cuando uno de ellos tiene un número de nuevos certificados considerable, entonces se emite de nuevo.

Para ello nosotros definimos la variable U_s, la cual es calculada por las CAs para cada uno de los segmentos de CRL. Esta variable indica si el segmento debe ser actualizado o no. Si su valor está por encima de un cierto umbral no es necesaria su actualización, si por el contrario su valor es menor, la CA deberá emitir el segmento actualizado. El cálculo de este valor depende del número de usuarios que hay en la red (N), de la tasa de revocación de certificados (R_c) y del número de nuevos certificados revocados que deben ser añadidos al segmento (Δ_s):

$$U_s = \frac{N}{R_c \Delta_s} \tag{1}$$

Cabe destacar que el número de certificados revocados en un segmento puede crecer relativamente rápido debido a una alta tasa de revocación de certificados. Por lo tanto, en ese caso, el tiempo que pasa sin que una CA actualice un segmento ha de ser cada vez más pequeño, ya que existe el riesgo de que haya certificados revocados que estén siendo utilizados. Este es el problema de la frescura de la información de revocación. Sin embargo, aunque ambas variables parecen estar muy relacionadas, no siempre una tasa de revocación elevada provoca un incremento en el tamaño de un segmento, y vice versa. Por esta razón nosotros hemos definido U_s.

Desde el punto de vista de los nodos, debería haber alguna forma de conocer si un segmento de CRL es fresco o no; ya que los segmentos de CRL se van actualizando según sea necesario. Por lo tanto, las CAs deben añadir una marca temporal. En este caso utilizan dos campos de datos de cada segmento, *This Update* y *Next Update*. El primero indica cuando fue emitido ese segmento y el segundo cuando será emitido el segmento actualizado. Obviamente, el segundo campo define el tiempo que como máximo puede pasar sin que el segmento sea actualizado, lo que no quiere decir que no se vaya a actualizar antes.

Teniendo en cuenta que los segmentos de CRL se pueden actualizar en cualquier instante dentro de ese periodo de tiempo, la CA responsable de un segmento es la única que sabe si ese segmento ha sido actualizado, o no. Por lo tanto, los nodos deben decidir si utilizan un segmento que tienen en memoria, o buscan una actualización en la red, en función de su periodo de validez.

V. Análisis del Rendimiento

En nuestro sistema distribuido, las CAs proporcionan nuevos segmentos de CRL a todos los nodos que lo soliciten. Pero a partir de ese momento, estos nodos también se convierten en servidores de los segmentos obtenidos. Por lo tanto, el principal beneficio de distribuir los segmentos de CRL entre diferentes nodos es la reducción del número de peticiones recibidas por los servidores, ya sean CAs o nodos.

Para analizar la tasa de peticiones recibidas por las CAs nosotros definimos la función de densidad de probabilidad de que un nodo envíe una petición de un segmento de CRL a una CA.

Si un segmento de CRL se emite en $t = 0$, la probabilidad de que un nodo envíe una petición dentro del intervalo $[t, t + dt]$ depende de la probabilidad de que el nodo deba realizar

una validación dentro de este intervalo. Un nodo pedirá un determinado segmento dentro del intervalo $[t, t+dt]$, sí y sólo sí, necesita validar un certificado que requiere el uso de ese segmento y durante el periodo $[0, t]$ no ha necesitado validar ningún certificado que también precise del mismo segmento.

Ya que el número de nodos que normalmente componen la red KAD es elevado, nosotros podemos asumir que los tiempos de llevar a cabo la validación de un certificado son independientes y siguen una distribución aleatoria, por lo tanto se cumple la Ley de Poisson. La probabilidad de intentar validar un certificado n en t es:

$$\left[\frac{(vt)^n}{n!}\right] e^{-vt} \ , \ n = 0, 1, 2, 3... \tag{2}$$

Donde e^{-vt} es la probabilidad de que un nodo no realice una validación dentro del intervalo $[0, t]$ y v es la tasa de validación (número de validaciones por unidad de tiempo). Además, nosotros asumimos que todas las validaciones son igualmente propensas a requerir acceso a cualquier segmento de CRL. Si tenemos f segmentos, hay una probabilidad igual a $\frac{1}{f}$ de que un cierto segmento i sea necesario para realizar cualquier validación. De esta forma, la probabilidad de que un segmento no sea necesario para cualquiera de las n validaciones es:

$$\left(1 - \frac{1}{f}\right)^n \tag{3}$$

Combinando las ecuaciones (2) y (3), la probabilidad de que un nodo pida el segmento i dentro del intervalo $[0, t]$ es:

$$\sum_{n=0}^{\infty} \left(1 - \frac{1}{f}\right)^n \left[\frac{(vt)^n}{n!}\right] e^{-vt} = e^{-vt/f} \tag{4}$$

La probabilidad de que un nodo necesite el segmento i dentro del intervalo $[t, t+dt]$, asumiendo que la probabilidad de que se intente llevar a cabo más de una validación es 0 debido a que el intervalo $[t, t+dt]$ es infinitamente pequeño, es:

$$ve^{-vdt}\ dt = v\ dt \tag{5}$$

Y como la probabilidad de que una validación requiera el uso del segmento i es $\frac{1}{f}$, la probabilidad de que este segmento sea necesario en el intervalo $[t, t+dt]$ es:

$$\frac{v\ dt}{f} \tag{6}$$

Usando las ecuaciones (4) y (5), y multiplicando por el número de nodos de la red (N), el número total de peticiones esperado para el segmento i dentro del intervalo $[t, t+dt]$ es expresado como:

$$N_f(t) = \frac{Nve^{-vt/f}\ dt}{f} \tag{7}$$

Y la tasa total de peticiones para un nuevo, o actualizado, segmento de CRL es:

$$R_f(t) = \frac{fN_f(t)}{dt} = Nve^{-vt/f} \tag{8}$$

Teniendo en cuenta que la tasa de peticiones de una CRL entera a una CA en el instante t es $R(t) = Nve^{-vt}$, la tasa de peticiones de segmentos de CRL disminuye con el número de segmentos en los que se divide la CRL, pero no así el pico de peticiones, ya que $R_f(0) = R(0) = Nv$.

Esta diferencia se puede apreciar si se comparan las Figuras 3 y 4. La Figura 3 muestra la tasa de peticiones para una CRL entera y la Figura 4 para segmentos de CRL, ambas durante 24 horas. Nosotros hemos asumido que tanto la CRL entera como los segmentos de CRL fueron emitidos en el instante 0, y que no se realizó ninguna otra emisión durante esas 24 horas. También hemos asumido que el número de nodos dentro de la red KAD es 1 millón, que la tasa de validación (v) es de 50 certificados por día, y que el número de segmentos de CRL es de $2^7 = 128$.

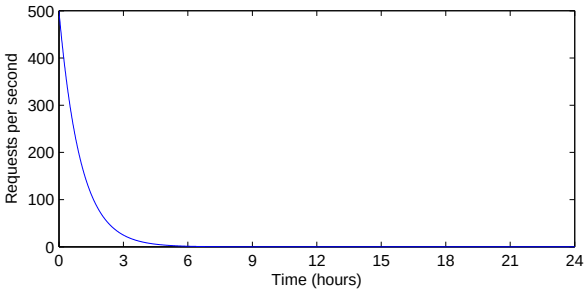


Fig. 3. Sistema estándar de CRLs.

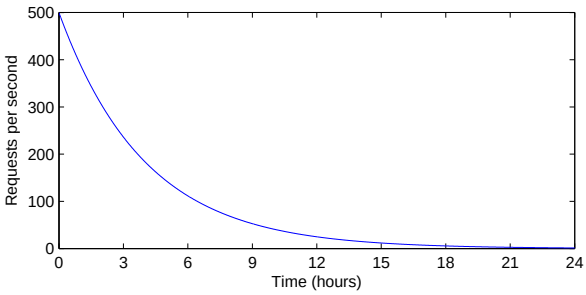


Fig. 4. Sistema con Segmentos de CRL.

Pero en nuestro sistema, un segmento de CRL es compartido por varios nodos. Por lo tanto, nosotros también determinamos la tasa de peticiones de un cierto segmento por parte de un nodo. Además, los segmentos de CRL se actualizan de forma independiente. Para ello nosotros asumimos que todos los nodos servidores son seleccionados con la misma probabilidad, ya que los nodos normalmente se descargan los segmentos de los nodos que tienen más cerca.

La probabilidad de que un nodo no realice la petición del segmento i al nodo j dentro del intervalo $[0, t]$ es:

$$(N/P)e^{\frac{-vt(N/P)}{f}} \tag{9}$$

Donde N es el número de nodos que realizan una petición, P el número de servidores potenciales del segmento i y $\frac{N}{P}$ es el número medio de nodos que se descargan el segmento i del mismo servidor. La probabilidad de que uno de esos nodos pida dicho segmento de CRL al nodo j dentro del intervalo $[t, t+dt]$ es:

$$\frac{ve^{-vdt}\ dt}{f} = \frac{v\ dt}{f} \tag{10}$$

Combinando las ecuaciones (9) y (10) se puede determinar el número total de peticiones del segmento i realizadas al nodo j en el intervalo $[t, t+dt]$:

$$N'_f(t) = \frac{(N/P)ve^{\frac{-vt(N/P)}{f}}\ dt}{f} \tag{11}$$

Y así la tasa total de peticiones es:

$$R'_f(t) = \frac{fN'_f(t)}{dt} = (N/P)ve^{\frac{-vt(N/P)}{f}} \tag{12}$$

Como podemos ver en la Figura 5, el pico de peticiones ha disminuido, ya que $R'_f(0) = (N/P)v$, y la tasa de peticiones continua disminuyendo con el número de segmentos en los que se divide la CRL. Así, nuestro sistema mejora la distribución de las CRLs en comparación con los sistemas estándar y de segmentación de CRLs.

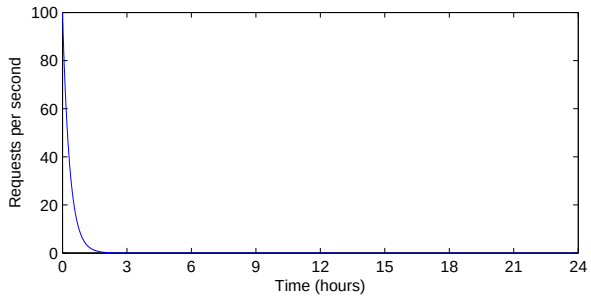


Fig. 5. Sistema con Segmentos de CRL Distribuidos.

En cuanto al rendimiento de los nodos cliente, nuestro sistema introduce una sobrecarga computacional debido al cálculo necesario para conocer que segmento de CRL se necesita, pero a la vez reduce el espacio necesario para almacenar la información de revocación. Los nodos han de calcular una función de hash modular cada vez que necesitan validar un certificado, aunque el tiempo necesario hoy en día para realizar este tipo de operaciones es imperceptible para el usuario. Además, los nodos sólo almacenan ciertos segmentos de CRL y en ningún caso la CRL entera.

En cuanto al rendimiento de las CAs, el número de funciones de hash que deben calcular es mucho mayor, en concreto una por cada certificado revocado. La diferencia con los nodos cliente es que las CAs pueden tener calculados estos valores de antemano, así que la sobrecarga computacional en este sentido se puede considerar irrelevante. Diferente es el caso de la firmas, ya que las CAs deben firmar todos y cada uno de los segmentos de CRL emitidos, o actualizados. De todas formas, el número de segmentos no es comparable al de certificados revocados, y además, cada segmento es emitido, o actualizado, de forma independiente; así y todo, la sobrecarga es mínima para una CA con unos recursos mínimamente aceptables.

VI. Conclusiones

Las redes P2P estructuradas todavía no están maduras, a nivel de seguridad, como para implementar aplicaciones comerciales. Sin embargo, el uso de una Infraestructura de Clave Pública (PKI) parece no ser una sencilla solución para poder cumplir con los requisitos necesarios. Las PKIs tienen problemas para distribuir la información de revocación en este tipo de entornos. Las CAs se pueden convertir en cuellos de botella, ya que el tamaño de las CRLs crece exponencialmente con el número de usuarios que hay en la red. Y dichas listas deben actualizarse con mucha frecuencia para mantener la información fresca.

Por ello nosotros hemos propuesto un nuevo sistema distribuido de revocación para la red KAD, donde las CAs segmentan las CRLs y cada segmento es almacenado en varios nodos para así mejorar la accesibilidad y la disponibilidad de la información. Además, estos segmentos podrán ser emitidos de forma independiente, cosa que mejorará la frescura de la información sin suponer un gran coste para la red.

La distribución y replicación de los segmentos de CRL dentro de una overlay P2P disminuye el pico máximo de peticiones, evitando cuellos de botella en los servidores y mejorando la disponibilidad de la información de revocación. Sin embargo, mientras la segmentación de las CRLs no reduce ese pico de peticiones, ésta sí que reduce el tamaño de los ficheros a almacenar por parte de los nodos. Ahora los nodos sólo necesitan descargar el segmento de CRL que debería contener el número de serie del certificado que quieren validar en caso de estar revocado.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por la Comisión Interministerial de Ciencia y Tecnología (CICYT) bajo el proyecto SERVET TEC2011-26452, por el Ministerio de Ciencia y Educación bajo el proyecto CONSOLIDER CSD2007-00004 (ARES), y por la Generalitat de Catalunya bajo la ayuda 2009 SGR-1362 para grupos de investigación consolidados.

Referencias

[1] A. Aikebaier, T. Enokido, and M. Takizawa. Trustworthy Group Making Algorithm in Distributed Systems. *HCIS*, 1(6), 2011.

[2] A. M. Elmisery and D. Botvich. Enhanced Middleware for collaborative Privacy in IPTV Recommender Services. *JoC*, 2(2):33–42, 2011.

[3] T. Teraoka. Organization and exploration of heterogeneous personal data collected in daily life. *HCIS*, 2(1), 2012.

[4] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard), May 2008.

[5] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560 (Proposed Standard), June 1999.

[6] Gnutella Home Page. http://rfc-gnutella.sourceforge.net.

[7] G. Ying and Z. Jiang. Research on CRL distribution in P2P systems. In *2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, 2009.

[8] I. Stoica, R. Morris, D. Karger, M.F. Kaaskoek, and H. Balakrishman. Chord: A scalable peer-to-peer lookup service for Internet applications. In *ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communication (SIGCOMM)*, 2001.

[9] J. Huang, Z. Wang, Z. Qiu, and M. Chen. Theoretical Analysis of Issuing Mechanism in Distributive Digital Certificate Revocation List. In *International Conference on Computer and Electrical Engineering (ICCEE)*, 2008.

[10] M.C. Morogan and S. Muftic. Certificate Revocation System Based on Peer-to-Peer CRL Distribution. In *International Workshop on Cryptology and Network Security (CANS)*, 2003.
[11] Agapios Avramidis, Panayiotis Kotzanikolaou, Christos Douligeris, and Mike Burmester. Chord-PKI: A distributed trust infrastructure based on P2P networks. *Computer Networks*, 56(1):378–398, 2012.
[12] T. Beth, M. Borcherding, and B. Klein. Valuation of Trust in Open Networks. In *Proceedings of the Third European Symposium on Research in Computer Security*, pages 3–18, 1994.
[13] R. Chen and W. Yeager. Poblano: A Distributed Trust Model for Peer-to-Peer Networks. Jxta security project white paper, Microsystems, Sun, 2002.
[14] Sun Microsystems. JXTA. https://jxta.kenai.com.
[15] G. Abhilash and Jong P. Yoon. Modeling Group Trust For Peer-to-Peer Access Control. In *International Workshop on Database and Expert Systems Applications*, pages 971–978, 2004.
[16] P. Maymounkov and D. Mazières. Kademlia: A Peer-to-peer Information System Based on the XOR Metric. In *1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002.
[17] eMule Home Page. http://www.emule-project.net.
[18] aMule Home Page. http://www.amule.org.
[19] B. Cohen. Brian's BitTorrent FAQ and guide. http://www.bthq.net.

Mejora del Protocolo RADIUS para Soportar la Fragmentación de Datos de Autorización

Alejandro Pérez[1], Fernando Pereñíguez[1], Rafael Marín[1], Gabriel López[1], Diego R. López[2]

[1]Departamento de la Ingeniería de la Información y las Comunicaciones.
Universidad de Murcia. Facultad de Informática. Campus Universitario de Espinardo. 30100. Murcia.
{alex, pereniguez, rafa, gabilm}@um.es

[2]Telefónica I+D.
Don Ramon de la Cruz, 84. 28006. Madrid.
diego@tid.es

***Resumen*—RADIUS (*Remote Access Dial-In User Server*) es uno de los protocolos AAA (*Authentication, Authorization, Accounting*) más conocidos y utilizados en la actualidad, con un gran éxito entre los operadores de telecomunicaciones. Sin embargo, RADIUS presenta ciertas limitaciones para su aplicación en las nuevas iniciativas sobre control de acceso a servicios, como la propuesta ABFAB definida en el *Internet Engineering Task Force* (IETF), o el intercambio de políticas de filtrado de tráfico sobre el propio RADIUS. Esto se debe principalmente a su estricto límite en cuanto al tamaño máximo de atributo RADIUS (255 bytes) y de paquete RADIUS (4096 bytes). Mientras que dentro del IETF se han desarrollado diversas soluciones para extender el tamaño máximo de atributo mediante técnicas de fragmentación *intra-paquete*, no existe ninguna propuesta que permita el intercambio de información que sobrepase el tamaño máximo de paquete sin obligar a modificaciones en los equipos de red (p.ej. *firewalls* y *routers*). Este artículo define una propuesta de fragmentación inter-paquete que permite a las entidades RADIUS intercambiar información de cualquier tamaño sin requerir ningún canal de comunicación adicional ni la modificación de los equipos intermedios o *proxies*.**

***Palabras Clave*—RADIUS, fragmentación, autorización, ABFAB**

I. INTRODUCCIÓN

RADIUS (*Remote Access Dial-In User Server*) [1] es uno de los protocolos más conocidos para asistir los procesos de Autenticación, Autorización y Accounting (*AAA*) que son necesarios para controlar el acceso a los servicios de red. RADIUS permite el intercambio de información entre un *servidor de acceso a la red* (NAS - *Network Access Server*) y un *servidor de autenticación* (AS - *Authentication Server*). Mediante RADIUS, el NAS realiza consultas al AS solicitando, por ejemplo, la verificación de las credenciales de un usuario o la comprobación de sus privilegios de acceso. De forma similar, el AS emplea RADIUS para comunicar al NAS los resultados de sus solicitudes, así como para proporcionar cualquier tipo información que sea necesaria para un correcto acceso al servicio del usuario.

Desde su publicación en el año 1997, el protocolo RADIUS ha cosechado un enorme éxito entre los operadores de telecomunicaciones, pasando a ser una de las tecnologías de uso más extendido para el control de importantes servicios de seguridad relacionados con el control de acceso a la red y la facturación asociada al consumo de recursos. Durante estos años, RADIUS ha continuado siendo objeto de estudio con el fin de adaptarlo a nuevas necesidades que no fueron consideradas originalmente durante su diseño. De hecho, en el seno del *Internet Engineering Task Force* (IEFT), existe un grupo de trabajo denominado *RADEXT* (*RADius EXTensions*) [2] encargado de continuar con la evolución y desarrollo del protocolo.

Una limitación conocida de RADIUS se basa en el tamaño de atributos y paquetes impuesto por el protocolo. Cada paquete RADIUS está compuesto por una cabecera que, opcionalmente, va acompañada por un conjunto de atributos. De acuerdo con la especificación del protocolo [1], el tamaño máximo de un paquete RADIUS no puede exceder los 4096 bytes (incluyendo la cabecera), mientras que cada atributo podrá transportar como máximo 255 bytes de información, de los que únicamente 253 corresponden a la carga útil. Inicialmente, surgió el problema de enviar información de autenticación que no se podía transportar en un único atributo, es decir, cuyo tamaño era mayor a 253 bytes. Una de las primeras soluciones a este problema fue propuesta por el mecanismo de autenticación RADIUS-EAP [3], que planteó la posibilidad de emplear varios atributos del mismo tipo insertados en orden dentro del paquete RADIUS para representar un atributo de mayor tamaño. En el destino, el contenido de estos atributos se extrae y une para reconstruir los datos de autenticación originales. Esta técnica de *fragmentación intra-paquete* ha demostrado ser útil, ya que recientemente RADEXT ha publicado una especificación de fragmentación intra-paquete [4] genérica basada en la misma.

Sin embargo, en la actualidad están surgiendo nuevas aplicaciones de uso de RADIUS [5] donde se requiere el envío de grandes cantidades de información (p.ej. de autorización) que no sólo exceden el tamaño máximo de un atributo, sino también el de un paquete. Un ejemplo de este tipo de aplicación es ABFAB (*Application Bridging for Federated Access Beyond web*) [5], que es una propuesta de control de acceso federado a servicios más allá del web que está en proceso de estandarización dentro del IETF. Otro ejemplo es el intercambio de grandes políticas de filtrado de paquetes entre el AS y el NAS tal y como se describe en [6]. El primer caso define el intercambio de sentencias SAML entre

las entidades RADIUS que, en general, van a sobrepasar las limitaciones de tamaño impuestas por RADIUS. El segundo caso define un formato para la codificación y transmisión de reglas de filtrado de paquetes entre entidades RADIUS, cuyo tamaño total puede exceder los límites establecidos en el estándar. En estos casos, además de una técnica de fragmentación intra-paquete, es necesaria una solución que permita al NAS y el AS intercambiar estos grandes volúmenes de datos empleando para ello una serie de paquetes RADIUS (*fragmentación inter-paquete*).

Esta necesidad se acentúa aún más cuando se tiene en cuenta la recomendación [7] de mantener el tamaño de los paquetes RADIUS por debajo del PMTU (*Path Maximum Transmission Unit*) existente entre el NAS y el AS. Esta recomendación se apoya en que, en la práctica, parte del equipamiento de red desplegado (p.ej. routers, puntos de acceso) no soporta el transporte de paquetes UDP fragmentados, lo que provocaría la pérdida de datos y retrasos en las comunicaciones. Por tanto, el tamaño máximo posible de un paquete RADIUS ya no será de 4096 bytes, sino que se verá reducido al PMTU disponible en la red.

Aunque existen otros protocolos AAA como Diameter que solventan este problema, la realidad es que los operadores de red son reacios a realizar cambios sobre los sistemas existentes que, mayoritariamente, están basados en RADIUS. Por este motivo, este artículo propone una mecanismo de fragmentación flexible en RADIUS que permite a entidades intercambiar grandes cantidades de datos de autorización que exceden el límite de tamaño del paquete. Concretamente, la solución que se propone fragmenta el contenido a través de varios intercambios de mensajes tradicionales RADIUS entre NAS y AS. Además, no impone ninguna restricción a los administradores ni les obliga a realizar configuraciones adicionales (p.ej. modificar reglas en firewalls, configurar routers, etc.). La solución es también compatible con las actuales soluciones de fragmentación intra-paquete anteriormente mencionadas [3], [4]. Finalmente, el coste de despliegue de la solución es mínimo, ya que sólo debe ser implementada por aquellos sistemas que requieran intercambiar grandes cantidades de información, operando de forma transparente para aquellos servidores RADIUS que actúen como nodos intermedios o proxies.

El resto de este artículo se estructura de la siguiente manera. La sección II presenta la operación del protocolo RADIUS, mientras que la sección III analiza los trabajos relacionados. A continuación, la sección IV describe el mecanismo de fragmentación propuesto y la sección V discute algunas particularidades de su funcionamiento. La sección VI describe la aplicabilidad de la solución sobre dos casos de uso reales. Finalmente, la sección VII remarca las conclusiones más notorias de este trabajo y esboza vías de trabajo futuro.

II. OPERACIÓN GENERAL DE RADIUS

RADIUS es un protocolo de aplicación basado en un modelo de interacción cliente/servidor que emplea UDP (*User Datagram Protocol*) como protocolo de transporte. Normalmente, el *cliente RADIUS* se despliega en un NAS, que recibe peticiones de acceso a servicios por parte de usuarios. Con la asistencia de un *servidor RADIUS*, implementado por un AS, el NAS ejerce un control de acceso que, por lo general, implica una autenticación del usuario (para verificar su identidad), una autorización (para determinar bajo qué condiciones se le debe conceder acceso) y un proceso de *accounting* (para registrar el consumo de recursos efectuado). En algunos escenarios (p.ej. eduroam), la comunicación entre NAS y AS no será directa, sino que se realizará a través de un conjunto de servidores RADIUS (denominados *proxy*). Esta situación será habitual cuando, por ejemplo, un usuario solicita acceso a un servicio perteneciente a un dominio distinto de donde el usuario está registrado.

Una conversación RADIUS (Fig. 1) se inicia cuando el NAS envía un paquete *Access-Request* solicitando al AS la autenticación y/o autorización de un usuario. En el caso más típico, el AS responderá con un paquete *Access-Challenge* solicitando más información acerca del usuario. Este proceso de intercambios *Access-Request*/*Access-Challenge* se repite hasta que el AS dispone de suficiente información para tomar una decisión de acceso. La decisión se comunica al NAS mediante un paquete *Access-Accept* o *Access-Reject* según la solicitud de acceso sea concedida o denegada, respectivamente. El paquete *Access-Accept* podría, opcionalmente, contener directivas de autorización que condicionen el acceso al servicio.

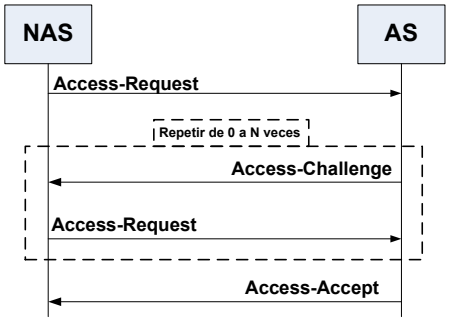


Fig. 1. Conversación típica RADIUS

El protocolo define también paquetes que permiten el intercambio de información de *accounting* (*Accounting-Request*/*Accounting-Response*), así como del estado de las entidades (*Status-Client*/*Status-Server*). El formato de todos los paquetes es común, tal y como se describe en la Fig. 2. Un paquete RADIUS está formado por una *cabecera* y un *cuerpo*. La cabecera contiene un *Code* que identifica el tipo de paquete RADIUS, un *Identifier* que relaciona paquetes de petición y respuesta, la longitud (*Length*) del paquete y un *Authenticator* que proporciona integridad al mismo. El cuerpo contiene la información (p.ej. de autenticación) transportada en forma de *atributos*.

Un atributo RADIUS es una pieza de información auto-contenida de un determinado tipo y longitud. Algunos ejemplos de atributos son *User-Name* y *Service-Type*, que contienen la identidad del usuario y el tipo de servicio solicitado por éste, respectivamente. También *State*, que se emplea por el AS para ligar todos los paquetes pertenecientes a una misma conversación. El grupo RADEXT del IETF ha publicado recientemente un nuevo formato de *atributos extendidos* [4], que tiene como objetivo ampliar el número de posibles atributos RADIUS. Además, su estructura se ha sido enriquecida para permitir la fragmentación intra-paquete de

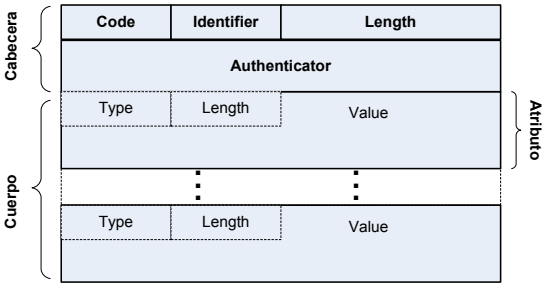


Fig. 2. Formato Paquete RADIUS

atributos. En este caso, cuando la información a transportar excede el tamaño máximo de atributo (253 bytes), se emplea una secuencia de atributos extendidos donde todos (a excepción del último) contienen un flag "M" activado. Este flag indica que hay más fragmentos pertenecientes a dicho atributo en el paquete.

III. TRABAJO RELACIONADO

El único trabajo previo que discute el problema de transmisión de grandes cantidades de datos sobre RADIUS lo encontramos en [7], donde se proponen tres esquemas para resolverlo. Sin embargo, ninguno de ellos soluciona por completo el problema planteado en este artículo.

El primer esquema propone el uso de una secuencia de paquetes *Access-Request/Access-Challenge* para el envío de información desde el AS al NAS, de forma similar a como se opera en RADIUS-EAP [3]. Sin embargo, este esquema no permite la transmisión de grandes datos de autorización en la dirección opuesta, es decir, desde el NAS al AS. Además, existe una gran cantidad de atributos ya definidos y ampliamente usados que no pueden transportarse en paquetes de tipo *Acces-Challenge*, limitando su aplicación.

El segundo esquema propone el envío de nombres en lugar de valores. Los nombres referencian a una serie de valores pre-establecidos entre AS y NAS para la información en cuestión. Sin embargo, esta alternativa no resulta adecuada cuando la naturaleza de los datos a enviar es dinámica (p.ej. sentencias SAML o reglas de filtrado de tráfico), ya que las entidades no pueden conocer todos los posibles valores pre-configurados. Una forma de solventar este problema sería usar URLs para indicar la localización real de los datos, que se obtendrían por otra vía diferente a RADIUS (p.ej. HTTPS). Sin embargo, este esquema requiere, además de mensajes de intercambio adicionales que aumenta la sobrecarga de la red, proporcionar un método seguro de acceso a los datos que sea accesible para sistemas remotos (p.ej. servidor web securizado con TLS). La configuración de este método de acceso precisa la modificación de reglas en *firewalls* y cambios en las políticas de acceso, haciendo su despliegue muy complicado. Además, sobre un escenario donde intervengan varias organizaciones conectadas a través de RADIUS (i.e. eduroam) esto va a implicar el establecimiento de mecanismos de confianza adicionales, por ejemplo, el uso de una PKI común.

El tercer esquema descrito en [7] no propone una alternativa como tal, sino que recomienda el uso de técnicas de descubrimiento del PMTU [8] entre el AS y el NAS, de forma que se evite generar paquetes RADIUS que superen dicho valor y que puedan provocar errores en las comunicaciones.

Una solución simple para permitir el envío de grandes cantidades de datos de autorización consistiría en ampliar el tamaño máximo de paquete impuesto por RADIUS. Dado que el campo *Length* de la cabecera RADIUS tiene en realidad 16 bits de tamaño, un simple cambio en las implementaciones RADIUS podría obviar el límite de 4096 bytes y permitir paquetes de hasta 64 Kilobytes. Además, con el fin de no generar paquetes UDP de tamaño mayor al PMTU disponible, se podría usar RADIUS sobre TCP [9]. Sin embargo, estos cambios requerirían la actualización de todas las entidades que forman la infraestructura RADIUS, limitando el número de implementaciones y dispositivos *hardware* que podrían usarse en la infraestructura RADIUS.

La solución propuesta en este artículo proporciona un mecanismo de fragmentación que evita la modificación de la infraestructura RADIUS existente. Sólo el NAS y el AS que van a participar en el intercambio de datos fragmentados necesitan tener soporte para el mismo. El resto de proxies que conforman la infraestructura pueden permanecer inalterados. Por ello, este mecanismo sólo requiere una actualización en las implementaciones tanto del NAS como de AS.

IV. PROPUESTA DE MECANISMO DE FRAGMENTACIÓN PARA RADIUS

El mecanismo de fragmentación inter-paquete que se presenta a continuación ha sido concebido para permitir el envío de grandes volúmenes de datos (mayores a 4096 bytes) entre un cliente y un servidor RADIUS. Aunque el mecanismo es de propósito general y válido para cualquier tipo de datos, su aplicación práctica se reduce a la fragmentación de datos de autorización. Tal y como se explicó en la sección II, RADIUS es capaz de transportar también datos de autenticación y accounting. Sin embargo, a día de hoy, el tamaño máximo de paquete impuesto por RADIUS no hay sido un problema para el transporte de este tipo de información. Por un lado, los mecanismos de autenticación existentes han sido concebidos para operar sin exceder el tamaño máximo de 4096 bytes, y utilizan sus propios mecanismos para asegurar que así sea. Por otro lado, el proceso de accounting está basado en pequeñas transmisiones de información. Para aquellas situaciones más complejas donde es necesario gestionar el accounting asociado a varios flujos de información, ya existe un mecanismo descrito en [10].

El intercambio de datos de autorización puede tener lugar antes o después de que el usuario sea autenticado por el AS. Por este motivo, distinguimos tres fases:

- *Pre-Autorización*. En esta fase, el NAS puede enviar cierta información de autorización al AS antes de que el usuario sea autenticado. Por ejemplo, en la propuesta ABFAB [5] el NAS es capaz de solicitar atributos de usuario específicos (p.ej. rol) al AS.
- *Autenticación*. El usuario es autenticado empleando un mecanismo concreto (p.ej. RADIUS-EAP). En este fase, no es necesario aplicar una técnica de fragmentación inter-paquete.
- *Post-Autorización*. El AS envía información de autorización al NAS para configurar el tipo de acceso que debe ser proporcionado al usuario. Por ejemplo, el

AS puede enviar atributos adicionales de usuario al NAS para que éste tome una decisión final sobre el acceso al servicio. En algunos casos, esta fase puede derivar en una conversación donde NAS y AS intercambian datos de autorización.

A continuación presentamos el modo de operación general del mecanismo de fragmentación, para después detallar su funcionamiento específico.

A. Descripción General

Asumimos que una entidad RADIUS (NAS o AS) necesita enviar una gran cantidad de información de autorización. Inicialmente, mediante alguna técnica de fragmentación intra-paquete como la descrita en [4], la información será fragmentada para que pueda ser transportada empleando varios atributos RADIUS cuyo tamaño no exceda de 255 bytes. No obstante, el paquete RADIUS resultante supera el tamaño máximo permitido (4096 bytes). Para resolver este problema, nuestro mecanismo de fragmentación propone el envío de información usando una serie de paquetes RADIUS más pequeños llamados *chunk*. Un chunk es un paquete RADIUS normal que transporta parte de la información del paquete original más grande. Un chunk debe ser un paquete válido sujeto a las normas de formato y requisitos de seguridad impuestos por la especificación RADIUS. De este modo, los servidores RADIUS *proxy* que existan entre NAS y AS pueden procesar los chunks de forma transparente aunque no implementen este mecanismo de fragmentación.

El proceso de construcción de un chunk es el siguiente. El chunk será del mismo tipo que el paquete original y contendrá un subconjunto de los atributos del mismo. El subconjunto de atributos incluidos en el chunk deberán preservar el mismo orden con el que aparecen en el paquete original, con el fin de respetar las restricciones impuestas por la especificación RADIUS. El número de atributos incluidos en el chunk (discutido en la sección V-A) dependerá de diversos factores: tamaño máximo de paquete, tamaño de cada atributo, número de proxies existentes entre en NAS y AS, sobrecarga impuesta por la señalización asociada a la fragmentación, etc.

Una vez generados los chunks, la información fragmentada se envía por medio de una serie de intercambios del tipo *Access-Request/Access-Accept*. Este intercambio se realiza de forma controlada gracias al uso de un nuevo atributo denominado *Frag-Status*. Por ejemplo, asumiendo que el mecanismo de fragmentación es iniciado por el NAS, los chunks serán paquetes del tipo *Access-Request* identificados por medio del atributo *Frag-Status* que contiene el valor *More-Data-Pending*. Gracias a este atributo, el AS reconoce que se trata de un intercambio de información fragmentada. En este caso, el AS responde al NAS con un mensaje *Access-Accept* que también contiene un atributo *Frag-Status*, con el valor *More-Data-Request*, para asentir la recepción del primer chunk y solicitar el envío de más información.

Todos los paquetes RADIUS que pertenezcan a la misma sesión de fragmentación se enlazan usando los mecanismos estándar de RADIUS: el NAS emplea el campo *Identifier* del paquete RADIUS para ligar un *Access-Request* con su correspondiente *Access-Accept*, mientras que el AS hace uso del atributo *State* para asociar un *Access-Accept* con el siguiente *Access-Request*. Una vez que el AS recibe toda la información fragmentada, se reconstruye el paquete original y se procesa como si se hubiese recibido un único paquete *Access-Request*. En caso de que el AS sea la entidad que envía información fragmentada, el proceso es análogo.

Durante la generación y envío de chunks puede ocurrir una situación especial cuando el mecanismo de fragmentación se combina con el uso de atributos extendidos fragmentados [4], el cual exige que un atributo extendido fragmentado (marcado con el flag “M”) se transporte íntegramente dentro de un mismo paquete RADIUS. Sin embargo, el proceso de generación de chunks aquí propuesto podría ocasionar que un mismo atributo sea transportado por medio de 2 o más chunks. Para solventar esta situación, se define un nuevo flag “T”, que combinado con el flag “M”, indica que se trata de un atributo extendido fragmentado pero donde todos los fragmentos no están contenidos en un mismo chunk.

B. Fragmentando Datos de Autorización

Vamos a describir con ejemplos el funcionamiento del mecanismo tanto cuando es empleado por el NAS (fase de pre-autorización) como cuando es usado por el AS (fase de post-autorización). Por simplicidad, en lugar de manejar tamaños en bytes, asumiremos que un paquete RADIUS sólo puede incluir 8 atributos. La notación empleada será:

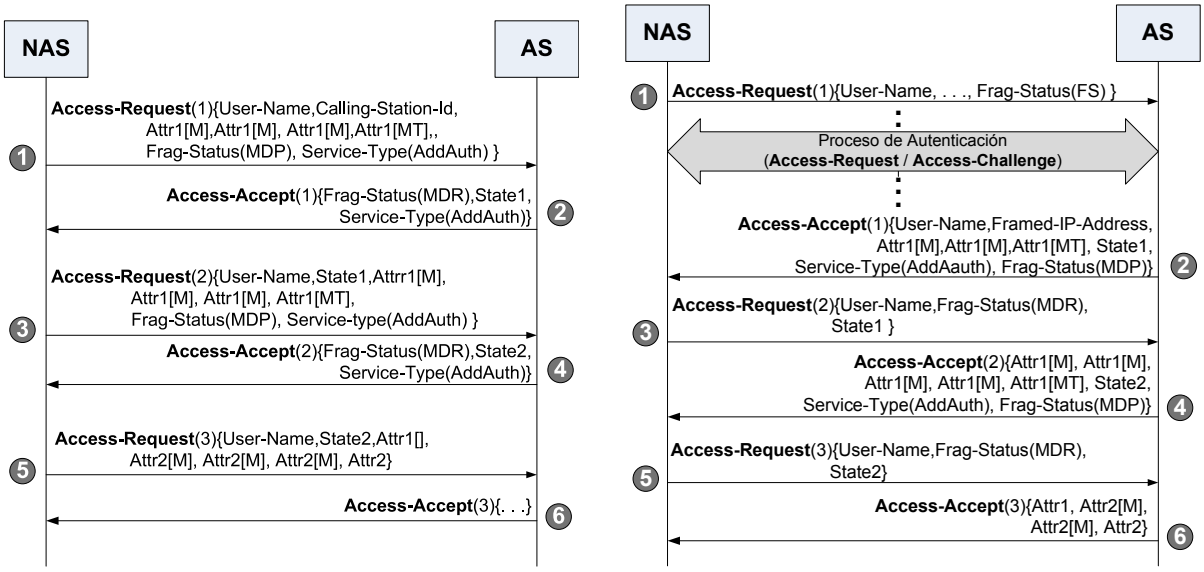
```
Paquete(ID){Atributo1, Atributo2, ...}
```

donde `"Paquete"` referencia al tipo de paquete RADIUS, `"ID"` es el valor del campo *Identifier* de la cabecera del paquete RADIUS y entre llaves se indica el conjunto de atributos que conforman el cuerpo del paquete. Los atributos se expresan según la notación `Atributo[Flags]`, donde `"Atributo"` referencia al nombre del tipo de atributo y `"Flags"` representa los flags activos en el mismo.

1) Pre-Autorización (Datos enviados por el NAS): La Fig. 3(a) muestra el funcionamiento del mecanismo de fragmentación cuando el NAS desea enviar el siguiente paquete *Access-Request* que excede el tamaño máximo permitido (4096 bytes):

```
Access-Request(){User-Name, Calling-Station-Id,
Attr1[M], Attr1[M], Attr1[M], Attr1[M], Attr1[M],
Attr1[M], Attr1[M], Attr1[M], Attr1, Attr2[M],
Attr2[M], Attr2[M], Attr2}
```

Como podemos observar, el paquete contiene dos atributos extendidos `"Attr1"` y `"Attr2"` compuestos por 9 y 3 fragmentos, respectivamente. El proceso de fragmentación se inicia cuando el NAS construye el primer chunk que envía al AS *(1)*. Este primer chunk contiene 2 atributos de señalización insertados por el proceso de fragmentación. Por un lado, se inserta el atributo *Frag-Status* con el valor *More-Data-Pending* (MDP) para indicar que el NAS tiene más datos fragmentados que enviar en un posterior *Access-Request*. Por otro lado, el atributo *Service-Type* con el valor *Additional-Authorization* (AddAuth), que indica que este paquete es parte de un proceso de fragmentación. De este modo, este primer chunk incluye 6 atributos del paquete original hasta completar el máximo permitido (8 atributos). Es importante notar que en el último atributo ”Attr1” con el flag ”M” activado, el proceso de fragmentación también



(a) Datos enviados por el NAS

(b) Datos enviados por el AS

Fig. 3. Fragmentación de Datos

activa el flag ”T” para indicar que el resto de fragmentos de este atributo extendido se enviarán en chunk posteriores.

Cuando el AS recibe el primer chunk, cualquier proceso de autenticación o autorización se suspende hasta que se reciba el resto de los datos fragmentados. Estos datos pendientes se solicitan al NAS mediante un paquete *Access-Accept (2)* que contiene 3 atributos: *Frag-Status* con valor *More-Data-Request* (MDR), *State* que permita ligar esta respuesta con el siguiente mensaje del NAS y un *Service-Type* con el servicio solicitado por el NAS. Si un NAS recibe una respuesta distinta a ésta, entenderá que el AS no soporta fragmentación y abortará el proceso.

Cuando el NAS recibe esta respuesta, emplea el valor del campo *Identifier* para asociarlo con la operación de fragmentación en curso. El proceso continúa con la generación de un segundo chunk *(3)* con datos fragmentados. Además de los atributos *Frag-Status* y *Service-Type* indicando que existen más datos pendientes de enviar, este chunk incluye dos atributos de señalización adicionales: el *State* recibido del AS en el *Access-Accept*, y el *User-Name* del paquete original. Aunque este último ya ha sido incluido en el primer chunk, debe ser incluido en todos los chunks ya que es un atributo necesario para que los servidores proxy encaminen correctamente el paquete RADIUS hacia el servidor final. Tras insertar estos atributos de señalización, el chunk puede albergar 4 atributos del paquete original hasta completar el tamaño máximo de 8 atributos.

Cuando el AS recibe este chunk, busca un estado asociado al atributo *State* recibido. Si existe, este paquete pertenece al proceso de fragmentación y los datos fragmentados recibidos en este paquete se asocian a los recibidos en el chunk anterior. Puesto que el atributo *Frag-Status* indica que existen todavía datos pendientes por enviar, el AS envía un paquete *Access-Accept (4)* solicitando la recepción de más datos (*Frag-Status* con valor MDR) y un nuevo atributo *State* asociado a esta conversación.

Cuando el NAS recibe la respuesta del AS se genera el último chunk *(5)*, insertando los atributos restantes del paquete original. Este chunk sólo incluye los atributos de señalización estándar de RADIUS (*User-Name* y *State*). Cuando el AS recibe el paquete, la ausencia de un atributo *Frag-Status* indica que este último chunk concluye el proceso de fragmentación. A continuación, el AS reconstruye el paquete original y lo procesa como si fuera un único paquete RADIUS de gran tamaño. El AS generará la respuesta adecuada a dicho paquete *(6)* conforme al comportamiento estándar de RADIUS.

2) Post-Autorización (Datos Enviados por el AS): El proceso de fragmentación dirigido por el AS guarda ciertas similitudes con el empleado por el NAS. Por un lado, el campo *Identifier* y el atributo *State* siguen siendo necesarios para que NAS y AS puedan asociar los paquetes RADIUS pertenecientes a un intercambio de fragmentación concreto. El atributo *Frag-Status* también se emplea para coordinar el intercambio de datos fragmentados entre NAS y AS. Finalmente, el atributo *Service-Type* desempeña un papel fundamental en cada chunk con el objetivo de informar al NAS que el acceso al servicio concreto no es concedido hasta que no finalice el intercambio de fragmentación.

En este sentido, cuando el paquete RADIUS original ya contiene un atributo *State* o *Service-Type*, deben de tratarse de una manera especial, como se describe en la sección V-B.

La Fig. 3(b) muestra el proceso de fragmentación cuando el AS desea enviar el siguiente paquete *Access-Accept* que excede el tamaño máximo permitido:

```
Access-Accept(){User-Name, Framed-IP-Address,
Attr1[M], Attr1[M], Attr1[M], Attr1[M], Attr1[M],
Attr1[M], Attr1[M], Attr1[M], Attr1, Attr2[M],
Attr2[M], Attr2 }
```

Antes de iniciar el envío de chunks, el AS debe haber recibido una notificación del NAS informando que soporta el mecanismo de fragmentación. Esto se realiza mediante la inclusión del atributo *Frag-Status* con el

valor *Fragmentation-Supported* (FS) en el primer paquete *Access-Request (1)* enviado por el NAS. Tras esto, y una vez que el usuario ha sido autenticado, el AS envía el primer chunk *(2)*. Como podemos observar, este chunk contiene tres atributos de señalización propios de fragmentación: *Service-Type* con valor *Additional-Authorization* (AddAuth) para indiciar al NAS que este paquete no concluye la conversación RADIUS; *Frag-Status* con valor *More-Data-Pending* (MDP) indicando que el AS debe enviar todavía más chunk; y *State* necesario para ligar este chunk con el siguiente *Access-Request* enviado por el NAS. Por este motivo, el chunk se completa solo con 5 atributos del paquete original hasta completar el tamaño máximo (8 atributos). Hay que destacar que el último atributo de tipo "Attr1" contiene el flag T activado para indicar que todos los fragmentos de este atributo no se encuentran en este chunk.

Cuando el NAS recibe este *Access-Accept*, la presencia del atributo *Frag-Status* le indica que el AS ha iniciado un intercambio de fragmentación. Por este motivo, almacena los atributos y construye un paquete *Access-Request* de respuesta *(3)* que contiene el atributo *User-Name* (con la identidad del usuario necesario para que el paquete sea enrutado correctamente a través de la infraestructura de servidores RADIUS), *Frag-Status* (con el valor MDR) y el atributo *State* recibido del AS en el chunk.

La recepción de este *Access-Request* informa al AS que el NAS ha recibido y procesado correctamente el primer chunk, por lo que continua con la generación de un segundo chunk. Este chunk *(4)* contiene los atributos de señalización anteriormente descritos (*Service-Type* = AddAuth, *Frag-Status* = MDP y nuevo atributo *State*) y 5 atributos del paquete original. Cuando el NAS recibe este chunk determina que todavía queda más información por recibir, por lo que envía un *Access-Request (5)* solicitando el envío de más información.

Finalmente, el proceso concluye cuando el AS genera el último chunk *(6)* con todos los atributos restantes del paquete original. Puesto que este *Access-Accept* concluye la conversación RADIUS, no es necesario la inclusión de un atributo tipo *State*.

Cuando el NAS recibe el chunk final, reconstruye el paquete original y lo procesa de acuerdo con la operación estándar de RADIUS como si se hubiera recibido completo.

V. DISCUSIÓN

En esta sección se discuten algunas particularidades acerca del funcionamiento de la solución propuesta que requieren una explicación más detallada.

A. Tamaño Útil de Chunk

En un escenario ideal, los chunks contendrían exactamente 4096 bytes, 20 bytes correspondientes a la cabecera y el resto (4076 bytes) utilizados para transportar atributos del paquete original. Sin embargo, el tamaño disponible para carga útil se ve disminuido por diferentes razones. En primer lugar, los chunks deben ajustarse al tamaño PMTU disponible en la red, con el fin de evitar los problemas que pueden surgir derivados de la fragmentación de datagramas UDP [7]. Por tanto, el tamaño máximo teórico del chunk se ve reducido de 4096 al tamaño real del MTU de la red. Además, un chunk sólo puede contener atributos completos del paquete original, nunca partes de los mismos. Por tanto, en cada chunk podrá quedar un espacio sin utilizar que no pueda ser ocupado por ningún atributo del paquete original. En tercer lugar, el mecanismo de fragmentación introduce una serie de atributos de señalización en cada chunk (p.ej. *Frag-Status*, *State* o *Service-Type*) que reducen la cantidad de espacio disponible para los atributos del paquete original. Además, los atributos *Proxy-State* introducidos por los proxies también consumen un espacio en el chunk.

B. Manejo de Atributos Especiales

Cuando se utiliza el mecanismo de fragmentación propuesto, algunos atributos RADIUS requieren un tratamiento especial tanto durante el envío como la recepción de chunks.

1) Envío de chunks: Tanto el atributo *State* como el atributo *Service-Type* se utilizan como señalización durante el proceso de envío de chunks. Sin embargo, estos atributos también podrían estar presentes en el paquete original, con un uso completamente diferente a la fragmentación. Dado que RADIUS prohíbe expresamente la presencia de más de un atributo *State* o *Service-Type* en el mismo paquete [1], los atributos originales deberán enviarse en un chunk que no contenga estos atributos usados como señalización, es decir, en el último chunk cuando el emisor es el AS, o en el primer chunk cuando el emisor es el NAS. Esta re-ordenación de atributos está permitida por el estándar RADIUS.

2) Recepción de chunks: Cuando se está recibiendo un paquete fragmentado, el receptor almacena los atributos contenidos en cada chunk para, posteriormente, reconstruir el paquete original y procesarlo. Sin embargo, los atributos de señalización no se deben almacenar dado que no forman parte del paquete original. En concreto, un NAS deberá considerar como atributos de señalización a todos los *State* (excepto si se recibe en el último chunk), *Service-Type* = *AddAuth* y *Frag-Status*. Por su parte, un AS deberá considerar como señalización a todos los *State* (excepto si se recibe en el primer chunk), *Frag-Status*, *Proxy-State* y *User-Name* (excepto si se recibe en el primer chunk).

C. Operación con Proxies

El mecanismo de fragmentación definido en este artículo se ha diseñado para que funcione de forma transparente a través de aquellos proxies que no lo soporten (*legacy proxies*), siempre y cuando éstos no requieran la modificación de ningún atributo fragmentado. Conforme a la operación estándar de RADIUS, estos proxies pueden introducir atributos *Proxy-State* en los mensajes que van del NAS al AS. Por este motivo, el AS incluirá en sus respuestas estos atributos *Proxy-State* de forma que, para un *legacy proxy*, la conversación RADIUS es completamente válida.

En el caso de que los proxies soporten este mecanismo (*updated proxies*), podrán además modificar cualquier información transmitida, incluso aunque esté fragmentada. En este caso el updated proxy interacciona con el emisor del paquete con el fin de obtener todos los chunks que componen el paquete original, lo reconstruye localmente, y lo modifica según sus necesidades, para enviarlo finalmente hacia su destinatario original. Tanto el emisor como el receptor original

no serán conscientes de este proceso, tal y como ocurre en el estándar RADIUS con paquetes no fragmentados.

D. Consideraciones de Seguridad

La seguridad en RADIUS ha sido ampliamente analizada en [11], [7]. El mecanismo de fragmentación descrito en este artículo no cambia ningún aspecto relacionado con la seguridad del protocolo RADIUS en sí. Sin embargo, para evitar el falsificado y reenvío de paquetes, se requiere que todos los chunks de tipo *Access-Request* vayan protegidos con integridad mediante el uso del atributo *Message-Authenticator* [3].

Por otro lado, el envío de datos fragmentados desde una entidad a otra puede ser problemático. Dado que tanto el NAS como el AS tienen que almacenar grandes cantidades de información por cada sesión, es posible que se puedan producir ataques de denegación de servicio. Por tanto se sugiere que las implementaciones permitan limitar la cantidad máxima de datos de autorización que se pueden recibir para cada sesión. Unos límites razonables para cada paquete a fragmentar podrían ser unos 64 Kilobytes, repartidos en no más de 20 chunks. De esta forma, tanto NAS como AS pueden configurar el tamaño de sus buffers de antemano.

VI. CASOS DE USO DE APLICABILIDAD

A continuación se describe dos casos de uso reales donde la aplicación del mecanismo de fragmentación soluciona algunas limitaciones del uso de RADIUS existentes en la actualidad.

A. ABFAB

El grupo de trabajo ABFAB (*Application Bridging for Federated Access Beyond web*) [5] está desarrollando una arquitectura para proporcionar un mecanismo de control de acceso federado que sea aplicable a cualquier tipo de aplicación. La capa de federación se establece mediante la infraestructura AAA (RADIUS o Diameter), que determina las relaciones de confianza. En concreto, la solución planteada por ABFAB propone un proceso de autenticación basado en el protocolo EAP, donde el transporte de los paquetes entre el usuario (*End User* - EU) y la aplicación (*Relaying Party* - RP) se realiza mediante un nuevo mecanismo GSS-API [12] definido para tal fin, mientras que el transporte de los paquetes EAP entre la aplicación y el servidor de autenticación (AS) se realiza mediante el protocolo AAA correspondiente.

ABFAB define además un mecanismo de autorización mediante el que se proporciona a la aplicación información de identidad acerca del usuario autenticado. En concreto, en el momento de finalizar la autenticación del usuario, el servidor AAA obtiene del proveedor de identidad (*Identity Provider* - IdP) de su organización una sentencia SAML [13] (*SAMLAttributeStatement*) que contiene atributos del usuario (p.ej. edad, nombre o rol). Esta sentencia se envía a la aplicación usando el protocolo AAA. La aplicación usará esta información para realizar un proceso de autorización más refinado que la simple verificación de autenticación. Por ejemplo, la aplicación puede decidir que si un usuario ”estudiante” o ”profesor”, ”mayor de edad” puede acceder a determinados servicios o no. La Fig. 4 muestra un intercambio simplificado de autenticación y autorización.

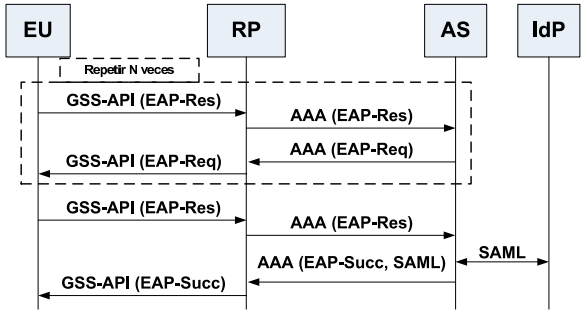


Fig. 4. Autenticación y autorización en ABFAB

Uno de los objetivos que persigue ABFAB es que se reutilicen las infraestructuras AAA existentes, sin requerir la modificación de los nodos intermedios, con el fin de facilitar y acelerar el despliegue de la arquitectura. Dado que hoy en día una gran parte estas infraestructuras están basadas en RADIUS, es necesario que toda la arquitectura pueda llevarse a cabo usando este protocolo AAA. El principal problema para hacerlo reside en que las sentencias SAML a menudo superan los 4096 bytes, ya que pueden contener elementos como clave pública RSA, firma digital, identidades y un número indefinido de atributos de usuario. Ante esta problemática, el mecanismo de fragmentación descrito en este artículo se presenta como la propuesta más adecuada para enviar esta información sobre RADIUS.

Además, el grupo de trabajo de ABFAB también se plantea la posibilidad de que la aplicación envíe datos de autorización al servidor AAA de forma previa a la autenticación del usuario. En concreto, una aplicación podría enviar una sentencia SAML (*SAMLAuthenticationRequest*) al servidor AAA que incluya información sobre el nivel de confianza (*LoA - Level of Assurance*) mínimo requerido para conceder acceso al usuario, así como los atributos necesarios para realizar el proceso de autorización. En base al LoA solicitado, el servidor AAA elegirá el método EAP (EAP-TLS [14], EAP-AKA [15]...) más adecuado para autenticar al usuario, de forma que se satisfagan los requerimientos de la aplicación. Además, en base a la lista de atributos solicitados, el servidor AAA podría verificar unas políticas de privacidad para determinar si es factible proporcionar los atributos solicitados por la aplicación. Al igual que ocurre con las sentencias SAML generadas por el servidor AAA, los mensajes de solicitud SAML podrían tener un gran tamaño, siendo necesario el uso del mecanismo de fragmentación descrito en este trabajo durante la fase de pre-autorización.

B. Envío de reglas de filtrado en el acceso a la red.

Como consecuencia de la autenticación correcta de un usuario durante el acceso a la red, el AS puede indicar a un NAS el conjunto de reglas de filtrado que deberán aplicarse sobre el tráfico generado y recibido por dicho usuario. Estas reglas pueden transmitirse de dos formas. Por un lado, mediante el uso de atributos *Filter-Id* [1] se puede indicar una serie de nombres de reglas para ser aplicadas en el NAS. Esta alternativa tiene la ventaja de permitir la transmisión de muchas reglas en poco espacio, pero tiene el inconveniente de que ambas entidades deben tener una lista de

reglas y sus correspondientes nombres en común, dificultando su gestión y limitando la escalabilidad.

Por otro lado, hay situaciones donde AS y NAS no comparten una lista común de reglas, y es necesario describirlas de forma explícita. Para ello se utiliza la sintaxis *IPFilterRule* definida en [16]. Estas reglas se concatenan una detrás de la otra mediante una secuencia de atributos RADIUS de tipo *NAS-Filter-Rule* [6]. Concatenando los atributos *NAS-Filter-Rule*, el NAS reconstruye la secuencia de reglas para su aplicación.

Cualquiera de estas alternativas podría requerir la inclusión de una gran cantidad de atributos en el paquete RADIUS, de forma que su tamaño exceda el máximo permitido. Esto es especialmente probable cuando las reglas son transmitidas de forma explícita mediante el atributo *NAS-Filter-Rule*. Por tanto, la capacidad de control que tiene un AS sobre el tráfico de sus usuarios está hoy en día limitada por el tamaño máximo de paquete RADIUS, y deberá ajustarse al mismo. El mecanismo de fragmentación para post-autorización descrito en este artículo solventa este inconveniente ya que permitiría la transmisión de reglas de filtrado de longitudes muy superiores, incrementando la flexibilidad y capacidad de control de tráfico de los operadores de red.

VII. CONCLUSIONES Y VÍAS FUTURAS

RADIUS es uno de los protocolos AAA más usados en la actualidad, desplegado en multitud de organizaciones. Sin embargo, dada su edad presenta ciertas limitaciones a la hora de afrontar algunos de los desafíos que plantean los nuevos escenarios de las telecomunicaciones. En particular, una de estas limitaciones se deriva del tamaño máximo de paquete, acotado en 4096 bytes. Este tamaño impide su uso en situaciones donde se requiere el envío de grandes cantidades de información de autorización (p.ej. sentencias SAML). Aunque se han hecho algunos esfuerzos por proponer soluciones a este problema, ninguna de ellas proporciona un mecanismo que permita tanto al cliente como al servidor enviar una cantidad indefinida de datos de autorización de naturaleza completamente dinámica, sin la necesidad de establecer canales seguros de comunicaciones alternativos.

Este artículo describe un mecanismo de fragmentación flexible que permite este intercambio de información usando el propio transporte RADIUS. Los datos se fragmentan en el origen y se envían a través de varios intercambios de paquetes de tamaño menor al máximo autorizado (llamados *chunks*). Finalmente, el paquete original se reconstruye en el destino y se procesa como si hubiera sido recibido de forma atómica. Este mecanismo está diseñado para funcionar de forma transparente a través de equipos intermedios (proxies) que no lo soportan, así como permitir a aquellos que sí lo hagan un control total sobre la información del paquete original, tal y como ocurriría si el paquete no estuviera fragmentado de acuerdo con la operación estándar de RADIUS. Además, no impone ninguna restricción a los administradores ni les obliga a realizar configuraciones adicionales (p.ej. modificar reglas en firewalls). La solución es compatible con las soluciones de fragmentación intra-paquete existentes [3], [4]. Finalmente, el coste de despliegue de la solución es mínimo, ya que sólo debe ser implementada por aquellos sistemas que requieran intercambiar grandes cantidades de información.

Además de las descripción detallada del proceso de fragmentación, este artículo discute algunos de los aspectos del mismo que admiten matizaciones o que requieren una explicación más detallada, como son el cálculo del tamaño útil de *chunk*, el procesamiento especial de ciertos atributos, la operación con proxies, consideraciones de seguridad. Finalmente, se demuestra la utilidad del mismo mediante la descripción de dos casos de uso reales en los que la aplicación de este mecanismo soluciona un problema existente a día de hoy que limita el uso de RADIUS.

Este mecanismo de fragmentación ha sido presentado al grupo de trabajo *RADEXT* del IETF, para su adopción como estándar para la fragmentación de datos en RADIUS. En Agosto de 2013 fue aceptado como documento del grupo de trabajo, tras recibir numerosos apoyos dentro de la comunidad. Esta adopción es un paso previo a su publicación como estándar consolidado. Además, en colaboración con Telefónica I+D, se ha desarrollado un prototipo que ha servido para demostrar que, usando el mecanismo descrito en este artículo, es posible transmitir datos que sobrepasen los 4096 bytes entre un cliente y un servidor RADIUS, a través de una infraestructura sin actualizar. Como trabajo futuro, se pretende emplear este prototipo para evaluar el rendimiento de la solución y validar su funcionamiento en entornos reales.

AGRADECIMIENTOS

Este trabajo está financiado por el proyecto GÉANT (GN3plus) y por la Fundación Séneca (Programa de Ayuda a los Grupos de Excelencia - 04552/GERM/06). Parte del proceso de desarrollo del prototipo se encuentra financiado por un contrato de exploración tecnológica de Telefónica I+D.

REFERENCIAS

[1] C. Rigney, S. Willens, A. Rubens, and W. Simpson. *Remote Authentication Dial In User Service (RADIUS)*. IETF RFC 2865, June 2000.
[2] Radius extensions (radext ietf working group. http://datatracker.ietf.org/wg/radext/charter/.
[3] B. Aboba and P. Calhoun. *RADIUS support for EAP*. IETF RFC 3579, June 2003.
[4] A. DeKok. *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*. IETF RFC 6929, April 2013.
[5] Application bridging for federated access beyond web (abfab) ietf working group. http://datatracker.ietf.org/wg/abfab/charter/.
[6] P. Congdon, M. Sanchez, and B. Aboba. *RADIUS Filter Rule Attribute*. IETF RFC 4849, April 2007.
[7] A. DeKok and G. Weber. *RADIUS Design Guidelines*. IETF RFC 6158, March 2011.
[8] M. Mathis and J. Heffnet. *Packetization Layer Path MTU Discovery*. IETF RFC 4821, March 2007.
[9] A. DeKok. *RADIUS over TCP*. IETF RFC 6613, May 2012.
[10] C. Rigney. *RADIUS Accounting*. IETF RFC 2866, June 2000.
[11] D. Nelson and A. DeKok. *Common Remote Authentication Dial In User Service (RADIUS). Implementation Issues and Suggested Fixes*. IETF RFC 5080, Dec 2007.
[12] S. Hartman and J. Howlett. *A GSS-API Mechanism for the Extensible Authentication Protocol*. IETF Internet Draft, IETF draft-ietf-abfab-gss-eap-09, Ago 2012.
[13] Assertions and protocol for the OASIS Security Assertion Markup Language (SAML) V1.1, Sept. 2003. OASIS standard.
[14] D. Simon, B. Aboba, and R. Hurst. *The EAP-TLS Authentication Protocol*. IETF RFC 5216, March 2008.
[15] J. Arkko and H. Haverinen. *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*. IETF RFC 4187, Jan. 2006.
[16] P. Calhoun and J. Loughney. *Diameter Base Protocol*. IETF RFC 3588, Sept. 2003.

Fingerprinting basado en códigos cuasi separables con identificación eficiente

José Moreira [#1], Marcel Fernández [#2], Grigory Kabatiansky [*3]

[#] Departament d'Enginyeria Telemàtica
Universitat Politècnica de Catalunya
C/Jordi Girona 1-3, Edif. C3, 08034 Barcelona, Spain
[1] jose.moreira@entel.upc.edu, [2] marcel@entel.upc.edu

[*] Dobrushin Mathematics Laboratory, Institute for Information Transmission Problems,
Russian Academy of Sciences
Bol'shoi Karetnyi per. 19, 127994 Moscow, Russia
[3] kaba@iitp.ru

***Resumen*—Los códigos separables son estructuras combinatorias con numerosas aplicaciones. Áreas tan diversas como la síntesis de autómatas, el análisis exhaustivo de circuitos lógicos o el diseño de códigos de fingerprinting se han beneficiado del uso de dichos códigos. En este trabajo analizamos una versión menos estricta de la propiedad de separación, llamada *cuasi separación*. En concreto, mostramos la existencia de códigos cuasi separables de mejor tasa que los códigos separables ordinarios que se conocen actualmente. Además, mostramos como los códigos cuasi separables pueden utilizarse para construir una familia de códigos de fingerprinting con probabilidad de error decreciente con la longitud del código. De nuevo, las construcciones presentadas tienen mejor tasa que las construcciones basadas en códigos separables ordinarios. Finalmente, mostramos como el algoritmo de Koetter-Vardy puede emplearse para decodificar los códigos construidos, obteniendo un algoritmo de decodificación eficiente, en tiempo polinómico en la longitud del código.**

***Palabras Clave*—Fingerprinting, códigos separables, protección del copyright, algoritmo de Koetter-Vardy**

I. INTRODUCCIÓN

El concepto de código separable fue introducido por primera vez en [1] por Friedman et ál. hace unos 50 años. Un código separable es una estructura combinatoria natural con aplicación en multitud de campos. Diagnóstico técnico, síntesis de autómatas, análisis exhaustivo de circuitos lógicos, generación de funciones de hash, y sistemas de identificación de traidores son algunos ejemplos de campos que se han beneficiado del uso de códigos separables. Estos códigos han sido ampliamente investigados por diversos autores, obteniéndose cotas inferiores y superiores sobre su tasa asintótica y estableciéndose conexiones con conceptos similares. Véase, por ejemplo, [2], [3], [4], [5], [6], [7].

En relación con el campo del *fingerprinting digital* [8], [9], los códigos separables han vuelto a suscitar nuevamente un gran interés. El ámbito del fingerprinting digital es el ámbito de la identificación de traidores [10], [11] aplicado a la distribución de contenidos digitales. En este nuevo dominio de aplicación, los códigos separables se conocen también con el nombre de *códigos seguros contra incriminaciones* (secure frameproof codes) [12], [13].

En un sistema de fingerprinting, las copias de un objeto digital a distribuir se hacen únicas mediante la inserción de una marca diferente en cada copia. Entregando copias únicas de dicho objeto a cada uno de los usuarios autorizados se disuade a éstos de realizar una redistribución simple. No obstante, una coalición de usuarios deshonestos, llamados *traidores*, puede realizar un *ataque de confabulación*.

En un ataque de confabulación un grupo de traidores comparan sus copias, revelando las posiciones donde sus marcas difieren. Mediante la modificación de estas posiciones detectadas crean una nueva copia, generalmente llamada *copia pirata*. La generación de una copia pirata por parte de los traidores tiene como objetivo camuflar sus identidades. La modificación de posiciones arbitrarias del contenido se considera peligrosa, ya que podría dañar la funcionalidad del mismo. Por eso, es habitual restringir las posiciones modificables a aquellas en las que se han detectado diferencias, y por tanto, se sabe con seguridad que contienen parte de la marca. Este supuesto se conoce como *marking assumption* [8], [9].

Por tanto, la construcción de un código de fingerprinting consiste en encontrar, para cada copia de un contenido digital, un conjunto diferente de marcas (palabras código) que ayude al distribuidor a identificar traidores en presencia de ataques de confabulación.

I-A. Contribución del trabajo

En un código (c, c)-*separable* cada subconjunto de palabras código de tamaño como máximo c está "separado" de cualquier otro subconjunto disjunto también de tamaño como máximo c. El significado concreto de lo que se entiende por "separado" se precisará más adelante.

El concepto de *código cuasi separble* fue introducido en [14]. En contraposición al concepto ordinario de de (c, c)-separación, en un código cuasi (c, c)-separable cualquier subconjunto de palabras código de tamaño como máximo c está separado *con alta probabilidad* del resto de subconjuntos disjuntos, también de tamaño máximo c. En [14] se muestra que la relajación de la definición de código separable en códigos cuasi separables y códigos cuasi seguros contra incriminaciones conduce a dos conceptos diferentes. Además, también en [14], se obtienen cotas de existencia para códigos binarios cuasi $(2, 2)$-separables.

En este artículo nos centraremos en el caso general de códigos binarios cuasi (c, c)-separables, es decir, para $c \geq 2$.

Diremos que un subconjunto de un máximo de c palabras código es "bueno" si está separado de todos los otros subconjuntos disjuntos de palabras código de tamaño máximo c. Informalmente, en un código cuasi (c, c)-separable la relación de subconjuntos "buenos", entre el total de subconjuntos de tamaño como máximo c, se puede hacer tan pequeña como se desee. Utilizando el concepto de *conjuntos típicos* [15], una definición informal de código cuasi (c, c)-separable se puede realizar de dos maneras. Por un lado, se puede considerar que un *conjunto típico* de palabras código está separado de todos los otros conjuntos disjuntos de palabras código con muy alta probabilidad. Por otra parte, dado que casi todos los subconjuntos son típicos con alta probabilidad, (esta afirmación se demostrará más adelante), entonces también podemos considerar que un conjunto típico de palabras código está separado de todos los otros conjuntos disjuntos típicos de palabras código con alta probabilidad. En las Secciónes III-A y III-B obtendremos cotas de existencia de estos códigos.

Nuestra motivación para estudiar los códigos separables y cuasi separables viene de su uso en la construcción de códigos de fingerprinting. Es un hecho probado que la propiedad de separación (y por tanto, la propiedad de cuasi separación) es una condición necesaria pero no suficiente para permitir la identificación de traidores en presencia de ataques de confabulación [16]. No obstante, pueden utilizarse como pieza para construir familias de códigos de fingerprinting. En la sección IV-A, presentamos una familia de códigos de fingerprinting basados en códigos cuasi separables, junto con un algoritmo de decodificación eficiente basado en el algoritmo de decodificación de lista de Koetter-Vardy [17], [18].

II. DEFINICIONES Y RESULTADOS PREVIOS

Sea Q un alfabeto q-ario, es decir $|Q| = q$. Utilizaremos la notación $\mathbb{F}_q$ cuando Q sea el cuerpo finito de q elementos. Denotaremos por Q^n el conjunto de todos los vectores de longitud n sobre Q. Los elementos de Q^n los escribiremos en negrilla, por ejemplo, $\mathbf{a} = (a_1, \ldots, a_n) \in Q^n$. La *distancia (de Hamming)* entre dos elementos $\mathbf{a}, \mathbf{b} \in Q^n$, denotada por $d(\mathbf{a}, \mathbf{b})$, es el número de posiciones en las que $\mathbf{a}$ y $\mathbf{b}$ difieren. Un (n, M)-*código* C sobre Q es un subconjunto de Q^n de tamaño M. Los elementos de C se denominan *palabras código*. Además, si $C \subseteq \mathbb{F}_q^n$ y C es un espacio vectorial k-dimensional, diremos que C es un $[n, k]$-código. La *distancia mínima* de un código C, denotada por $d(C)$, es la menor distancia entre cualquier par de palabras código diferentes,

$$d(C) \stackrel{\text{def}}{=} \min_{\mathbf{u}, \mathbf{v} \in C} \{d(\mathbf{u}, \mathbf{v}) : \mathbf{u} \neq \mathbf{v}\}.$$

Sea $U = \{\mathbf{u}^1, \ldots, \mathbf{u}^c\} \subseteq C$ un subconjunto de C de tamaño c, nos referiremos a U como una *coalición de tamaño* c. Esta denominación está motivada por su uso en el campo del fingerprinting digital. Véase [8], [9]. Denotaremos por $P_i(U)$ el conjunto de elementos que toman las palabras código de U en la posición i, es decir

$$P_i(U) \stackrel{\text{def}}{=} \{u_i^1, \ldots, u_i^c\}. \tag{1}$$

Una posición i es *indetectable* para los integrantes de una coalición U si $u_i^1 = \cdots = u_i^c$. Mediante la comparación de las c palabras código de U, un vector $\mathbf{z} = (z_1, \ldots, z_n)$, llamado *descendiente*, se puede construir de acuerdo a unas determinadas reglas. El descendiente se corresponde con la palabra de la copia pirata. En las posiciones indetectables i se tiene que $z_i = u_i^1 = \cdots = u_i^c$. En el resto de posiciones existen diversas alternativas a considerar. Nosotros asumiremos que el conjunto de descendientes que una coalición U puede generar, denotado por $\mathrm{desc}(U)$, es el siguiente

$$\mathrm{desc}(U) \stackrel{\text{def}}{=} \{\mathbf{z} \in Q^n : z_i \in P_i(U)\}. \tag{2}$$

Es importante recalcar que, para códigos binarios, el hecho de considerar este conjunto de descendientes u otros conjuntos más sofisticados (es decir, permitir que los traidores realicen ataques más elaborados) aporta el mismo beneficio en términos de diseño de códigos y probabilidad de error máxima [16].

Dados dos subconjuntos disjuntos de un código $U, V \subseteq C$, una posición de i se denomina *separada* si se satisface que $P_i(U) \cap P_i(V) = \emptyset$. Diremos que los subconjuntos U, V están *separados* si tienen al menos una posición separada.

Definición 1: Un código $C \subseteq Q^n$ es (c, c')-*separable* si cualquier par de subconjuntos disjuntos $U, V \subseteq C$, tales que $|U| \leq c$ y $|V| \leq c'$, están separados.

Seguiremos la misma notación que la empleada en [14]. Sea $R = R(C) \stackrel{\text{def}}{=} n^{-1} \log_q |C|$ la *tasa* de un (n, M)-código sobre un alfabeto q-ario Q. Denotaremos por $R_q(n, c)$ a la tasa máxima que puede alcanzar un código q-ario (c, c)-separable de longitud n. Es decir,

$$R_q(n, c) \stackrel{\text{def}}{=} \max_{\substack{C \subseteq Q^n \colon C \text{ es} \\ (c,c)\text{-separable}}} R(C).$$

Definiremos también los límites asintóticos de dicha tasa

$$\underline{R}_q(c) = \liminf_{n \to \infty} R_q(n, c),$$
$$\overline{R}_q(c) = \limsup_{n \to \infty} R_q(n, c).$$

En este artículo nos centraremos en códigos sobre el alfabeto binario, es decir, $Q = \{0, 1\}$. En el caso de códigos binarios $(2, 2)$-separables, se sabe que $\underline{R}_2(2) \geq 0{,}0642$ [3], [2] y $\overline{R}_2(2) < 0{,}2835$ [2], [5]. Para valores arbitrarios de c, en [16] se obtiene que

$$\underline{R}_2(c) \geq -\frac{\log_2(1 - 2^{-2c+1})}{2c - 1}. \tag{3}$$

Finalizamos esta sección revisando algunos conceptos matemáticos que utilizaremos en el artículo. Denotaremos por $h(k; N, K, n)$ al valor en k de la función de probabilidad de una variable aleatoria hipergeométrica con tamaño de población N, número de elementos con las características deseadas K, y número de muestras tomadas n, es decir,

$$h(k; N, K, n) \stackrel{\text{def}}{=} \frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}. \tag{4}$$

Recordamos también el valor asintótico del coeficiente binomial,

$$\lim_{n \to \infty} n^{-1} \log_2 \binom{n}{k} = H(k/n), \tag{5}$$

donde $H(p)$ denota la función de entropía binaria,

$$H(p) \stackrel{\text{def}}{=} -p \log_2 p - (1 - p) \log_2 (1 - p).$$

Dicho valor asintótico es fácil de obtener utilizando la fórmula de Stirling.

Finalmente, denotaremos por $D(p\|q)$ la *divergencia de Kullback-Leibler* entre dos variables aleatorias de Bernoulli de parámetros p y q, respectivamente,

$$D(p\|q) \stackrel{\text{def}}{=} p\log_2(p/q) + (1-p)\log_2((1-p)/(1-q)).$$

Obsérvese que $D(p\|q) \geq 0$ y $D(p\|q) = 0$ si y sólo si $p = q$.

III. CÓDIGOS CUASI SEPARABLES

Dado un código C, diremos que una coalición $U \subseteq C$ de tamaño c es una *coalición separada* si U está separada de cualquier otra coalición disjunta $V \subseteq C$ de tamaño c.

Definición 2 ([14]): Un código $C \subseteq Q^n$ es *ε-cuasi (c,c)-separable* si la proporción de coaliciones separadas de tamaño c, entre todas las posibles coaliciones de tamaño c, es como mínimo $1-\varepsilon$.

Una secuencia de códigos $(C_i)_{i\geq 1}$ de longitud n_i creciente es una *familia asintóticamente cuasi (c,c)-separable* si cada código C_i es un código ε_i-cuasi (c,c)-separable y $\lim_{i\to\infty}\varepsilon_i = 0$.

Para una familia de códigos $\mathcal{C} = (C_i)_{i\geq 1}$ definimos su tasa asintótica como

$$R(\mathcal{C}) \stackrel{\text{def}}{=} \liminf_{i\to\infty} R(C_i).$$

Nuestro interés reside en estimar el valor máximo de dicha tasa asintótica, $R_q^*(c)$, entre todas las familias de códigos asintóticamente cuasi (c,c)-separables.

Para demostrar la existencia de familias de códigos cuasi separables, utilizaremos el concepto de *conjuntos típicos* [15] de palabras código. Es decir, conjuntos que se obtienen con alta probabilidad en códigos generados aleatoriamente. Para nuestro objetivo, nos será útil considerar la siguiente definición de tipicalidad.

Consideremos un (n,M)-código binario C. Para cualquier coalición $U = \{\mathbf{u}^1,\ldots,\mathbf{u}^c\} \subseteq C$, de tamaño c, y cualquier $\alpha \in Q$, denotaremos por $N(\alpha;U)$ el número de posiciones i tales que $u_i^1 = \cdots = u_i^c = \alpha$. Por ejemplo, si

$$\begin{aligned} U = \{&(1,0,0,1,0,1,0)\\ &(0,0,1,1,0,1,1)\\ &(1,0,1,1,0,0,0)\}, \end{aligned}$$

entonces $N(0;U) = 2$ y $N(1;U) = 1$.

Definición 3: Dado $0 < \delta < 2^{-c}$ y un (n,M)-código binario C, definimos el *conjunto de coaliciones δ-típicas* (de tamaño c) de C, denotado por $A_\delta^c(C)$, como

$$\begin{aligned} A_\delta^c(C) \stackrel{\text{def}}{=} \{&U \subseteq C : |U| = c, \text{ con}\\ &N(0;U), N(1;U) \in [n(2^{-c}-\delta), n(2^{-c}+\delta)]\ \}. \end{aligned}$$

Informalmente, $A_\delta^c(C)$ contiene todas las coaliciones $U \subseteq C$ de tamaño c tales que las palabras código de U toman todas el valor 0 (respectivamente, el valor 1) en aproximadamente $n2^{-c}$ posiciones.

III-A. Cota de existencia I

Con las definiciones que se acaban de presentar, tenemos las herramientas necesarias para obtener cotas de existencia (cotas inferiores) para familias de códigos asintóticamente cuasi (c,c)-separables. Como se planteó en la Sección I, primero impondremos la condición de que una coalición típica esté separada de todas las demás coaliciones. En este caso obtenemos el siguiente resultado.

Teorema 1: El valor máximo de la tasa asintótica $R_2^*(c)$ entre todas las familias de códigos binarios asintóticamente cuasi (c,c)-separables satisface que

$$R_2^*(c) \geq -\frac{\log_2(1-2^{-c})}{c\,2^{c-1}}.$$

Demostración: Consideremos un (n,M)-código binario aleatorio. Es decir, generamos aleatoriamente y de forma independiente M vectores binarios de longitud n, $\mathbf{u} = (u_1,\ldots,u_n) \in C$ tales que $\Pr\{u_i = 0\} = \Pr\{u_i = 1\} = 1/2$.

La probabilidad de que una coalición $U = \{\mathbf{u}^1,\ldots,\mathbf{u}^c\} \subseteq C$ de tamaño c sea δ-típica es de como mínimo $1 - f(\delta,c,n)$, donde

$$\begin{aligned} f(\delta,c,n) &= 2^{-nD(2^{-c}-\delta\|2^{-c})+1} + 2^{-nD(2^{-c}+\delta\|2^{-c})+1}\\ &\leq 4e^{-2n\delta^2}. \end{aligned} \quad (6)$$

Esto se obtiene de la simple observación de que los valores $N(0;U)$ y $N(1;U)$ pueden interpretarse como una variable aleatoria binomial de parámetros n y 2^{-c}. Por tanto, una cota superior de la probabilidad de que $N(0;U)$ o $N(1;U)$ estén fuera del rango $[n(2^{-c}-\delta), n(2^{-c}+\delta)]$ (Ec. 6) puede obtenerse fácilmente aplicando las cotas de Chernoff y Hoeffding [19].

Además, la probabilidad de que la coalición U esté separada de otra coalición aleatoria V, también de tamaño c, es

$$(1-2^{-c})^{N(0;U)+N(1;U)}.$$

Ciertamente, hay $N(0;U)+N(1;U)$ posiciones i en las que $u_i^1 = \cdots = u_i^c$. Para cada una de esas posiciones, la probabilidad de que $P_i(U) = \{u_i^1,\ldots,u_i^c\}$ y $P_i(V) = \{v_i^1,\ldots,v_i^c\}$ no sean disjuntos es igual a $1-2^{-c}$.

Por tanto, el ratio ε (probabilidad) de coaliciones de tamaño c que no son separadas satisface

$$\begin{aligned} \varepsilon &\leq \Pr\{U \text{ no separada} \,|\, U \text{ es típica}\} + \Pr\{U \text{ no es típica}\}\\ &\leq M^c(1-2^{-c})^{n(2^{-c+1}-2\delta)} + f(\delta,c,n). \end{aligned}$$

Tomando un valor apropiado de δ, por ejemplo, $\delta = \delta(n) = \ln n/\sqrt{n}$, y utilizando Ec. 6, podemos observar que para cualquier tasa R tal que

$$R < -\frac{\log_2(1-2^{-c})}{c\,2^{c-1}}$$

tenemos $\lim_{n\to\infty}\varepsilon \to 0$.

En conclusión, existe una familia de códigos binarios asintóticamente cuasi (c,c)-separable $\mathcal{C}$ tal que $R(\mathcal{C}) < -\frac{\log_2(1-2^{-c})}{c\,2^{c-1}}$. ■

III-B. Cota de existencia II

En esta sección, vamos a tener en cuenta las consecuencias de Ec. 6 para obtener una cota de existencia más refinada que la obtenida en la sección anterior.

En un código aleatorio, como el empleado en la demostración del Teorema 1, una coalición dada es típica con alta probabilidad. Con esta idea en mente, nos proponemos obtener una cota inferior imponiendo sólo que una coalición típica esté separada de todas las demás coaliciones típicas disjuntas.

En primer lugar, vamos a obtener un límite superior de la probabilidad de que dos coaliciones típicas de tamaño c estén separadas.

Lema 1: Sean U, V dos coaliciones de tamaño c de un (n, M)-código binario C. Si se cumple que

$$N(0;U) = N(1;U) = N(0;V) = N(1;V) = n2^{-c},$$

entonces la probabilidad de que U y V no estén separadas, denotada por p_c, satisface

$$\lim_{n\to\infty} n^{-1} p_c \le G(c),$$

donde

$$G(c) \stackrel{\text{def}}{=} n\Big((1-2p+\ell)H\big(\tfrac{p}{1-2p+\ell}\big) + p\,H\big(\tfrac{\ell}{p}\big) + (1-2p)H\big(\tfrac{p-\ell}{1-2p}\big) - H(p) - (1-p)H\big(\tfrac{p}{1-p}\big)\Big), \quad (7)$$

con $p = 2^{-c}$ y $\ell = (2p - 1 + \sqrt{8p^2 - 4p + 1})/2$.

Demostración: Consideremos dos coaliciones

$$U = \{\mathbf{u}^1, \ldots, \mathbf{u}^c\}, \qquad V = \{\mathbf{v}^1, \ldots, \mathbf{v}^c\}$$

que satisfagan las condiciones del enunciado. Definimos X_0 como la variable aleatoria que cuenta el número de posiciones no separadas i tales que las elementos U satisfacen $u_i^1 = \cdots = u_i^c = 0$. Es decir, en estas posiciones hay al menos un vector $\mathbf{v} \in V$ tal que $v_i = 0$. Equivalentemente, definimos la variable aleatoria X_1 para el caso $u_i^1 = \cdots = u_i^c = 1$.

Tomemos $p = 2^{-c}$ y $t = np$. Obviamente, $0 \le X_0, X_1 \le t$. En resumen, las coaliciones U y V no están separadas cuando $X_0 = t$ y $X_1 = t$. La probabilidad de este evento puede expresarse como

$$\begin{aligned} p_c &= \Pr\{X_0 = t, X_1 = t\} = \Pr\{X_0 = t\}\Pr\{X_1 = t | X_0 = t\} \\ &= \Pr\{X_0 = t\}\sum_{j=0}^{t} \Pr\{Y_0 = j | X_0 = t\}\Pr\{X_1 = t | X_0 = t, Y_0 = j\}. \end{aligned} \quad (8)$$

La variable aleatoria auxiliar Y_0 cuenta el número de posiciones no separadas i tales que

$$u_i^1 = \cdots = u_i^c = v_i^1 = \cdots = v_i^c = 0.$$

No es difícil observar que todas las probabilidades que aparecen en Ec. 8 se pueden expresar en base a la función de probabilidad de una variable hipergeométrica, Ec. 4, de la siguiente manera:

$$\begin{aligned} \Pr\{X_0 = t\} &= h(t; n, n-t, t), \\ \Pr\{Y_0 = j | X_0 = t\} &= h(j; n-t, t, t), \\ \Pr\{X_1 = t | X_0 = t, Y_0 = j\} &= h(t; n-t, n-2t+j, t). \end{aligned}$$

Expandiendo los términos de la función de probabilidad hipergeométrica, Ec. 8 se reduce a

$$\begin{aligned} p_c &= \Pr\{X_0 = t, X_1 = t\} \\ &= \frac{1}{\binom{n}{t}\binom{n-t}{t}} \sum_{j=0}^{t} \binom{n-2t+j}{t}\binom{t}{j}\binom{n-2t}{t-j}. \end{aligned}$$

Utilizando Ec. 5 obtenemos

$$\lim_{n\to\infty} n^{-1}\log_2 p_c = \Big((1-2p+j')H\big(\tfrac{p}{1-2p+j'}\big) + p\,H\big(\tfrac{j'}{p}\big) + (1-2p)H\big(\tfrac{p-j'}{1-2p}\big) - H(p) - (1-p)H\big(\tfrac{p}{1-p}\big)\Big),$$

donde $j' \in [0, p]$. Es rutinario comprobar que el máximo de esta expresión se obtiene para $j' = \ell$. ∎

El resultado anterior nos permitirá obtener una mejora sobre el valor máximo de la tasa asintótica de familias de códigos cuasi (c, c)-separables obtenido en el Teorema 1.

Teorema 2: El valor máximo de la tasa asintótica $R_2^*(c)$ entre todas las familias de códigos binarios asintóticamente cuasi (c, c)-separables satisface que

$$R_2^*(c) \ge -c^{-1}G(c),$$

donde $G(c)$ es la expresión Ec. 7 del Lema 1.

Demostración: Consideremos de nuevo un (n, M)-código aleatorio C como en la demostración del Teorema 1. Según Ec. 6, la proporción E de de coaliciones δ-típicas de tamaño c satisface $\lim_{n\to\infty} E = 1$. Por tanto, puede considerarse que todas las coaliciones de tamaño c de C son δ-típicas en el límite.

Sean $U, V \subseteq C$ dos coaliciones δ-típicas de tamaño c, y sea p'_c la probabilidad de que U y V no estén separadas. El número esperado de parejas de coaliciones separadas $\{U, V\}$, de tamaño c, donde U y V son δ-típicas, es como máximo $\binom{M}{c}\binom{M-c}{c}p'_c$, y la probabilidad ε de que una coalición δ-típica de tamaño c, U, no sea separada satisface

$$\varepsilon \le M^c p'_c.$$

Por tanto, utilizando el Lema 1,

$$\lim_{n\to\infty} n^{-1}\log_2 \varepsilon \le c\,R + G(c).$$

De nuevo, puede verse que para cualquier tasa

$$R < -c^{-1}G(c)$$

tenemos $\lim_{n\to\infty} \varepsilon \to 0$.

Es decir, existen familias de códigos binarios asintóticamente cuasi (c, c)-separables $\mathcal{C}$ con $R(\mathcal{C}) < -c^{-1}G(c)$. ∎

III-C. Comparación de resultados obtenidos

En esta sección presentamos una breve comparación de las cotas de existencia de familias de códigos asintóticamente cuasi (c, c)-separables (Teoremas 1 y 2) con las cotas que se conocen para códigos (c, c)-separables ordinarios.

En la Tabla I tenemos que

- R_1 denota la cota inferior obtenida en el Teorema 1,
- R_2 denota la cota inferior obtenida en el Teorema 2,
- R_{ord} denota la cota inferior para códigos separables ordinarios [16, Proposición 3.4].

Intuitivamente, la cota inferior R_2 es mejor que R_1 porque en la condición impuesta en el Teorema 2 sólo se requiere que

Tabla I
COMPARACIÓN DE TASAS DE CÓDIGOS CUASI SEPARABLES Y CÓDIGOS SEPARABLES ORDINARIOS.

c	R_1	R_2	R_{ord}
2	$1{,}03759374 \cdot 10^{-1}$	$1{,}14223348 \cdot 10^{-1}$	$6{,}42150259 \cdot 10^{-2}$
3	$1{,}60537564 \cdot 10^{-2}$	$1{,}70347237 \cdot 10^{-2}$	$9{,}16073792 \cdot 10^{-3}$
4	$2{,}90966888 \cdot 10^{-3}$	$3{,}00072486 \cdot 10^{-3}$	$1{,}61647331 \cdot 10^{-3}$
10	$2{,}75306690 \cdot 10^{-7}$	$2{,}75441139 \cdot 10^{-7}$	$1{,}44827633 \cdot 10^{-7}$
20	$1{,}31212412 \cdot 10^{-13}$	$1{,}31212474 \cdot 10^{-13}$	$6{,}72883844 \cdot 10^{-14}$

las coaliciones típicas estén separadas del resto de coaliciones típicas disjuntas, mientras que la condición en el Teorema 1 requería que las coaliciones típicas estuviesen separadas de todas las demás coaliciones disjuntas. Obsérvese que R_1 y R_2 son aproximadamente el doble que las mejores cotas que se conocen para códigos separables ordinarios.

IV. APLICACIÓN A CÓDIGOS DE FINGERPRINTING

En esta sección mostraremos como códigos binarios ε-cuasi (c, c)-separables se pueden utilizar para construir una familia de códigos de fingerprinting binarios. En primer lugar, mostraremos la construcción propuesta y posteriormente derivaremos condiciones de existencia de dichos códigos.

IV-A. Códigos de fingerprinting

Un ataque de confabulación descrito anteriormente se materializa mediante la generación de un descendiente. En este caso el descendiente es la palabra en la copia pirata y los padres son las palabras código que pertenecen a los traidores.

Como se muestra en [8], [9], [16], en un sistema de fingerprinting, para alcanzar una probabilidad de error tan pequeña como se desee (exponencialmente pequeña en la longitud del código) un único código no es suficiente. Se necesita una *familia de códigos de fingerprinting*.

Denotaremos una familia de códigos de fingerprinting como $\mathcal{F} = \{F_t\}_{t \in T}$, donde T es un conjunto finito. Un sistema de fingerprinting requiere, como pieza fundamental, una fuente de aleatoriedad entendida como se explica a continuación. La familia $\mathcal{F}$ es conocida públicamente. Sin embargo, el código específico F_t utilizado por el distribuidor para marcar las copias del contenido es elegido al azar con probabilidad $\pi(t)$, y esta elección se mantiene en secreto.

Para cada uno de los códigos de la familia $\mathcal{F}$ necesitamos también un *algoritmo de identificación*. Un algoritmo de identificación A_t para el código $F_t \in \mathcal{F}$ es una función que toma como argumento un descendiente generado por alguna coalición de F_t y retorna un subconjunto de palabras de F_t.

Definición 4: [8], [9] Sea T un conjunto finito y sea $c \geq 2$. Una familia de códigos de fingerprinting binarios, $\mathcal{F} = \{F_t\}_{t \in T}$, es *c-segura con probabilidad de error* p_e si existe un conjunto de algoritmos de identificación A_t tales que se satisface la siguiente condición: si una coalición U de tamaño como máximo c crea un descendiente $\mathbf{z}$, entonces

$$\Pr\{A_t(\mathbf{z}) \subseteq U \text{ y } A_t(\mathbf{z}) \neq \emptyset\} > 1 - p_e,$$

donde probabilidad se considera sobre las elecciones al azar realizadas por la coalición al crear el descendiente y sobre los elementos $t \in T$.

IV-B. Construcción de la familia de códigos y condiciones de existencia

Sea Q un alfabeto q-ario, y sea C_{in} un (l, q)-código binario. Consideremos el vector $(\phi_1, \ldots, \phi_n)$, donde $\phi_i, 1 \leq i \leq n$ son biyecciones $Q \to C_{\text{in}}$. Claramente, hay $(q!)^n$ de tales vectores. Si numeramos estos vectores arbitrariamente de 1 a $(q!)^n$, entonces $(\phi_1^{(t)}, \ldots, \phi_n^{(t)})$ denotará el t-ésimo de dichos vectores.

Construcción 1: Sea C_{ex} un (n, M)-código sobre un alfabeto q-ario Q, y sea C_{in} un (l, q)-código binario. La familia de códigos de fingerprinting $\mathcal{F}$ se define como el conjunto de códigos $\{F_t\}$, donde

$$F_t = \{(\phi_1^{(t)}(w_1), \ldots, \phi_n^{(t)}(w_n)) : (w_1, \ldots, w_n) \in C_{\text{ex}}\},$$

para todo $1 \leq t \leq (q!)^n$. el código C_{ex} se denomina *código externo* y C_{in} se denomina *código interno*. Cada uno de los códigos de la familia $\mathcal{F}$ es un (ln, M)-código binario.

Nótese que existe una relación biunívoca entre las palabras del código externo C_{ex} y las palabras del código concatenado F_t.

Como se ha comentado anteriormente, para usar la familia $\mathcal{F} = \{F_t\}$ de la Construcción 1, primero tenemos que seleccionar un valor $1 \leq t \leq (q!)^n$ en base a una función de probabilidad $\pi(t)$. Este valor t debe mantenerse en secreto. A cada usuario se le asignará una palabra código de F_t.

Sea

$$\mathbf{z} = (\underbrace{z_{11}, \ldots, z_{1l}}_{\mathbf{z}_1}, \ \ldots, \ \underbrace{z_{n1}, \ldots, z_{nl}}_{\mathbf{z}_n}) \in \text{desc}(U),$$

un descendiente creado por una coalición de tamaño c. En el análisis del algoritmo de identificación consideraremos que en el proceso de decodificación de cada bloque $\mathbf{z}^i$ se obtiene un conjunto $V \subseteq C_{\text{in}}$ de, como máximo, c palabras código tal que $\mathbf{z}^i \in \text{desc}(V)$. Si el código interno C_{in} es ε-cuasi separable, entonces con probabilidad $\geq 1 - \varepsilon$ este conjunto contiene una palabra del código interno $\mathbf{v}_j^i$ tal que coincide con el bloque i-ésimo de una palabra de uno de los traidores. Obviamente, $(\phi_i^{(t)})^{-1}(\mathbf{v}_j^i)$ es el símbolo en la i-ésima posición de la palabra correspondiente del código externo.

Obsérvese que la decodificación de cada uno de los n bloques del código interno se realiza para un código relativamente pequeño. El paso más costoso del Algoritmo de Identificación 1 es, por tanto, el paso 3. En la Sección IV-C mostraremos como puede realizarse este paso de forma eficiente (en tiempo polinómico en la longitud del código) mediante el uso del algoritmo de Koetter-Vardy [17], [18].

A continuación, exponemos en forma de teorema los parámetros precisos de los códigos de la Construcción 1 que nos permiten obtener una probabilidad de error en la identificación de traidores exponencialmente pequeña, cuando es utilizado en conjunción con el Algoritmo de Identificación 1.

Teorema 3: Sea C_{ex} un (n, M)-código sobre un alfabeto q-ario Q, de distancia mínima $d = d(C_{\text{ex}})$, y sea C_{in} un (l, q)-código ε-cuasi (c, c)-separable binario. Sea $\mathcal{F} = \{F_t\}$ la familia de la Construcción 1 con código externo C_{ex}, código interno C_{in} y las biyecciones $(\phi_1^{(t)}, \ldots, \phi_n^{(t)})$, con $1 \leq t \leq (q!)^n$. Para $q > c^2$ y $\varepsilon < \sigma < (q - c^2)/(q - c)$,

Algoritmo de Identificación 1

Entrada: El código concatenado F_t de la Construcción 1, satisfaciendo las condiciones del Teorema 3, y un descendiente de una coalición U de tamaño máximo c, $\mathbf{z} \in \mathrm{desc}(U)$,

$$\mathbf{z} = (\underbrace{z_{11}, \ldots, z_{1l}}_{\mathbf{z}_1}, \ \ldots, \ \underbrace{z_{n1}, \ldots, z_{nl}}_{\mathbf{z}_n}).$$

Salida: Un subconjunto de palabras código de F_t.

Ejecutar:

1. Para $1 \le i \le n$, decodificar cada bloque $\mathbf{z}_i = (z_{i1}, \ldots, z_{il})$ del descendiente $\mathbf{z}$:
   a) Encontrar todas las coaliciones $V \subseteq C_{\mathrm{in}}$ de tamaño c tales que $\mathbf{z}_i \in \mathrm{desc}(V)$.
   b) Si la intersección de todas las coaliciones V encontradas en el paso 1a) es vacia, $\mathcal{Z}_i = \emptyset$.
   c) Si no, seleccionar una coalición arbitraria V del paso 1a). Invertir la biyección
   $$(\phi_i^{(t)})^{-1} : C_{\mathrm{in}} \to Q$$
   obteniendo un subconjunto $\mathcal{Z}_i$ de c símbolos de Q.
2. Construir el vector de conjuntos
   $$\mathcal{Z} := (\mathcal{Z}_1, \ldots, \mathcal{Z}_n).$$
3. Determinar todas las palabras código $\mathbf{w}^1, \ldots, \mathbf{w}^s \in C_{\mathrm{ex}}$, tales que
   $$\mathrm{s}(\mathbf{w}, \mathcal{Z}) \ge n\frac{1-\sigma}{c},$$
   donde
   $$\mathrm{s}(\mathbf{w}, \mathcal{Z}) \stackrel{\mathrm{def}}{=} |\{i : w_i \in \mathcal{Z}_i, \text{ para } 1 \le i \le n\}|.$$
4. Retornar el conjunto $L := \{\mathbf{u}^1, \ldots, \mathbf{u}^s\}$, donde
   $$\mathbf{u}^i = (\phi_1^{(t)}(w_1^i), \ldots, \phi_n^{(t)}(w_n^i)),$$
   para cada palabra $\mathbf{w} = (w_1, \ldots, w_n)$ obtenida en el paso 3. Si $L = \emptyset$, declarar error en la identificación.

si la distancia mínima del código externo, d, satisface

$$d > n - \frac{n(1-\sigma)}{c^2} + \frac{n(c-1)}{c(q-c)}, \tag{9}$$

entonces, la familia de códigos concatenados $\mathcal{F}$ junto con el Algoritmo de Identificación 1 es una familia c-segura con probabilidad de error p_e exponencialmente pequeña en la longitud del código,

$$p_e \le q^k 2^{-nD(\rho \| \frac{c-1}{q-c})} + 2^{-nD(\sigma\|\varepsilon)} = \exp(-\Omega(n)), \tag{10}$$

donde $\rho = \frac{1-\sigma}{c} - c(1 - d/n)$.

Demostración: Sea $U \subseteq C_t$ una coalición de tamaño c, y sea $W \subseteq C_{\mathrm{ex}}$ el conjunto de las palabras del código externo asociadas a U. Consideremos que

$$\mathbf{z} = (\underbrace{z_{11}, \ldots, z_{1l}}_{\mathbf{z}_1}, \ \ldots, \ \underbrace{z_{n1}, \ldots, z_{nl}}_{\mathbf{z}_n})$$

es un descendiente creado por la coalición U.

En primer lugar, obsérvese que en el paso 1b) del Algoritmo de Identificación 1 estamos "descartando" todos los bloques no separados al imponer $\mathcal{Z}_i = \emptyset$. Este evento ocurrirá con probabilidad $\le \varepsilon$ debido a la propiedad de cuasi separación del código interno. Por tanto, $\mathcal{Z}_i \cap P_i(W) \ne \emptyset$, es decir, $\mathcal{Z}_i$ contiene como mínimo un elemento w_i de alguna palabra $\mathbf{w} = (w_1, \ldots, w_n) \in W$, con probabilidad $\ge 1 - \varepsilon$.

Es fácil ver que el número de bloques descartados puede acotarse por una variable binomial X de parámetros n y ε. Dado que $\sigma > \varepsilon$, podemos acotar el valor máximo del número de bloques descartados utilizando la cota de Chernoff [19],

$$\Pr\{X \ge n\sigma\} \le 2^{-nD(\sigma\|\varepsilon)}, \tag{11}$$

viendo que este valor decrece exponencialmente con n.

Utilizando el principio del palomar, tenemos que, con alta probabilidad, existe una palabra $\hat{\mathbf{w}}$ del código externo asociada a uno de los traidores, $\hat{\mathbf{w}} \in W$, tal que su "similitud" con $\mathcal{Z}$ satisface

$$\mathrm{s}(\hat{\mathbf{w}}, \mathcal{Z}) \ge n\frac{1-\sigma}{c}, \tag{12}$$

y por tanto, el usuario asociado será identificado como traidor.

Por otra parte, para un usuario inocente, es decir con $\mathbf{w} = (w_1, \ldots, w_n) \notin W$, si el elemento w_i aparece en $\mathcal{Z}_i$ puede ser porque $w_i \in P_i(W)$. Como cualquier par de palabras de C_{ex} pueden coincidir en $\le n - d$ posiciones, este evento ocurrirá en $\le c(n-d)$ posiciones. Además, cuando $w_i \notin P_i(W)$ la probabilidad de que $w_i \in \mathcal{Z}_i$ se puede acotar como

$$p_i = \Pr\{w_i \in \mathcal{Z}_i | w_i \notin P_i(W)\} \le \frac{c-1}{q-c}. \tag{13}$$

Para $1 \le i \le n$, sea Y_i una variable aleatoria indicadora que vale 1 con probabilidad p_i y 0 con probabilidad $1 - p_i$. Entonces, para una palabra de un usuario inocente $\mathbf{w} \notin W$,

$$\begin{aligned}
&\Pr\Big\{\mathrm{s}(\mathbf{w}, \mathcal{Z}) \ge n\frac{1-\sigma}{c}\Big|\mathbf{w} \notin W\Big\} \\
&\quad\le \Pr\Big\{c(n-d) + \sum_{i=1}^{\substack{n-X-\\ c(n-d)}} Y_i \ge n\frac{1-\sigma}{c}\Big\} \\
&\quad\le \Pr\Big\{c(n-d) + \sum_{i=1}^{n} Y_i \ge n\frac{1-\sigma}{c}\Big\} \\
&\quad= \Pr\Big\{\sum_{i=1}^{n} Y_i \ge n\rho\Big\} \\
&\quad\stackrel{\text{(a)}}{\le} \Pr\Big\{Y \ge n\rho\Big\} \\
&\quad\le 2^{-nD(\rho\|\frac{c-1}{q-c})}.
\end{aligned}$$

La desigualdad (a) se deriva de Ec. 13, comparando la suma $\sum_{i=1}^n Y_i$ mediante una variable aleatoria binomial Y de parámetros n y $(c-1)/(q-c)$. Además, dado que $(c-1)/(q-c) < \rho$, condición derivada de la restricción en la distancia mínima del código externo, Ec. 9, aplicando la cota de Chernoff [19] de nuevo, obtenemos la última desigualdad.

Dado que hay q^k palabras, tanto en el código externo como en C_t, la probabilidad de acusar a un usuario inocente puede acotarse por

$$\begin{aligned}
&\Pr\Big\{\max_{\mathbf{w}\notin W} \mathrm{s}(\mathbf{w}, \mathcal{Z}) \ge n\frac{1-\sigma}{c}\Big\} \\
&\quad\le q^k \Pr\Big\{\mathrm{s}(\mathbf{w}, \mathcal{Z}) \ge n\frac{1-\sigma}{c}\Big|\mathbf{w} \notin W\Big\} \\
&\quad\le q^k 2^{-nD(\rho\|\frac{c-1}{q-c})}.
\end{aligned} \tag{14}$$

Recordemos que la probabilidad de identificar a un traidor real es Ec. 11. Poniendo estos dos resultados en conjunto tenemos que

$$p_e \leq q^k 2^{-nD(\rho\|\frac{c-1}{q-c})} + 2^{-nD(\sigma\|\varepsilon)}.$$

Además, los argumentos presentados sirven para demostrar que con probabilidad de error como máximo p_e ninguna palabra del código externo $\mathbf{w} \notin W$ estará dentro del radio de decodificación, Ec. 12.

Por último, mediante la relación biunívoca que existe entre las palabras de C_t y $C_{\rm ex}$, el algoritmo retorna las palabras de C_t asociadas a las palabras del código externo identificadas como pertenecientes a usuarios traidores. ■

La existencia de una familia de códigos de fingerprinting satisfaciendo las condiciones del Teorema 3 (con probabilidad de error decreciendo exponencialmente con la longitud del código) está garantizada mediante argumentos similares a los presentados en [16]. Utilizando códigos de Reed-Solomon como códigos externos obtenemos el siguiente resultado, que asume c fijado y q creciente.

Corolario 1: Sea $C_{\rm ex}$ un $[n,k]$-código de Reed-Solomon extendido sobre $\mathbb{F}_q$, de tasa $R_{\rm ex} = R(C_{\rm ex})$, y sea $C_{\rm in}$ un (l,q)-código ε-cuasi (c,c)-separable binario, de tasa $R_{\rm in} = R(C_{\rm in})$. Sea $\mathcal{F} = \{F_t\}$ la familia de la Construcción 1 con código externo $C_{\rm ex}$, código interno $C_{\rm in}$ y las biyecciones $(\phi_1^{(t)}, \ldots, \phi_n^{(t)})$, con $1 \leq t \leq (q!)^n$. Para $q > c^2$, $\varepsilon < \sigma < (q-c^2)/(q-c)$ y cualquier tasa

$$R_{\rm ex} < \frac{1-\sigma}{c(c+1)}, \tag{15}$$

la familia de códigos concatenados $\mathcal{F}$ junto con el Algoritmo de Identificación 1 es una familia c-segura de tasa

$$R = R_{\rm ex}\, R_{\rm in}$$

y con probabilidad de error p_e exponencialmente pequeña en la longitud del código,

$$p_e \leq 2^{-n\, l(\frac{1-\sigma}{c} R_{\rm in} - (c+1)R + o(1))} + 2^{-nD(\sigma\|\varepsilon)}.$$

Demostración: Si $C_{\rm ex}$ es un código de Reed-Solomon extendido de distancia mínima d, tenemos que $n = q$ y $1 - d/n = R_{\rm ex} - 1/n$. Por tanto, del Teorema 3,

$$\rho = \frac{1-\sigma}{c} - c\Big(R_{\rm ex} - \frac{1}{n}\Big). \tag{16}$$

La probabilidad de error, Ec. 10, puede expresarse como

$$\varepsilon \leq 2^{-n\, l\, R_{\rm in}((\log_2 q)^{-1} D(\rho\|\frac{c-1}{q-c}) - R_{\rm ex})} + 2^{-nD(\sigma\|\varepsilon)}.$$

La demostración concluye tras sustituir Ec. 16 en la ecuación anterior y teniendo en cuenta que

$$\lim_{q\to\infty} (\log_2 q)^{-1} D\Big(\rho \Big\| \frac{c-1}{q-c}\Big) = \rho$$

para c fijado y q creciente. ■

Además de códigos de Reed-Solomon, en [16] se presentan construcciones basadas en códigos algebro-geométricos como códigos externos. Como se ha comentado en la Sección III-C, reemplazar códigos separables ordinarios por códigos cuasi separables nos permite doblar la tasa asintótica de los códigos presentados en [16].

IV-C. Decodificación eficiente del código externo

Ya se ha comentado anteriormente que el paso más costoso del Algoritmo de Identificación 1 es la decodificación del código externo, en el paso 3, en el que se obtienen todas las palabras $\mathbf{w} \in C_{\rm ex}$ tales que

$$\mathrm{s}(\mathbf{w}, \mathcal{Z}) \geq n\frac{1-\sigma}{c}.$$

Habitualmente, esto significa establecer un radio de decodificación más allá de la capacidad correctora tradicional del código, $\lfloor (d(C_{\rm ex})-1)/2 \rfloor$, por lo que será necesario el uso de algoritmos de decodificación de lista. Nuestra motivación por el uso de un código de Reed-Solomon en el Corolario 1 es debido a que este paso puede realizarse de forma eficiente (en tiempo polinómico en la longitud del código) empleando los algoritmos de decodificación de lista de Guruswami-Sudan [20].

En esta sección mostraremos como el algoritmo de Koetter-Vardy [17], [18], que es una extensión del algoritmo de Guruswami-Sudan, nos ofrece una interfaz natural y apropiada para llevar a cabo nuestro propósito.

En primer lugar, describimos brevemente las condiciones de decodificación para el algoritmo de Koetter-Vardy aplicado a la decodificación en un canal ruidoso.

Sea $C_{\rm ex}$ un $[n,k]$-código de Reed-Solomon sobre $\mathbb{F}_q$, y sea $\alpha_1, \ldots, \alpha_q$ un orden arbitrario de los elementos de $\mathbb{F}_q$. Si se transmite la palabra código $\mathbf{w} = (w_1, \ldots, w_n) \in C_{\rm ex}$ y se recibe para cada posición i un conjunto de información de canal $X_1, \ldots, X_n$, el receptor es el encargado de utilizar esa información para calcular una matriz de dimensiones $q, \times n$ llamada *matriz de fiabilidad* $\mathcal{R} = (r_{ji})$, tal que

$$r_{ji} \stackrel{\rm def}{=} \Pr\{w_i = \alpha_j | X_i\}.$$

Es decir, $\mathcal{R}$ refleja cuán verosímil es el hecho de que el símbolo transmitido sea cada uno de los símbolos del alfabeto, dada la información recibida por el canal.

Sean $A = (a_{ji})$ y $B = (b_{ji})$ dos matrices de dimensiones $q \times n$. Definimos el producto

$$\langle A, B \rangle \stackrel{\rm def}{=} \sum_{j=1}^{q} \sum_{i=1}^{n} a_{ji} b_{ji}.$$

Además, una palabra $\mathbf{w} \in C_{\rm ex}$, la expresamos en forma matricial como

$$[\mathbf{w}]_{ji} \stackrel{\rm def}{=} \begin{cases} 1 & \text{si } w_i = \alpha_j, \\ 0 & \text{en otro caso.} \end{cases}$$

Con estas definiciones, la palabra $\mathbf{w} \in C_{\rm ex}$ será retornada en la lista de salida del algoritmo de Koetter-Vardy si se cumple la siguiente *condición de decodificación* [17], [18]:

$$\frac{\langle \mathcal{R}, [\mathbf{w}] \rangle}{\sqrt{\langle \mathcal{R}, \mathcal{R} \rangle}} \geq \sqrt{k-1}. \tag{17}$$

Por tanto, tenemos que construir una matriz de fiabilidad apropiada para garantizar que todas las palabras $\mathbf{w} \in C_{\rm ex}$ que satisfacen la condición del paso 3 del Algoritmo de Identificación 1 sean retornadas en a lista de salida del algoritmo de Koetter-Vardy. Observemos que para cada posición i, la única "información de canal" que tenemos en este caso es la de los conjuntos $\mathcal{Z}_i$. Además, sabemos que con alta probabilidad

$\mathcal{Z}_i$ contiene, como mínimo, uno de los símbolos de $\mathbf{w}$ en la posición i. Esto sugiere construir una matriz de fiabilidad $\mathcal{R} = (r_{ji})$ de la siguiente manera

$$r_{ji} = \begin{cases} \dfrac{1}{c} & \text{si } \alpha_j \in \mathcal{Z}_i, \\ 0 & \text{si } \alpha_j \notin \mathcal{Z}_i \text{ y } \mathcal{Z}_i \neq \emptyset, \\ \dfrac{1}{q} & \text{en otro caso.} \end{cases}$$

Es decir, en las posiciones en las que $\mathcal{Z}_i$ no está vacío, y tiene por tanto tamaño c, distribuimos el error (fiabilidad) equitativamente entre los elementos de $\mathcal{Z}_i$. En el resto de posiciones en las que $\mathcal{Z}_i$ está vacío no tenemos ningún tipo de "información de canal", y por tanto distribuimos el error equitativamente entre todos los símbolos del alfabeto.

Es rutinario comprobar que si $\mathbf{w} \in C_{\text{ex}}$ satisface la condición del paso 3 del Algoritmo de Identificación 1, entonces la condición de decodificación del algoritmo de Koetter-Vardy, Ec. 17, se traduce a

$$\frac{(n-n\sigma)\frac{1}{c}+n\sigma\frac{1}{q}}{\sqrt{(n-n\sigma)\frac{1}{c}+n\sigma\frac{1}{q}}} > \sqrt{\frac{n(1-\sigma)}{c^2}+\frac{n(c-1)}{c(q-c)}}. \qquad (18)$$

No es difícil ver que esta condición se cumple bajo las hipótesis que hemos supuesto en el Teorema 3 y en el Corolario 1, y por tanto $\mathbf{w}$ será retornada por el algoritmo de Koetter-Vardy.

En resumen, utilizando el algoritmo de Koetter-Vardy como parte central en el proceso de decodificación del código externo, el Algoritmo de Identificacion 1 se ejecuta en tiempo polinómico en la longitud del código.

V. CONCLUSIÓN

Los códigos cuasi separables son una versión relajada de los códigos separables ordinarios. Hemos utilizado el concepto de tipicalidad para obtener cotas asintóticas de existencia para estos códigos, empleando dos estrategias diferentes. En la primera, hemos considerado que todas las coaliciones típicas están separadas del resto de coaliciones disjuntas con alta probabilidad. En la segunda, hemos utilizado el hecho de que una coalición dada es típica con alta probabilidad para imponer que las coaliciones típicas estén sólo separadas del resto de coaliciones típicas disjuntas con alta probabilidad. Intuitivamente, obtenemos mejores resultados en este segundo caso, ya que la condición que imponemos es más débil.

Además, hemos presentado una comparación de los valores asintóticos de las tasas de los códigos cuasi separables, observando que estos valores doblan, aproximadamente, los valores que se obtienen para códigos separables ordinarios.

Nuestro objetivo en el estudio de los códigos cuasi separables es su aplicación al fingerprinting. Hemos presentado cómo los códigos cuasi separables pueden utilizarse para construir una familia de códigos de fingerprinting segura, con probabilidad de error exponencialmente pequeña en la longitud del código, y de mejor tasa que las construcciones obtenidas utilizando códigos separables ordinarios. Es importante recalcar que los términos de error introducidos por el hecho de que los códigos internos empleados no son completamente separables decrece también exponencialmente con la longitud del código.

Para concluir, hemos mostrado como el uso del algoritmo de Koetter-Vardy en el algoritmo de identificación que proponemos nos permite ejecutar dicho algoritmo de forma eficiente, en tiempo polinómico.

AGRADECIMIENTOS

J. Moreira y M. Fernández han sido financiados por el Gobierno de España mediante los proyectos CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES" y TEC2011-26491 "COPPI", y por la Generalitat de Catalunya mediante la ayuda 2009 SGR-1362.

G. Kabatiansky ha sido financiado por la Russian Foundation for Basic Research mediante las ayudas RFBR 13-07-00978 y RFBR 12-01-00905.

REFERENCIAS

[1] A. D. Friedman, R. L. Graham, and J. D. Ullman, "Universal single transition time asynchronous state assignments," *IEEE Trans. Comput.*, vol. C-18, no. 6, pp. 541–547, Jun. 1969.

[2] Y. L. Sagalovich, "Separating systems," *Probl. Inform. Transm.*, vol. 30, no. 2, pp. 105–123, 1994.

[3] M. S. Pinsker and Y. L. Sagalovich, "Lower bound on the cardinality of code of automata's states," *Probl. Inform. Transm.*, vol. 8, no. 3, pp. 59–66, 1972.

[4] Y. L. Sagalovich, "Completely separating systems," *Probl. Inform. Transm.*, vol. 18, no. 2, pp. 140–146, 1982.

[5] J. Körner and G. Simonyi, "Separating partition systems and locally different sequences," *SIAM J. Discr. Math. (SIDMA)*, vol. 1, no. 3, pp. 355–359, Aug. 1988.

[6] G. D. Cohen and H. G. Schaathun, "Asymptotic overview on separating codes," Department of Informatics, University of Bergen, Norway, Tech. Rep. 248, Aug. 2003.

[7] G. D. Cohen and H. G. Schaathun, "Upper bounds on separating codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1291–1294, Jun. 2004.

[8] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in *Proc. Int. Cryptol. Conf. (CRYPTO)*, ser. Lecture Notes Comput. Sci. (LNCS), vol. 963, Santa Barbara, CA, Aug. 1995, pp. 452–465.

[9] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1897–1905, Sep. 1998.

[10] B. Chor, A. Fiat, and M. Naor, "Tracing traitors," in *Proc. Int. Cryptol. Conf. (CRYPTO)*, ser. Lecture Notes Comput. Sci. (LNCS), vol. 839, Santa Barbara, CA, Aug. 1994, pp. 480–491.

[11] B. Chor, A. Fiat, M. Naor, and B. Pinkas, "Tracing traitors," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 893–910, May 2000.

[12] D. R. Stinson, T. van Trung, and R. Wei, "Secure frameproof codes, key distribution patterns, group testing algorithms and related structures," *J. Stat. Plan. Infer.*, vol. 86, no. 2, pp. 595–617, May 2000.

[13] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1042–1049, Mar. 2001.

[14] M. Fernández, G. Kabatiansky, and J. Moreira, "Almost separating and almost secure frameproof codes," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Saint Petersburg, Russia, Aug. 2011, pp. 2696–2700.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.

[16] A. Barg, G. R. Blakley, and G. Kabatiansky, "Digital fingerprinting codes: Problem statements, constructions, identification of traitors," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 852–865, Apr. 2003.

[17] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Sorrento, Italy, June 2000, p. 61.

[18] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2809–2825, Nov. 2003.

[19] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *J. Amer. Statist. Assoc.*, vol. 58, no. 301, pp. 13–30, Mar. 1963.

[20] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1757–1767, Sept. 1999.

Analysis of *relod.net*, a basic implementation of the RELOAD protocol for peer-to-peer networks

Marcos López Samaniego*, Isaias Martinez-Yelmo †, Roberto Gonzalez-Sanchez*

* Departamento de Ingeniería Telemática
Universidad Carlos III de Madrid
Avda. Universidad, 30. 28911 Leganés (Madrid). Spain
marcos.lopez@uc3m.es, rgonza1@it.uc3m.es

† Escuela Politécnica - Dpto. Automática
Universidad de Alcalá
Ctra. Madrid-Barcelona, km 33,600. 28871 Alcalá de Henares (Madrid). Spain
isaias.martinezy@uah.es

Abstract- **The P2PSIP Working Group is chartered to develop protocols and mechanisms for the use of SIP in distributed environments, thus minimizing the need for centralized servers. Under this premise, the RELOAD protocol was created, whose design was generalized to accept other applications with similar requirements, and which is currently in process of standardization by the IETF. In this paper, we present a basic implementation and an analysis of this protocol proposed standard, given the great interest displayed in recent years by the scientific and business community in issues related to peer-to-peer networks. Later, we conduct several experiments in order to validate its correct operation in real scenarios and provide feedback in relation with the current specification.**

Palabras Clave- **RELOAD, peer-to-peer, Chord**

I. INTRODUCTION

Peer-to-peer networks emerged last decade to make possible the replacement and recovery of resources over the Internet in a distributed way by creating overlay networks. Nevertheless, although peer-to-peer applications are popular nowadays, some open issues have not been addressed yet. One of the most challenging issues is the incompatibility between overlay algorithms, because their development was isolated. The Internet community is making some efforts to define mechanisms that allow the interoperability among different peer-to-peer networks. [1]

The P2PSIP Working Group is developing a protocol: RELOAD (acronym for REsource LOcation And Discovery), which allows the implementation of any peer-to-peer network, defining a common architecture and format. This protocol will become in the next months a new standard (RFC 6940) by the Internet Engineering Task Force (IETF), whose purpose is to provide support to applications that can work in distributed environments.

Even though it was linked to SIP from the beginning, RELOAD has not been developed only as a VoIP protocol, but rather its field of application has been extended so that it can be used by any other protocol with similar requirements.

This protocol acts by establishing an overlay network. Its modular design makes it possible to use it with any type of P2P network which is previously defined in the standard. A Chord algorithm is mandatory to implement.

In order to carry out the implementation, an object-oriented design based on a functional subset of the protocol was first carried out, and was then coded in such a way that the application can be easily modified and reused.

The structure of the paper is as follows. Section II presents the state of the art in relation with Pee-to-Peer networks. Later, section III introduces the main concepts of the RELOAD specification. Afterwards, section IV summarizes the main aspects of ***relod.net***. In section V, some results from our current implementation are shown to illustrate the operability of our design. Finally, a summary of our experiences and feedback from this work is provided in section VI. To conclude, conclusions can be found in section VI and future work in section VII.

II. STATE OF THE ART

A. Overlay peer-to-peer networks

A peer-to-peer (P2P) overlay network is a distributed collection of autonomous computers called *peers* that form a set of interconnections. These peers self-organize the overlay and have symmetric roles: they act as client and server simultaneously. Any peer can store objects, support queries and performs routing of messages [2].

These overlay networks have the following principles: self-organization, role symmetry, resource sharing, scalability, peer autonomy and resiliency [2].

There are three main types of P2P overlay networks:

1. Structured

Peers and, sometimes, resources are organized following specific criteria and algorithms, which lead to overlays with specific topologies and properties. They typically use distributed hash table-based (DHT) indexing [3]. This kind of networks is touted for their abilities to scale, tolerate failures, and self-manage, making them well-suited for Internet-scale distributed applications [4]. Some examples for DHT algorithms DHT are: CAN, Chord, Kademlia, or Pastry.

2. Unstructured

Unstructured peer to peer networks do not provide any algorithm for organization or optimization of network

connections. There are three models: the pure P2P systems or decentralized, like Gnutella and Freenet, the entire network consists solely of equipotent peers; there are no preferred nodes with any special infrastructure function. Hybrid peer-to-peer systems, like Kazaa, allow such infrastructure nodes to exist often called super nodes. Finally, centralized peer-to-peer systems, such as Napster, where a central server is used for indexing functions and to bootstrap the entire system. [3].

3. *Hierarchical*

A hierarchical overlay network is one in which several overlay networks of different types are connected to each other by means of another overlay network. This interconnection is usually performed by means of nodes known as super-peers, which are simultaneously part of two overlay networks. One example is H-P2PSIP [5].

III. RELOAD

A. *Introduction to the protocol*

The internet draft followed during design and implementation is *REsource LOcation And Discovery (RELOAD) Base Protocol draft-ietf-p2psip-base-26*, which expires on August 28, 2013 [6]. In this document the protocol is summarized as follows:

RELOAD is «a peer-to-peer (P2P) signaling protocol for use on the Internet. A P2P signaling protocol provides its clients with an abstract storage and messaging service between a set of cooperating peers that form the overlay network. RELOAD is designed to support a P2P Session Initiation Protocol (P2PSIP) network, but can be utilized by other applications with similar requirements by defining new usages that specify the kinds of data that needs to be stored for a particular application. RELOAD defines a security model based on a certificate enrollment service that provides unique identities. NAT traversal is a fundamental service of the protocol. RELOAD also allows access from "client" nodes that do not need to route traffic or store data for others.» [1]

B. *Basic concepts*

RELOAD is defined as a protocol for the application layer, the highest level of the TCP/IP protocol suite. As a transport level, it makes it possible to use the "secure" TLS (connection-oriented) or DTLS protocols (connectionless).

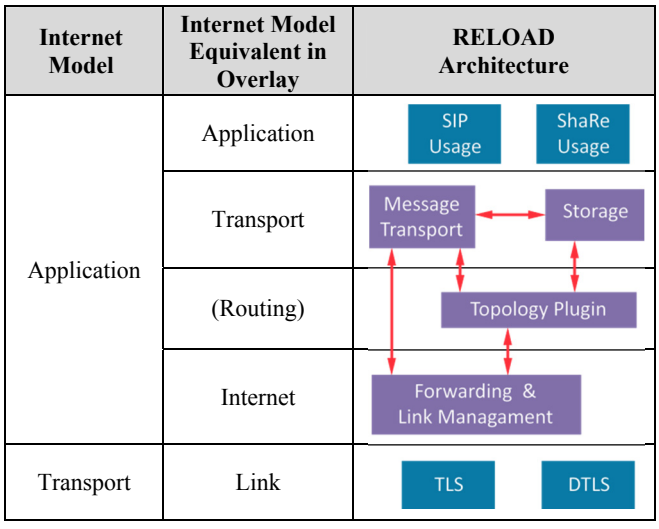


Fig. 1. RELOAD architecture.

This protocol forms basically an overlay network in which internet, transport, and application levels are redefined, as well as a new routing level.

It can work with structured and unstructured overlay networks, which work as genuinely exchangeable plugins. The Topology Plugin is the RELOAD module that provides this functionality

The RELOAD node identifier is the Node-ID. It is composed of a variable number of bits – 128 in Chord. The Resource-ID occupies the same space as Node-ID, and identifies the resources stored in the overlay.

Each node is responsible for those Resource-IDs which are equal to or lower than their own Node-ID, and which in turn are higher than the immediately previous Node-ID.

C. *Functional modules*

1. *Message Transport*

This layer is responsible for end-to-end message transactions. It communicates with the use layer and with the storage component, and must be able to deliver messages to the destination node, whether it is a Node-ID or a Resource-ID.

Likewise, in the opposite direction, when Message Transport receives a new message, it delivers it to the relevant module, depending on the message type.

2. *Storage*

One of the features of RELOAD is the fact that is not only a messaging network; it is also a storage network. The overlay nodes keep available data which the usage needs. The storage component is in charge of storing the data and returning it when requested.

A Node-ID will necessarily store the resources of which is responsible, but it will also be sent requests to store Resources-ID which another node is in charge of. In this way, replicated data can be stored throughout the entire overlay, and a certain degree of redundancy against a node failure exists.

The kind of data that can be stored by a node is known as their Kind and is identified by its Kind-ID, which is a 32-bit integer assigned by IANA (or else belonging to a private range). A Resource-ID can contain several Kind-IDs.

The model for the data that can be stored in a Kind-ID is known as a Data Model. In principle, three Data Models are considered, although future usages might define new models. The possible types to be stored can be: an individual value; an array, multiple values indexed by a number; or a dictionary, several values indexed by a key or String.

3. *Topology Plugin*

The Topology Plugin defines a generic structure on which several structured and unstructured peer-to-peer overlay algorithms can work. The functions of these plugins are basically defining the network topology and routing the messages through the nodes.

However, not any type of pre-existing algorithm can work, but rather different algorithms will be defined or redefined in the future so that they can work on RELOAD. The only plugin currently defined is Chord, a DHT algorithm, which has been slightly modified with respect to its original design so it can work on RELOAD. It must be possible to replace Chord by another algorithm without

affecting the rest of levels to continue to work without being modified in any way.

The topology plugin is responsible for the routing and connection table maintenance. The configuration of these tables depends on the algorithm in use. The Topology Plugin must be queried to make decisions about the packets routing.

4. Forwarding & Link Management

This layer communicates with the Topology Plugin to obtain connection tables and routes, and thus deliver the message to the following node. It is responsible for establishing connections with new nodes and passes through NAT and firewalls using ICE.

Forwarding & Link Management has access to the TCP/IP transport level, and is in charge of maintaining connections, so it is responsible for receiving overlay messages and place new packets on the network at the request of higher layers.

5. Link layer

Link provides an extra header known as the Framing Header (FH), which only makes sense in the context of the link and is removed at each hop.

On the one hand, when a reliable protocol (e.g.: TCP) is selected, it is used to frame messages and to provide timing. On the other hand, due to the unreliable nature of UDP, when DTLS is chosen at the link level of the overlay network, use of the Simple Reliability protocol is required. This protocol makes use of the Framing Header to provide congestion control and semi-reliability.

D. Basic fields

Unlike the Internet architecture, RELOAD levels do not define their own headers. Rather, there is a common message to all overlay network levels, which has three parts: Forwarding Header, Message Contents, and Security Block.

1. Forwarding Header

This header includes fields that identify the RELOAD protocol (RELO token), version, overlay name (e.g.: Chord-RELOAD), number of the sequence identifying the configuration file, TTL (time-to-life in number of hops), fragmentation, transaction identifier (a random number), maximum response length, routing addresses, and options.

Addresses include two fields. The first one is the DESTINATION LIST, an array of destination addresses. A message will be routed in strict order through the nodes that appear in the list.

The other relevant field is the VIA LIST, a second array where nodes are being crossed by the message in every hop are gradually added. When a node forwards a message, it places the peer that delivered the packet at the end of the VIA LIST.

RELOAD works with recursive symmetrical routing, which consists in the fact that, when a destination node receives a request which must be answered, it generates a DESTINATION LIST in the answering message, turning the VIA LIST around.

2. Message Contents

The fields in this block are the message code, the message body, and the extensions.

The message code is an integer that identifies the content of the message (Store, Fetch, Join, Leave…, and whether it is a request or an answer). Once identified, the message body is delivered to the responsible module (Storage, Topology…), which will decode it and generate an answer if required.

3. Security Block

This last block includes a number of certificates required to verify signatures (they can be of various types, e.g.: X.509), it specifies the hash and signature algorithms and, finally, includes the certificate hash and the value of the signature.

E. Usage layer

RELOAD cannot work by itself, it is designed to support a variety of applications. The usages that can be given to RELOAD are precisely known as *usages*. A usage defines how an application can store its information in the overlay; it may define its own data types, along with the rules for their use. One single application may require multiple usages.

A vast number of usages are being currently defined to work on RELOAD, in addition to SIP. Some of them are Distributed Conference Control (DisCo) [10], Shared Resources (ShaRe) [11], Constrained Application Protocol (CoAP) [12], Simple Network Management Protocol (SNMP) [13], Service Discovery [14], Public Switched Telephone Network (PSTN) Verification [15]…

F. Encapsulation example

Fig.-2 shows an example of how a Join Request packet is processed. Link layer delivers the message to Forwarding & Link Management but this module does not contribute with any header. Afterwards, it comes to Message Transport, which will be able to decode the structure. The Message Body field, which is opaque to Message Transport module, is delivered to the responsible layer: Topology Plugin in the case of a Join message. Header and Footer do not represent any particular field in the message, just the rest of the structure after and before Message Body.

G. Working diagram

It can be seen in fig.-3 how the different modules communicate with each other. This diagram of course does not represent all classes in detail; this is an extremely simplified scheme that represents how the implementation is designed, to validate RELOAD architecture in the standard.

Link, Forwarding & Link Management and Storage are symbolized by a single class, this class has in fact all the main code from these modules, but other secondary classes exist and are not represented in the diagram.

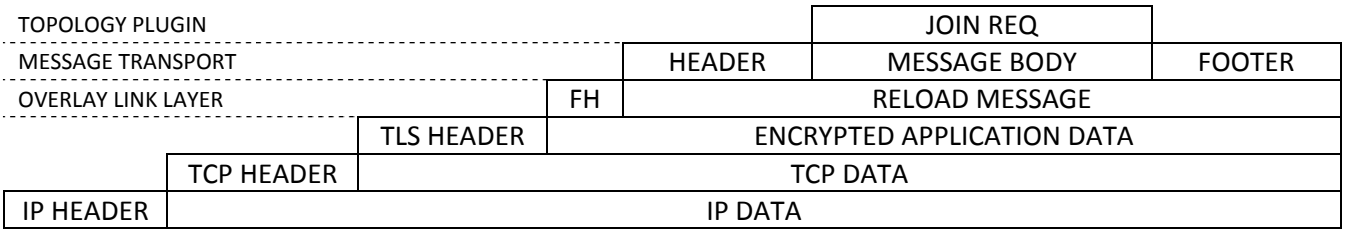


Fig. 2. Encapsulation example in RELOAD.

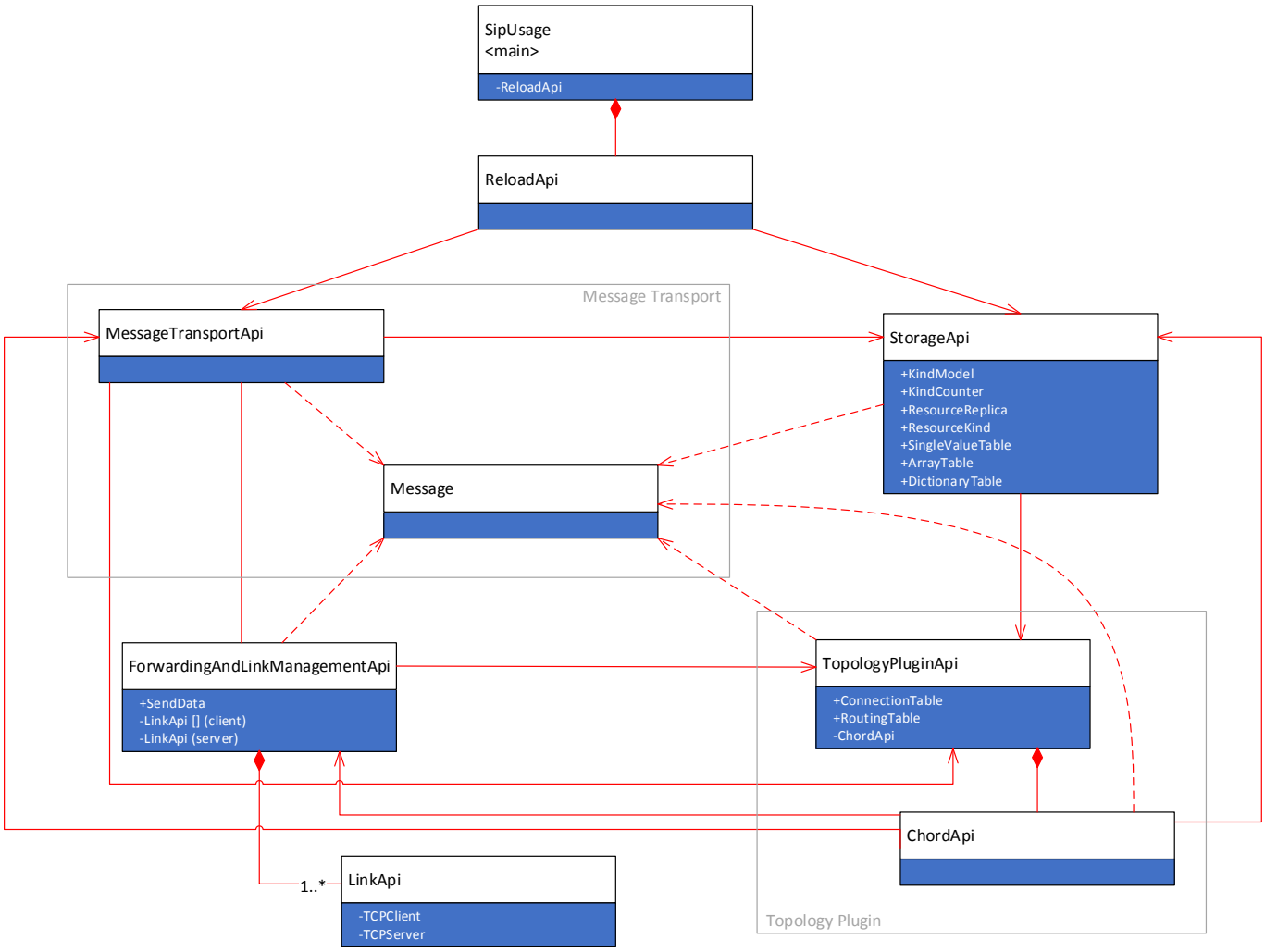


Fig. 3. UML Diagram.

By the other hand, Message Transport and Topology Plugin have two classes.

The Topology Plugin module will have an additional API-class for every algorithm implemented. While ChordApi has the code from Chord, the TopologyPluginApi is a standard API which has all the methods that can be called by the rest of the layers, thus, it is impossible for the other modules know the algorithm in use.

MessageTransportApi is the API for the Message module, which includes all the needed methods in this layer; while Message class is just an object containing the message structure in RELOAD, which will be instantiated by the most of the modules.

Finally, RelodApi and SipUsage are real classes, where any other usage can be implemented instead of SIP.

IV. Implementation

A. Introduction

Our work consists in an implementation and benchmark for RELOAD: ***relod.net***. Due the specification length, a subset with basic functionality is described here.

In addition, a reduced version of SIP has been implemented to check the operation of the entire system, taking as its base the existing draft: *A SIP Usage for RELOAD draft-ietf-p2psip-sip-09* [7].

The chosen programming language is Java. So far, no Java implementation of the protocol is known – only C and C++ implementations have been carried out and they are not publicly available yet. In addition to previous reasons, Java is chosen due to its object orientation and its multi-platform nature.

B. Code structure

There are seven main Java packages in each of the modules that form RELOAD: the link level, Forwarding and Link Management, Topology Plugin, Message Transport, Storage, one more for common classes to various modules, and finally, one for the specific packages of the usage in question, in this case SIP. In turn, these may contain more subpackages.

C. Design considerations

A modular design was developed, emphasizing the independence of the various layers in the overlay network.

Each package has a class, which is the Application Programming Interface (API) – they are the only means for access from other modules. This fact simplifies operation and ensures that, for example, all requests that can be made from the Storage module are addressed to the StorageApi class only. However, internally within each layer, there are no restrictions on how classes communicate with each other. This design makes possible for each module to be independent, retaining control over how some parts of the code communicate with others.

Likewise, there is a class that groups all protocol modules: ReloadApi. These APIs mask the complexity of each of the modules and the application itself.

The code seeks to make maximum use of Java's object orientation. Therefore, each structure defined in the draft is encoded in a different class. This implementation is innovative, since instead of using classic mechanisms such as parsers to encode and decode structures, a new procedure has been designed.

D. Object structure

Each structure is modeled as simple as possible: each one of the fields is encoded by means of an attribute, which may be a basic Java type or another structure (i.e. an object). Each structure usually has two builders: the first one, whose arguments are the same as the class attributes and whose assignation is thus trivial; and a second builder whose only argument is a byte array which also fills in the attributes after the structure is decoded.

The purpose of the first builder is to generate a message that will be delivered through the overlay, whereas the second builder is used when a packet is received from the network and we need to know its contents. Decoding is made recursively: each class decodes its structure and, if it contains attributes that are not primitive types, it calls the builders of those structures in turn. Coding is performed by calling the *getBytes()* method and it is also recursive.

V. Results

A. Testing environment

Several tests are documented here. Various aspects of the implementation are tested, such as the overlay registration – when they access the overlay for the first time –, storage, or the way in which they exchange routing information by means of Update messages.

A Peer-to-Peer overlay network forms with twelve peers is used in our tests. All peers are in the same LAN network or they are reachable through public IP addresses, NAT traversal support has not been implemented yet.

A number higher than ten is selected in order to be big enough in order to validate the behavior of routing tables based on fingers in Chord. Therefore, it will typically be one or two fingers, and some nodes will not be connected to each other, so messages must be routed through the overlay.

A basic implementation of SIP as usage [7] is being used in the tests, so when each node is registered its overlay location information is saved in the peer-to-peer network, so any overlay node participating in the peer-to-peer overlay can later retrieve it.

B. Basic operation sequence

Even though all the overlay nodes are only identified by their Resource-ID / Node-ID, their IP addresses are mentioned so that figures illustrating the text can be more easily understood. In this section, diagrams show the theorist working from the RFC and they can be compared to the real-application Wireshark captures.

1. Overlay registration (Fig.-4)

When a node accesses the overlay – Joining Peer (JP), with IP 192.168.1.15 –, it makes a connection to a Bootstrap Node (BN), whose IP address it previously knows, in this case: 192.168.1.70. This is the fifth node to initialize, so it contacts 4 other peers, which are added to the neighbor table.

Then an Attach message is sent to the relevant Resource-ID – its own Node-ID plus one –, which is routed via the bootstrap to its Admitting Peer (AP), whose IP address is 192.168.1.13.

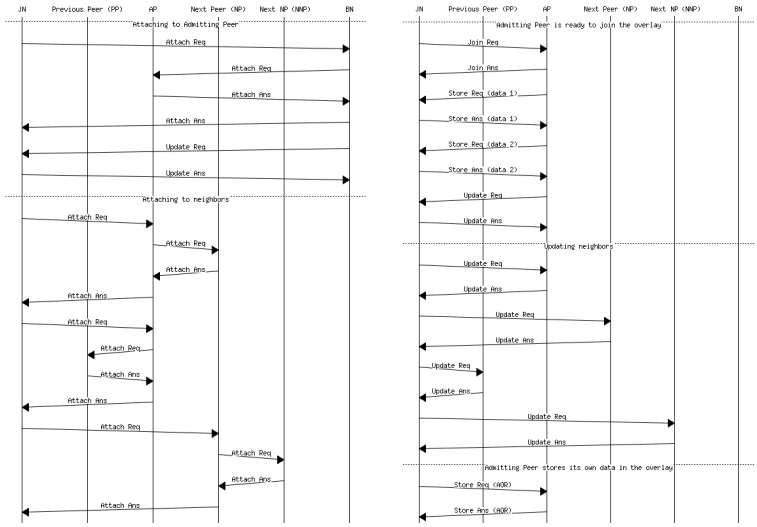
After receiving the Attach message, a direct connection is established between the Joining Peer and the Admitting Peer, direct messages are sent between these two nodes, and by this means the JP receives information about the AP's neighbors, which are also its own neighbors. It then sends an Attach message to the three other overlay nodes (two of which were routed through the AP), and, as it is now ready to become a part of the overlay, it sends a Join message to its Admitting Peer.

After this, the JP sends three Store messages in which it provides information about three Resource-IDs of which the AP will now be responsible. The JP then sends an Update to the AP, stating that it is now one more node in the overlay. The AP now sends Updates to its entire routing table to make it known that it is ready to route for them. Finally, SIP usage registered its Address Of Record (AOR) in the overlay by means of a Store message (the fact that the peer responsible for storing this information is the AP is coincidental, and any other peer in the overlay might have played this role).

2. Data procurement and remove (Fig.-5)

Once all the nodes have been initialized a mapping of an AOR in another AOR is stored in the overlay by sending a Store message and receiving the corresponding answer.

Then, a couple of queries for different AORs are made



Time	Source	Destination	Protocol	Length	Info
0.022979	192.168.1.15	192.168.1.70	RELOAD	1269	Attach Request
0.158876	192.168.1.70	192.168.1.15	RELOAD	1304	Attach Response
0.199647	192.168.1.13	192.168.1.15	RELOAD	1304	Update Request
0.255607	192.168.1.15	192.168.1.13	RELOAD	1246	Update Response
0.399271	192.168.1.15	192.168.1.13	RELOAD	1268	Attach Request
0.420789	192.168.1.13	192.168.1.15	RELOAD	1286	Attach Response
0.443881	192.168.1.15	192.168.1.13	RELOAD	1268	Attach Request
0.462110	192.168.1.13	192.168.1.15	RELOAD	1286	Attach Response
0.478593	192.168.1.15	192.168.1.14	RELOAD	1268	Attach Request
0.562027	192.168.1.14	192.168.1.15	RELOAD	1286	Attach Response
0.625787	192.168.1.15	192.168.1.13	RELOAD	1261	Join Request
0.643610	192.168.1.13	192.168.1.15	RELOAD	1245	Join Response
0.772796	192.168.1.13	192.168.1.15	RELOAD	1453	Store Request
0.786422	192.168.1.15	192.168.1.13	RELOAD	1261	Store Response
0.791981	192.168.1.13	192.168.1.15	RELOAD	1453	Store Request
0.797329	192.168.1.15	192.168.1.13	RELOAD	1261	Store Response
0.811386	192.168.1.13	192.168.1.15	RELOAD	1320	Update Request
0.844412	192.168.1.15	192.168.1.13	RELOAD	1246	Update Response
1.005322	192.168.1.15	192.168.1.13	RELOAD	1250	Update Request
1.011821	192.168.1.13	192.168.1.15	RELOAD	1246	Update Response
1.030923	192.168.1.15	192.168.1.14	RELOAD	1250	Update Request
1.040872	192.168.1.14	192.168.1.15	RELOAD	1246	Update Response
1.045741	192.168.1.15	192.168.1.12	RELOAD	1250	Update Request
1.053522	192.168.1.12	192.168.1.15	RELOAD	1246	Update Response
1.063275	192.168.1.15	192.168.1.70	RELOAD	1250	Update Request
1.112422	192.168.1.70	192.168.1.15	RELOAD	1250	Update Request
1.118390	192.168.1.15	192.168.1.70	RELOAD	1246	Update Response
1.123321	192.168.1.70	192.168.1.15	RELOAD	1246	Update Response
1.140494	192.168.1.15	192.168.1.13	RELOAD	1454	Store Request
1.166302	192.168.1.13	192.168.1.15	RELOAD	1311	Store Response

Fig. 4. Peer initialization messages.

Time	Source	Destination	Protocol	Length	Info
8.7396110	192.168.1.15	192.168.1.2	RELOAD	1350	Store Request
8.7410840	192.168.1.2	192.168.1.15	RELOAD	1261	Store Response
10.674067	192.168.1.15	192.168.1.13	RELOAD	1279	Fetch Request
10.691594	192.168.1.13	192.168.1.15	RELOAD	1471	Fetch Response
15.695138	192.168.1.15	192.168.1.16	RELOAD	1279	Fetch Request
15.706263	192.168.1.16	192.168.1.15	RELOAD	1453	Fetch Response
23.638374	192.168.1.15	192.168.1.13	RELOAD	1330	Store Request
23.655468	192.168.1.13	192.168.1.15	RELOAD	1297	Store Response

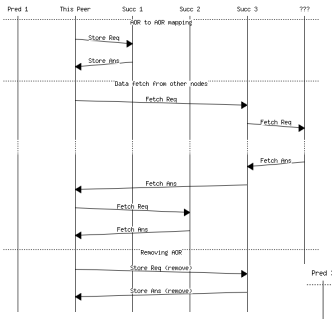
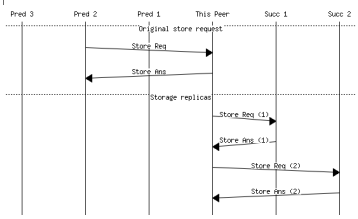


Fig. 5. Data storage and fetch.



Time	Source	Destination	Protocol	Length	Info
1.016677	192.168.1.1	192.168.1.15	RELOAD	1490	Store Request
1.024823	192.168.1.15	192.168.1.1	RELOAD	1329	Store Response
1.025991	192.168.1.15	192.168.1.2	RELOAD	1453	Store Request
1.029554	192.168.1.2	192.168.1.15	RELOAD	1261	Store Response
1.034978	192.168.1.15	192.168.1.16	RELOAD	1453	Store Request
1.043227	192.168.1.16	192.168.1.15	RELOAD	1261	Store Response

Fig. 6. Replica storage.

Fig. 7. Join Request message detail.

via the console. The Fetch requests and answers are shown, which, in this case, provide the Node-ID for the AOR in question. The answer to this Fetch message is shown on the screen via the console.

Finally, we remove our AOR, by means, as we will see, of a Store that crushes the stored information, as there is no specific message for removals.

3. *Replication (Fig.-6)*

Once our peer has become a part of the overlay, another one, whose IP address is 192.168.1.19, wishes to store its information in a Resource-ID that belongs to us.

Firstly, we receive a Store message, but it does not come from the expected node. This happens because, given that the overlay has many nodes, we are not the neighbor or the finger of the node generating the packet, so that the packet is routed through the overlay – in this case, with an intermediate hop, through the peer with IP address 192.168.1.1. Given that routing is symmetrical and recursive, the answer is returned to that same node.

This information must be replicated twice, so it is forwarded to our two first successors. Our immediate successor is the node with IP 192.168.1.2, so that the information is directly delivered. The next successor is 192.168.1.16, so it is delivered in the same way.

C. *Join traffic (Fig.-7)*

This screenshot shows the Join Request message in the previous section (*Overlay registration*). This picture is a detail of the eleventh packet in fig. 4.

The Forwarding Header shows the values mentioned above. The RELOAD version is $0x0A_{16} = 10_{10} = \mathbf{1.0}$. The message is sent to a Node-ID (the Admitting Peer), the message code is 15 (Join Request), and its only content is the Joining Peer's Node-ID.

D. *Fetch traffic (Fig.-8)*

The following packet to be analyzed is the first Fetch message in fig. 5, from *Data procurement and remove*, in the previous section.

It can be seen how, in the DESTINATION LIST FIELD, the destination is a Resource-ID, so the responsible Node-ID for that resource will receive the message. The message code is number 33 (Join Request), and the message body includes the Resource-ID again. It is a simple request that has only one Kind-ID (number 1: "SIP-REGISTRATION"). A GENERATION COUNTER of 0 specifies that it is an original (not replicated) message, and no dictionary keys are specified (*0 keys*), as SIP usage indicates that requests must be empty, so that all the values stored in that resource will be returned in the answer.

E. *Store traffic (Fig.-9)*

Finally, a Store Request from *Replication* will now be examined. The picture is a detail of the third packet in fig. 6, where a request to store some replicas was made.

Even though it is not shown due to space constraints, the destination of this message is a node, the Node-ID where we want to store the replicated message. The message code is 7 (Store Request), and in the content appears the Resource-ID where the original content is stored – a resource for which the node receiving this message is of course not responsible.

It can be seen that this is a "SIP-REGISTRATION" Kind-ID, the GENERATION COUNTER is 1, which means that this is a replicated message in the first successor, and that a single dictionary entry is stored, with one key and one value. SIP usage defines that the key is a node identifier where the person to be called can be located, while the value is a structure with additional SIP data.

VI. Analysis

A. Implementation performance

These values include the Java Virtual Machine resource consumption. This test was made on an Intel Core i7 950 Quad-core clocked at 3 GHz, on Microsoft Windows 7.

In a small network with 10 or 12 nodes running ***relod.net***, the CPU usage is at 2.1% maximum during the registration in the overlay, after this, the usage drops to a value very close to 0%. The RAM consumption is between 23.8 and 25.8 MB, peaking at the initialization.

B. Feedback and suggested improvements

1. Feedback

Generally speaking, the standard structure is complex. Just taking a look to it, it is not clear to which module messages belong, or how the layers are encapsulated. In this sense, other protocols such as P2PP are easier to understand, and even most of the documents published by the IETF published are less complex.

Further, some of the relationships between modules are not so obvious. In certain messages, such as a Ping Request, when a node receives a message in the link layer of the overlay network, it delivers the message to Forwarding, so that it decides whether it belongs to it or whether it must be forwarded to another node. To do so, it queries the Message Transport layer, as it is unable to understand the structure by itself, given that Forward has no associated header. After checking that the message belongs to it, it is finally sent to the higher layer, which is again Message Transport.

Message analyses the packet, checks that it is a Ping Request and that the responsible module is Forwarding, so the message body is delivered to this layer, which will be able to process its content. This module generates the answer, which will be sent through the opposite path.

It is obvious that it is not easy for such a relevant layer as Forwarding & Link Management not to have any associated header (it would be perfectly possible for it to have access to the data that would enable it to decide whether to forward the message or not). It is in no way understandable the fact that the Forwarding layer delivers a message to a higher layer, which immediately returns the message to this same Forwarding layer.

2. Suggested improvements

The RFC does not define a link layer proper in the overlay network. It merely specifies that the Link level can be TLS or DTLS but then, incoherently, it defines an extra header on that same level: Framing Header.

We suggest creating a new intermediate layer between TLS and Forwarding called “Link”, which would be responsible for the tasks assigned by the document: congestion control, semi-reliability, and timing.

C. Benefits

The creation of a standard protocol such as RELOAD can be regarded as a landmark in the history of the Internet. Its approach involves a shift from the current client-server model to a new model distributed between peers. It can be expected that businesses will tend to gradually assume this paradigm shift, due to the high costs of centralized servers.

This protocol is particularly significant due to the extensibility it allows, as is it not conceived for a specific protocol, but rather it allows multiple usages. It also stands out for its ease in adapting new protocols and turning them into RELOAD usages. Finally, it is highly flexible, as any type of peer-to-peer algorithm can be used.

Fig. 8. Fetch Request message detail.

Fig. 9. Store Request message detail.

This implementation was carried out to promote these features. Its extremely modular design makes it possible to create new topology plugins with no need to change the rest of the code, and even if the source code is missing, as each of the modules has an easily accessible API as a standard access from other modules.

In addition, a general class is given: ReloadApi, which provides a high-level API for the whole protocol. Any usage to be programmed on this implementation of RELOAD will only need to create a ReloadApi-type object and make calls to the methods in this class.

VII. Conclusions

This paper analyzes ***relod.net***, one of the first RELOAD implementations, protocol that will become peer-to-peer networks' new standard. However, it does not only represent a change when it comes to the creation of new software that works in a distributed way; its main challenge is the redefinition of widely accepted protocols by the industry, which once adapted, the Internet will gradually change from the client-server model into a new paradigm that will minimize the need of centralized servers.

This work aims to show how possible is to make a basic implementation of RELOAD extracting the main features of the standard, at the same time that it suggests a modular design that would even allow that two different modules encoded by different companies could work jointly.

To provide the interoperability, it's necessary to define certain APIs, which determine what calls are permitted from one module to another. Regarding this issue, it is especially important to reach agreement on the Topology Plugin module, and to set a standardized API as a way to ensure that future overlay algorithms can operate with existing implementations.

Therefore, we have published the Java API documentation and we have also decided to release the source code to the community, which is available in:

http://download.relod.net/

This application has been programmed through a whole year. The program consists of 11,000 code lines, which occupy a total of 554 kilobytes, stored in 163 Java classes, in 28 packages.

Although this is an *alpha* version that, due to their level of maturity, interoperability with other implementations cannot be guaranteed, we believe it could become a reference to other developers, for its proper design and simple code. In addition, the program will be updated while is being completed, until it becomes a fully functional application.

VIII. Future work

The first of our goals is to complete the missing parts, such as transversal NAT, security, and clients. It is also very important to focus on interoperability with other implementations: once the security module is completed, it will be possible to test it using other programmers' software.

The creation of a second algorithm that works jointly with Chord is proposed. No other peer-to-peer has currently been defined yet, so potential work might involve adapting an existing algorithm for usage on RELOAD. Designing a usage from scratch might be equally interesting, modifying an already existing protocol to work in distributed environments, or else designing a new one.

In the storage module, data are stored in RAM memory. This might suffice in many scenarios, but in others it might be preferable for data to be stored in a hard disk or a solid-state drive. For this reason, the use of databases is suggested.

Finally, it would be advisable to test the scalability of the implementation on a larger number of nodes using a network emulator such as ModelNet or PlanetLab. To ensure proper operation, the idea is to try different scenario setups with at least 1,000 peers.

Acknowledgments

This research was supported in part by the Comunidad de Madrid grant S-2009/TIC-1468 (MEDIANET project).

References

[1] Isaias Martinez-Yelmo, Roberto Gonzalez-Sanchez and Carmen Guerrero. "Validation of H-P2PSIP, a scalable solution for interoperability among different overlay networks". *Peer-To-Peer Networking and Applications*, vol. 6. no. 2, pp. 175-193, 2013.

[2] John F. Buford, Heather Yu and Eng Keong Lua, *P2P Networking and Applications*. Burlington, Massachusetts: Elsevier, 2008, pp. 29-31.

[3] D. Vivekanandreddy, Allamprabhu Vastrad and R. M. Nareshkumar, "Implementation of a novel optimized trust based search approach for the peer to peer (P2P) platform", *World Journal of Science and Technology*, vol. 2, no. 10, pp. 129-132, 2012.

[4] Tallat M. Shafaat, Ali Ghodsi and Seif Haridi, "Dealing with network partitions in structured overlay networks", *Peer-To-Peer Networking and Applications*, vol. 2. no. 4, pp. 334-347, 2009.

[5] Isaias Martinez-Yelmo, Alex Bikfalvi, Ruben Cuevas, Carmen Guerrero and Jaime Garcia. "H-P2PSIP: Interconnection of P2PSIP domains for Global Multimedia Services based on a Hierarchical DHT Overlay Network". *Computer Networks: The International Journal of Computer and Telecommunications Networking*. vol. 53 no. 4, pp. 556-568, 2009.

[6] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset and H. Schulzrinne, *REsource LOcation And Discovery (RELOAD) Base Protocol draft-ietf-p2psip-base-26*, February 24, 2013. [Online]. Available: http://tools.ietf.org/html/draft-ietf-p2psip-base-26

[7] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset and H. Schulzrinne, *A SIP Usage for RELOAD draft-ietf-p2psip-sip-09*, February 25, 2013. [Online]. Available: http://tools.ietf.org/html/draft-ietf-p2psip-sip-09

[10] A. Knauf, G. Hege and M. Waehlisch, *A RELOAD Usage for Distributed Conference Control (DisCo) draft-ietf-p2psip-disco-00*. October 9, 2012. [Online]. Available: http://tools.ietf.org/html/draft-ietf-p2psip-disco-00

[11] A. Knauf, T C. Schmidt, G. Hege and M. Waehlisch, *A Usage for Shared Resources in RELOAD (ShaRe) draft-ietf-p2psip-share-01*. February 24, 2013. [Online]. Available: http://tools.ietf.org/html/draft-ietf-p2psip-share-01

[12] J. Jimenez, J. Lopez-Vega, J. Maenpaa and G. Camarillo, A Constrained Application Protocol (CoAP) *Usage for REsource Location And Discovery (RELOAD) draft-jimenez-p2psip-coap-reload-03*. February 18, 2013. [Online]. Available: http://tools.ietf.org/html/draft-jimenez-p2psip-coap-reload-03

[13] Y. Peng, W. Wang, Z. Hao and Y. Meng, *An SNMP Usage for RELOAD draft-peng-p2psip-snmp-05*. October 18, 2012. [Online]. Available: http://tools.ietf.org/html/draft-peng-p2psip-snmp-05

[14] J. Maenpaa and G. Camarillo, *Service Discovery Usage for REsource LOcation And Discovery (RELOAD) draft-ietf-p2psip-service-discovery-08*. February 23, 2013. [Online]. Available: http://tools.ietf.org/html/draft-ietf-p2psip-service-discovery-08

[15] M. Petit-Huguenin, J. Rosenberg and C. Jennings, *A Usage of Resource Location and Discovery (RELOAD) for Public Switched Telephone Network (PSTN) Verification draft-petithuguenin-vipr-reload-usage-04*. March 12, 2012. [Online]. Available: http://tools.ietf.org/html/draft-petithuguenin-vipr-reload-usage-04

Protocolo S-ALOHA multi-ranura con disciplinas de servicio *FIFO-Blocking* y *LIFO-Pushout*

Vicente Casares Giner, Víctor Sempere Payá, David Todolí Ferrandis
Departamento de Comunicaciones,
Universidad Politécnica de Valencia
Camino de Vera, S/N, 46022 Valencia.
vcasares@dcom.upv.es, vsempere@dcom.upv.es, datofer@upv.es

***Resumen*—El presente artículo considera el protocolo S-ALOHA multi-ranura para un número finito de terminales. De forma independiente, cada terminal genera paquetes de datos, acorde con un proceso de Bernoulli. La duración de una multi-ranura temporal o trama, equivale a la duración de un número entero V de ranuras. El tiempo de transmisión de un paquete es igual a la duración de una ranura. Cada terminal dispone de una cola de espera de capacidad unitaria. Se han estudian los parámetros de caudal y retardo en los casos de disciplinas de servicio FIFO-BL y LIFO-PO. En concreto, se han obtenido las funciones de distribución de probabilidades para los tiempos de estancia de los paquetes de datos en contienda, tanto los transmitidos con éxito como los perdidos. El análisis se ha llevado a cabo mediante herramientas de Markov. Se sugiere el escenario de redes de sensores inalámbricos, WSN, como idóneo para la aplicabilidad de la propuesta.**

***Palabras Clave*—S-ALOHA, FIFO-BL, LIFO-PO, WSN.**

I. INTRODUCCIÓN

Cuando dos o más terminales desean compartir un canal de radio, el acceso aleatorio con mínima coordinación entre ellos ha sido la solución más comúnmente implementada. Soluciones pioneras que marcaron el origen de los protocolos de acceso aleatorio son el protocolo ALOHA [1] y posteriormente su versión ranurada, S-ALOHA [2]. Desde entonces, los estudios sobre el caudal y retardo así como la estabilidad de tales protocolos han proliferado en la literatura abierta [3]. Aun teniendo en cuenta los grandes avances en el conocimiento y propuestas de mejora de tales protocolos, el esquema básico del protocolo S-ALOHA sigue estando implementado en muchos sistemas inalámbricos. Tal es el caso del sistema GSM (2G) y de generaciones posteriores, en los cuales los terminales hacen uso del protocolo S-ALOHA para contactar por primera vez con la red fija [4].

Hemos considerado el protocolo S-ALOHA multi-ranura temporal según muestra la Fig. 1, [5]. Según se comenta en [6] varias son las razones que invitan a considerar el S-ALOHA multi-ranura en lugar del S-ALOHA estándar. Por ejemplo, puede ser conveniente enviar los ACKs (del Inglés *acknowledgments*) periódicamente (uno por trama) en lugar de uno al final de cada ranura. También, S-ALOHA multi-ranura posibilita el reparto por grupo de las V ranuras, implementando una asignación en proporción al tamaño de los grupos.

En el presente trabajo revisamos el protocolo S-ALOHA multi-ranura para un número finito de terminales, disponiendo cada uno de ellos de una cola de espera de tamaño unitario. Se aportan varios resultados. En primer lugar ofrecemos una formulación recurrente para las probabilidades de ranura vacía, de ranura con un único paquete (éxito) y de ranura con más de un paquete de datos (colisión). En segundo lugar, y para las disciplinas de servicio FIFO (*First-in first-out*) y LIFO (*Last-in first-out*), obtenemos las distribuciones de los tiempos de residencia para los paquetes con transmisión exitosa y para los paquetes que finalmente se descartan.

La estructura del trabajo es como sigue. Tras la presente breve introducción, en la sección II se modela el sistema en estudio mediante herramientas de Markov. En la sección III abordamos la caracterización de las distribuciones de los tiempos de residencia o estancia de los paquetes con transmisión exitosa y de los paquetes perdidos. En la sección IV se ilustran y comentas algunos resultados. Finalmente, las conclusiones se reportan en la sección V.

II. MODELO DE SISTEMA

Se considera un número finito de M terminales o fuentes que acceden a una única portadora de radio TDMA (*Time Division Multipole Access*) según se muestra en la Fig. 1. La portadora está estructurada en tramas de V ranuras por trama. Cada terminal genera paquetes de datos según el modelo de Bernoulli. En concreto, en cada ranura temporal se genera un paquete con probabilidad p_{act} y con probabilidad $1 - p_{act}$ no se genera paquete alguno. Cada terminal dispone de una cola de espera de capacidad unitaria, de manera que en cada instante de tiempo únicamente puede gestionar un sólo paquete de datos. A la llegada de un paquete, éste ocupa la única posición de la cola si se encuentra vacía. Caso contrario consideraremos dos situaciones, FIFO-BL (*FIFO – Blocking* y LIFO-PO (*LIFO – Pushout*) [7]. En el primer caso, el paquete se descarta y en el caso LIFO-PO el nuevo paquete desplaza o expulsa al paquete ya existente en la cola.

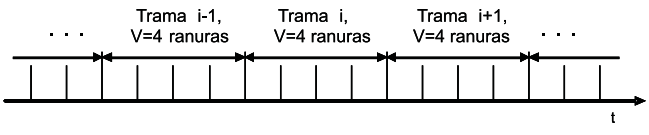


Fig. 1. Estructura de la trama de acceso: $V = 4$ ranuras por trama.

Acorde con la Fig. 1 se ha definido una trama como el conjunto de V ranuras consecutivas. Entonces, para una fuente o terminal cualquiera, la probabilidad de que al menos haya generado un paquete durante una trama, viene dada por $a = 1 - (1 - p_{act})^V$. El protocolo de acceso opera como sigue. Supongamos que al comienzo de una trama, tenemos i paquetes en espera, en sus respectivas colas. Con probabilidad r elegirán si intentan acceder en la citada trama. La probabilidad de permiso r podría ser estimada por un control centralizado y transferida a los terminales mediante *broadcast* [8]. Entonces, la probabilidad de que j paquetes $(0 \leq j \leq i)$ obtengan permiso para intentar acceder viene dada por la distribución binomial, la cual denotamos por $B(i, j, r)$, Eq. (42). El acceso de los j paquetes a las V ranuras se lleva a cabo según [5] - [6], esto es, cada uno de los j terminales que ha obtenido permiso para acceder, con probabilidad $1/V$ elegirá una de las V ranuras de la trama. Sea $S(j, k, V)$ la probabilidad de que k paquetes de entre j, consigan finalmente acceder, $(0 \leq k \leq j)$, Eq. (45)-(46). Conjuntemos las dos acciones anteriores y denotemos por $D_k^i(V, r)$ la probabilidad de que k paquetes de un total de i paquetes accedan en la trama de V ranuras. $D_k^i(V, r)$ es

$$D_k^i(V,r) = \sum_{j=k}^{i} B(i,j,r)S(j,k,V), \quad i \geq j \geq k. \tag{1}$$

En lo sucesivo, agilizaremos la notación, empleando D_k^i en lugar de $D_k^i(V, r)$ (D_k^i de *Departure*).

Es claro que podemos definir una cadena de Markov en los instantes de comienzo de las tramas. Sea $P_{i,j}$ la probabilidad condicionada a que teniendo i paquetes de datos prestos para el acceso al inicio de una trama, al inicio de la siguiente trama tengamos j paquetes disponibles para acceder. $P_{i,j}$ viene dada por:

$$\begin{aligned} P_{i,j} &= \sum_{k=\min(0,i-j)}^{i} D_k^i A(M-i+k, j-i+k, a) \\ 0 &\leq i,j \leq M. \end{aligned} \tag{2}$$

en donde $A(m, n, a)$, del inglés *Arrival*, se rige por una distribución binomial y tiene en cuenta la probabilidad de que en una trama de V ranuras, se ofrezcan n paquetes de un total de m terminales. Obsérvese que, para una fuente dada, la probabilidad de que genere al menos un paquete por trama $a = 1 - (1 - p_{act})^V$ aumenta con V para una p_{act} fija, lo cual parece razonable. Si una fuente dada genera más de un paquete por trama, a efectos de posible ocupación de la cola unitaria sólo se considera un paquete, descartándose el resto.

Denotemos por $\boldsymbol{P} = \{P_{i,j}\}$ la matriz estocástica correspondiente. El vector estocástico de probabilidades en régimen permanente, $\boldsymbol{\pi} = [\pi_0, \pi_1, ..., \pi_M]$, se obtiene al resolver

$$\boldsymbol{\pi} = \boldsymbol{\pi}\boldsymbol{P} \tag{3}$$

con la correspondiente normalización de $\boldsymbol{\pi}\boldsymbol{e} = 1$, siendo $\boldsymbol{e}$ un vector columna de adecuadas dimensiones con todos sus elementos iguales a 1. La componente π_i indica la probabilidad de encontrar i paquetes de datos al comienzo de una trama.

III. SISTEMA OBSERVADO POR UN PAQUETE DE DATOS AL AZAR

En esta sección observaremos un paquete de datos al azar, *nuestro paquete*, que se ofrece al sistema. Se analiza la probabilidad de pérdida o rechazo y, en el caso de ser admitido, la distribución del tiempo de espera previo a ser transmitido con éxito. El estudio se ha conducido para las dos políticas de admisión FIFO-BL y LIFO-PO. Para tal fin, se hará uso de la propiedad BASTA (*Bernoulli Arrivals See Time Averages*), equivalente en tiempo discreto a la propiedad PASTA (*Poisson Arrivals See Time Averages*) en tiempo continuo para llegadas según Poisson.

Por lo tanto, haciendo uso de la propiedad BASTA, cuando nuestro paquete en observación se ofrece al sistema, encontrará k paquetes con probabilidad π_k, según (3) dada por $\boldsymbol{\pi} = [\pi_0, \pi_1, ..., \pi_k, ...\pi_M]$. Entonces, fijado k, podemos diferenciar tres casos disjuntos que integran todo el espacio muestral:

Caso A: Con probabilidad $(M - k)/M$ nuestro paquete encuentra su cola vacía; esto es, es admitido con probabilidad:

$$P_A(M,k) = \frac{M-k}{M} \tag{4}$$

Nuestro paquete permanecerá en su cola hasta que sea transmitido de forma exitosa (disciplina FIFO-BL) o bien hasta que sea desplazado por otro con llegada posterior procedente del mismo terminal (disciplina LIFO-PO).

Caso B: Con probabilidad k/M nuestro paquete encuentra su cola ocupada por otro paquete de datos de su propia fuente, un paquete predecesor al nuestro. Pero si de entre el total de k paquetes encontrados en competición, l han sido transmitidos con éxito y el paquete predecesor se encuentra entre ellos -lo cual sucederá con probabilidad l/k-, la salida del sistema del paquete predecesor es inminente por lo que nuestro paquete será admitido. Por lo tanto, la probabilidad de este suceso es:

$$P_B(M,k,l) = \frac{k}{M}\frac{l}{k}D_l^k = \frac{l}{M}D_l^k \tag{5}$$

Al igual que en el caso A, nuestro paquete permanecerá en su cola hasta que sea transmitido de forma exitosa (disciplina FIFO-BL) o bien hasta que sea desplazado por otro con llegada posterior procedente de la misma fuente o terminal (disciplina LIFO-PO).

Caso C: Complementa el caso anterior. Con probabilidad k/M nuestro paquete encuentra en su cola un paquete de su propia fuente, un paquete predecesor al nuestro, pero tal paquete sigue a la espera de ser transmitido con éxito. Este caso sucede con probabilidad:

$$P_C(M,k,l) = \frac{k}{M}\frac{k-l}{k}D_l^k = \frac{k-l}{M}D_l^k \tag{6}$$

Entonces, nuestro paquete será rechazado, si implementamos la disciplina FIFO-BL o reemplazará al paquete que le precedió en la llegada, si usamos la disciplina LIFO-PO.

Para la disciplina FIFO-BL, de los razonamientos anteriores podemos derivar la probabilidad de que nuestro paquete sea admitido, para más pronto o más tarde alcanzar un acceso exitoso con probabilidad dada por

$$P_{AF} = \sum_{k=0}^{M} \left[P_A(M,k) + \sum_{l=0}^{k}(P_B(M,k,l)\right]\pi_k \qquad (7)$$

En (7) se asume que el paquete en espera no abandona la cola, que hay impaciencia nula. Por otra parte, la probabilidad de rechazar un paquete en disciplina FIFO-BL resulta ser:

$$P_{RF} = \sum_{k=0}^{M}\sum_{l=0}^{k}(P_C(M,k,l)\pi_k \qquad (8)$$

Evidentemente, de (4), (5) y (6), o alternativamente de (7) y de (8) tenemos que $P_{AF} + P_{RF} = 1$.

A partir de los anteriores resultados, se pueden derivar algunos valores medios. Por ejemplo, de nuevo teniendo en mente la disciplina FIFO-BL, denotemos por Mn_{RF} el número medio de paquetes que, procedentes del terminal en observación, son rechazados durante el período de espera de *nuestro paquete* en cola. Obviamente, P_{AF} y Mn_{RF} satisfacen la relación:

$$P_{AF} = \frac{1}{Mn_{RF}+1}; \quad \rightarrow Mn_{RF} = \frac{1}{P_{AF}} - 1 \qquad (9)$$

A partir de (9) el valor medio de la estancia en cola de nuestro paquete, Mv_F, se deriva en base a las siguientes consideraciones. En primer lugar, se sabe que la distancia temporal medida en tramas (que no en ranuras), entre dos paquetes consecutivos ofrecidos desde cualquier terminal sigue una ley geométrica de valor medio $1/a$. En segundo lugar, teniendo en cuenta que si otro paquete de la misma fuente o terminal se ofrece al sistema justo en la trama de transmisión exitosa de *nuestro paquete*, la última de su espera, tal paquete es admitido por el sistema. En consecuencia Mv_F puede expresarse como:

$$Mv_F = \frac{Mn_{RF}}{a} + 1 \qquad (10)$$

En referencia a LIFO-PO, la propia disciplina indica que todos los paquetes de nuestro terminal en observación son inicialmente admitidos. Unos serán desplazados por otros con instantes de llegada posterior, otros finalmente serán transmitidos con éxito. Las respectivas probabilidades, denotadas por P_{RL} y P_{AL} se calculan en la siguiente sección y obviamente han de coincidir, y coinciden, con las del caso FIFO-BL esto es $P_{RL} = P_{RF}$ y $P_{AL} = P_{AF}$. Ello en base a la evidencia de que el comportamiento del protocolo y por consiguiente el caudal del sistema, no dependen de la disciplina FIFO-BL o LIFO-PO implementada. Igualmente, el número medio de paquetes desplazados previo a la transmisión exitosa de nuestro paquete, Mn_{RL}, debe de coincidir, y coincide, con Mn_{RF}, esto es, $Mn_{RL} = Mn_{RF}$.

En las siguientes líneas derivamos otros valores medios y además se obtienen expresiones cerradas para las distribuciones de los tiempos de estancia en los dos casos en estudio; tanto para los paquetes con transmisión exitosa (disciplinas FIFO-BL y LIFO-PO) como para los paquetes que habiendo sido admitidos a su llegada, finalmente son desplazado por otros con instantes de llegada posterior (disciplina LIFO-PO).

A. Distribuciones temporales en disciplinas FIFO-BL y LIFO-PO

Para cada una de las disciplinas, FIFO-BL y LIFO-PO, a continuación, deduciremos las distribuciones de los tiempos de espera de un paquete de datos elegido al azar, *nuestro paquete*. Son distribuciones del tipo PH (*Phase type distributions*) representada por $(\boldsymbol{\alpha}, \boldsymbol{T})$, [9], [10], en donde $\boldsymbol{\alpha}$ es el vector de probabilidades inicial, $\boldsymbol{T}$ es la matriz de probabilidades de transición entre estados transitorios, $\boldsymbol{T}^0 = \boldsymbol{e} - \boldsymbol{T}\boldsymbol{e}$ es el vector columna de probabilidades de transición hacia el estado absorbente y $\mathbf{e}$ es un vector columna definido con anterioridad, tras la Eq. (3). Para FIFO-BL y LIFO-PO identificamos, respectivamente $(\boldsymbol{\alpha}_F, \boldsymbol{T}_F)$, $\boldsymbol{T}_F^0$ y $(\boldsymbol{\alpha}_L, \boldsymbol{T}_L)$, $\boldsymbol{T}_L^0$.

1) Estados iniciales en disciplinas FIFO-BL y LIFO-PO: En el caso FIFO-BL, tras ser admitido por el sistema, casos A y B, *nuestro paquete* competirá en el acceso, junto con otros paquetes. Para saber el número de paquetes que inicial y conjuntamente van a competir, hemos de tener en cuenta tanto los paquetes que siguen pendientes de ser transmitidos como los paquetes que han llegado al sistema a la vez con el nuestro. Consideremos los casos factibles A y B:

Caso A: La probabilidad de que nuestro paquete compita por primera vez junto con otros j paquetes ($j = 0, 1, \ldots, M' = M-1$) viene dada por, ver Ec. (4),

$$P_{A-F}(M,k,j) = P_A(M,k) \sum_{l=\max(0,k-j)}^{k} D_l^k A(M'-k+l, j-k+l, a) \qquad (11)$$

Caso B: La probabilidad de que nuestro paquete compita por primera vez junto con otros j paquetes ($j = 0, 1, \ldots, M' = M-1$) viene dada por, ver Ec. (5),

$$P_{B-F}(M,k,j) = \sum_{l=\max(0,k-j)}^{k} P_B(M,k,l)A(M'-k+l, j-k+l, a) \qquad (12)$$

De (11) y (12) tenemos que la probabilidad de que *nuestro paquete* inicialmante compita junto con otros j paquetes resulta ser, tras la ponderación con las probabilidades π_k de (3) -propiedad BASTA-:

$$\alpha_{F;j} = \sum_{k=0}^{M}(P_{A-F}(M,k,j) + P_{B-F}(M,k,j))\pi_k \qquad (13)$$

y en notación vectorial

$$\boldsymbol{\alpha}_F = \left[\begin{array}{cccc} \alpha_{F;0}, & \alpha_{F;1}, & \ldots, & \alpha_{F;M'} \end{array} \right] \tag{14}$$

$\alpha_{F;M} = 1 - \boldsymbol{\alpha}_F \boldsymbol{e}$ es la probabilidad de bloqueo, coincidente con la probabilidad de que, en terminología de la distribución PH, el sistema inicialmente se encuentre en el estado absorbente[1]. En concreto

$$\boldsymbol{\alpha}_F \boldsymbol{e} = P_{AF} = 1 - P_{RF} \tag{15}$$

Para el vector inicial en disciplina LIFO-PO, es claro que cualquier paquete es inicialmente admitido. Tal paquete, a veces desplaza a un paquete existente en cola, y que originado en la misma fuente precedió al nuestro. Ello sucederá con probabilidad P_{RF}, caso C. En otras ocasiones, casos A y B, no hay desplazamiento alguno. En otras palabras, además de considerar los casos A y B, hemos de incluir el caso C que tiene en cuenta los desplazamientos. Por lo tanto, de (6):

$$P_{C-L}(M,k,j) = \sum_{l=\max(0,k-j)}^{k} P_C(M,k,l) A(M'-k+l, j-k+l, a) \tag{16}$$

Así que, en disciplina LIFO-PO, la probabilidad de que *nuestro paquete* compita por primera vez junto con otros j paquetes $\alpha_{L;j}$, resulta ser,

$$\alpha_{C;j} = \sum_{k=0}^{M} P_{C-L}(M,k,j)) \pi_k \tag{17}$$

$$\alpha_{L;j} = \alpha_{F;j} + \alpha_{C;j} \tag{18}$$

y en notación vectorial

$$\boldsymbol{\alpha}_C = \left[\begin{array}{cccc} \alpha_{C;0}, & \alpha_{C;1}, & \ldots, & \alpha_{C;M'} \end{array} \right] \tag{19}$$

$$\boldsymbol{\alpha}_L = \boldsymbol{\alpha}_F + \boldsymbol{\alpha}_C \tag{20}$$

Conviene observar que, mientras el vector $\boldsymbol{\alpha}_F$, Ec. (14) es un vector sub-estocástico, $\boldsymbol{\alpha}_F \boldsymbol{e} < 1$, el vector $\boldsymbol{\alpha}_L$ en (20) es de por sí un vector estocástico, $\boldsymbol{\alpha}_L \boldsymbol{e} = \boldsymbol{\alpha}_F \boldsymbol{e} + \boldsymbol{\alpha}_C \boldsymbol{e} = 1$.

[1]Identificamos como estados transitorios el $0, 1, 2 \ldots M'$ y como absorbente el estado $M = M' + 1$

Obviamente, en congruencia con la situación del *Caso C* tenemos que

$$\boldsymbol{\alpha}_C \boldsymbol{e} = 1 - \boldsymbol{\alpha}_F \boldsymbol{e} = \alpha_{F;M} = P_{RF} = 1 - P_{AF} \tag{21}$$

2) Matrices $\boldsymbol{T}$ y $\boldsymbol{T}^0$ en disciplinas FIFO-BL y LIFO-PO: En disciplina FIFO-BL, supongamos que tras la incorporación al sistema, nuestro paquete compite en una trama dada de V ranuras junto con otros i paquetes. Si *nuestro paquete* colisiona con otro(s) intentará de nuevo el acceso en la siguiente trama. Además de la probabilidad de colisión, hay que considera la llegada de nuevos paquetes durante el período de una trama. En definitiva, condicionado a que nuestro paquete compite con otros i paquetes, la probabilidad de colisión y de que en la siguiente trama nuestro paquete compita en el acceso junto con otros j paquete, $j = 0, 1, \ldots, M' = M - 1$ viene dada por

$$T_{F;i,j} = \sum_{k=\max(0,i-j)}^{i} (1 - \frac{k}{i+1}) D_k^{i+1} A_{k-i+j}^{M-i-1+k} \tag{22}$$

en donde $A_n^m = B(m,n,a)$ es, acorde con el modelo de Bernoulli, la probabilidad de que m terminales o fuentes generen n paquetes de datos durante la actual trama de V ranuras. Recuérdese que dado un terminal, éste puede generar hasta un máximo de V paquetes por tramas y sólo uno de ellos es ofrecido al sistema.

Por otra parte, nuestro paquete no sufrirá colisión alguna -acceso exitoso- con probabilidad, $T_{F;i}^0$, dada por:

$$T_{F;i}^0 = \sum_{k=1}^{i+1} \frac{k}{i+1} D_k^{i+1} \tag{23}$$

En notación matricial las expresiones de $\boldsymbol{T}_F$ y $\boldsymbol{T}_F^0$ figuran en, respectivamente (24) y (25).

$$\boldsymbol{T}_F^0 = \left[\begin{array}{ccc} D_1^1, & \sum_{k=1}^{2} \frac{k}{2} D_k^2, & \ldots \quad \sum_{k=1}^{M} \frac{k}{M} D_k^M \end{array} \right] \tag{25}$$

En consecuencia, para el caso FIFO-BL, la función generatriz de la distribución del tiempo de residencia en el sistema de un paquete al azar, expresado en número de tramas, $R_F(z)$ resulta ser:

$$\boldsymbol{T}_F = \left[\begin{array}{cccc} D_1^1 A_0^{M'} & D_1^1 A_1^{M'} & D_1^1 A_2^{M'} & \ldots \quad D_1^1 A_{M'}^{M'} \\ \frac{1}{2} D_1^2 A_0^{M'} & \sum_{k=0}^{1} \frac{2-k}{2} D_k^2 A_k^{M'-1+k} & \sum_{k=0}^{1} \frac{2-k}{2} D_k^2 A_{k+1}^{M'-1+k} & \ldots \quad \sum_{k=0}^{1} \frac{2-k}{2} D_k^2 A_{k+M'-1}^{M'-1+k} \\ \frac{1}{3} D_2^3 A_0^{M'} & \sum_{k=1}^{2} \frac{3-k}{3} D_k^3 A_{k-1}^{M'-2+k} & \sum_{k=0}^{2} \frac{3-k}{3} D_k^3 A_k^{M'-2+k} & \ldots \quad \sum_{k=0}^{2} \frac{3-k}{3} D_k^3 A_{k+M'-2}^{M'-2+k} \\ \frac{1}{4} D_3^4 A_0^{M'} & \sum_{k=2}^{3} \frac{4-k}{4} D_k^4 A_{k-2}^{M'-3+k} & \sum_{k=1}^{3} \frac{4-k}{4} D_k^4 A_{k-1}^{M'-3+k} & \ldots \quad \sum_{k=0}^{3} \frac{4-k}{4} D_k^4 A_{k+M'-3}^{M'-3+k} \\ \vdots & \vdots & \vdots & \ddots \quad \vdots \end{array} \right] \tag{24}$$

$$R_F(z) = \alpha_M + z\boldsymbol{\alpha}_F\big[\boldsymbol{I} - z\boldsymbol{T}_F\big]^{-1}\boldsymbol{T}_F^0 \tag{26}$$

Para la disciplina LIFO-PO, si *nuestro paquete* colisiona con otro(s) intentará de nuevo el acceso en la próxima secuencia de V mini-ranuras siempre y cuando no haya sido desplazado por la llegada de otro paquete posterior, desplazamiento que puede producirse con probabilidad a. Con el mismo razonamiento que en FIFO-BL, condicionado a que nuestro paquete compite con otros i paquetes, la probabilidad de colisión y de que en la siguiente trama nuestro paquete compita en el accesor con otros j paquete, $j = 0, 1, \ldots, M' = M - 1$ viene dada por

$$T_{L;i,j} = (1-a)T_{F;i,j} \tag{27}$$

Por otra parte, nuestro paquete no sufrirá colisión alguna -acceso exitoso- con probabilidad idéntica a la dada en (23). Alternativamente puede ser desplazado o expulsado del sistema con probabilidad $a\sum_{j=0}^{M'} T_{F;i,j}$, véase Ec. (22). Por lo tanto:

$$T_{L;i}^0 = T_{F;i}^0 + a\sum_{j=0}^{M'} T_{F;i,j} \tag{28}$$

En notación matricial tendremos que $\boldsymbol{T}_L = (1-a)\boldsymbol{T}_F$ y $\boldsymbol{T}_L^0 = \boldsymbol{T}_F^0 + a\boldsymbol{T}_F\boldsymbol{e}$. Con ello, dado que $\alpha_{L;M} = 0$ (en terminología PH, la probabilidad de que el sistema inicialmente se encuentre en el estado absorbente es cero), escribimos:

$$\begin{aligned} R_L(z) &= \alpha_{L;M} + z\boldsymbol{\alpha}_L\big[\boldsymbol{I} - z\boldsymbol{T}_L\big]^{-1}\boldsymbol{T}_L^0 = \\ &= z\boldsymbol{\alpha}_L\big[\boldsymbol{I} - z(1-a)\boldsymbol{T}_F\big]^{-1}\big[\boldsymbol{T}_F^0 + a\boldsymbol{T}_F\boldsymbol{e}\big] \\ &= z\boldsymbol{\alpha}_L\big[\boldsymbol{I} - z(1-a)\boldsymbol{T}_F\big]^{-1}\boldsymbol{T}_F^0 \\ &+ z\boldsymbol{\alpha}_L\big[\boldsymbol{I} - z(1-a)\boldsymbol{T}_F\big]^{-1}a\boldsymbol{T}_F\boldsymbol{e} = \\ &= R_{AL}(z) + R_{RL}(z) \end{aligned} \tag{29}$$

En (29), $R_{AL}(z) = z\boldsymbol{\alpha}_L\big[\boldsymbol{I} - z(1-a)\boldsymbol{T}_F\big]^{-1}\boldsymbol{T}_F^0$ es la función generatriz del número de tramas necesarias para que *nuestro paquete* tenga una transmisión exitosa, mientras que $R_{RL}(z) = z\boldsymbol{\alpha}_L\big[\boldsymbol{I} - z(1-a)\boldsymbol{T}_F\big]^{-1}a\boldsymbol{T}_F\boldsymbol{e}$ refleja la función generatriz del número de tramas que *nuestro paquete* ha permanecido en el sistema hasta que ha sido desplazado o expulsado sin haber sido servido.

Dados los resultados anteriores, en lo sucesivo denotaremos por $\mathbf{T}_F = \mathbf{T}$ y por $\mathbf{T}_F^0 = \mathbf{T}^0$ tal que

$$\begin{aligned} R_F(z) &= R_{AF}(z) + R_{RF}(z) \\ R_{RF}(z) &= \alpha_M \\ R_{AF}(z) &= z\boldsymbol{\alpha}_F\big[\boldsymbol{I} - z\boldsymbol{T}\big]^{-1}\boldsymbol{T}^0 \end{aligned} \tag{30}$$

$$\begin{aligned} R_L(z) &= R_{AL}(z) + R_{RF}(z) \\ R_{AL}(z) &= z\boldsymbol{\alpha}_L\big[\boldsymbol{I} - z(1-a)\boldsymbol{T}\big]^{-1}\boldsymbol{T}^0 \\ R_{RL}(z) &= z\boldsymbol{\alpha}_L\big[\boldsymbol{I} - z(1-a)\boldsymbol{T}\big]^{-1}a\boldsymbol{T}\boldsymbol{e} \end{aligned} \tag{31}$$

Evidentemente $R_F(1) = 1$ y $R_L(1) = 1$. Subrayar también que, en conexión con (7) y (8), las probabilidades de que un paquete de datos al azar sea finalmente transmitido con éxito o rechazado, vienen dadas por, respectivamente:

$$P_{Adm} = R_{AF}(1) = P_{AF} = R_{AL}(1) = P_{AL} \tag{32}$$

$$P_{Rej} = R_{RF}(1) = P_{RF} = R_{RL}(1) = P_{RF} \tag{33}$$

Los diferentes momentos factoriales se obtienen al evaluar las sucesivas derivadas de (30) y (31) en $z = 1$:

$$R_F^{(k)}(1) = R_{AF}^{(k)}(1) = k!\boldsymbol{\alpha}_F\boldsymbol{T}^{k-1}\big[\boldsymbol{I} - \boldsymbol{T}\big]^{-k}\boldsymbol{e} \tag{34}$$

y

$$\begin{aligned} &R_{AL}^{(k)}(1) = \\ &k!(1-a)^{k-1}\boldsymbol{\alpha}_L\boldsymbol{T}^{k-1}\big[\boldsymbol{I} - (1-a)\boldsymbol{T}\big]^{-(k+1)}\boldsymbol{T}^0 \end{aligned} \tag{35}$$

$$\begin{aligned} &R_{RL}^{(k)}(1) = \\ &k!(1-a)^{k-1}\boldsymbol{\alpha}_L\boldsymbol{T}^{k-1}\big[\boldsymbol{I} - (1-a)\boldsymbol{T}\big]^{-(k+1)}a\boldsymbol{T}\boldsymbol{e} \end{aligned} \tag{36}$$

Los valores medios se obtienen para $k = 1$:

$$R_{AF}^{(1)}(1) = \boldsymbol{\alpha}_F\big[\boldsymbol{I} - \boldsymbol{T}\big]^{-1}\boldsymbol{e} \tag{37}$$

$$R_{AL}^{(1)}(1) = \boldsymbol{\alpha}_L\big[\boldsymbol{I} - (1-a)\boldsymbol{T}\big]^{-2}\boldsymbol{T}^0 \tag{38}$$

$$R_{RL}^{(1)}(1) = \boldsymbol{\alpha}_L\big[\boldsymbol{I} - (1-a)\boldsymbol{T}\big]^{-2}a\boldsymbol{T}\boldsymbol{e} \tag{39}$$

Por conservación de la cantidad de trabajo en el sistema, se cumple que

$$R_{AF}^{(1)}(1) = R_{AL}^{(1)}(1) + R_{RL}^{(1)}(1) \tag{40}$$

y teniendo en cuenta que $\big[\boldsymbol{I} - (1-a)\boldsymbol{T}\big]^{-1}\big[\boldsymbol{T}^0 + a\boldsymbol{T}\boldsymbol{e}\big] = \boldsymbol{e}$ la Ec. (40) puede reescribirse como

$$\boldsymbol{\alpha}_F\big[\boldsymbol{I} - \boldsymbol{T}\big]^{-1}\boldsymbol{e} = \boldsymbol{\alpha}_L\big[\boldsymbol{I} - (1-a)\boldsymbol{T}\big]^{-1}\boldsymbol{e} \tag{41}$$

IV. RESULTADOS Y APLICABILIDAD

A continuación se ofrecen algunos resultados para un número de fuentes $M = 8$ y un tamaño de trama de $V = 5$. Las Fig. 2 y 3 muestran la función de distribución de probabilidades (FDPs) del tiempo de espera, expresado en tramas de $V = 5$ ranuras/trama, relativo al colectivo de paquetes transmitidos con éxito para los caso FIFO-BL y LIFO-PO; respectivamente obtenidas de $R_{AF}(z)$ y $R_{AL}(z)$. Para la Fig. 2 hemos mantenido la probabilidad de permiso $r = 0.75$ variando como parámetro la probabilidad de generar un paquete por ranura y por fuente, con $p_{act} = 0.01$, 0.05, 0.1, 0.15 y 0.20, equivales a las probabilidades de generar al menos un paquete por trama de, respectivamente $a = 1 - (1 - p_{act})^V = 0.049$, 0.226, 0.409, 0.556 y 0.672. Para la Fig. 3 hemos fijado la probabilidad $p_{act} = 0.05$, variando la probabilidad de permiso, con $r = 0.2$, 0.4, 0.6, 0.8 y 1.

En primer lugar se observa que, fijada una p_{act} en la Fig 2 o una r en la Fig.3, el límite de las FDPs en FIFO-BL y LIFO-PO coinciden con la probabilidad de que un paquete al azar sea transmitido con éxito. Así por ejemplo, para las cargas indicadas de $p_{act} = 0.01$, 0.05, 0.1, 0.15 y 0.20, Fig. 2, las probabilidades de éxito, P_{Adm} en Eq. (32), respectivamente

son, 0.979, 0.801, 0.578, 0.440 y 0.364; y las probabilidades de pérdida o rechazo, P_{Rej} en Eq. (33), respectivamente son, 0.021, 0.199, 0.422, 0.560 y 0.636.

En la Fig. 3 observamos el mejor comportamiento cuando $r = 1$. Ello es debido a la baja carca de tráfico generada por fuente $p_{act} = 0.05$ y $a = 1 - (1 - p_{act})^V = 0.2262$, implicando que al inicio de cada trama habrá una media de, al menos $M \times a = 8 \times 0.2262 = 1.8098$ fuentes con paquete presto para transmitir[2]. Por lo que, según el apéndice, $r_{opt} = \min(1, V/m) = \min(1, V/(M \times a + backlog) \leq \min(1, V/(M \times a) = \min(1, 5/1.8098) = 1$. Siempre que el número de paquetes en estado de reintento, *backlog*, sea tal que $backlog < V/e - M \times a \approx 1.8394 - 1.8098 = 0.096$ tendríamos que $r_{opt} = 1$. No obstante, se precisa de un estudio más detallado del comportamiento dinámico del sistema en donde la probabilidad r debe de adaptarse según resultados observables por trama: transmisión exitosa, con colisión o con ranura temporal vacía [8].

Por otra parte, una inspección visual a las gráficas indica que, para cualquier valor del número de tramas, la FDP del caso LIFO-PO supera a la del caso FIFO-BL, alcanzando antes el valor asintótico común P_{Adm}. Ello implica que el tiempo medio de espera previo a una transmisión exitosa en el caso de disciplina LIFO-PO resulta inferior al de la disciplina FIFO-BL. Pero hemos de remarcar que para bajas cargas de tráfico, la diferencia entre ambas disciplinas es mínima. Ello es debido a que, en el caso FIFO-BL la gran mayoría de los paquetes generados encuentran a su llegada la cola vacía y por lo tanto son admitidos; y en el caso LIFO-PO rara vez se producen desplazamientos. Las diferencias entre ambas disciplinas se hace significativa a medida que aumenta la carga de tráfico ofrecida, aumentando al mismo tiempo el porcentaje de paquetes perdidos.

Es claro que la disciplina LIFO-PO siempre va a transmitir el paquete de datos de más reciente generación. La disciplina LIFO-BL puede preferirse frente a otras como la FIFO-BL en escenarios con redes de sensores, WSN (*Wireless Sensor Networks*), en donde determinadas aplicaciones precisan captar valores de temperatura, de humedad, de presión atmosférica, de velocidad del viento, etc. Y a la vista de los resultados, es clara la ventaja de implementar LIFO-PO en lugar de FIFO-BL; pues se viene a confirmar la idea de NBO o NBU *New Better Than Old, Used*; esto es, es mejor la información reciente que la antigua u ¿obsoleta? [11].

Finalmente, y para el entorno de WSN comentamos brevemente la aplicabilidad del estudio abordado. En WSN, a menudo, los sensores con cierta proximidad geográfica forma grupos *clusters*. Entre los elementos de un grupo, se elige un líder o CH (*cluster head*). El CH es el encargado de colectar la información captada por todos y cada uno de los sensores de su grupo. Teniendo en cuenta el bajo tráfico generado por grupo, para el fin indicado se suelen sugerir protocolos tipo S-ALOHA, habida cuenta de la baja complejidad en su

[2]Además habría que añadir $backlog$, el número medio de paquetes que hubiesen quedado pendientes de transmitir en la trama anterior.

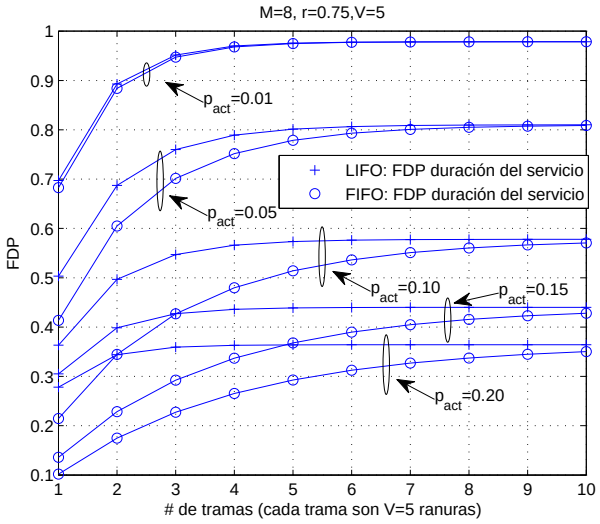


Fig. 2. Función de Distribución de Probabilidad (FDP) de la variable aleatoria número de tramas necesarias para alcanzar un acceso (transmisión con éxito). Disciplinas FIFO-BL y LIFO-PO con varias cargas de tráfico por fuente.

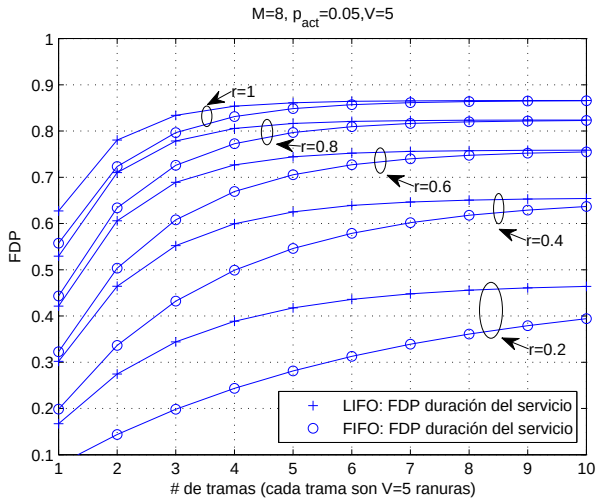


Fig. 3. Función de Distribución de Probabilidad (FDP) de la variable aleatoria número de tramas necesarias para alcanzar un acceso (transmisión con éxito). Disciplinas FIFO-BL y LIFO-PO con varias probabilidades de permiso de acceso.

implementación. Es el CH quien, ademas de ser un sensor más del grupo, puede gestionar el acceso de forma centralizada, mediante sencillos esquemas de control, por ejemplo facilitando la probabilidad de permiso r. Cabe añadir que la información recogida por los CHs, puede encaminarse hacia otro(s) CH(s) en forma multi-salto hasta alcanzar algún nodo sumidero (*Sink*). Entre los CHs se configura una red mallada de alta conectividad que ofrece la robustez necesaria para escenarios con medias y altas cargas de tráfico [12],[13].

V. CONCLUSIONES

El presente artículo ofrece un modelado analítico para evaluar el protocolo S-ALOHA multi-trama (*framed*). A nuestro

entender se han aportado dos nuevos resultados. El primero son las expresiones recursivas para el cálculo de las probabilidades de ranura vacía, de éxito y de colisión. La segunda contribución consiste en el análisis del protocolo contemplando disciplinas FIFO-BL y LIFO-PO. Haciendo uso de modelos de Markov, se han aportado expresiones cerradas para la distribución de los tiempos de residencia de los paquetes servidos (en FIFO-PL y LIFO-PO) y perdidos (en LIFO-PO). El análisis se ha formulado en términos de distribuciones PH (*Phase type*), una atractiva herramienta de fácil uso.

AGRADECIMIENTOS

Este trabajo ha sido financiado a través del proyecto nacional TIN2010-21378-C02-02

REFERENCIAS

[1] N. Abramson, "The ALOHA system-Another alternative for computer communications," in AFZPS Conf. Proc., I970 Fall Joint Computer Conf., vol. 37, 1970, pp. 281-285.
[2] L. G. Roberts, "Extensions of packet communication technology to a hand held personal terminal," in AFZPS Conf. Proc., I972 Spring Joint Computer Conf., vol. 40, 1972, pp. 295-298.
[3] R. Rom, M. Sidi, "Multiple access protocols". Springer-Verlag, 1989.
[4] M. Mouly, M. B. Pautet, "The GSM System for Mobile Communications". Published by the authors, 1992.
[5] W. Szpankowski, "Analyisis and stability considerations in a reservation multiaccess system". IEEE Trans on Communications, Vol. 31, No. 5, pp 684-692, May 1983.
[6] J. Weiselthier, A. Ephremides, L. A. Michaels, "An exact analysis and performance evaluation of framed ALOHA with capture". IEEE Trans on Communications, Vol. 37, No. 2, pp 125-137, February 1989.
[7] B. T. Doshi, H. Heffes, "Overload performance of several processor queueing disciplines for the M/M/1 queue". IEEE Trans on Communications, Vol. 34, No. 6, pp 538-546, June 1986.
[8] R. L. Rivest, "Network Control by Bayesian Broadcast," IEEE Trans. on Information Theory, Vol. IT-33, N0. 3, pp 323-328 , May 1987.
[9] M. F. Neuts, "Matrix-geometric solutions in stochastic models - An algorihthmic approach". The Johns Hopkins University Press, Baltimore, 1981.
[10] A. S. Alfa, "Queueing theory for telecommunications. Discrete time modelling of a sigle node system", Springer, 2010.
[11] D. Stoyan, "Comparison methods for queues and other stochastic models", Akademie-Verlag Berlin / John Wiley, 1983.
[12] V. Casares-Giner, D. Felipe-Pacheco, D. Todolí Ferrandis, "Análisis y modelado en redes de sensores inalámbricas", 10ª Jornadas de Ingeniería Telemática, JITEL-2011), Proceedings pp: 309-316, Universidad de Cantabria. Santander (Spain), Septiembre 28-30, 2011.
[13] V. Casares-Giner, P. Wüechner, D. Felipe-Pacheco, H. de Meer, "Combined Contention and TDMA-Based Communication in Wireless Sensor Networks", In Proc. of the 8th Euro-NF Conf. on Next Generation Internet (NGI2012), pp: 1-8, BTH, Karlskrona (Sweden), June 25-27, 2012.

APÈNDICE

Consideremos una asignación aleatoria de m bolas (o paquetes de datos) en V urnas (o ranuras temporales). La asignación aleatoria obedece a una distribución uniforme, esto es, con probabilidad $1/V$ a un determinado paquete se le asigna una de las V ranuras. El anterior juego de probabilidades es equivalente a la siguiente captura secuencia de ranura. Dado un paquete de datos, la primera ranura será elegida con probabilidad $1/V$ y con probabilidad $(1-1/V) = (V-1)/V$ será descartada. La segunda ranura se elegirá con probabilidad $(1-1/V)(1/(V-1) = 1/V$ y con probabilidad $(1-1/V)(1-1/(V-1) = (V-2)/V$ se descartarán las dos primeras ranuras. Con probabilidad $1/V$ se elegirá la tercera ranura y con probabilidad $(V-3)/V$ se descartarán las tres primeras ranuras. Y así sucesivamente. Evidentemente, la probabilidad de descartar todas las V ranuras es 0, por lo que obviamente, una y solamente una de las V ranuras temporales será elegida por nuestro paquete de datos.

A. Recurrencias para las probabilidades de ranura vacía, con éxito o con colisión.

Denotemos por $X = E, S, C$, respectivamente la observación de ranura vacía, ranura con un único paquete y ranura con más de un paquete de datos; respectivamente de *Empty, Successful, Collision*. Sea $X(y,k,V)$ la probabilidad condicionada a que, teniendo y paquetes prestos para competir por ganar el acceso de una de las V ranuras, se observen k ranuras en el estado X, ($k \leq \min(y,V)$). En lo sucesivo denotaremos la distribución binomial como:

$$B(M,k,a) = C_k^M p^k (1-p)^k = \frac{M!}{k!(M-k)!} p^k (1-p)^k. \quad (42)$$

en donde C_j^i es el combinatorio de i elementos tomados de j en j. Entonces, para $X = E$ podemos escribir la siguiente fórmula recurrente relativa al numero de ranuras vacías,

$$E(y,0,V) = \sum_{j=1}^{y} B(y,j,1/V) E(y-j,0,V-1). \quad (43)$$

$$E(y,k,V) = B(y,0,1/V) E(y,k-1,V-1) + \\ + \sum_{j=1}^{y} B(y,j,1/V) E(y-j,k,V-1); \quad k = 1,\ldots,V. \quad (44)$$

Para la distribución del número de ranuras ocupadas con un único paquete, $X = S$, tenemos que,

$$S(y,0,V) = \sum_{j=0,\neq 1}^{y} B(y,j,1/V) S(y-j,0,V-1). \quad (45)$$

$$S(y,k,V) = B(y,1,1/V) S(y-1,k-1,V-1) + \\ + \sum_{j=0,\neq 1}^{y-k} B(y,j,1/V) S(y-j,k,V-1); \\ k = 1,\ldots,\min(y,V). \quad (46)$$

y para la distribución del número de ranuras con más de un paquete de datos, con colisión, $X = C$, escribimos,

$$C(y,0,V) = \sum_{j=0}^{1} B(y,j,1/V) C(y-j,0,V-1) \quad (47)$$

$$C(y,k,V) = \sum_{j=0}^{1} B(y,j,1/V) C(y-j,k,V-1) + \\ + \sum_{j=2}^{y-k} B(y,j,1/V) C(y-j,k-1,V-1); \\ k = 1,2,\ldots,V. \quad (48)$$

B. Valores medios.

De las anteriores expresiones se pueden inferir las funciones generatrices de $E(y,k,V)$ y $S(y,k,V)$, las cuales se expresan como:

$$E^*(y,z,V) = \sum_{k=0}^{V} E(y,k,V)z^k = \\ = \sum_{n=0}^{V} C_{n-1}^{V-1} \left(\frac{n}{V}\right)^{y-1} (z-1)^{V-n} \quad (49)$$

$$S^*(y,z,V) = \sum_{k=0}^{\min(y,V)} S(y,k,V)z^k = \\ = \frac{V!y!}{V^y} \sum_{k=0}^{\min(y,V)} \frac{(V-n)^{y-n}}{(V-1)!(y-n)!} \frac{(z-1)^n}{n!} \quad (50)$$

A partir de las sucesivas derivadas de (49) y (50 se obtienen los diferentes momentos. En particular los valores medios resultan

$$\frac{dE^*(y,z,V)}{dz}_{/z=1} = (V-1)\left(\frac{V-1}{V}\right)^{y-1} \quad (51)$$

$$\frac{dS^*(y,z,V)}{dz}_{/z=1} = y\left(\frac{V-1}{V}\right)^{y-1} \quad (52)$$

$$\frac{dC^*(y,z,V)}{dz}_{/z=1} = V - (V+y-1)\left(\frac{V-1}{V}\right)^{y-1} \quad (53)$$

El caudal se maximiza valorando (51) en $z=1$. Esto es,

$$V-1 < y_{opt} = \left(\ln\frac{V}{V-1}\right)^{-1} < V \quad (54)$$

Cabe observar las siguientes igualdades

$$\frac{dE^*(V-1,z,V)}{dz}_{/z=1} = \\ \frac{dS^*(V-1,z,V)}{dz}_{/z=1} = \frac{dS^*(V,z,V)}{dz}_{/z=1} \quad (55)$$

A modo ilustrativo, la Fig. 4 muestran el número medio de ranuras vacía, con paquete único y con colisiones, para el caso de $V=3$.

C. Acceso con permiso probabilístico

Consideremos ahora que tenemos un total de m paquetes dispuestos a acceder en una trama de V ranuras. Cada paquete va a intentar el acceso con probabilidad r, denominada probabilidad de permiso. Entonces, la probabilidad de que k paquetes, de un total de m consigan el acceso, vendrá dada por.

$$D_k^m(r,V) = \sum_{y=k}^{m} B(m,y,r)S(y,k,V), \\ k \le m = 0,1,\ldots,V. \quad (56)$$

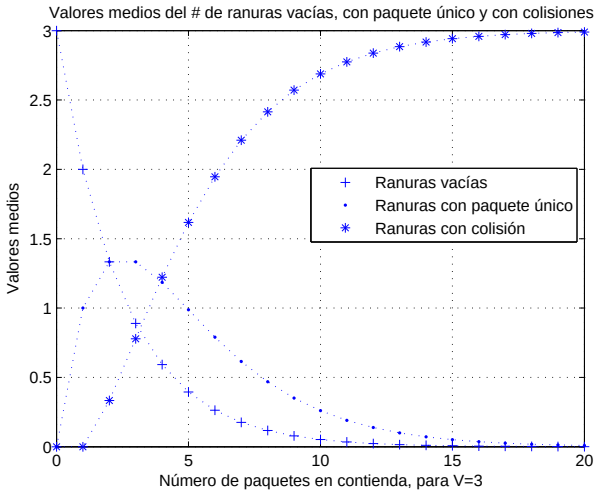


Fig. 4. Número medio de ranuras vacías, con un único paquete y con colisión, para el caso de $V=3$.

Con respecto a la v.a. k la función generatriz de $D_k^m(r,V)$ resulta ser:

$$\Delta_z^m(r,V) = \sum_{k=0}^{\min(m,V)} D_k^m(r,V)z^k = \\ = \sum_{y=0}^{m} B(m,y,r)\frac{V!y!}{V^y} \sum_{j=0}^{\min(y,V)} \frac{(V-j)^{y-j}}{(V-j)!(y-j)!} \frac{(z-1)^j}{j!}. \quad (57)$$

La primera derivada de (57) con respecto a z, en $z=1$, nos da el número medio de paquetes con transmisión exitosa, resultando ser, tras algo de álgebra

$$\frac{d\Delta_z^m(r,V)}{dz}_{/z=1} = rm\left(\frac{V-r}{V}\right)^{m-1} \quad (58)$$

El valor de r que maximiza (58), r_{opt}, es

$$r_{opt} = \begin{cases} 1, & \text{si } m \le V \\ \frac{V}{m}, & \text{si } V \le m \end{cases} \quad (59)$$

y el valor del caudal óptimo resultante es

$$Th_{opt} = \begin{cases} m\left(1-\frac{1}{V}\right)^{m-1}, & \text{si } m \le V \\ V\left(1-\frac{1}{m}\right)^{m-1}, & \text{si } V \le m \end{cases} \quad (60)$$

De (60), fijado V y cuando $m \to \infty$, la probabilidad de permiso tiende a cero, Ec. (59), al tiempo que el caudal óptimo tiende a $V/e \approx 0.367879V$. Esto es, S-ALOHA multi-ranura ofrece un caudal por ranura igual al protocolo S-ALOHA estándar, por lo que desde el punto de vista de caudal, no hay ventaja alguna. Sin embargo S-ALOHA multi-ranura ofrece otras ventajas, algunas de ellas han sido comentadas en la sección I.

Estudio de las prestaciones del protocolo de enrutamiento BATMAN con tráfico VoIP

Ramón Sánchez-Iborra, María-Dolores Cano
Grupo de Ingeniería Telemática. Departamento de Tecnologías de la Información y las Comunicaciones
Universidad Politécnica de Cartagena
Antiguo Cuartel de Antigones. Plaza del Hospital, Nº 1, 30202 Cartagena (Murcia)
{ramon.sanchez, mdolores.cano}@upct.es

***Resumen*- Actualmente, una de las redes de acceso que está recibiendo una mayor atención por parte de la comunidad científica son las redes móviles ad-hoc, conocidas como redes MANET. Este tipo de redes ofrece una arquitectura completamente descentralizada, muy adecuada para situaciones donde no es viable implantar una red de infraestructura. Por su parte, los servicios multimedia como VoIP están logrando una gran expansión y comienzan a utilizarse de forma generalizada por los usuarios finales. La necesidad de transmisión de contenidos en tiempo real, junto con la inherente naturaleza dinámica de las redes MANET, hacen necesarios algoritmos de enrutamiento altamente eficientes. En este trabajo se presentan los resultados de evaluación de prestaciones del protocolo de enrutamiento BATMAN para redes MANET con transmisión de tráfico VoIP. Los resultados obtenidos en una topología en cadena gestionada por BATMAN se han comparado con las prestaciones en idénticas condiciones para el protocolo OLSR, obteniendo que BATMAN se ve menos afectado por el desvanecimiento en los canales (fading) que OLSR. También se muestra como, en entornos de muy bajas pérdidas, el protocolo BATMAN presenta unas prestaciones muy degradadas debido al exceso de paquetes de control de los que hace uso.**

***Palabras Clave*- QoE, BATMAN, OLSR, MANET, fading**

I. INTRODUCCIÓN

Actualmente las comunicaciones *Voice over IP* (VoIP) se están extendiendo a multitud de arquitecturas y topologías de red. Este servicio de comunicación de voz ofrece llamadas a bajo coste y con un nivel de calidad aceptable, permitiendo además, comunicar a personas situadas en cualquier punto del planeta. Si a estas características se le añade la movilidad que ofrecen las redes de transmisión inalámbricas, se obtiene un producto muy atractivo para el usuario final. Centrándonos en el estándar inalámbrico más extendido hoy en día, el IEEE 802.11, podemos encontrar multitud de trabajos que estudian el funcionamiento de los sistemas de comunicación VoIP sobre este tipo de redes en modo infraestructura [1–3]. Estos trabajos analizan la calidad obtenida con transmisiones VoIP en diversos escenarios, evaluando el efecto que distintos parámetros, como la pérdida de paquetes, el retardo o el desvanecimiento en el canal de transmisión, tienen sobre la calidad de las llamadas. Estos trabajos concluyen que las redes IEEE 802.11 en modo infraestructura son sistemas de comunicación válidos para mantener un alto número de llamadas VoIP con unos niveles elevados de calidad.

Sin embargo, existe otra arquitectura de acceso que emplea el estándar 802.11 y que ha recibido menor atención por parte de la comunidad científica, en cuanto a la evaluación de sus prestaciones para poder soportar tráfico VoIP con unos niveles mínimos de calidad; en particular, nos referimos a las redes MANET (*Mobile Ad-hoc NETwork*). Estas redes resultan muy atractivas en su concepto, pues ofrecen una arquitectura completamente descentralizada, permitiendo una alta movilidad de los nodos que la componen, y se muestran muy adecuadas para situaciones donde no es posible desplegar un sistema de transmisión centralizado, como en caso de catástrofes o redes temporales. Las redes MANET son capaces de auto-configurarse y reaccionar ante cambios en su topología, ya que todos los nodos que la forman colaboran en las tareas de enrutamiento. La inherente naturaleza dinámica de este tipo de redes dificulta en gran medida estas labores. Además, la transmisión de servicios multimedia conlleva una serie de exigencias, como la transmisión de contenidos en tiempo real, necesarias para poder proveer dichos servicios con unos niveles de calidad aceptables. Es por ello que se necesitan algoritmos de enrutamiento altamente eficientes, capaces de configurar la red en el menor tiempo posible y de reaccionar positivamente ante una alta diversidad de escenarios.

En este trabajo, evaluamos mediante simulación el funcionamiento del protocolo BATMAN [4] para gestionar redes MANET soportando tráfico VoIP. Con el fin de analizar el desempeño de BATMAN, que aún se encuentra en estado de borrador por el IETF, los resultados obtenidos se compararán con los logrados haciendo uso del protocolo OLSR [5], el cual ha mostrado un funcionamiento superior que otros algoritmos pro-activos, en escenarios con tráfico VoIP [6] y que es protocolo estándar del IETF. Concretamente, realizaremos una evaluación de la Calidad de Experiencia de usuario (*Quality of user Experience*, QoE) obtenida en comunicaciones VoIP en una red MANET con topología en cadena y gestionada por los protocolos de enrutamiento anteriormente citados. Como esquema de codificación se ha escogido el conocido códec estándar de la ITU-T G.711 ley-A, que trabaja a 64 Kbps (códec sin compresión). Además, se realizará un análisis del impacto que tiene el canal físico sobre la calidad de las comunicaciones, caracterizando el entorno mediante el modelo de propagación Nakagami-m y evaluando el efecto de los canales con desvanecimiento. Los resultados obtenidos en estos entornos más adversos serán comparados con los que se obtengan en situaciones en espacio libre.

El resto del documento se organiza como sigue. En la Sección 2 se analizan los trabajos relacionados, centrándonos en aquéllos que evalúan el desempeño de los protocolos de

enrutamiento *ad-hoc*, trabajando con tráfico VoIP. La Sección 3 describe los algoritmos de enrutamiento bajo estudio (BATMAN y OLSR). La plataforma utilizada para llevar a cabo las distintas simulaciones realizadas se explicita en la Sección 4. En la Sección 5 se muestran y discuten comparativamente los resultados obtenidos. Finalmente, se presentan las principales conclusiones extraídas de este trabajo.

II. Literatura relacionada

Como se ha comentado en la sección anterior, el funcionamiento de VoIP sobre redes MANET no ha sido estudiado de forma tan intensiva como se ha hecho en redes en modo infraestructura. No obstante, se pueden encontrar algunos trabajos que evalúan la adecuación de las redes *ad-hoc* para soportar tráfico VoIP [6–8], aunque ninguno de ellos incorpora en su estudio el protocolo BATMAN.

El trabajo presentado en [6], analiza el comportamiento de un sistema de transmisión VoIP, utilizando distintos esquemas de codificación y arquitecturas de red inalámbricas; para ello, se estudia la evolución de parámetros básicos en calidad de servicio, como la pérdida de paquetes y el retardo. Con estos índices de calidad, los autores realizan una comparativa del funcionamiento de distintos protocolos de enrutamiento, llegando a la conclusión de que OLSR es el que alcanza mayores cotas de calidad, en términos de *throughput* (caudal) y retardo. Los resultados mostrados en este trabajo son los que nos llevan a escoger a OLSR como comparativa de referencia con respecto a BATMAN.

Por su parte, los autores de [7] analizan el efecto del esquema de codificación empleado sobre la calidad de una comunicación VoIP. Éstos encontraron que en escenarios con un número reducido de nodos, los códec sin compresión, como el G.711, proporcionan mayores niveles de calidad. Por el contrario, los códecs de baja tasa de codificación, como el G.729 o GSM, se muestran más apropiados en redes muy densas, es decir, con un número elevado de nodos.

Finalmente, el trabajo presentado en [8] analiza mediante simulación el impacto del nivel físico en las transmisiones VoIP sobre entornos *ad-hoc*. Los autores hacen uso del Modelo-E (ITU-T Rec. G.107) para estimar la QoE en escenarios caracterizados por distintos modelos de propagación: espacio libre, dos rayos y sombras (*shadowing*). Como se desprende de sus resultados, al igual que en [3], el nivel físico tiene un severo impacto sobre la QoE de las comunicaciones VoIP; cuanto mayor sea la hostilidad del canal de transmisión, mayor es la bajada de calidad que experimentan las llamadas de voz. Además, se demuestra que OLSR es un protocolo que se ve altamente afectado por las condiciones del canal físico.

III. Protocolos de enrutamiento

Los protocolos de enrutamiento en redes *ad-hoc* pueden clasificarse de distintas formas; una de las clasificaciones más extendidas es dividirlos en (i) protocolos pro-activos, (ii) protocolos reactivos y (iii) protocolos híbridos.

Los protocolos pro-activos son aquéllos en los que los nodos tienen conocimiento de la topología de la red (completa o en parte), incluso antes de necesitarla. Esto se logra mediante un intercambio de información de enrutamiento entre nodos, de forma periódica. La principal desventaja de este tipo de protocolos es la necesidad de una gran cantidad de información de control viajando por la red, realizando un consumo extra de ancho de banda y, por tanto, disminuyendo el *throughput* de los nodos. Además, los protocolos pro-activos pueden presentar problemas de escalabilidad en redes con un alto número de nodos, pues la información de enrutamiento a manejar puede ser demasiado elevada. En contrapartida, las redes gestionadas por este tipo de protocolos tienen la ventaja de que los nodos siempre disponen de la información de enrutamiento actualizada y, de esta forma, están preparados para encaminar hacia su destino un paquete recién recibido, sin añadir un retardo adicional en las transmisiones. Algunos ejemplos de protocolos pro-activos son DSDV (*Destination-Sequenced Distance Vector*), OLSR (*Optimized Link State Routing*) o BATMAN (*Better Approach To Mobile Adhoc Networking*).

Los protocolos reactivos, o bajo-demanda, sólo calculan la ruta de destino cuando ésta es necesaria. Dicho de otra forma, no existe información de control ni cálculo de rutas cuando no hay comunicación entre nodos de la red; cuando un extremo de la comunicación quiere comunicarse con otro, la ruta se calcula bajo-demanda por los nodos intermedios de la comunicación, conforme avanza el flujo de transmisión hacia su destino. Este proceso permite ahorrar ancho de banda, pues mientras una conexión esté activa no se envía información de control adicional, pero añade un retardo elevado durante el proceso de búsqueda de la ruta óptima. Éste último hecho puede ser un factor limitante muy importante para servicios de comunicación en tiempo real, como VoIP. Ejemplos de este tipo de protocolos son TORA (*Temporally-Ordered Routing Algorithm*) o DYMO (*DYnamic Manet On-demand routing*).

Finalmente, los protocolos de enrutamiento híbridos tratan de combinar las ventajas de los protocolos pro-activos y reactivos. Un ejemplo es ZRP (*Zone Routing Protocol*), en el cual la red se divide en zonas de enrutamiento, formadas por nodos vecinos. Las rutas entre los nodos que forman una zona se calculan de forma pro-activa; sin embargo, si se desea realizar una transmisión con un nodo fuera de la zona de enrutamiento propia, las rutas adicionales se calculan bajo demanda.

A continuación se presenta una breve descripción de los dos protocolos de enrutamiento bajo estudio en este trabajo: BATMAN y OLSR.

A. BATMAN

Este protocolo pro-activo ha sido desarrollado por la Comunidad Freifunk [9] y aún se encuentra bajo discusión, en forma de borrador del IETF. La principal novedad que aporta BATMAN [4] es la descentralización total del conocimiento de las rutas por parte de los nodos; es decir, éstos no poseen en ningún momento tablas de enrutamiento con información completa de la red. En cambio, cada nodo sólo conoce el siguiente salto a dar para llegar a otro nodo sea cual sea su posición en la red. De esta forma, el algoritmo de enrutamiento resulta altamente eficiente y rápido en converger, creando una red de inteligencia colectiva. El funcionamiento del protocolo es como sigue. Cada uno de los nodos lanza a la red un mensaje llamado *OriGinator Message* (OGM), informando a sus vecinos más cercanos de su existencia. Estos vecinos retransmiten el paquete a sus

correspondientes vecinos y así sucesivamente hasta que todos los nodos hayan recibido, al menos una vez, el OGM de cada uno de los nodos de la red. Los OGMs dejan de circular bien por la pérdida de los mismos, o por la expiración del campo TTL. El número de OGMs recibidos de un nodo en concreto a través de un vecino se emplea como una estimación de la calidad de la ruta hacía el nodo generador del OGM; es decir, el siguiente salto que escoja un nodo para llegar a otro, será aquel vecino que le haya hecho llegar más OGMs del nodo destino. Usando esta sencilla información, BATMAN mantiene una tabla con el mejor vecino para alcanzar a cualquier nodo de la red. Mediante un número de secuencia incluido en cada OGM, BATMAN permite distinguir estos mensajes para no contarlos de forma duplicada.

Este protocolo ha atraído una gran atención por parte de la comunidad investigadora. Así, se puede encontrar un considerable número de trabajos evaluando su eficiencia en diversos escenarios. Por ejemplo, Kulla *et al.* han realizado un extenso trabajo sobre BATMAN, evaluando sus prestaciones en distintas situaciones, analizando también su reacción ante la movilidad de los nodos [10, 11]. La seguridad asociada al protocolo BATMAN también ha sido evaluada y mejorada por algunos autores [12, 13]. Sin embargo, no se tiene conocimiento de que existan trabajos en los que se realice una evaluación de BATMAN soportando tráfico multimedia (específicamente VoIP), desde una perspectiva de QoS/QoE. Tal y como se ha descrito anteriormente, este tipo de servicios tiene unos requerimientos muy estrictos, en relación a poder mantener la comunicación en tiempo real; esto los convierte en una clase de tráfico muy particular y que requiere de una gestión muy cuidadosa para poder alcanzar unas cotas mínimas de calidad. Por lo tanto, es necesaria una evaluación de los protocolos de enrutamiento en general, y de BATMAN en particular, que permita estimar el funcionamiento de los mismos ante condiciones de tráfico de voz.

B. OLSR

Este protocolo ha sido muy estudiado ya que se ha establecido como el estándar de enrutamiento del IETF en redes MANET. Está basado en el concepto clásico de los protocolos de estado de enlace. La novedad que aporta OLSR [5] es que la cantidad de tráfico de control que fluye por la red se ve reducida al utilizar retransmisiones multi-punto (*Multi-Point Relaying*, MPR). Esta estrategia consiste en elegir una serie de nodos vecinos que serán los que retransmitan la información de control; el resto de nodos puede recibir y leer estos paquetes, pero no retransmitirlos. Con una estrategia apropiada a la hora de elegir los nodos retransmisores, todos los destinos son alcanzables por todos los nodos, sin necesidad de inundar toda la red con paquetes de control.

El funcionamiento de OLSR en distintos escenarios y bajo diversas condiciones ha sido estudiado de forma exhaustiva por diversos autores [6, 8]. Concretamente, para el caso de transmisión de tráfico VoIP, se han obtenido buenos resultados en términos de QoS, para redes gestionadas por OLSR, en comparación con otros protocolos de enrutamiento, como AODV, DSR o GRP. Como se comentó anteriormente, estos resultados son los que nos han llevado a elegir OLSR como el protocolo con el que comparar la eficiencia de BATMAN.

IV. ENTORNO DE SIMULACIÓN

La plataforma utilizada para llevar a cabo las simulaciones de las que hemos extraído nuestros resultados ha sido el simulador de redes Omnet++ en su versión 4.2.2. Además, se ha empleado el conjunto de librerías incluidas en *Inet Framework* v2.1 [14], las cuales proveen multitud de modelos de dispositivos de red, así como diferentes protocolos de comunicación.

El escenario de simulación desarrollado consiste en una red siguiendo el estándar IEEE 802.11g a 54 Mbps. Se ha empleado una topología en cadena, en la que cada nodo sólo es capaz de comunicarse con su vecino más próximo (ver Fig. 1). Los transmisores y receptores VoIP se sitúan en los extremos de esta cadena. Se ha estudiado esta topología con un número variable tanto de transmisores/receptores VoIP como de nodos intermedios. De esta forma, se ha analizado el efecto que tiene el número de saltos en la calidad de las llamadas establecidas. Esta configuración también nos ha permitido comprobar la carga que es capaz de soportar un único nodo, puesto que todos los transmisores VoIP deben conectarse al primer nodo intermedio de la cadena, para poder establecer la comunicación a través de la misma.

Las tarjetas de red inalámbricas se han fijado a una potencia de transmisión de 1 mW y una sensibilidad de -85 dBm, con una frecuencia central de trabajo determinada por el estándar 802.11g, es decir 2.4 GHz, y un umbral mínimo de relación señal a ruido de 4dB.

Como parte de las librerías *Inet*, hemos hecho uso del generador de tráfico VoIP, el cual a partir de un archivo de audio, permite crear flujos de tráfico VoIP empleando distintos esquemas de codificación que pueden ser elegidos por el usuario; en nuestras simulaciones hemos utilizado el estándar de la ITU-T G.711 ley-A, el cual tiene una tasa de codificación de 64 Kbps. Para realizar las estimaciones de calidad, se ha empleado la implementación oficial del algoritmo PESQ, definido por la Rec. P.862. Dicha implementación fue añadida al entorno de simulación que generamos mediante Omnet++. Las cabeceras VoIP (por ejemplo, RTP), se fijaron a 12 bytes y se empleó un intervalo de paquetización de 20 ms. El tiempo de iniciación de cada llamada se ha establecido siguiendo una distribución de Poisson en un intervalo de tiempo (0, 10) s después del tiempo de convergencia de los protocolos de enrutamiento. Los ficheros de audio empleados tienen una duración de 30 s. El resto de parámetros adicionales relacionados con 802.11g se han fijado según se indica en la Tabla I.

Finalmente, el efecto de los canales con desvanecimiento fue medido comparando los resultados en situaciones

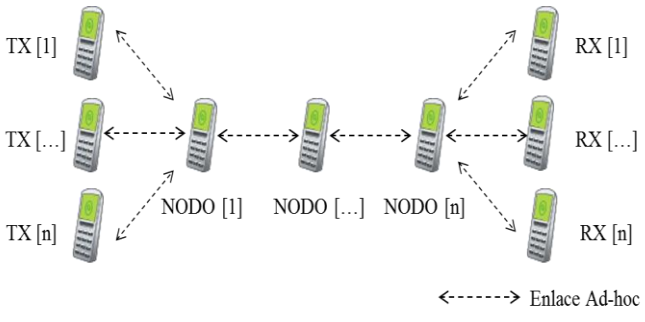


Figura 1. Topología en cadena de nodos *ad-hoc*.

TABLA I
PARÁMETROS 802.11g

Parámetros	Bytes	Tiempo	
		11 Mbps	***54 Mbps***
SIFS, DIFS, SLOT (µs)	-	{10, 50, 20}	{10, 50, 20}
CW_{MIN} (ranuras temporales)	-	31	31
Preámbulo PLCP (µs)	-	144	4
Cabeceras {PLCP, MAC, SNAP} (µs)	-, 28, 8	{48, 20.36, 5.81}	{16, 4.15, 1.18}
Cabeceras IP + UDP + RTP (µs)	40	29.09	5.92
Voz (G.711, 20 ms) (µs)	160	116.36	23.70
ACK (µs)	14	10.18	2.07

de espacio libre con los obtenidos en escenarios caracterizados por el modelo de propagación Nakagami-m. El nivel de *fading* introducido en el canal ha sido moderado, por lo que el parámetro que permite caracterizar este modelo, *m*, se ha fijado a un valor de 5.

V. RESULTADOS

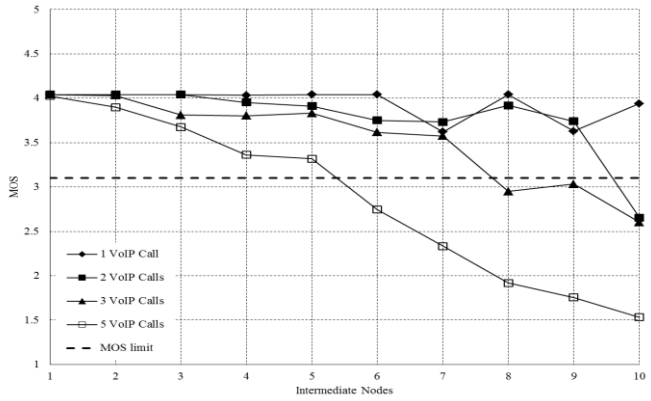
En esta sección mostramos los resultados obtenidos de la serie de simulaciones realizada, con el objetivo de estudiar el comportamiento del sistema VoIP descrito en secciones anteriores. Nos centraremos en evaluar cómo distintos parámetros como el desvanecimiento, el número de saltos y el número de llamadas simultáneas en la red, afectan al funcionamiento de BATMAN y, consecuentemente, a la calidad de las llamadas. Con este fin, se han realizado mediciones de retardos, pérdidas de paquetes y MOS (*Mean Opinion Score*) para cada llamada.

Para determinar si una llamada es válida (desde una perspectiva de QoE/QoS), en la bibliografía relacionada se hace uso de un gran número de métricas, como el MOS, el retardo en un sentido o la probabilidad de pérdida de paquetes. Siguiendo las directrices de las Rec. G.114 y G.1010 de la ITU-T, se define una llamada como válida cuando el MOS final estimado para la misma esté por encima de 3.1 (obsérvese que el MOS se representa en una escala de 1 a 5, de menor a mayor calidad). Esta medida permite unir el efecto de multitud de desajustes sufridos por la comunicación VoIP en un solo parámetro. Tal y como se indicó anteriormente, la estimación de MOS se ha realizado utilizando el algoritmo PESQ, descrito en la Rec. P.862.

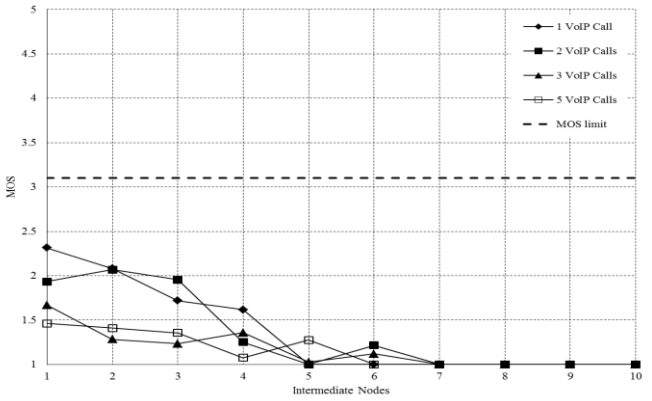
La Fig. 2 muestra una comparación entre la estimación de QoE obtenida para diferente número de llamadas simultáneas accediendo a la topología en cadena mostrada en la Fig. 1. En relación al efecto de los canales con desvanecimiento, obsérvese la importante caída en el MOS sufrida en escenarios Nakagami-m cuando se emplea el protocolo OLSR (Fig. 2.b) en comparación con los niveles de MOS obtenidos en escenarios de espacio libre (Fig. 2.a). Ni siquiera se acepta una sola llamada en el sistema (todos los valores de MOS por debajo de 3.1) sin importar el número de saltos entre los interlocutores. Estos resultados concuerdan con los obtenidos por Nascimento *et al.* [8], en los cuales se muestra una importante bajada en el rendimiento de OLSR en escenarios hostiles. En dicho trabajo se hizo uso de unos modelos de propagación menos realistas que Nakagami-m (2 rayos y modelo de sombras), comparando el desempeño de OLSR con el de otro protocolo de distinta naturaleza, como AODV (protocolo reactivo). Atribuimos esta caída tan pronunciada en el rendimiento de OLSR al tamaño de sus mensajes de control: los paquetes de control usados por OLSR tienen una longitud considerablemente superior a los de BATMAN, por lo que se ven más expuestos al efecto de los canales con desvanecimiento, provocando un aumento en la pérdida de estos paquetes y dificultando el correcto establecimiento de las rutas.

Por su parte, la caída de MOS en escenarios con *fading* es menor empleando BATMAN (Fig. 2.c). El sistema es capaz de soportar hasta 5 llamadas con 3 saltos entre los comunicantes. Además, se aceptan 1, 2 y 3 llamadas simultáneas con buenos niveles de calidad cuando los nodos VoIP están separados por 8, 7 y 5 saltos, respectivamente. Por tanto, podemos concluir que BATMAN se muestra más robusto que OLSR ante condiciones adversas del canal.

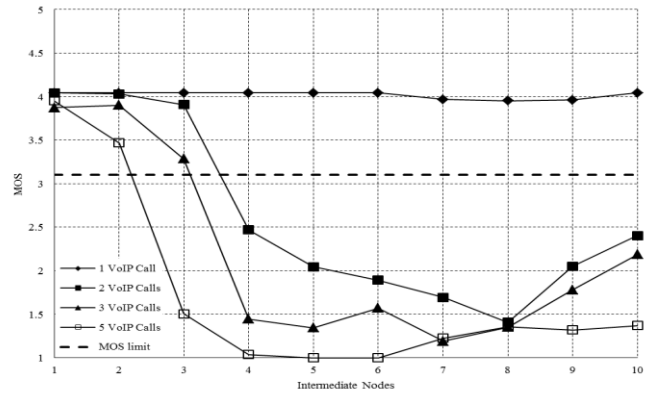
Sin embargo, OLSR obtiene mejores resultados que BATMAN es situaciones de espacio libre (véanse las Fig. 2.a y 2.c). Haciendo uso de OLSR, el sistema acepta hasta 3 llamadas VoIP simultáneas en conexiones de hasta 7 saltos y 5 llamadas VoIP en conexiones de 3 saltos. Sin embargo, con BATMAN, cuando hay más de tres saltos entre los interlocutores, sólo se acepta una llamada VoIP. De igual forma, el sistema sólo permite hasta 3 llamadas VoIP simultáneas cuando la distancia entre nodos VoIP es de hasta 3 saltos. Observando las Fig. 2.c y 2.d, se aprecia claramente que el sistema BATMAN funciona mejor en entornos con pérdidas (desvanecimiento). La pronunciada caída en el rendimiento del sistema BATMAN en entornos de espacio libre se debe a la gran cantidad de mensajes de control (OGMs) de los que hace uso. Por defecto, el intervalo entre el envío de estos mensajes por parte de un nodo es de 1 s, lo que causa un aumento de la ocupación del canal y de las colas de los nodos de la red. La Fig. 3 muestra una comparación entre el MOS obtenido con BATMAN, haciendo uso del intervalo entre OGMs por defecto (Fig 3.a) y aumentado el mismo a 2 s (Fig. 3.b). Nótese como al aumentar el intervalo entre OGMs, el número de llamadas aceptadas por el sistema y el número de saltos en los que el MOS de la llamada queda por encima del límite establecido aumenta. Con un intervalo de 2 s entre el envío de mensajes de control de BATMAN se aceptan hasta 3 llamadas con 4 nodos intermedios, obteniendo además, niveles de MOS superiores a los alcanzados con la configuración por defecto de 1 s. Para analizar más en profundidad el efecto del excesivo número de OGMs sobre la calidad de la llamada, la Fig. 4 muestra la evolución de la probabilidad de pérdida de paquetes VoIP en un escenario con 2 comunicaciones VoIP simultáneas. Podemos observar la diferencia en los niveles de pérdida de paquetes VoIP en ambos escenarios, donde claramente las pérdidas usando un intervalo de 1 s son mayores que usando un intervalo de 2 s, escenario en el que al haber menos OGMs en la red el sistema funciona mejor. De acuerdo con [15], el protocolo BATMAN se apoya en la pérdida de paquetes para su correcto desempeño. Esto se debe a la ya mencionada inundación periódica de la red de paquetes OGM por parte de todos los nodos, la cual, ante una escasa tasa de pérdida de paquetes, puede provocar el colapso de la red. Debido a que el modelo de espacio libre no introduce muchas pérdidas de paquetes, los paquetes de



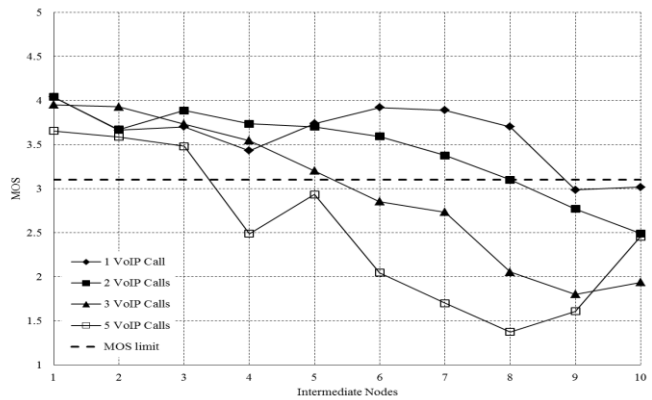
(a) OLSR. Espacio libre.



(b) OLSR. Nakagami-m.

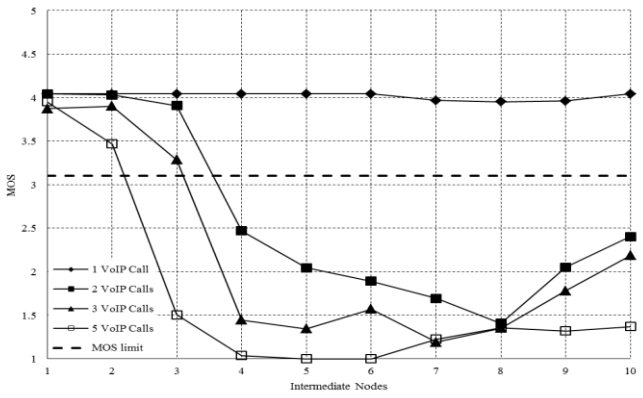


(c) BATMAN. Espacio libre.

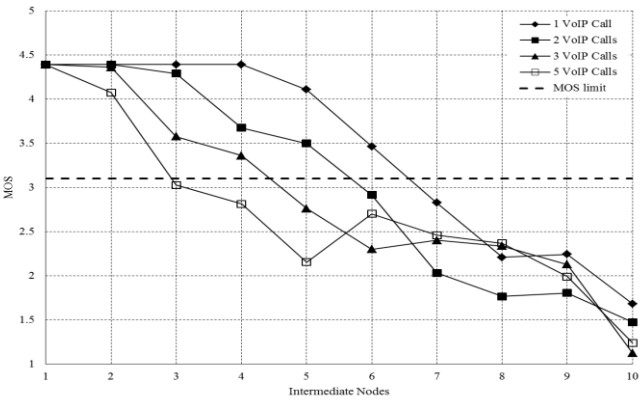


(d) BATMAN. Nakagami-m.

Figura 2. MOS obtenido para un número variable de llamadas VoIP simultaneas y de saltos entre interlocutores. Protocolo OLSR en escenarios de espacio libre (a) y Nakagami-m (b) y protocolo BATMAN en escenarios de espacio libre (c) y Nakagami-m (d).



(a) Intervalo entre OGMs: 1 s.



(b) Intervalo entre OGMs: 2 s.

Figura 3. MOS obtenido para un número variable de llamadas VoIP en el sistema y saltos entre interlocutores, usando el protocolo BATMAN con intervalo entre OGMs de 1 s (a) y 2 s (b). Entorno de espacio libre.

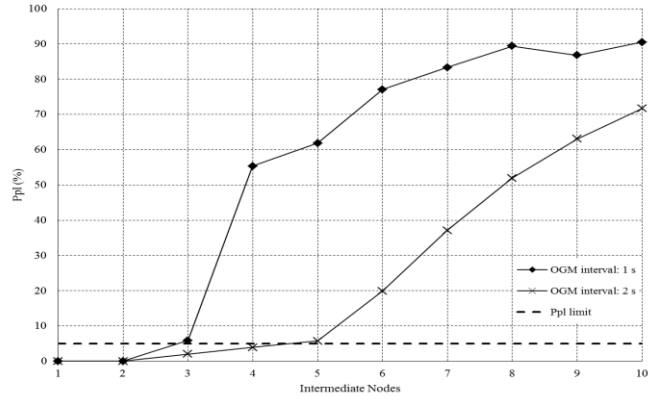


Figura 4. Probabilidad de pérdida de paquetes VoIP en espacio libre, usando dos intervalos diferentes entre OGMs de BATMAN.

control llenan las colas de los nodos, lo que afecta seriamente al tráfico VoIP, haciendo que decaiga la QoS en las transmisiones.

Respecto a la calidad de experiencia de las llamadas VoIP, los valores de MOS estimados con PESQ muestran que la calidad de las comunicaciones, en condiciones favorables del entorno, no viene determinada por el protocolo de enrutamiento empleado, puesto que el MOS obtenido es similar para ambos algoritmos. Como se muestra en la Fig. 2 el nivel máximo de MOS alcanzado es 4 empleando tanto BATMAN como OLSR. Serán las condiciones del entorno (desvanecimiento) y de la propia red (numero de nodos y disposición de estos) las que influyan directamente en los niveles de QoE alcanzados en las llamadas.

VI. Conclusiones

En este trabajo se presentan los resultados de evaluación de prestaciones del protocolo de enrutamiento BATMAN para redes MANET con transmisión de tráfico VoIP. En concreto, se ha utilizado la tecnología inalámbrica 802.11g y se han obtenido los niveles de QoE para llamadas VoIP en una topología en cadena. Los resultados obtenidos en BATMAN se han comparado con las prestaciones en idénticas condiciones del protocolo OLSR (ambos clasificados como pro-activos). En primer lugar, podemos concluir que BATMAN se ve menos afectado por el desvanecimiento en los canales (*fading*) que OLSR, dado que el tamaño de los paquetes de control en BATMAN es mucho menor que en OLSR. No obstante, en un entorno de muy bajas pérdidas, como es el de espacio libre, el protocolo BATMAN presenta unas prestaciones muy degradadas. Esto se debe, como hemos demostrado, a que el propio funcionamiento de BATMAN confía en que se producirán pérdidas en la red para un correcto funcionamiento, ya que emplea la inundación como parte de su algoritmo para el cálculo de las rutas. De lo contrario, en escenarios con bajas pérdidas, la red se ve colapsada con el tráfico generado por el propio protocolo, degradando notablemente las prestaciones de los servicios que están empleando el sistema. La calidad de las llamadas VoIP no manifiesta una mejora sustancial empleando uno u otro algoritmo; en condiciones favorables, se obtienen valores de MOS muy similares tanto para BATMAN como para OLSR, siendo las condiciones del entorno físico y de la propia red las que determinan la calidad final de la llamada.

Agradecimientos

Este trabajo ha sido financiado por el MINECO/FEDER con el proyecto TEC2010-21405-C02-02/TCM (CALM) y por el "Programa de Ayudas a Grupos de Excelencia de la Región de Murcia", de la Fundación Séneca, Agencia de Ciencia y Tecnología de la RM.

Referencias

[1] J. Lee, W. Liao, J.-M. Chen, and H.-H. Lee, "A practical QoS solution to voice over IP in IEEE 802.11 WLANs," *IEEE Communications Magazine*, vol. 47, no. 4, pp. 111–117, Apr. 2009.

[2] S. Shin and H. Schulzrinne, "Measurement and analysis of the VoIP capacity in IEEE 802.11 WLAN," *IEEE Trans. on Mobile Computing*, vol. 8, no. 9, pp. 1265–1279, Sep. 2009.

[3] R. Sanchez-Iborra, M. D. Cano, and J. Garcia-Haro, "On the effect of the physical layer on VoIP Quality of user Experience in wireless networks," in Proc. *IEEE International Conference on Communications (IEEE ICC'13) - 3rd IEEE International Workshop on Smart Communication Protocols and Algorithms (SCPA 2013)*, 2013, pp. 1056 – 1060.

[4] C. Aichele, S. Wunderlich, A. Neumann, and M. Lindner, "Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.)," *IETF Draft*, 2008.

[5] T. Clausen and P. Jacquet, "Optimized Link State Routing (OLSR) Protocol," *RFC 3626*, 2003.

[6] G. C. Sai Anand, R. R. Vaidya, and T. Velmurugan, "Performance Analysis of VoIP Traffic using various Protocols and Throughput enhancement in WLANs," in Proc. *International Conference on Computer, Communication and Electrical Technology (ICCCET)*, 2011, pp. 176–180.

[7] M. S. Islam, M. N. Islam, M. S. Alam, M. A. Riaz, and M. T. Hasan, "Performance evaluation of various vocoders in mobile ad hoc network (MANET)," in Proc. *International Conference on Electrical & Computer Engineering (ICECE'2010)*, 2010, pp. 670–673.

[8] A. Nascimento, S. Queiroz, L. Galvao, E. Mota, and E. Nascimento, "Influence of propagation modeling on VoIP quality performance in wireless mesh network simulation," in Proc. *IEEE International Symposium on Modeling, Analysis and Simulation of Computers and Telecommunication Systems*, 2008, pp. 1–3.

[9] F. Community, "Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.)"http://www.open-mesh.org/.

[10] L. B. Elis Kulla, Masahiro Hiyama, Makoto Ikeda, "Comparison of experimental results of a MANET testbed in different environments considering BATMAN protocol.," in Proc. *Third International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, 2011, pp. 1 – 7.

[11] E. Kulla, M. Ikeda, L. Barolli, and R. Miho, "Impact of source and destination movement on MANET performance considering BATMAN and AODV protocols," in Proc. *International Conference on Broadband, Wireless Computing, Communication and Applications*, 2010, pp. 94–101.

[12] A. G. Bowitz, E. G. Graarud, L. Brown, and M. G. Jaatun, "BatCave: Adding security to the BATMAN protocol," in Proc. *Sixth International Conference on Digital Information Management*, 2011, pp. 199–204.

[13] A. Morais and A. Cavalli, "Route manipulation attack in wireless mesh networks," in Proc. *IEEE International Conference on Advanced Information Networking and Applications*, 2011, pp. 501–508.

[14] "Omnet++"<www.omnetpp.org>.

[15] D. Murray, M. Dixon, and T. Koziniec, "An experimental comparison of routing protocols in multi hop ad hoc networks," in Proc. *Australasian Telecommunication Networks and Applications Conference*, 2010, pp. 159–164.

Towards a multi-criteria adaptation mechanism for time-based sliding windows

Fernando Terroso-Saenz, Mercedes Valdes-Vela, Antonio F. Skarmeta-Gomez
Dept. of Information and Communication Engineering,
University of Murcia,
Faculty of Computer Science,
Campus de Espinardo S/N, 30100 Murcia, Spain.
fterroso@um.es, mdvaldes@um.es, skarmeta@um.es

***Resumen*—Complex Event Processing (CEP) has arisen as a suitable approach to process *on-line* data in a timely way. In this frame, time-based sliding windows are an instrumental tool for CEP systems to deal with unbounded streams of events. However, defining the proper time *length* of these windows in each domain is a difficult choice. The present paper puts forward an overview of three novel adaptation solutions to dynamically adjust the length of this type of windows in runtime. Moreover, a battery of tests has been undertaken to study the particular strengths and disadvantages of each solution.**

***Palabras Clave*—Complex Event Processing (CEP), sliding window, dynamic adaptation.**

I. INTRODUCTION

On the verge of the Big Data era, which has recently emerged as one of the most important new technological topics [1], [2], Complex Event Processing (CEP) has become an important approach so as to cope with time constraints in a wide range of environments [3].

A CEP system endlessly reads the streams of events from a set of event producers. Then, it performs a set of filtering, derivation and/or aggregation operations on these streams of events to give insight into new knowledge in the form of new derived events. In the CEP scope, an event is *"an occurrence within a particular system or domain; it is something that has happened, or is contemplated as having happened in that domain"* [3].

One of the most common tasks of a CEP system is to join several streams to correlate the events of these streams. For instance, a CEP-based task dispatcher would join the stream of events informing about the workers who do not have any assigned duty and the stream of events indicating the current pending tasks in order to assign a task to each of these workers.

Since it is not possible to store the whole unbounded event streams in a bounded memory, most CEP systems rely on sliding windows to bound the streams of events and perform their operations on the events contained in the windows. Although several types of sliding windows exist, a foremost type is the time-based sliding windows [4]. This type of windows basically gathers the events of a stream received during the last t time units.

Apart from that, in certain CEP domains, the events represent real-world occurrences which last a certain period of time. For example, a CEP-based surveillance service may received as input events informing about the movement of suspicious vehicles from one location to another which are not immediate occurrences but they last a certain time interval. In these cases, a join operation should take into account in its matching policy the time intervals reported by the incoming events. In this scope, one common policy is the *join-if-overlap*. This policy states that two different events can be joined if their reported time intervals overlap as it indicates that the real-world occurrences that they represent have occurred at the same time. The interest to detect this type of *simultaneous* actions is quite frequent in many domains. For example, a network-management system receiving events reporting network errors and their time intervals could apply this join policy so as to detect if the same error has happened in two different networks at the same time. This could be a sign of a suspicious behaviour.

Nevertheless, as it has been explained above, the CEP systems make use of sliding windows to bound its incoming streams. In this frame, the t value of a time-based window has a direct impact on the results of a join using a *join-if-overlap* policy. When the t value is low, only the events emitted during the last time units are considered which might lead to the fact that not all the matches are discovered. On the contrary, if the t value is too high, it is necessary to keep more events in memory which results in a high memory consumption which may not be feasible in certain environments. Besides, the length of the time intervals reported by the events could not be fixed but vary throughout time (e.g. going from one place to another may not take two different suspicious vehicles the same time). In this frame, it is necessary to dynamically adjust the t parameter of the sliding windows in runtime by considering the trade-off between the matching detection rate and the memory consumption.

In this context, the present paper puts forward three novel possible solutions to dynamically adjust the t parameter of a time-based window. These solutions aim at CEP domains where the events report occurrences which last non-fixed time intervals. In particular, this work focuses on study the strengths and drawbacks of each solution and give an overview about which one is more suitable depending on the environment.

This work should be regarded as a first step towards the development of an eventual multi-criteria mechanism intended to adjust the length of the time-based windows of a CEP system. With the Big Data era more and more data is going to become available in the form of stream of events, and much of them will be timestamped by means of time intervals. Therefore, it is necessary to develop the instrumental tools to make CEP system capable of dealing with such type of

events. As a result, the aforementioned eventual mechanism would be useful in a varied range of applications. For instance, in a CEP movement-aware service, it could be used in order to adjust the sliding window used to correlate the stream of events informing about the trajectories of the set of moving entities, which are real-world occurrences that usually cover a period of time, to detect a set of movement interactions such as convergence, divergence and so forth.

The remainder of the paper is structured as follows, an overview of the state of the art of the CEP and sliding window domains is put forward in section II. Next, section III is devoted to explain an example scenario to completely understand the proposal. A detailed explanation of the proposed solutions is stated in section IV. Then, section V discusses the results of the different experiments performed to test all the described adaptation solutions. Finally, the main conclusions and the future work are summed up in section VI.

II. RELATED WORK

The CEP paradigm is an evolution of the former publish/subscribe model to deal with more complex subscription patterns [5]. Hence, it can be regarded as a relatively recent technology which was initially defined in [6] and comprehensively described in [3] afterwards. In the CEP domain, there have been two foremost courses of action.

On the one hand, one trend has focused on developing CEP-based solutions in those domains which may profit from the event processing capabilities of the paradigm. In this frame, an overriding line of work in the CEP domain has been the deployment of event-based systems in the business field [7], [8], [9], [10]. Nevertheless, several CEP-based proposals have gone beyond that field and have widened the CEP's usage range in several scopes such as advertisement management [11], road-traffic monitoring [12], context-aware services [13] or telemedical systems [14].

On the other hand, the other course of action pursues to develop tools and event-based languages able to process streams of events in a timely way so that the aforementioned solutions can be developed [15], [16], [17]. In this context, some works have focused on developing effective mechanisms to perform joins of event streams [18], [19]. Nevertheless, these works either focus on strategies related to the *order* in which the events must be correlated or consider that events as instant occurrences instead of lasting a time interval. Unlike these works, the present work is centred on the length of the sliding windows used for the join (not on the evaluation order of the events) and focuses on the events timestamped not with single instants but with time intervals. Consequently, this work opens a new line of work in the CEP domain in order to perform stream joins in a more efficient and accurate way.

III. ILLUSTRATIVE EXAMPLE

For the sake of clarity, an example of the *join-if-overlap* policy is shown in Fig. 1a where the events of two different streams (A and B) are joined. The projection of each event in the left axis indicates the time length of the real-world occurrence represented by the event. For example, the event a_1 informs about an occurrence that lasted from the instant t_0+1 to the instant t_0+2. Thus, such event was emitted at instant t_0+2.

According to the *join-if-overlap* policy, a correlation occurs among a set of events if their reported time intervals overlap. In total, there are 5 different matches in the event sequence depicted in the figure.

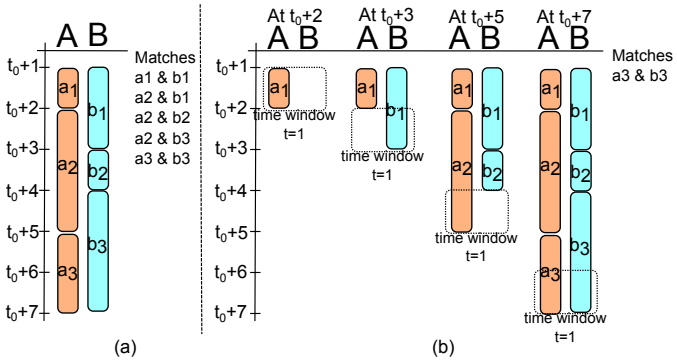


Fig. 1. Example of *join-if-overlap* join policy with no sliding window (a) and with a time-based window with (t=1). The length of each event ($a_1, ..a_3, b_1, .., b_3$) indicates the time interval covered of the occurrence they represent.

Apart from that, Fig. 1b shows the matches that would be detected if a time-based window with t=1 was used. Such window is depicted as a dashed square and it contains the events that totally or partially fit into the square. As a matter of fact, at instant t_0+3 the window only contains the event b_1, but at instant t_0+7 it contains two different events, a_3 and b_3. In that sense, only the events contained in the window can be correlated. From this figure, we can see that only 1 out of 5 correlations was detected, the one involving events a_3 and b_3 at instant t_0+7. This is because the time length of the window defined by the t parameter is too small to contain all the events that overlap at each instant. This is an example of the poor correlation capabilities that are achieved when a small time window is used.

An straightforward solution is to increase the t parameter to a much higher value so that the window contains all the events emitted during a long interval. However, this approach leads to a waste of memory resources as not all the events contained in the window will be *joinable* with the new events entering the window. As a matter of fact, if a window with t=7 was used, it would contain all the events of the sequence at instant t_0+7 (a_1-a_3 and b_1-b_3), but at such instant the events a_1, b_1 and b_2 are not *joinable* with the new incoming events (a_3 and b_3) so the window is consuming memory resources when it is not really necessary. Consequently, this also shows that defining static high t values are not a suitable solutions in memory-constrained environments.

IV. ADAPTATION SOLUTIONS

The present section is devoted to explain in detail a set of possible adaptation solutions that may be used to dynamically adjust the length of a time window in runtime so that it is suitable to contain enough events to accurately correlate different streams of events without implying a extreme consumption of resources.

A. Maximum-length adaptation

This mechanism adjusts the window's length to the maximum time interval's length reported by any received event. Hence, whenever a new event is received, its reported time interval's length is compared with current sliding window's length. Provided that the event's length is higher than the window's t parameter then this parameter is set to the event's length. Fig. 2 depicts the evolution of the window's length given the event sequence used in section III along with the detected correlations when this mechanism is used.

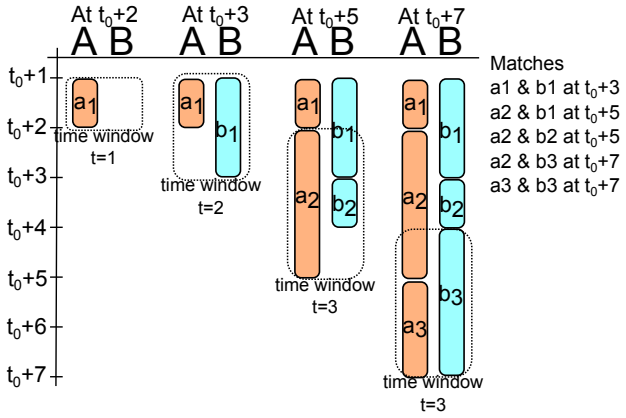


Fig. 2. Example of a window's length evolution along with the matches in the correlation when the maximum-length adaptation mechanism is used.

As this figure shows, the window length is modified each time an event reports a higher time interval than the window's one. For example, at instant t_0+3 the event b_1 is received, and its time interval's length is 2. Since such value is higher than the current window's length ($t = 1$), the window's length is set to the interval's length reported by b_1. A similar situation also occurs at instant t_0+5 with event a_2.

This mechanism is suitable to achieve high detection rates of the overlapped events, but it is also quite *greedy* in terms of memory consumption. Therefore, it is suitable for those domains where it is paramount to perform an accurate correlation of the events with no resource constraints.

B. Average-length adaptation

In this case, the window's length is the average length of the time intervals reported by all the received events. Hence, this approach pursues to adjust the window's length in a more dynamic way than the maximum length solution. Fig. 3 shows the different values of the window's t parameter given the same event sequence used in the previous sections.

The main benefit of this mechanism is that the consumption of resources is low compared to the maximum length solution. However, as a side effect, the correlation capabilities tend to decrease because the number of events contained in window is usually not enough to detect all the overlapped events. As a result, the present solution is feasible for those domains where there exist quite important resource constrains and/or it is not necessary to achieve quite accurate correlation capabilities.

C. Heuristic-based-length adaptation

The key idea of this mechanism is dynamically adjust the window's length by making use of an heuristic previously proposed in the literature to modify the step size to approach

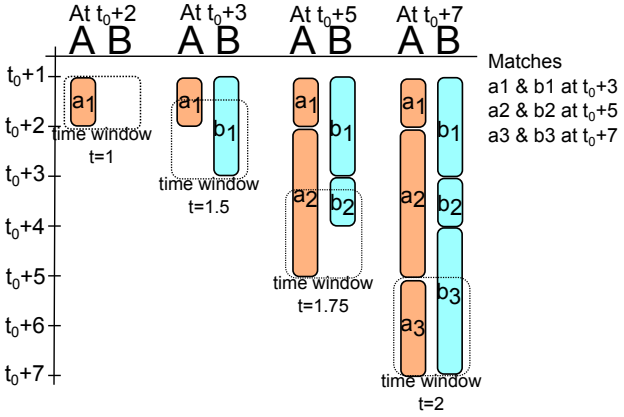


Fig. 3. Example of a window's length evolution along with the matches in the correlation when the average-length adaptation mechanism is used.

the optimum in the gradient method [20]. In particular, this mechanism modifies the sliding window's length on the basis of each new received event (e_{new}) by applying this criterion,

1) If the the current window's length is shorter than e_{new}'s time interval then it is enlarged in a win_{modify} factor.
2) If the the current window's length is larger than e_{new}'s time interval then it is shortened in a win_{modify} factor.

Besides, the size of the win_{modify} factor is also adjusted by the following criterion,

1) If the window is enlarged m times in a row then $win_{modify} = (1 + p)win_{modify}$.
2) If the window is shortened n times in a row then $win_{modify} = (1 - q)win_{modify}$.

The parameters win_{modify}, m, n, p and q are domain-dependant because depending on their values the window's length will be modified in many different ways. In this frame, Fig. 4 shows how a window's length changes according to this mechanism when win_{modify}=1, m=2, n=2, p=0.25 and q=0.2

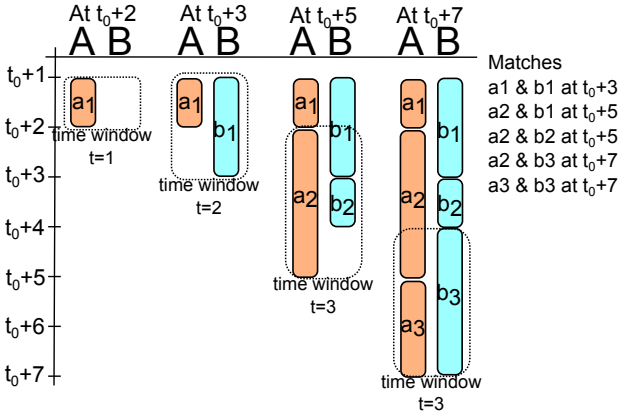


Fig. 4. Example of a window's length evolution along with the matches in the correlation when the heuristic-based-length adaptation mechanism is used.

According to the figure, the window's length is increased at some instants during the event sequence's lifespan. For example, it is increased in 1 time unit (the value of win_{modify}) at instant t_0+3 because the new received event (e_{new}), which in this case is b_1, has an interval's length higher that the current length of the window. At instant t_0+5, the window's length is

also increased as the new received event a_2 reports a higher time interval (3) than the current window's one (2), so the length of the window is increased in win_{modify} time units (1).

By means of this mechanism, it is possible to adjust a window's length in a more accurate way than when the average length mechanism is used. However, the heuristic logic can lead to an extra computing effort which might be unsuitable in quite demanding scenarios.

All in all, the three described mechanisms offer quite different behaviours to adjust a time-based window. Whilst the maximum length can be viewed as an almost-static mechanism where the length of the window is only modified when a particular condition occurs, the average and the heuristic-based length approaches are less reluctant to modify the window's length. In order to give insight into the particular capabilities of each of these mechanism, a set of tests have been carried out. The results of these tests are put forward in the next section.

V. VALIDATION OF THE SOLUTIONS

A. Preliminaries

The three aforementioned mechanisms were tested by means of several simulations. These simulations have been developed whereby the CEP platform Esper [21]. Esper is a well-established GNU open-source CEP tool that has already been used in several research projects [12], [11].

Esper defines its own stream-oriented *Event Processing Language* (EPL) which comprises several built-in tools such as sliding windows or aggregation functions. The EPL syntax is based on SQL-92 and, among its features, it allows to define *continuous queries* (CQs) to process the events from one or more streams. A CQ is deployed once and it continuously produces new results as new events arrive through its incoming streams. Moreover, Esper also features a CEP engine embedded in Java able to execute the defined CQs.

For the present work, it was defined a CQ that joined the streams of two different events (*testEventA* and *testEventB*). Such CQ is depicted in listing 1.

```
select
 A.id + "_" + A.iTime + "_" + A.fTime,
 B.id + "_" + B.iTime + "_" + B.fTime
from
 TestEventA A unidirectional,
 TestEventB.win:expr(getWinSize()) B
where
 B.fTime.between(A.iTime,A.fTime)
```

Listing 1. Simplified version of join CQ to test the adaptation mechanisms.

The *from* clause defines the two incoming streams the CQ is intended to process where the *unidirectional* keyword indicates that the CQ should be executed each time a new *testEvent A* is received. Furthermore, the CQ uses an Esper's built-in sliding window (*win:expr*) to bound the stream of *testEventBs*. This type of window allows to modify its time length in runtime. In that sense, the *getWinSize* is an ad-hoc method that returns the window's length calculated by the adjustment method used at each moment. Apart from that, the *where* clause lists the correlation condition that must be fulfilled so that a match arises. In that sense, such condition indicates that two events must overlap as the *iTime* and *fTime* attributes define the initial and final time of the time interval reported by each event. This condition corresponds to the *join-if-overlap* policy. Finally, the *select* clause defines the information that must be composed when the *where* conditions are fulfilled.

This CQ has been used to undertake several experiments to study the adjustment mechanisms. In particular, those experiments have focused on two features, 1) the number of overlapped events that the aforementioned CQ was capable of detecting when each mechanism was used (the detection rate), 2) the memory consumption f each mechanism.

B. Result Discussion

Fig. 5 shows the detection rate (DR) for the three mechanism. Its value has been calculated by means of the following formula,

$$DR = \frac{\#\ detected\ pairs\ of\ overlapped\ events}{\#\ totalpairs\ of\ overlapped\ events}$$

Whilst the numerator stands for the number of pairs of overlapped events (*testEventA*, *testEventB*) that the join CQ was capable of detecting by using a particular adaptation mechanism, the denominator indicates the total number of pairs of overlapped events contained in the incoming streams processed by the CQ.

Apart from that, the x-axis of Fig. 5 indicates the maximum length of the interval reported by any event. For instance, the value 10000 in such axis indicates that the events in that experiment could report randomly-generated time intervals ranging from 1 to 10000 seconds. Hence, the higher the value is, the more varied the time intervals of the events.

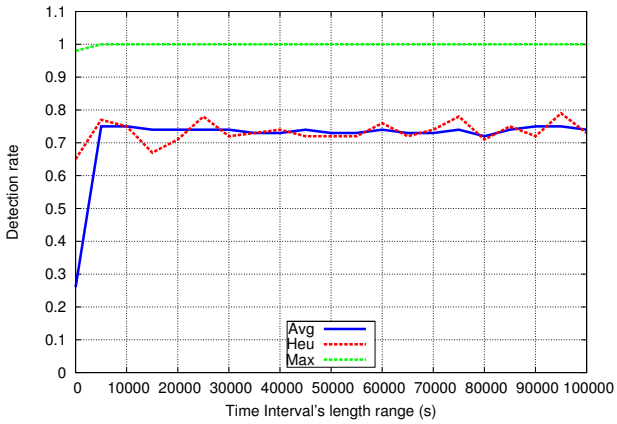


Fig. 5. Detection rate of the mechanisms with different event's time intervals.

As for the results, Fig. 5 depicts that the maximum-length mechanism achieved the highest DR in all the experiments. This is because such mechanism is the one that makes the sliding window used by the join CQ contain more *TestBEvents*. Hence, each time a new *TestAEvent* is received, it is possible to correlate it with more *TestBEvents* than when the other two mechanism are used. This leads to detect more matches with the maximum length approach.

Nevertheless, both the average and the heuristic-based solutions achieved fairly good results in all the experiments as their average DR was roughly 0.7 which might be suitable in domains where it is not essential that all the overlapped events

are detected. In this frame, the variability of the heuristic-based results is due to the fact that, depending on the arrival order of the events, the system will converge to an appropriate window size more or less fast and, as a result, it will detect more or less matches.

Furthermore, Fig. 6 show the memory consumption of each mechanism. As expected, the maximum-length mechanism was the one which required more memory resources. On the contrary, the heuristic-based and the average-length approaches reduced the memory consumption with respect to the maximum length solution in at least 1000 KB in all the experiments. This is particularly noticeable with small time intervals (10s) where the average-length mechanism outperformed the other two approaches by consuming 2596KB less than the maximum-length mechanism (a 31% decrease) and 1443KB less than the heuristic-based length (a 20% decrease).

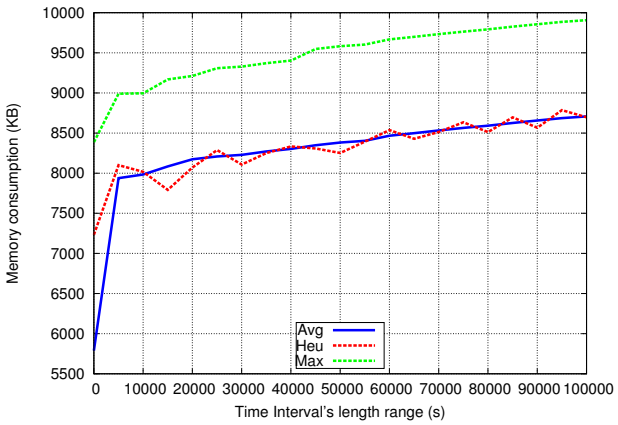


Fig. 6. Memory consumption (in kilobytes) of the mechanisms with different event's time intervals.

Finally, the trade-off between the *accuracy* of each mechanism (its DR) and its memory consumption was also studied. This would provide a comprehensive overview about the effectiveness of each mechanism. In this frame, Fig. 7 shows the relationship between the DR and the memory consumption for each mechanism. In particular, it shows the result of dividing the memory consumption by the achieved DR of each experiment. This way, the lower the value, the better.

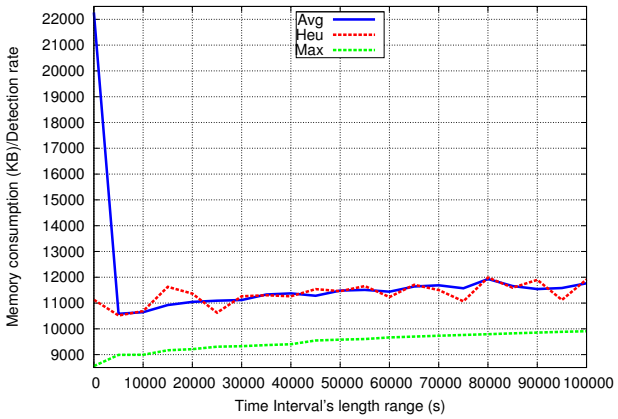


Fig. 7. Trade off rate between the detection rate and the memory consumption of each mechanism.

As the figure depicts, the maximum-length solution clearly improved the other two mechanisms. The rationale of this fact is that although the maximum-length approach is quite *greedy* in terms of memory usage, it is also true that its DR results are quite high (roughly 1.0 in almost all the experiments according to Fig. 5). Similarly, the other two solutions achieved worse results than the maximum-length one because their low memory consumption did not overcome the fact that their DRs are much poorer than the maximum-length ones.

To conclude, experimental results have proved that the maximum-length mechanism is, without a shadow of a doubt, the best option of the ones described in this work when it comes to achieve high DR. Furthermore, tests have also shown that the trade-off between its DR capabilities and its memory consumption requirements is also the best of all the proposed solutions. However, both the average-length and the heuristic-based-length mechanisms have achieved quite good results in terms of memory usage. Since their DR results are quite similar, any of them could be used as an alternative to the maximum-length mechanism in environments where saving memory resources is a very important factor.

VI. CONCLUSIONS AND FUTURE WORK

At the dawn of the Big Data era, the Complex Event Processing (CEP) paradigm has arisen as a suitable approach to timely deal with huge amounts of streaming data. When it comes to perform is event-based operations, most CEP systems make use of sliding windows in order to bound the its incoming event streams. In this frame, one of the most common actions carried out by a CEP system is to join streams of different events to correlate them.

The present work states a set of novel solutions to dynamically adjust the length of the time-based sliding windows aiming to optimize stream joining. In particular, three different approaches have been presented. Each of them follow a quite different criteria so as to modify a window's length in runtime. As the test results have shown, each mechanism is suitable for certain types of environments considering the available memory resources and the desired correlation capabilities.

The final goal of the course of action initiated by this work is the development of a multi-criteria adjustment mechanism for sliding windows. This mechanism will combine the three approaches described in this paper and select the most appropriate in runtime depending on both the available resources and the characteristics of the events composing the incoming events. Afterwards, this mechanism could be integrated in any CEP system where the correlation of events is a paramount task. To sum up, by means of this mechanism, it is intended to ease the development of future CEP applications.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 241598 (SeaBILLA project) and from the Fundación Séneca Programme for Helping Excellent Research Groups 04552/GERM/0.

REFERENCIAS

[1] J. Bughin, M. Chui, and J. Manyika, "Clouds, big data, and smart assets: Ten tech-enabled business trends to watch," *McKinsey Quarterly*, vol. 56, 2010.

[2] S. Prentice, "CEO advisory: Three technology trends at the leading edge you cannot afford to overlook in 2012," Gartner, Tech. Rep., 2012.

[3] O. Etzion and P. Niblett, *Event Processing in Action*. Manning Publications, 2010.

[4] B. Babcock, M. Datar, and R. Motwani, "Sampling from a moving window over streaming data," in *Proceedings of the thirteenth annual ACM-SIAM symposium on Discrete algorithms*, ser. SODA '02. [Online]. Available: http://dl.acm.org/citation.cfm?id=545381.545465

[5] A. Margara and G. Cugola, "Processing flows of information: from data stream to complex event processing," in *Proceedings of the 5th ACM international conference on Distributed event-based system*, ser. DEBS '11. New York, NY, USA: ACM, 2011, pp. 359–360.

[6] D. Luckham, *The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems*. Addison-Wesley Professional, 2002.

[7] B. Magoutas, D. Riemer, D. Apostolou, J. Ma, G. Mentzas, and N. Stojanovic, "An Event-Driven System for Business Awareness Management in the Logistics Domain," in *Business Process Management Workshops*, ser. Lecture Notes in Business Information Processing, M. Rosa and P. Soffer, Eds. Springer Berlin Heidelberg, 2013, vol. 132, pp. 402–413. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-36285-9_43

[8] M. Daum, M. Götz, and J. Domaschka, "Integrating CEP and BPM: how CEP realizes functional requirements of BPM applications (industry article)," in *Proceedings of the 6th ACM International Conference on Distributed Event-Based Systems*, ser. DEBS '12. New York, NY, USA: ACM, 2012, pp. 157–166. [Online]. Available: http://doi.acm.org/10.1145/2335484.2335503

[9] A. Adi, D. Botzer, G. Nechushtai, and G. Sharon, "Complex event processing for financial services," in *IEEE Services Computing Workshops*, vol. 0, 2006, pp. 7–12.

[10] N. Museux, J. Mattioli, C. Laudy, and H. Soubaras, "Complex Event Processing approach for Strategic Intelligence," in *Proc. 9th Int. Conf. on Inf. Fusion*, 2007, pp. 1–8.

[11] P. Evensen and H. Meling, "AdScorer: an event-based system for near real-time impact analysis of television advertisements (industry article)," in *Proceedings of the 6th ACM International Conference on Distributed Event-Based Systems*, ser. DEBS '12. New York, NY, USA: ACM, 2012, pp. 85–94. [Online]. Available: http://doi.acm.org/10.1145/2335484.2335494

[12] F. Terroso-Saenz, M. Valdes-Vela, C. Sotomayor-Martinez, R. Toledo-Moreo, and A. Gómez-Skarmeta, "A Cooperative Approach to Traffic Congestion Detection With Complex Event Processing and VANET," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 13, no. 2, pp. 914–929, 2012.

[13] F. Terroso-Sáenz, M. Valdés-Vela, F. Campuzano, J. Botía, and A. F. Skarmeta-Gómez, "A complex event processing approach to perceive the vehicular context," *Information Fusion*, no. 0, pp. –, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1566253512000723

[14] S. Meister, "Telemedical Events: Intelligent Delivery of Telemedical Values Using CEP and HL7," in *Workshops on Business Informatics Research*, ser. Lecture Notes in Business Information Processing, L. Niedrite, R. Strazdina, and B. Wangler, Eds. Springer Berlin Heidelberg, 2012, vol. 106, pp. 1–13. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-29231-6_1

[15] A. Adi and O. Etzion, "Amit - the situation manager," *The VLDB Journal*, vol. 13, no. 2, pp. 177–203, May 2004. [Online]. Available: http://dx.doi.org/10.1007/s00778-003-0108-y

[16] S. Schwiderski-Grosche and K. Moody, "The SpaTeC composite event language for spatio-temporal reasoning in mobile systems," in *Proceedings of the Third ACM International Conference on Distributed Event-Based Systems*, ser. DEBS '09. New York, NY, USA: ACM, 2009, pp. 11:1–11:12. [Online]. Available: http://doi.acm.org/10.1145/1619258.1619273

[17] R. Strom, C. Dorai, G. Buttner, and Y. Li, "Smile - distributed middleware for event stream processing," in *Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on*, 2007, pp. 553–554.

[18] L. Golab and M. T. Özsu, "Processing sliding window multi-joins in continuous queries over data streams," in *Proceedings of the 29th international conference on Very large data bases - Volume 29*, ser. VLDB '03. VLDB Endowment, 2003, pp. 500–511. [Online]. Available: http://dl.acm.org/citation.cfm?id=1315451.1315495

[19] R. Gwadera, "Multi-stream join answering for mining significant cross-stream correlations," *Frontiers of Computer Science*, vol. 6, no. 2, p. 131–142, 2012. [Online]. Available: http://dx.doi.org/10.1007/s11704-012-2862-8

[20] J. S. R. Jang, C. T. Sun, and E. Mizutani, *Neuro-Fuzzy and Soft Computing. A computational Approach to Learning and Machine Intelligence*. Prentice-Hall Inc., 1997.

[21] Espertech. (2012) Esper reference documentation, version 4.6. [Online]. Available: http://esper.codehouse.org

Optimal Distribution of Remotely-Subscribed Multicast Traffic within a Proxy Mobile IPv6 Domain by Using Explicit Multicast

Luis M. Contreras *, Carlos J. Bernardos †
* Core Network Evolution
Telefónica I+D
Don Ramón de la Cruz, 82-84, 28006, Madrid, Spain
† Departament of Telematics Engineering,
Universidad Carlos III de Madrid
Avda. Universidad, 30, 28911, Leganés, Spain.
lmcm@tid.es, cjbc@it.uc3m.es

Abstract— **Distribution of remotely subscribed multicast content in a Proxy Mobile IPv6 (PMIPv6) domain is performed by means of bi-directional IP-in-IP tunnels established between the mobility anchor and the visited access gateways where the mobile terminals consuming such traffic are attached to. Each access gateway subscribing to content on behalf of an attached mobile terminal requires a separate copy of the remote multicast flow being distributed over the PMIPv6 domain. In many cases, these individual copies traverse the same routers in the path from the mobility anchor towards the access gateways, incurring in an inefficient distribution, which is equivalent to the unicast delivery of the remote multicast content within the domain. This paper explores the potential gain obtained by using explicit multicast instead of the standard IP-in-IP tunneling, showing relevant capacity savings with lower overhead respect to the standard distribution case. This transport service based on explicit multicast emerges then as an attractive transport alternative for PMIPv6 domain operators serving visiting mobile multicast consumers.**

Keywords-component; PMIPv6; multicast; xcast; optimization.

I. INTRODUCTION

The new capabilities being offered by the mobile wireless technologies are bringing broadband capacity networks outside the home, representing additional delivery options for the distribution of broadband services on the move. The commercial success of mobile multimedia-enabled terminals, mainly because of the success of iOS and Android based devices, is rapidly increasing the demand of mobile data access, especially audiovisual contents.

IP multicast basically facilitates the delivery of a single copy of a data stream to multiple listeners interested in receiving the same content simultaneously. This capability is commonly used nowadays in telecom networks, for instance, to distribute TV content (known as IPTV service). The need for supporting the same kind of services both in fixed and mobile networks brings the necessity of delivering IP multicast also to mobile receivers.

Proxy Mobile IPv6 (PMIPv6) [1] is a network-based mobility management protocol which enables the network to provide mobility support to standard IP terminals residing in the network. These terminals enjoy this mobility service without being required to implement any mobility-specific IP operations. Namely, PMIPv6 is one of the mechanisms adopted by the 3GPP to support the mobility management in future Evolved Packet System (EPS) networks [2].

PMIPv6 allows a Mobile Access Gateway (MAG) to establish a distinct bi-directional tunnel with different Local Mobility Anchors (LMAs), being each tunnel shared by the attached Mobile Nodes (MNs). Each mobile node is associated with an LMA, which keeps track of its current location, that is, the MAG where the mobile node is attached. IP-in-IP encapsulation is used within the tunnel to forward traffic between the LMA and the MAG (see Figure 1).

The basic solution [3] of multicast traffic distribution within a PMIPv6 domain makes use of the bi-directional LMA-MAG tunnels. It follows the so-called remote subscription model, in which the subscribed multicast content is delivered from the Home Network. By doing so, an individual copy of every multicast flow is delivered through each tunnel connecting the mobility anchor to any of the access gateways in the domain. In many cases, these individual copies traverse the same routers in the path towards the access gateways, incurring in an inefficient distribution, equivalent to the unicast distribution of the multicast content in the domain, as shown in Figure 2.

This fact leads to distribution inefficiencies and higher per-bit delivery costs, incurred by a PMIPv6 domain operator offering transport capabilities to a Home Network operator for serving their MNs when attached to the PMIPv6 domain. As long as the remotely subscribed multicast service is not affected, it seems worthy to explore more optimal ways of distributing such content within the PIMPv6 domain.

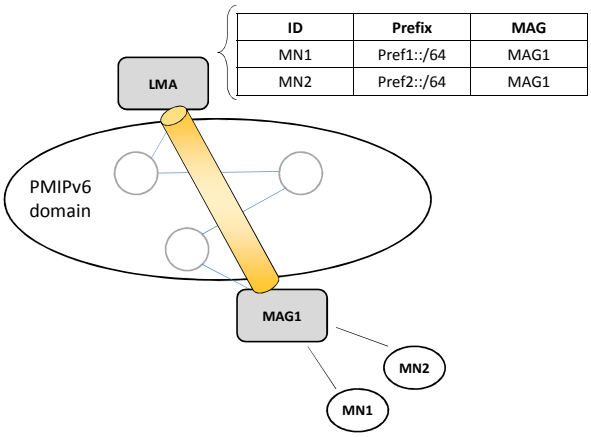


Figure 1. PMIPv6 mode of operation

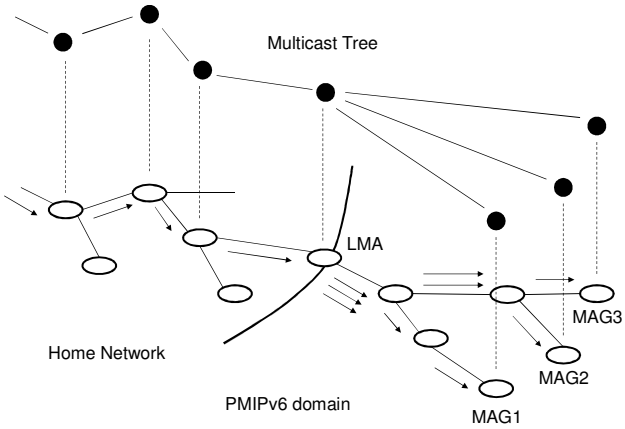


Figure 2. Inefficient distribution of remote subscribed multicast traffic in a PMIPv6 domain

As later discussed, local multicast distribution to the PMIPv6 domain (also known as *direct routing*) is not always feasible then we focused on the remote subscription case. This paper addresses this issue by analyzing the capabilities provided by Explicit Multicast (Xcast) [4] to provide an optimal and efficient multicast traffic distribution from the bandwidth consumption point of view. Section II describes the different alternatives existing today for multicast traffic distribution within a PMIPv6 domain, remarking the potential inefficiency observed in case of remotely-subscribed multicast. Section III introduces the applicability of the explicit multicast for the distribution of the multicast flows in the domain, and extensions needed for using explicit multicast in PMIPv6 are identified. Furthermore, in Section IV a performance evaluation is conducted to assess the potential gains due to the use of explicit multicast in the distribution network. Section V addresses some conclusions and advances some further work. Finally, Appendix A provides some insights on the PMIPv6 domain scalability to determine the viability of the proposed explicit multicast approach.

II. MULTICAST DISTRIBUTION IN PMIPV6

As a general procedure for subscribing to a multicast content, a mobile node expresses its interest in joining or leaving a multicast group by sending Multicast Listener Discovery (MLD) control messages to the MAG, which acts as the first hop at the point-to-point link established with the MN. The MAG maintains the individual multicast status of the interface for that link and handles the multicast traffic towards the MN accordingly to the MLD messages received. There are two alternatives to distribute multicast traffic within a PMIPv6 domain: remote subscription and direct routing.

The former is primary focused on the multicast distribution from networks outside the PMIPv6 domain (e.g., the Home network or third parties networks), while the later results convenient for the multicast distribution of content locally available at the PMIPv6 domain.

A. *Remote subscription*

The baseline solution [3] considers only the remote subscription case, where the MN obtains the desired multicast stream from its home network, through the local mobility anchor. The LMA is in charge of interacting with the multicast infrastructure out of the PMIPv6 domain.

In the base solution, the MAG instantiates a distinct MLD proxy functionality per every set of MNs associated to a specific LMA. Each MLD proxy instance is responsible of summarizing the subscription requests of the MNs connected to it on a per LMA association basis. The different proxy instances of the same MAG are isolated one from the other.

With the remote subscription model, the multicast traffic reaches the MNs after going through the corresponding LMA (note that there might be multiple LMAs in the same domain). For every proxy instance in the MAG, the tunnel interface pointing to the LMA becomes the proxy upstream interface, whereas the links towards the MNs are the corresponding downstream interfaces of each instance.

Then, every MAG-LMA tunnel is part of a separate MLD proxy domain, being a branch of the multicast tree built for multicast traffic distribution internally to the domain. A single copy of a data stream will be sent per group of MNs (attached to a certain MAG) associated to the same LMA. The LMA will maintain the multicast state of every tunnel interface, reflecting the summarized view offered by the MAG on behalf of the attached MNs bound to the LMA.

The base solution suffers from the tunnel convergence problem, where several copies from the same multicast stream can reach the access gateway when simultaneous subscriptions from MNs associated to distinct LMAs occur.

To avoid that, a central entity named Multicast Tree Mobility Anchor (MTMA) [5] can be deployed in the PMIPv6 domain to act as the topological anchor point for remotely serving multicast traffic to the MNs in the domain, independently of the LMA which maintain the association for receiving unicast traffic.

The MTMA connects to the MAG as described in [3]. The bi-directional tunnels among the MTMA and the access

gateways in the domain are part of the multicast tree for remote multicast traffic distribution. Therefore, a copy of every multicast channel subscribed by a MAG on behalf of an attached MN is transported on those tunnels to reach the corresponding access gateway. The MTMA can be then considered as a form of upstream multicast router with tunnel interfaces allowing remote subscription for the MNs.

B. *Direct routing*

A second option to limit the number of copies of the same content at the MAG is the usage of a native multicast infrastructure in the PMIPv6 domain [5] allowing direct multicast routing from locally available multicast sources. In this case, the MAG can be directly connected to an upstream multicast router in the PMIPv6 domain, while the unicast traffic remains served as normally by the corresponding LMAs.

Following this approach, the usage of the bi-directional tunnels is totally avoided, since the multicast traffic is natively distributed within the PMIPv6 domain. This is the most effective way of multicast distribution within the domain, but unfortunately it is not always possible for non-technical reasons, such as for example:

- The multicast source is not local to the PMIPv6 domain, being located either in the Home network or hosted by a third party.
- The multicast content cannot be natively distributed within the local PMIPv6 domain due to administrative or regulatory reasons; as for instance, multicast address allocation issues between the assigned addresses in the local PMIPv6 domain and in the multicast source home network (i.e., a certain multicast IP address identifies different multicast content channels in both the Home and the PMIPv6 domains), or some contents may be not allowed for distribution in a certain network, like regional or ethnical channels out of the target region.
- The multicast content is not natively distributed in the local PMIPv6 domain due to commercial and business intelligence reasons; for instance, the Home network operator might not be interested on providing visibility about what content its MNs subscribe to.

These are some of the reasons why the remote subscription case is relevant and requires to be properly addressed. PMIPv6 domain operators can commercialize this service, offering transport capabilities to the Home network operators to reach its MNs with a multicast service. Providing this transport service in the most efficient manner is then economically attractive from the PMIPv6 domain operator point of view.

C. *Efficiency problems*

The transport of the remotely-subscribed multicast traffic by means of IP-in-IP unicast tunnels in the PMIPv6 domain is inefficient as several copies of the same content traverse the same links and are forwarded by the same routers. Two alternatives to improve this distribution can be taken into account: native multicast transport (direct routing) on the PMIPv6 domain, or explicit multicast (Xcast) transport of the multicast traffic. The former has been already described, and some situations could prevent its use. We now focus on the latter, by proposing the use of IP-in-Xcast encapsulation between the mobility anchor and the access gateways instead of the standard IP-in-IP tunneling.

III. MULTICAST DISTRIBUTION AMONG MOBILITY ANCHOR AND ACCESS GATEWAYS WITH EXPLICIT MULTICAST

A. *Introduction to Xcast*

The Xcast protocol has been proposed as a way of optimizing the delivery of multicast traffic for small groups. Basically, the Xcast mechanism eliminates the need of per-session signaling and per-session state information of traditional IP multicast schemes by including the list of destinations in the data packet, instead of using a multicast address. To do that, the source node keeps track of the final destinations in the multicast channel that it wants to send packets to.

With Xcast, each router in the path between the source and the destination parses the header and creates a new datagram for every next hop including only the destinations reachable through that next hop according to the routing table, in such a way that the header of the subsequent Xcast packets only contains the destinations available in the path. The Xcast packet always follows the ordinary unicast routing for a given destination.

When just one destination remains to be reached, the Xcast packet is transformed into a normal unicast packet. Figure 3 graphically describes the Xcast procedures for the case in which a node A simultaneously delivers data content to nodes B, C and D with Xcast encapsulation.

The processing that a router does for every Xcast packet is the following: *(i)* the router performs a route table lookup to determine the next hop for each of the destinations listed in the packet; *(ii)* the router partitions the set of destinations based on their next hops; *(iii)* it replicates the packet so that there is one copy of the packet for each of the next hops found in the previous steps; *(iv)* before delivering the new packet, it modifies the list of destinations in each of the copies so that the list in the copy for a given next hop includes just the destinations reachable through that next hop; *(v)* finally, the router sends the modified copies of the packet on the next hops.

B. *Benefits and impacts of using Xcast*

Regarding traditional multicast, Xcast offers a number of advantages that have been reported on [4], such as not needing to maintain multicast state per group in every router on the tree, or not requiring multicast address allocation. However, some drawbacks have also been identified, such as the incurred overhead, or the header processing complexity. Furthermore, as described later in the paper, the specified Xcast header allows a maximum of 127 destinations. This means that in case of having more destinations on the path, separate Xcast trees should be formed.

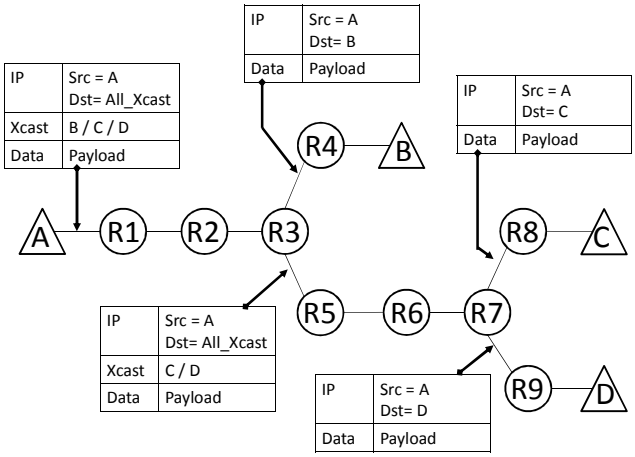


Figure 3. Explicit multicast (Xcast) mode of operation

This implies that, when applied to the PMIPv6 case, a limit of 127 access gateways per mobility anchor's downstream interface has to be considered in the distribution tree. In the Appendix A the number of access gateways in a domain is discussed in order to determine how this limit could impose restrictions in a typical PMIPv6 domain for the deployment of Xcast functionalities.

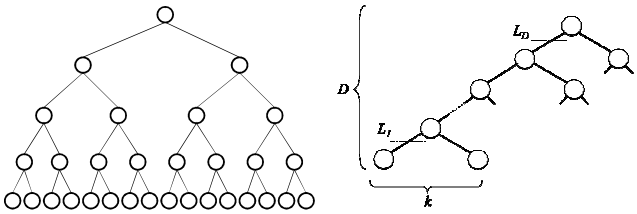
C. *Modifications to standard PMIPv6 procedures for using Xcast in a domain*

The MAG does not change its behavior and subscribes to the multicast content on behalf of the MNs (acting as a proxy) by using a multicast group membership protocol such as MLD. The multicast content requests will reach the mobility anchor through the tunnel, following the standard IP-in-IP encapsulation [1]. The mobility anchor will act as an Xcast source, and will take the decision of encapsulating the multicast traffic in an IP-in-Xcast mode in its downstream interfaces reaching the MAGs, instead of using the standard IP-in-IP tunnel.

The router present in the bifurcation point in the end to end path providing connectivity the last segment to reach a MAG (i.e., no more MAGs reachable through that branch from that router), will send the multicast packet in unicast fashion as in the IP-in-IP case (see Figure 2), so the MAG will not perceived any change in the multicast distribution regarding the standard case.

Two ways of Xcast distribution can be considered. On one hand, it can be considered that all the subscriptions between a set of MAGs and the mobility anchor are distributed over the same IP-in-Xcast tunnel, grouping all the multicast channels subscribed for a certain group of MAGs. On the other hand, it can be considered that a separate IP-in-Xcast tunnel is used per multicast channel.

The tunnel management is very complex in the first case, as the tunnel has to be dynamically updated. Furthermore, different subscription groupings should be arranged according to the subscriptions existing on the MAGs. The second case is simpler, and it is the one selected in this paper.



(a) (b)

Figure 4. Exampleof *k-tree* structure with *k*=2 and *D*=4 (a), and parameters defining a a *k-tree* structure (b).

D. *Handover dynamics using Xcast*

In the event of a handover, the movement of an MN can produce the need of creating a new branch for the distribution of the multicast content to the MAG where the MN is being attached (in case there is no other MN in that MAG subscribed to the desired content). Similarly, such movement can produce the removal of an existing branch from the MAG where previously it was attached (in case the MN was the last subscriber to a certain content).

As the LMA is aware of the channels subscribed per MAG in the remote subscription case, the LMA has to take the decision of Xcast forwarding to the MAG. When a new branch has to be formed due to a handover event, it will simply mean the need of adding a new destination to the Xcast header pointing to the requesting MAG. Furthermore, when an existing branch has to be removed also for a handover event, the LMA has just to remove the corresponding MAG from the desired destinations from the Xcast header.

IV. PERFORMANCE COMPARISON

A. *Definition of the scenarios under analysis*

In order to evaluate and compare the potential gains in the use of Xcast for transporting the multicast traffic between the mobility anchor and the access gateways within a PMIPv6 domain, we will model the distribution tree with a *k-tree* structure as considered in [6]. Figure 4 (a) shows an example of a *k-tree* composed by a total number of 31 nodes (i.e., *k*=2, *D*=4).

A *k-tree* structure can be characterized by two parameters, as depicted in Figure 4 (b): *k*, the degree of the tree or number of leaves recursively found from every previous leaf on the tree, and *D*, the depth of the tree, which indicates the number of levels in the distribution tree.

N, the total number of nodes in a certain *k-tree*, is given by:

$$N = \frac{k^{D+1} - 1}{k - 1}, \tag{1}$$

while the number of potential receivers (MAGs in this analysis), *m*, is obtained from:

$$m = k^{D} \tag{2}$$

B. *Performance evaluation*

The performance evaluation of Xcast versus the standard distribution is carried out by comparing the number of traversed links between the mobility anchor and the access gateways when each of these solutions is used to distribute a multicast channel.

1)General calculation

The previous calculation has considered that all MAGs subscribe to the same content. While this can be true for highly demanded content, it cannot be generalized. In this section we try to formulate the generic calculation of the links traversed in a PMIPv6 as a function of the demand.

A certain channel will be subscribed by the MAG if there is at least one attached MN demanding such channel. Let us consider p as the probability of a MAG demanding a certain channel, then it can be established that $p=1$ if there is at least an MN requesting the channel, and $p=0$ otherwise.

Then, in the standard case, the links traversed for serving the MAGs demanding the channel will be:

$$L_{MAG}^{std} = p \times D \,. \tag{3}$$

The total number of links traversed in the PMIPv6 domain can be established on:

$$L_{Total}^{std} = \sum_{i=1}^{m} p_i \times D = D \times \sum_{i=1}^{k^D} p_i \tag{4}$$

For the Xcast case, it is a bit more complex to calculate the link usage, as the usage at a level of the tree depends on the usage of the following level, as can be derived from Figure 4. A link of a certain level will not be traversed if none of the receivers (MAGs) below it subscribes to such content. This can be formulated in the following way:

$$L_1^{Total} = \sum_{i=1}^{m} (1-(1-p_i)) = \sum_{i=1}^{k^D} (1-(1-p_i)) \tag{5}$$

$$L_2^{Total} = \sum_{i=1}^{m/k} (1-(1-p_i)^k) = \sum_{i=1}^{k^{D-1}} (1-(1-p_i)^k), \tag{6}$$

and, in general:

$$L_d^{Total} = \sum_{i=1}^{m/k^{(d-1)}} (1-(1-p_i)^{k^{(d-1)}}) = \sum_{i=1}^{k^{D-(d-1)}} (1-(1-p_i)^{k^{(d-1)}}) \cdot \tag{7}$$

Then, the total number of links traversed in the Xcast case will be the sum of the links used for all the levels, given by:

$$L_{Total}^{Xcast} = L_1^{Total} + L_2^{Total} + \ldots + L_D^{Total} \tag{8}$$

Figures 5 and 6 show the comparison of the gain obtained for different *k-trees* distribution architectures connecting the same number of mobile access gateways, as a function of the probability of subscription p for a certain multicast channel per MAG (note that the probability of subscription of any MAG is independent of the probability of subscription of the other MAGs in the domain, then it can be stated that $p_i = p$, $\forall i$, assuming a similar average number of MNs per MAG). In the first figure, 64 MAGs are connected through two different *k-tree* structures, with 8 degrees and 2 depth levels in one case, and 4 degrees and 3 depth levels in the second. The number of intermediate nodes changes, obtaining in the first case a flatter architecture.

The second figure, considering 729 MAGs (which can be connected either by *k-trees* of parameters k=9 and D=3, or k=3 and D=6), is presented to evaluate the sensitivity of Xcast to the growth in the number of connected MAGs, only for illustrative purposes, as such high number of MAGs cannot be included in a unique Xcast tree due to the limitation on the number of destinations per Xcast header.

As observed from Figures 5 and 6, more hierarchical *k-tree* structures provide more savings that their flattened counterparts for connecting the same number of MAGs. This trend is more significant as the number of MAGs in the tree increases. The gain increases rapidly with the probability of subscription per MAG p, and it is asymptotically bounded, which means that the maximum network resource savings are closely reached even for moderately popular channels. Finally, it can be concluded that higher savings are obtained as the number of MAGs grows in the domain.

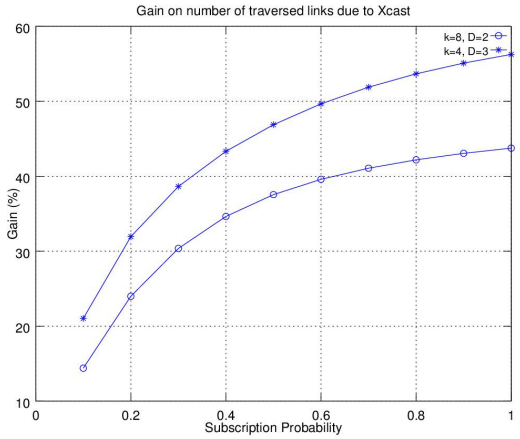


Figure 5. Gain due to multicast for two different *k-tree* structures connecting 64 MAGs

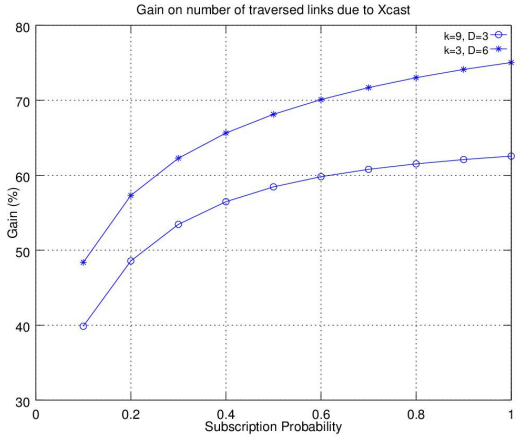


Figure 6. Gain due to multicast for two different *k-tree* structures connecting 729 MAGs (for illustrative purposes)

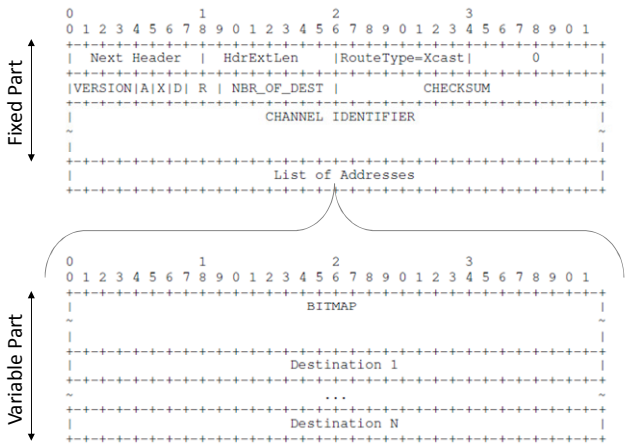


Figure 7. Xcast header format

C. Overhead calculation

Another relevant aspect is the comparison between multicast and Xcast in terms of the total overhead on the distribution structure under analysis. The standard distribution of the remotely subscribed multicast context uses IP-in-IP encapsulation, and therefore the overhead is due to the IP encapsulation in the bi-directional tunnel. In our proposal, the remotely subscribed multicast content is distributed in an IP-in-Xcast fashion; then the overhead will be originated by the Xcast mechanism.

1) Standard multicast case

Considering h_{IP} as the overhead bits needed for the encapsulation of the remote multicast channel (i.e. the 40 bytes of an IPv6 header in an IP-in-IP tunnel), the total overhead due for transporting a multicast channel all the path from the mobility anchor to an access gateway can be stated as:

$$O_{ch-MAG}^{std} = D \times h_{IP}. \tag{9}$$

Extending this formula to the set of MAGs in the domain, the total overhead for a multicast channel being distributed to all the MAGs across the PMIPv6 domain can be written as:

$$O_{ch-domain}^{std} = k^D \times D \times h_{IP}. \tag{10}$$

2) Xcast case

In Xcast definition, the encapsulation defined is composed of an IPv6 header and an Xcast header, carried as a routing extension, which is structured in a fixed part and a variable one.

The IPv6 header will have as source address the address of the Xcast sender (the mobility anchor in our case), being the destination address the "all_Xcast_routers" address. As consequence of the IPv6 header, every Xcast packet will account h_{IP} bytes.

The Xcast header presents a fixed 24-byte part including several protocol fields. Among them, the NBR_OF_DEST field determines the maximum number of destinations that can be included in the Xcast header. This field is 7 bit long, so a maximum of 127 destinations could be included in an Xcast distribution. The issue on the number of the maximum number of the destinations (i.e., MAGs) is discussed on Appendix A, at the end of the paper.

The variable part of the Xcast header will carry the list of the destination addresses for packet forwarding. Each Xcast router in the path will evaluate the list of destinations to replicate the packet accordingly for each of the corresponding next hops, including on the next packet just the destinations to be routed through the next hop, onwards. This variable part includes also a BITMAP field, of which size depends on the number of destinations, being a multiple of 64 bits.

Then, the size of an Xcast header for a certain distribution level in the *k-tree* can be can be formulated as:

$$h_{xcast}^{L_d}(bytes) = 24 + N_{L_d} \times 16 + \left\lceil \frac{N_{L_d}}{64} \right\rceil \times 8, \tag{11}$$

being N_{Ld} the number of destinations reachable from level L_d in a certain branch, that can be defined in the following manner:

$$N_{L_d} = k^{(d-1)}. \tag{12}$$

Each Xcast packet is converted into a normal unicast packet for reaching the last destination. In that case, corresponding to the first level in the tree, L_1, the applicable overhead will be just h_{IP}, with $h_{xcast}^{L_1} = 0$.

When extending these formulas to the whole set of MAGs in the domain, we obtain:

$$O_{ch-L_1}^{xcast} = k^D \times (h_{IP} + h_{xcast}^{L_1}) = k^D \times h_{IP} \tag{13}$$

$$O_{ch-L_2}^{xcast} = k^{D-1} \times \left(h_{IP} + h_{xcast}^{L_2}\right) = k^{D-1} \times h_{IP} + \\ + k^{D-1} \times \left(24 + k \times 16 + \left\lceil \frac{k}{64} \right\rceil \times 8\right) \tag{14}$$

$$O_{ch-L_3}^{xcast} = k^{D-2} \times \left(h_{IP} + h_{xcast}^{L_3}\right) = k^{D-2} \times h_{IP} + \\ + k^{D-2} \times \left(24 + k^2 \times 16 + \left\lceil \frac{k^2}{64} \right\rceil \times 8\right), \tag{15}$$

and, in general:

$$O_{ch-L_d}^{xcast} = k^{D-(d-1)} \times \left(h_{IP} + h_{xcast}^{L_d}\right) = k^{D-(d-1)} \times h_{IP} + \\ + k^{D-(d-1)} \times \left(24 + k^{d-1} \times 16 + \left\lceil \frac{k^{d-1}}{64} \right\rceil \times 8\right) \tag{16}$$

Then, considering the total distribution in the PMIPv6 domain, the general formulation of the overhead required for distributing a multicast channel to all the MAGs is given by:

$$O_{ch-domain}^{xcast} = \sum_{d=1}^{D} O_{ch-L_d}^{xcast} = \\ = \sum_{d=1}^{D} k^{D-(d-1)} \times h_{IP} + \sum_{d=2}^{D} k^{D-(d-1)} \times h_{xcast}^{L_d}, \quad (17)$$

that can be rewritten as:

$$O_{ch-domain}^{xcast} = k\frac{(k^D - 1)}{k-1} \times h_{IP} + \sum_{d=2}^{D} k^{D-(d-1)} \times h_{xcast}^{L_d} \cdot \quad (18)$$

Figures 8 and 9 present a comparison of the overhead for distributing a channel to all the MAGs in a domain, considering different *k-tree* configurations.

The Xcast option introduces less overhead than the standard case as the degree in the tree, *k*, grows for a given tree depth, *D*. At the same time, as the depth of the tree *D* increases, the advantage on using Xcast becomes more significant for higher *k-tree* degrees.

V. CONCLUSIONS AND FURTHER WORK

As shown in the previous analysis, the Xcast encapsulation can provide a lower cost per transported bit for a PMIPv6 domain operator offering remote multicast distribution capabilities to a Home Network operator, allowing for better benefit margins. It can also be concluded that the most efficient distribution structures for serving a certain number of MAGs in the PMIPv6 domain are those more hierarchical (i.e., with greater number of levels, *D*), instead of the flatten ones, because a higher gain is achieved respect to the standard multicast case. This matches existing operators' network topologies. Furthermore, higher degrees in the tree result in less overhead for the Xcast case.

As next steps, we are working on the characterization of the total overhead as a function of the channel subscription probability at the MAG. We are also studying how to dynamically decide when to use standard multicast versus Xcast transport depending on the locations of the MAGs subscribing the content in the *k-tree*, and in general, depending on the number of MAGs subscribing the content, for alleviating intermediate routers of the burden of Xcast processing in scenarios of low gain.

ACKNOWLEDGMENTS

The research of Carlos J. Bernardos leading to these results has received funding from the European's Community's Seventh Framework Programme (FP7-ICT-2009-5) under the grant agreement n. 258053 (MEDIEVAL project), being also partially supported by the Ministry of Science and Innovation (MICINN) of Spain under the QUARTET project (TIN2009-13992-C02-01).

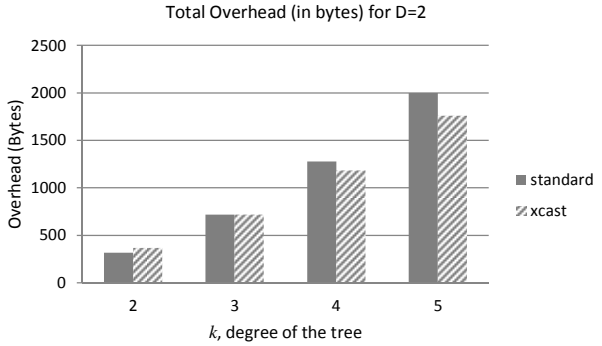


Figure 8. Total overhead comparison for different degrees values in a *k-tree* with depth *D*=2

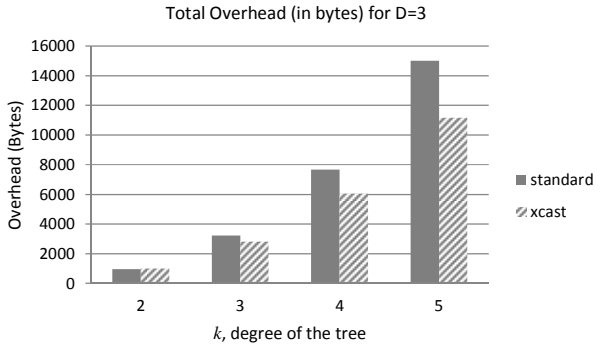


Figure 9. Total overhead comparison for different degrees values in a *k-tree* with depth *D*=3

REFERENCES

[1] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6", RFC 5213, August, 2008.

[2] 3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.402 10.5.0, September 2011.

[3] T.C. Schmidt, M. Waehlisch, and S. Krishnan, "A Minimal Deployment Option for Multicast Listeners in PMIPv6 Domains", RFC 6224, April, 2011.

[4] R. Boivie, N. Feldman, Y. Imai, W. Livens, D. Ooms, "Explicit multicast (Xcast) concepts and options", RFC 5058, November, 2007.

[5] J.C. Zuniga, L.M. Contreras, C.J. Bernardos, S. Jeon, Y. Kim, "Multicast mobility routing optimizations for Proxy Mobile IPv6", RFC 7028, September, 2013.

[6] P. Van Mieghem, G. Hooghiemstra, R. van der Hofstad, "On the efficiency of multicast", IEEE/ACM Transactions on Networking, Vol. 9, No. 6, pp. 719-732, December, 2001.

[7] H. Luo, H. Zhang, Y. Qin, V.C.M. Leung, "An approach for building scalable Proxy Mobile IPv6 domains", IEEE Transactions on Network and Service Management, Vol. 8, No.3, pp. 176-189, September, 2011.

[8] C. Perkins, D. Johnson, J. Arkko, "Mobility support in IPv6", RFC 6275, July 2011.

[9] Cisco 8500 Series Wireless Controller Deployment Guide, Document ID 113695, October 2012 (downloadable at: http://www.cisco.com/image/gif/paws/113695/8500-dg-00.pdf), accessed in November 2012.

APPENDIX A – ON THE NUMBER OF MAGS IN A PMIPV6 DOMAIN

This Appendix aims at discussing the typical number of MAGs in a PMIPv6 domain as a way of determining the potential limitations on the use of Xcast in a PMIPv6 domain.

The length of the field NBR_OF_DEST (7 bit) of the Xcast header limits the maximum of destinations to 127. Note that this limit applies to each branch of the *k-tree*, in such a way that the total number of MAGs per *k-tree* (i.e., per mobility anchor) can be raised to $k \times 127$. In order to evaluate how this number could be in line with the number of MAGs in a PMIPv6 deployment, we will analyze the potential scalability of a PMIPv6 domain in terms of users and number of access gateways.

We next partially follow the analysis considered in [7]. There, authors looked at the bandwidth requirements of the mobility anchor as one of the limiting factors for this entity. Being R_{OS} the rate of oversubscription in the LMA (that is, the rate of the total number of MNs registered in excess regarding the number of actually active MNs), and T_p the peak data throughput per active MN, the bandwidth delivered by the mobility anchor equals[1] to:

$$BW_{anchor} = M \times \frac{T_p}{(R_{OS}+1)}, \quad (19)$$

where M represents the total number of MNs registered at the mobility anchor in the PMIPv6 domain.

Commercial off-the-self core routers today are capable of delivering traffic in the order of Tbps. Table II summarizes the achievable number of MNs in the PMIPv6 domain assuming a mobility anchor forwarding capacity of 1 Tbps, considering different values of the observable peak data throughput and oversubscription ratios.

TABLE I. NUMBER OF REGISTERED MNS PER MOBILITY ANCHOR WITH A FORWARDING CAPACITY OF 1 TBPS

	Peak data throughput, T_p		
Oversubscr., R_{OS}	100kbps	1Mbps	10Mbps
0	10^7	10^6	10^5
5	6×10^7	6×10^6	6×10^5
10	11×10^7	11×10^6	11×10^5

For every attached MN, the mobility anchor has to keep an entry in the binding cache. Such an entry contains a number of fields [1] [8], like the MN identifier (128 bits), the MN's link layer identifier (64 bits), the MAG's link layer identifier (128 bits), the list of the Home Network Prefixes (HNPs) for the MN's interface (each prefix being 128 bits), the tunnel identifier (at most 128 bits), the Proxy Care-of-Address (128 bits), etc. These fields require a storage capacity above 1000 bits per MN. Taken this into account, the upper limit in the number of MNs observed in Table II imposes the need of handling a global binding cache memory in the order of 10 Tbits. This huge storage capacity, the corresponding number of associated routing entries, and the lookup capacity required to handle both of them, make that upper limit unachievable. Therefore, we can argue that a more realistic upper limit of MNs managed by a mobility anchor would be in the order of few hundreds of thousand terminals.

Current state-of-the-art MAG specifications [9] support a maximum number of 40,000 attached MNs. This implies that only a branch of the *k-tree* (that is, a downstream interface of the mobility anchor), with 127 of those MAGs, could potentially provide connectivity to more than 5 million MNs, much more than the total number of MNs per mobility anchor. To sum up, it can be stated that the number of MAGs per branch will be lower than the limit imposed by the field NBR_OF_DEST in the Xcast header.

[1] We have slightly modified the formula used for obtaining Fig. 19 in [7] because it is not totally correct from our point of view. In the original formula the denominator only considers the rate of oversubscription, R_{OS}, not providing a consistent result for the case when no oversubscription occurs.

Metodología de test de usuario y pruebas subjetivas para métodos de inserción de texto en aplicaciones iDTV

Aurora Barrero, David Melendi, Xabiel G. Pañeda, Roberto García, Sergio Cabrero
Departamento de Informática
Universidad de Oviedo
Campus de Viesques, SN 33204, Gijón, Asturias, España
{barreroaurora, melendi, xabiel, garciaroberto, cabrerosergio}@uniovi.es

***Resumen*- En la actualidad las aplicaciones interactivas en televisión demandan una introducción de texto de manera similar a como se hace en el ordenador. En este trabajo proponemos una metodología ágil que nos permita establecer un proceso para realizar test de usuario y pruebas subjetivas en el ámbito de la inserción de texto en televisión digital interactiva. Esta metodología abarcará todas sus etapas: desde la definición de métricas, pasando por el desarrollo de prototipos y realización de las pruebas hasta concluir con el análisis de resultados. Su aplicación a un caso de estudio muestra la importancia de elegir tanto un mecanismo de escritura como los dispositivos de interacción adecuados, puesto que su elección influye sobre la velocidad de escritura y el número de errores que se comenten.**

***Palabras Clave*- Metodología, test usuario, pruebas subjetivas, televisión, iDTV, escritura de texto.**

I. INTRODUCCIÓN

El mercado de la televisión digital interactiva está en auge debido a que muchos proveedores de contenidos han apostado por una convergencia entre la WEB y la televisión. Esta situación, ligada al hecho de que el número de usuarios está en continuo crecimiento, ha provocado un clima de competitividad elevado entre los diferentes proveedores que ofrecen sus servicios multimedia interactivos mediante una televisión conectada o un set-top-box (STB). Las aplicaciones para ofrecer estos servicios son mucho más avanzadas (navegar por internet, leer el correo electrónico, ver vídeos de YouTube, escribir comentarios en nuestro Facebook, etc...) debido a que los telespectadores han pasado de tener un rol pasivo a tener un rol cada vez más activo. Con ello se ha conseguido dar un giro al tipo de aplicaciones interactivas en las que los usuarios demandan una experiencia de usuario (UX) similar a la de los ordenadores, especialmente en el tema de la introducción de texto.

Aunque en los últimos años se ha producido una importante proliferación de test de usuario y evaluaciones subjetivas, no existen muchos trabajos en los que se trate el tema específico de la escritura de texto en aplicaciones de televisión digital interactiva (iDTV). Esto es debido a la problemática que se genera a la hora de abordar, de manera eficiente, el elevado número de pruebas que es necesario hacer por cada tipo de experimentación, puesto que el tiempo y el coste de algunos recursos suele ser elevado. Por tanto, surge la necesidad de encontrar un proceso que facilite la ejecución de las tareas necesarias a la hora de realizar los test, definir el entorno de pruebas, diseñar la interfaz de aplicación y analizar los resultados obtenidos. De la realización de este tipo de test de usuario y pruebas subjetivas, con usuarios reales, se pueden extraer conclusiones interesantes para el campo a estudiar: ¿Cuál es el mecanismo de inserción de texto óptimo?, ¿Cuál es el mejor dispositivo de interacción con iDTV?, ¿Cómo influye la edad de las personas?, ¿Cómo influye el nivel tecnológico de la persona?, ¿Está el usuario satisfecho con el método? etc.

En este artículo se presenta una metodología ágil e intuitiva, cuya aplicación será medir tanto la usabilidad, como la satisfacción de los usuarios en métodos de inserción de texto en iDTV. Se tendrán en cuenta cuestiones importantes como el diseño de la interfaz, las características del medio de interacción a utilizar y el entorno de pruebas.

El resto del artículo está organizado de la siguiente forma. En la Sección II se analizarán los trabajos relacionados. La sección III describe la metodología desarrollada. La sección IV relata cómo hemos aplicado la metodología en un caso práctico. Por último, en la sección V se presentan las conclusiones y trabajos futuros.

II. TRABAJOS RELACIONADOS

En sus orígenes la experiencia del usuario (UX) y la calidad de la experiencia (QoE) fueron promovidas por investigadores de Human-Computer Interaction (HCI). Desde entonces la usabilidad en iDTV ha sido un campo de investigación en continuo crecimiento en el que los investigadores hacen hincapié en la preocupación por los resultados de las personas que experimentan con tecnología.

Uno de los primeros trabajos en inserción de texto en iDTV fue presentado por Ingmarsson et al. [1] quienes diseñaron una nueva técnica llamada TNT. Se evaluó a cinco personas con edades comprendidas entre los 27 y 32 años. La prueba consistía en escribir una novela en sueco durante 10 sesiones de 45 minutos cada una. Los participantes recibieron una compensación económica.

Iatrino y Modeo [2] compararon 3 interfaces de introducción de texto para TDT (Digital Terrestrial Television). Participaron 36 personas que se dividieron en 2 grupos en función del nivel de experiencia en escribir SMS. La prueba consistió en realizar 6 tareas (2 con cada método) donde el orden de los métodos y de las tareas fue aleatorio para minimizar el efecto aprendizaje.

Por otra parte, Geleijnse et al [3] compararon tres métodos (Multitap, T9 y un teclado virtual) usando un mando a distancia con la escritura realizada con un teclado QWERTY convencional. El objetivo del experimento era buscar vídeos en YouTube escribiendo el par "artista-pista" utilizando cada uno de esos métodos. Participaron 22 usuarios (15 hombres y 7 mujeres) de edades comprendidas entre los 21 y 32 años. El experimento fue llevado a cabo en un laboratorio similar a una sala de estar.

Poco después, Aoki et al. [4] diseñaron un método de entrada de texto para mandos a distancia llamado Twist&Tap. Se evaluó a un conjunto de 14 mujeres diestras que fueron seleccionadas de una agencia de trabajo temporal. Su rango de edad estaba comprendido entre 24 y 33 años.

Gargi y Gossweiler [5] presentaron un nuevo sistema predictivo diseñado para mejorar la velocidad de escritura en teclados virtuales: QuickSuggest. Realizaron un estudio teórico del rendimiento y un experimento con 10 usuarios reales.

Más recientemente, Sporka et al.[6] realizaron un estudio comparativo de dos métodos: el ya conocido TNT [1] y TwiceTap que ellos desarrollaron. Participaron 18 usuarios (10 hombres y 8 mujeres) cuya media de edad fue 22.7 años. Los usuarios no eran expertos en introducir texto en iDTV pero estaban familiarizados con la escritura en teléfono móvil. El experimento fue organizado en 10 sesiones y cada una de ellas de unos 20 minutos de duración. El orden de los métodos fue contrabalanceado para minimizar el efecto aprendizaje.

Existen estudios con dispositivos diferentes al mando a distancia tradicional. Költringer et al. [7] compararon una técnica llamada Twostick con teclado QWERTY con el mando de una consola Xbox 360 Microsoft. En el experimento participaron 8 usuarios diestros (4 hombres y 4 mujeres), de entre 22 y 29 años. No tenían experiencia con el método Twostick pero si en el uso del teclado QWERTY.

Mackenzie et al. [8], compararon los teclados virtuales de un iPhone de Apple y de una Nintendo Wii. El estudio se realizó en un salón con ambiente relajado. Participaron 16 personas (9 hombres y 7 mujeres) cuyo rango de edad estaba comprendido entre los 18 y los 30 años. Fueron reclutadas del campus universitario local y se les dio una compensación económica por su colaboración.

Como se ha comprobado existen trabajos en los que se han realizado evaluaciones que tratan el tema específico de inserción de texto en aplicaciones iDTV, pero en ninguno de ellos se ha utilizado una metodología para su realización. No se han guiado por un proceso metodológico sino de forma intuitiva o por su propia experiencia. La mayoría realizan evaluaciones con usuarios reales pero seleccionan un grupo muy reducido de personas y/o con rangos de edad equivalentes y/o con un nivel tecnológico parecido. En definitiva con características muy similares. Tampoco suelen utilizar un entorno de pruebas equivalente al que un usuario tendría en su propia casa.

Hasta donde alcanza el conocimiento de los autores, no se tiene constancia de la existencia ninguna metodología específica para la realización de test de usuario y pruebas subjetivas para métodos de inserción de texto en aplicaciones iDTV. Este trabajo propone una metodología que indique a los experimentadores cómo tienen que proceder y qué tareas deben realizar para alcanzar los objetivos que se planteen en un estudio.

III. METODOLOGÍA

La metodología que se propone establece un método que abarca todas las etapas de una experimentación, desde la definición de métricas y objetivos, pasando por el diseño de la misma, el desarrollo de prototipos y la realización de las pruebas de usuario hasta finalizar con la recogida y validación de datos y el análisis de resultados.

Esta metodología está basada en una serie de fases, que a su vez, se van a subdividir en una serie de tareas. Para definir todas las fases se han tenido en cuenta las recomendaciones y reglas de la iDTV y de la experiencia del usuario encontradas en la literatura.

El diagrama de la Fig. 1 muestra un flujo de trabajo formal de las fases y tareas propuestas en notación Business Process Model and Notacion (BPMN).

A. Fase 1. Definición de Métricas

En esta fase se definirán los objetivos y se especificarán las métricas que los satisfagan.

Una métrica aportará información sobre sobre la interacción entre el usuario y el sistema de inserción de texto en iDTV. Se tendrán en cuenta aspectos como la efectividad (capacidad para completar una tarea), la eficiencia (la cantidad de esfuerzo requerido para completar una tarea) y la satisfacción (el grado con el que el usuario es feliz con su propia experiencia de realización de la tarea).

1) Definir Objetivos

Los objetivos marcarán lo que se quiere conseguir, y para tener una ayuda en su definición se responderá a preguntas del siguiente tipo: *¿Qué se va a estudiar?*; será necesario especificar un objetivo genérico. *¿Cuál es la motivación y el propósito?* es decir, precisar para qué se hará, (para evaluar, para mejorar...) y qué se pretende con ello (analizar los mecanismos de inserción de texto, evaluar los dispositivos, analizar un sector de la población...). *¿Desde qué punto de vista se definen los objetivos?*, por ejemplo, desde un punto de vista de usuario o desde un punto de vista investigador.

2) Estudiar Métricas

En esta tarea se tendrá que realizar un estado del arte para conocer las métricas y estándares a utilizar en la evaluación de mecanismos de inserción de texto aplicables a iDTV.

En el campo de la inserción de texto algunas métricas típicas son: velocidad de escritura, tasa de errores cometidos, satisfacción del usuario y curva de aprendizaje.

3) Especificar Métricas

Para poder evaluar el rendimiento de un usuario los objetivos y las métricas tienen que estar alineados. Así que, lo que se hará, en primer lugar, será transformar los objetivos en preguntas, y en segundo lugar, se buscará respuestas a esas preguntas, y a partir de ahí, se podrán especificar las métricas.

Es necesario establecer las unidades de medida de las métricas seleccionadas. Por ejemplo, la velocidad de escritura de un método de inserción de texto, puede medirse en WPM (palabras por minuto), CPS (caracteres por segundo) o KSPS (pulsaciones de tecla por segundo).

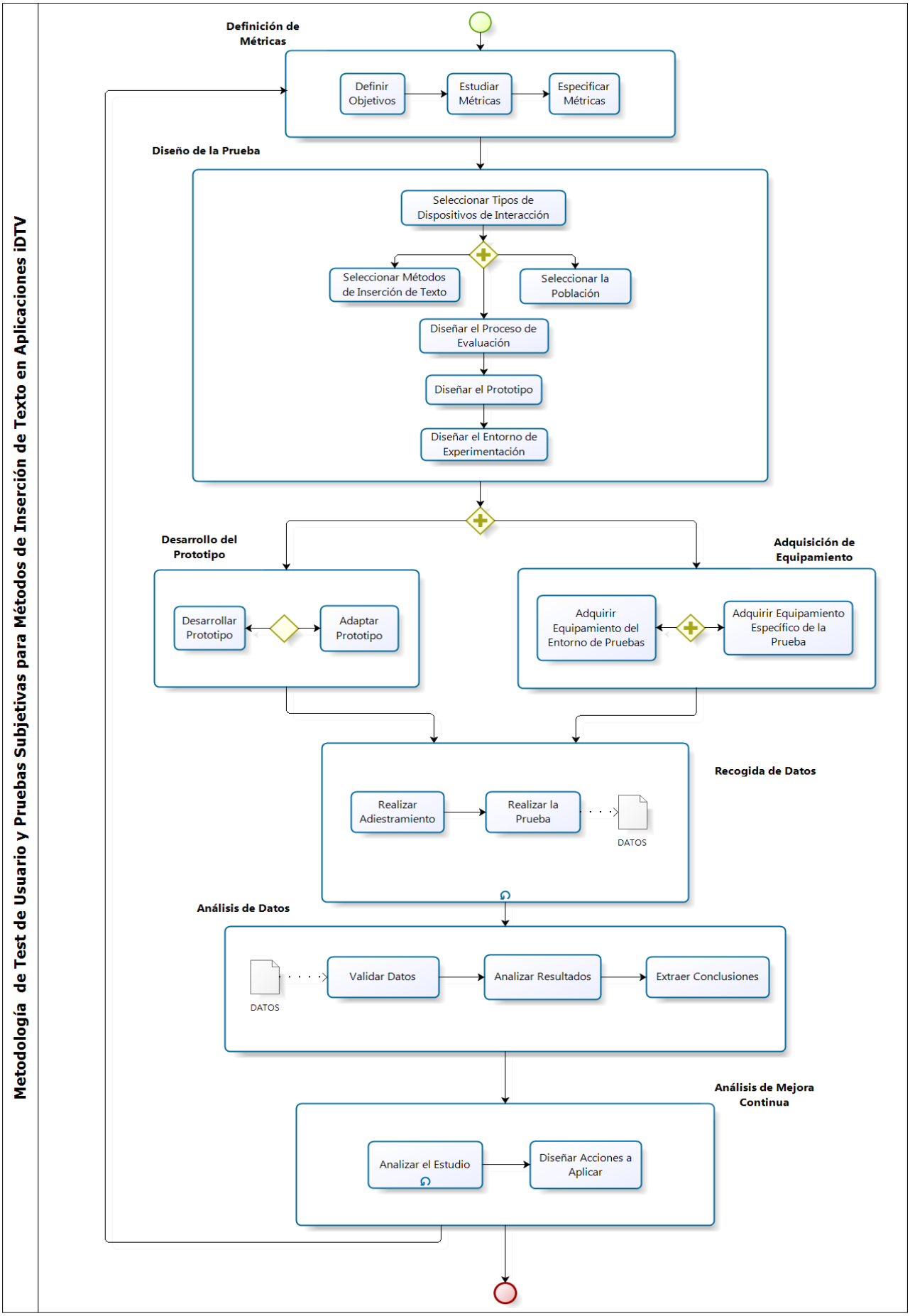


Fig. 1. Fases y tareas de la metodología en notación BPMN

B. Fase 2. Diseño de la Prueba

En esta fase se diseñará la experimentación a utilizar para realizar los test de usuario y evaluaciones subjetivas.

1) Seleccionar Tipos Dispositivos de Interacción

En esta tarea se seleccionarán los diferentes tipos de dispositivos con los que el usuario interactuará durante la realización de la prueba (mandos a distancia, teclados, apuntadores giroscópicos, touchpads, etc.). Se detallarán las características específicas de las que deberán disponer (disposición de teclas, tamaño, ergonomía, conexión, etc.).

2) Seleccionar Métodos de Inserción de Texto

En la literatura existen una gran variedad de mecanismos a utilizar para la inserción de texto. Por un lado, existen teclados virtuales: QWERTY, Square Alphabetic, Metropolis, FOLC, ATOMIK, Genetic, Wide Alphabetic, etc. Por otro lado, existen otros mecanismos como los de tipo teléfono móvil: MULTITAP, T9, 2-KEY, TNT, TwoStick, etc.

En esta tarea será necesario realizar una selección de mecanismos que deben ser probados en base a los objetivos del estudio, los dispositivos seleccionados, los resultados publicados y la conveniencia del método para servicios de televisión digital interactivos.

3) Seleccionar la Población

Cuando diseñamos un estudio de usabilidad es necesario prestar especial atención a las características de la población. Por eso, se hará necesario responder a cuestiones como: ¿Qué tipo de participantes se necesitarán?, ¿Cuántos participantes?, ¿Se compararán los datos con un único grupo o con varios grupos de participantes?, ¿Se necesitará contrabalancear el orden de las tareas?

En cuanto a la selección de participantes, la primera cuestión a tener en cuenta es que estos deberán ser seleccionados cuidadosamente debido a que deben ser representativos de la población objetivo del estudio. Se deberá establecer un criterio de selección de la población por el cual se determinará si una persona concreta es elegible para participar en el estudio. El criterio debe ser tan específico como sea posible para reducir la posibilidad de reclutar a un participante que no dé el perfil.

La segunda cuestión será saber si vamos a dividir los datos por diferentes tipos de participantes. Si es así, se tendrán que separar a los participantes en distintos grupos y entonces habrá que pensar qué grupos son y cuantos participantes irán en cada grupo. Los grupos más comunes de segmentos [9] son:

- Nivel de experiencia en un dominio: (novato, intermedio, experto).
- Frecuencia de uso.
- Demográficos (genero, edad, lugar de procedencia).
- Actividades (uso de funcionalidades o características particulares).

La tercera cuestión será la estrategia a seguir para seleccionar la muestra. El objetivo de un estudio de usabilidad es generalizar los "hallazgos" a una población mayor. Es importante conocer cómo de bien la muestra refleja a la población general y será necesario estar al tanto de cualquier posible sesgo que se produzca en los datos. Para localizar a los participantes se pueden emplear métodos como poner un anuncio o usar una lista de gente que ha participado en otras pruebas.

Respecto al tamaño de la muestra, no existe una regla que diga el número mínimo de participantes de un estudio. Pero el tamaño de la muestra se deberá escoger en base a dos factores: los objetivos del estudio y la tolerancia al margen de error. Se recomienda tener de 50 a 100 usuarios representativos [9] , ya que si escogemos un número menor, la varianza en los datos será más alta, haciendo difícil generalizar los resultados a la población objeto del estudio. En el caso de que la población sea agrupada será de ayuda tener al menos 4 participantes de cada grupo.

A veces, el orden en el que los usuarios realizan las tareas del estudio, tiene un impacto significativo en los resultados debido a que estos aprenden con la experiencia de uso. Si se sospecha que puede haber un efecto en el orden de realización de las tareas que influya en el aprendizaje de otra, se recomienda realizar un contrabalanceado.

Contrabalancear involucra cambiar simplemente el orden en el que diferentes tareas son realizadas. Se puede asignar aleatoriamente el orden de las tareas para cada participante, o crear previamente grupos con el orden de las tareas diferente y asignar a cada usuario a un grupo. Sin embargo, hay algunas situaciones en las que no es necesario o incluso pueden ser perjudicial para los objetivos del estudio. Un ejemplo sería, si las tareas no tienen ninguna relación entre sí, es poco probable que se dé el aprendizaje entre ellas, es decir, la realización de una tarea con éxito no va a ayudar a ninguna otra tarea. Otro ejemplo, que se puede dar, es cuando el orden de las tareas es inamovible porque, en ese caso, la sesión de prueba no tendría sentido. En esta situación habría que conocer el orden de los efectos como parte general del proceso de aprendizaje y no pensar que es un síntoma de un estudio de usabilidad mal diseñado.

4) Diseñar el Proceso de Evaluación

En esta tarea se establecerá el proceso de evaluación y las experimentaciones que se realizarán. También será necesario establecer el número de sesiones de cada experimentación en las que participará un usuario y el tiempo mínimo y máximo entre sesiones. Además, se concretará el número de frases y los textos que deberán escribir los usuarios, así como las encuestas y escalas de votación a las que se someterá cada uno de ellos. Consecuentemente, se establecerán los datos necesarios que deberán ser recabados para calcular las métricas que se han definido.

El número de sesiones de una experimentación dependerá de los objetivos y de las métricas especificadas. Puede suceder que las sesiones tengan la misma complejidad, se evalúen los mismos métodos y/o mismos dispositivos y se quiera medir la curva de aprendizaje [10] de los participantes. O puede suceder, que las sesiones sean independientes y en cada una de ellas se mida el rendimiento de un método o dispositivo diferente. También será necesario establecer el rango de duración de una cada sesión y el tiempo mínimo y máximo entre cada una de ellas.

Normalmente habrá que diseñar el corpus de frases que se utilizarán en el estudio y que serán distribuidas entre las distintas sesiones. La complejidad de las frases dependerá de los objetivos del estudio. Podrán contener minúsculas, y/o mayúsculas, y/o signos de puntuación, y/o números, y/o caracteres especiales, etc. Dependiendo del caso, se podrán seleccionar de algún medio (periódico, artículos de internet [11], etc.) o ser diseñadas a medida para el estudio [12]. El

orden en que las frases aparecerán durante una sesión tendrá que ser establecido. Por ejemplo, podrá ser aleatorio o tener un orden predeterminado.

En la mayoría de los casos será conveniente realizar una encuesta previa para conocer a la población. Las preguntas suelen ser sobre cuestiones demográficas, tecnológicas, de habilidades, de necesidades y hábitos. La encuesta se puede diseñar en formato WEB o papel. Es recomendable hacerla antes de la primera sesión de pruebas.

También es fundamental hacer encuestas de satisfacción, de preferencias y/o deseos del participante, ya que es muy importante conocer la información de la percepción de los usuarios del sistema y su interacción con él. Para recoger estos datos subjetivos, se suelen realizar encuestas mediante escalas de votación y/o cuestionarios donde los participantes describen con sus palabras como se han sentido y qué problemas se han encontrado.

Para las escalas de votación se recomienda la escala de Likert [13]. Esta propone una serie de preguntas y en las repuestas se especifica el nivel de acuerdo o desacuerdo con la pregunta. El formato típico de 5 niveles de respuesta sería: Totalmente en desacuerdo, En desacuerdo, Ni de acuerdo ni en desacuerdo, De acuerdo y Totalmente de acuerdo.

Los cuestionarios con escala de votación suelen hacerse al final de cada sesión de pruebas y suelen ir incorporadas en la aplicación de pruebas. Los cuestionarios en los que los usuarios describen sus impresiones suelen realizarse en la última sesión del estudio y su formato suele ser WEB o papel.

5) Diseñar el Prototipo

En esta tarea se diseñará la aplicación que permitirá a los participantes realizar la prueba y recogerá los datos necesarios que permitirán calcular las métricas seleccionadas.

Para la creación de una interfaz adaptada al entorno de la televisión será necesario utilizar reglas y recomendaciones para iDTV, ya que no debe de hacerse al azar. La norma ISO 14915-3:2002 [14] proporciona recomendaciones y orientaciones para el diseño, selección y combinación de interfaces de usuario interactivas que integran y sincronizan diferentes medios. Algunos autores como Perrinet at al. [15] señalan algunas recomendaciones respecto a colores, tamaño del texto, elementos de navegación o número de palabras por pantalla. Y Graham [16] mantiene que algunas de las Leyes de Gestalt, como las leyes de figura/fondo, proximidad, similaridad y simetría se pueden aplicar al diseño de la interfaz para aplicaciones iDTV.

Del mismo modo, será necesario seleccionar tanto la metodología de desarrollo como el lenguaje de programación, así como el formato de recogida de datos (por ejemplo, si se utilizará una base de datos o un fichero XML) para satisfacer los objetivos marcados y las métricas seleccionadas.

Respecto a la funcionalidad del prototipo se diseñarán ciertas cuestiones tales como disposición y/o combinación de teclas y qué métodos de alternancia utilizar (por ejemplo, mayúsculas y minúsculas) para cada uno de los dispositivos seleccionados. También serán importantes cuestiones relativas a cómo capturar los eventos de pulsación de teclas, cómo mostrar listados de desambiguación y si se implementarán o no métodos de recomendación.

Asimismo, se tendrán en cuenta las escalas de votación que irán incorporadas en la aplicación y el método de propuesta de frases diseñado en la tarea de "Diseñar el Proceso de Evaluación".

6) Diseñar el Entorno de Experimentación

Normalmente, los espectadores suelen interactuar con la televisión en un ambiente relajado y la distancia a esta suele ser de unos pocos metros. Esta separación espacial provoca que los usuarios tengan que alternar el foco de atención entre el dispositivo de interacción y la televisión.

Para que el resultado de la experimentación sea lo más realista posible, será necesario realizarlo en unas condiciones controladas y lo más parecidas posible a un entorno real. Así pues, en esta tarea se diseñará lo referente al entorno de experimentación. Será necesario establecer cuestiones tales como las relativas a qué características tiene que tener la sala donde se realizarán las experimentaciones: iluminación, mobiliario y recursos hardware (por ejemplo se necesitará una Televisión, qué características tiene que tener, cuantas pulgadas, qué resolución será necesaria, etc). En definitiva todo lo relacionado con los recursos del entorno.

En relación a los recursos hardware se necesitará al menos, una televisión y un ordenador. Por un lado, se seleccionarán las características de la televisión (pulgadas, resolución, distancia entre el espectador y la TV, etc.). Por otro lado, los requisitos hardware y software del ordenador tendrán que ir en consonancia con las necesidades del software a desarrollar.

Para la selección de los parámetros relacionados con iluminación de la sala, distancia de observación, formato de pantalla, resolución, pulgadas etc. es aconsejable utilizar las recomendaciones de la ITU-R BT.500-1 [17] que cubren todos estos aspectos.

El resultado de esta tarea generará un listado con todos los recursos necesarios para establecer un entorno apropiado para la realización de los test.

C. Fase 3 Adquisición de Equipamiento

1) Adquirir Equipamiento Específico de la Prueba

Se realizará un estudio de los distintos productos disponibles en el mercado para los tipos de dispositivos seleccionados en la fase anterior. Una vez concluido el estudio se procederá a la adquisición de los mismos.

2) Adquirir Equipamiento del Entorno de Pruebas

La tarea de Diseño del Entorno de experimentación nos proveerá el listado de equipamiento necesario. Se realizará un estudio de mercado para cada punto del listado, y se procederá a la adquisición del equipamiento.

D. Fase 4. Desarrollo del Prototipo

1) Desarrollar el Prototipo

En esta tarea se realizará la implementación de la aplicación de pruebas. Como entradas de la tarea se utilizarán el diseño del prototipo, las recomendaciones iDTV y la metodología de desarrollo de software elegida.

La aplicación será el medio para realizar las pruebas y medirá tanto la usabilidad, como la satisfacción de los usuarios de métodos de inserción de texto en iDTV.

2) Adaptar el Prototipo

Esta tarea solo será necesaria en caso de que de la fase de mejora continua se haya identificado una mejora y sus acciones correctivas impliquen la modificación de alguna funcionalidad del prototipo desarrollado.

E. Fase 5. Recogida de Datos

1) Realizar Adiestramiento

Para obtener resultados fiables, en algunos casos será necesario enseñar a los participantes mediante una sesión especial de adiestramiento. Esta se realizará con antelación a las sesiones de prueba.

Las frases utilizadas en la sesión de adiestramiento deberán ser diferentes de las utilizadas en la prueba. Sería recomendable la utilización de todos los dispositivos y/o métodos que se usarán en la prueba.

Un caso de utilización de adiestramiento sería, por ejemplo, en participantes de edades avanzadas y/o de perfil no tecnológico donde el uso de los métodos de inserción de texto y/o de los dispositivos puede ser una labor compleja.

2) Realizar la Prueba

Para llevar a cabo la evaluación, se concertarán citas con los usuarios que participarán en el experimento. Cuando el usuario acuda una sesión, se le darán indicaciones sobre lo que tendrá que hacer para interactuar con la aplicación: qué métodos de inserción de texto utilizará, con qué dispositivos interactuará, cuantas frases tendrán que escribir, cómo podrán corregir errores y cómo se tiene que rellenar la escala de votación. Estas indicaciones serán verbales y podrán ser reforzadas con una presentación de ordenador. También se recomienda hacer una demostración práctica.

Una vez que el participante realice la prueba, sus datos quedarán registrados para su posterior evaluación.

F. Fase 6. Análisis de Datos

1) Validar Datos

Una vez que se hayan recogidos los datos, se comprobará su validez, mediante el análisis de la información, verificando que sean correctos, estén completos y sean consistentes. Normalmente se realizará un pre-procesado de los mismos, que generará el conjunto de datos final, que se introducirá en el programa estadístico escogido para su análisis.

En el pre-procesado del conjunto de datos obtenido, será necesario realizar tareas tales como *Eliminar Datos Perdidos* (datos que por alguna razón no son conocidos), *Discretizar Datos* (convertir variables reales o enteras en nominales), *Filtrar Atributos* y/o *Eliminar Ruido*. Una vez realizadas estas tareas tendremos el conjunto de datos preparado para su análisis estadístico.

2) Analizar Resultados

Tras concluir las pruebas y una vez que se hayan valido los datos registrados, se realizará el análisis de los mismos y se elaborará la documentación necesaria.

El tipo de análisis estadístico, dependerá de la experimentación e irá en consonancia con los objetivos y métricas del estudio. Un ejemplo de operativa de análisis de datos podría ser la que sigue. En primer lugar, se comprobará la normalidad de los datos con test de Saphiro-Wilk y su homocedasticidad con test de Barlett. Dependiendo de estas características, se utilizarán Tests de ANOVA o de Kruskal-Wallis y, en caso de existir diferencias entre los datos que se estén analizando se utilizarán los test de Tukey con un coeficiente de confianza del 95% para realizar comparaciones dos a dos.

3) Extraer Conclusiones

Es esta tarea, una vez analizados los datos estadísticamente, se interpretarán sus resultados. Se recomienda generar un informe en el que se incluirán todas las observaciones, interpretaciones y conclusiones derivadas del análisis estadístico y de los comentarios subjetivos de los participantes.

G. Fase 7. Mejora Continua

En esta fase será necesario evaluar el estudio, dejar constancia de las lecciones aprendidas y seleccionar las acciones a realizar para que las distintas fases de la metodología se apliquen de forma eficiente. Así se obtendrá un mayor beneficio y los resultados obtenidos estarán alineados con los objetivos que se persiguen.

1) Analizar el Estudio

Después de efectuar una experimentación se realizará una evaluación de todo el proceso.

En primer lugar, es necesario aprender del proceso en sí, tanto de sus éxitos como de sus fracasos, y es necesario que quede reflejado para que sea una lección aprendida a tener en cuenta la siguiente vez que se realice un estudio.

En segundo lugar, hay que comprobar si con los resultados obtenidos se han alcanzado los objetivos esperados. Y si es el caso, habrá que encontrar cuál ha sido el motivo por el cual los objetivos y los resultados no están alineados.

En tercer lugar habría que identificar qué mejoras podremos aplicar al proceso. Por ejemplo, se puede mejorar el rendimiento o eficiencia de una fase o tarea. También puede suceder que a raíz del estudio surjan ampliaciones del estudio o estudios alternativos que complementen el estudio actual.

Para ayudarnos a identificar las mejoras se evaluarán los resultados obtenidos a partir de las conclusiones de la fase del análisis de datos y de los comentarios de los participantes que fueron recogidos en los cuestionarios.

2) Diseñar Acciones a Aplicar

En esta tarea se diseñarán las acciones a aplicar por cada una de las mejoras identificadas en la tarea anterior. Será necesario priorizarlas basándose en los objetivos del estudio, y valorar si son aplicables o no, puesto que en algún caso tendrán un coste (de recursos, de tiempo, etc.) demasiado elevado.

Un ejemplo de mejora sería ampliar la población objeto del estudio porque se ha detectado que la población está sesgada. Esto implicaría como acciones correctivas conseguir más participantes y realizar las pruebas con ellos para ampliar los resultados del estudio.

Otro ejemplo sería que, después de unos meses realizando las pruebas al hacer una revisión de los trabajos relacionados se encuentren nuevos dispositivos de interacción. Esto podría implicar como acciones a realizar añadir otra sesión para probar ese dispositivo y/o rediseñar el prototipo.

IV. CASO DE ESTUDIO

En esta sección se propone un caso de estudio resumido que ilustra la metodología propuesta.

A. Fase 1. Definición de Métricas

El principal objetivo de la experimentación es determinar la eficacia y la eficiencia de los diferentes métodos de entrada de texto, teniendo en cuenta diferentes perfiles de usuario y distintos contextos de uso. Con el fin de alcanzar este

objetivo, se eligieron varias métricas teniendo en cuenta, tanto los aspectos objetivos como subjetivos:

- Velocidad entrada de texto: palabras por minuto (WPM)
- Tasa de error: porcentaje de caracteres erróneos escritos
- Impresión subjetiva de la facilidad de uso, velocidad de escritura y satisfacción general: medidos con escalas de Likert de 0 a 4.

B. Fase 2. Diseño de la Prueba

1) Seleccionar Tipos Dispositivos

Se eligieron como dispositivos a utilizar 3 mandos a distancia que incorporan las teclas más comunes de los mandos a distancia convencionales: números, tecla OK y cursores. Estos serán diferentes entre sí, es decir, tendrán distinta ergonomía, tamaño y/o disposición de teclas.

2) Seleccionar Métodos de inserción de texto

Se eligieron para su evaluación dos métodos de inserción de texto virtuales (QWERTY y Genético) y un método tipo teléfono móvil Multitap.

3) Población

Participaron 42 usuarios, que se escogieron de forma heterogénea; con diferentes edades (comprendidas entre los 20 y los 70 años), de distinto género; así como, con diferentes habilidades tecnológicas y de diferente nivel de estudios.

Los usuarios se agruparon de acuerdo a su edad. Por lo tanto, varios usuarios pertenecen a la llamada "generación móvil", con edades comprendidas entre los 18 y 30 años; otros pertenecen a la llamada "generación ordenador", con edades comprendidas entre los 31 y 45 años. Y finalmente, los usuarios "pre-ordenador" que son mayores de 45 años.

4) Diseñar el Proceso de Evaluación

Se decidió que los participantes deberían completar tres sesiones, una por cada uno de los mandos a distancia escogidos. Durante una sesión (de unos 35 minutos) se le pedirá al usuario que introduzca 6 frases (que contendrán caracteres en minúsculas, mayúsculas, números, signos de puntuación y caracteres especiales), 5 serán datos personales (nombre y apellidos, DNI, fecha de nacimiento, dirección postal, correo electrónico) que ellos mismos habrán insertado en un formulario previo a la sesión, y otra que será una URI común para todos. El usuario tendrá que introducir las 6 frases (que se mostrarán en orden aleatorio) con cada uno de los 3 métodos de inserción de texto. Para evitar un "efecto aprendizaje", se realizará un contrabalanceado, asignando a cada usuario un grupo distinto, lo que cambiará el orden de uso de cada uno de los métodos y se neutralizará ese efecto.

Con el fin de recopilar datos de los usuarios y la información subjetiva, se diseñaron varios cuestionarios. Antes de la primera sesión de la experimentación, los usuarios rellenarán un cuestionario que permitirá saber el sexo, edad, profesión, nivel y tipo de estudios, hábitos de uso de la televisión, del teléfono móvil y del ordenador, y si son zurdos o diestros. Además, en la última sesión y después de realizar la prueba, los usuarios completarán un cuestionario final en el que los participantes describirán con sus palabras cada método, cómo se sienten, si tienen la impresión de estar mejorando, etc.

Los participantes tendrán que votar mediante escalas de Likert los siguientes parámetros: facilidad de uso, velocidad de escritura, y satisfacción global. El sistema de votación se implementará en el prototipo y se realizará al final de cada una de las sesiones de prueba.

5) Diseñar el Prototipo

Se diseñó una aplicación que más tarde fue implementada con Adobe ® AIR ®. Las fuentes utilizadas serán Verdana 65 puntos para las frases mostradas y los campos de texto, y Arial 60 puntos para la distribución de los teclados.

La aplicación se visualizará a pantalla completa sobre fondo de color negro y mostrará los textos que se tienen que escribir con cada uno de los métodos de inserción de texto.

Cuando se inicie una sesión en la aplicación, se dejarán 5 segundos antes de permitir al usuario escribir. Una vez que el usuario escriba una frase, la aplicación comprobará si la frase escrita coincide exactamente con la frase propuesta. Si coinciden, la aplicación mostrará una nueva frase o cambiará a un método de entrada de texto diferente.

La aplicación se comportará de manera diferente dependiendo del tipo de método usado, teclado virtual o tipo teléfono móvil (SMS). Cuando se utilicen teclados virtuales, los usuarios utilizarán los cursores del mando a distancia para moverse a través de una distribución del teclado en pantalla y el botón "OK" para confirmar una acción. Es importante tener en cuenta que cada vez que un usuario quiera escribir algo, necesitará encontrar la tecla deseada, moverse desde la posición actual a esa tecla y pulsar el botón OK.

Para hacer frente a errores, la aplicación deberá proporcionar mecanismos para borrar los caracteres mediante una tecla del mando a distancia.

La aplicación procesará los eventos que se producen durante la ejecución en un fichero XML. Se grabarán tanto los textos propuestos, como lo que escriben los usuarios. Quedará constancia de todas las pulsaciones que se realicen. El propósito será el de disponer de información para su posterior análisis estadístico.

6) Diseñar el Entorno de Experimentación

Se decidió que durante una sesión del experimento, el participante se quedaría solo en una habitación para evitar distracciones. Para crear la situación más realista posible, cada usuario se acomodará como si estuvieran en su propia sala de estar. Para ello será necesario un sillón donde se sentará el participante, un ordenador para ejecutar la aplicación y una televisión donde esta se mostrará.

El sillón se colocará frente a una televisión de 32" con 1024 x 768 de resolución; y ésta se situará encima de una mesa de alrededor de 1 metro de altura. El sillón se ubicará a una distancia de entre 2 o 3 metros.

El ordenador será necesario para ejecutar la aplicación y llevar a cabo las pruebas. Este necesitará como sistema operativo Windows XP y como característica Hardware 1 Gb de Memoria RAM. Además tendrá que disponer de un puerto USB donde se conectaran los receptores de radio frecuencia e infrarrojos de los diferentes mandos a distancia.

Fase 3. Adquisición de Equipamiento

1) Adquirir Equipamiento Específico de la Prueba

Del tipo de mandos seleccionados se compraron los siguientes (Fig.2): Un primer mando a distancia modelo SnapStream Firefly con el teclado numérico en la zona superior y las flechas y la tecla OK en el centro. Un segundo mando a distancia que se eligió porque los números y las flechas están situadas a un lado, es decir, tiene los números en la parte superior izquierda y las flechas y la tecla OK en la parte centro-derecha. Se trata de un mando a distancia Golden Interstar. Y un tercer mando que se eligió para comprobar si

el tamaño es importante o no, ya que es notablemente más pequeño que los otros dos. Además, este mando permitirá comprobar el impacto de invertir el orden de sus elementos, ya que tiene los números en la parte inferior y las flechas y la tecla OK en la parte superior. Se trata de un mando a distancia Aver Media.

Fig. 2. Mandos a distancia usados en la experimentación.

2) Adquirir Equipamiento del Entorno de Pruebas

El hardware adquirido fue: una televisión LG LCD de 32" con dimensiones de 814x599mm y un ordenador Dell Pentium 4, 3 GHz con 1 Gb de RAM y sistema operativo Windows XP.

Como mobiliario fue necesario adquirir un sillón modelo TULLSTA de color gris cuyas medidas son 80x70x77 cm y una mesa modelo BESTA de color blanco con las siguientes dimensiones 121x72x8 cm.

C. Fase 4. Desarrollo del Prototipo

El prototipo se desarrolló mediante Adobe ® AIR ®.

D. Fase 5. Recogida de Datos

Se tardaron dos meses en la realización de la evaluación. Para llevarla a cabo, se concertaron las citas con los usuarios que tomaron parte en el experimento. Se citó a cada participante con una diferencia de 1 semana cada sesión.

Cuando el usuario acudía a una sesión, se le dieron indicaciones sobre qué métodos de inserción de texto utilizaría, que mandos a distancia usaría, se le explicaba como corregir errores y cómo rellenar la escala de votación. Estas indicaciones se hicieron mediante una breve exposición mediante una presentación de ordenador. Después se hizo una breve demostración práctica de utilización de los mandos a distancia. Una vez que el participante entendió lo que tenía que hacer, se ejecutó la aplicación desarrollada y dio comienzo la prueba. Cuando finalizó la prueba el registro de sus datos quedaron almacenados en un fichero XML para su posterior evaluación.

E. Fase 6. Análisis de Datos

Una vez recogidos los datos de los usuarios en el XML que genera la aplicación, se procesaron y se validaron para poder analizar sus resultados. El análisis estadístico de los datos se realizó con el paquete estadístico RCommander.

Como resultado destacable se obtuvo que, en general, la forma y la localización de las teclas no producen diferencias significativas ni en la velocidad de escritura ni en la tasa de error de los métodos utilizados.

V. Conclusiones y Trabajos Futuros

A través de este trabajo, se ha diseñado una metodología, para avanzar en la interacción humana en el ámbito de los métodos de inserción de texto para iDTV. Su aplicación será medir tanto la usabilidad, como la satisfacción de los usuarios. Abarcará todas las etapas necesarias para la realización de los test de usuario y pruebas subjetivas; desde la definición de métricas, pasando por el desarrollo de prototipos y realización de las pruebas hasta concluir con el análisis de resultados. Esta metodología se validó de forma práctica con un caso de estudio, el cuál otorgó una importante retroalimentación que permitió aplicar ciertas mejoras.

La metodología desarrollada permite organizar estudios con usuarios reales de forma ordenada pero en el ámbito de la inserción de texto. Sería interesante realizar mejoras para que fuese más genérica y su ámbito de aplicación sea cualquier tipo de aplicaciones en iDTV con o sin inserción de texto.

Agradecimientos

El trabajo presentado en este artículo ha sido financiado por la Universidad de Oviedo y por el Principado de Asturias a través del Proyecto con referencia SV-PA-13-ECOEMP-75.

Referencias

[1] M. Ingmarsson, D. Dinka, y S. Zhai, «TNT: a numeric keypad based text input method», en *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2004, pp. 639–646.

[2] A. Iatrino y S. Modeo, «Text editing in digital terrestrial television: a comparison of three interfaces», *Euro Itv*, 2006.

[3] G. Geleijnse, D. Aliakseyeu, y E. Sarroukh, «Comparing text entry methods for interactive television applications», en *Proceedings of the seventh european conference on European interactive television conference*, 2009, pp. 145–148.

[4] R. Aoki, A. Maeda, T. Watanabe, M. Kobayashi, y M. Abe, «Twist tap: text entry for TV remotes using easy-to-learn wrist motion and key operation», *Ieee Trans. Consum. Electron.*, vol. 56, n.º 1, pp. 161 - 168, feb. 2010.

[5] U. Gargi y R. Gossweiler, «QuickSuggest: character prediction on web appliances», en *Proceedings of the 19th international conference on World wide web*, North Carolina, USA, 2010, pp. 1249–1252.

[6] A. J. Sporka, O. Polacek, y P. Slavik, «Comparison of two text entry methods on interactive TV», en *Proceedings of the 10th European conference on Interactive tv and video*, 2012, pp. 49–52.

[7] T. Költringer, P. Isokoski, y T. Grechenig, «TwoStick: writing with a game controller», en *Proceedings of Graphics interface 2007*, 2007, pp. 103–110.

[8] I. S. MacKenzie, M. H. Lopez, y S. Castelluci, «Text Entry with the Apple iPhone and the Nintendo Wii», presentado en CHI2009, Boston, MA, USA, 2009.

[9] T. Tullis y W. Albert, *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics*. Morgan Kaufmann, 2008.

[10] F. E. Ritter y L. J. Schooler, «The learning curve», *Int. Encycl. Soc. Behav. Sci. W Kintch N Smelser P Baltes Eds Oxf.*, pp. 8602–8605.ASterdam:Pergamon, 2001.

[11] T. Bellman y S. Mackenzie, «A Probabilistic Character Layout Strategy for Mobile Text Entry», en *Graphics Interface*, 1998, pp. 168-176.

[12] I. S. MacKenzie, H. Kober, D. Smith, T. Jones, y E. Skepner, «LetterWise: prefix-based disambiguation for mobile text input», en *Proceedings of the 14th annual ACM symposium on User interface software and technology*, 2001, pp. 111–120.

[13] R. Likert, «A technique for the measurement of attitudes.», *Arch. Psychol.*, 1932.

[14] ISO, «14915-3:2002: Software ergonomics for multimedia user interfaces -- Part 3: Media selection and combination», *Int. Organ. Stand.*

[15] J. Perrinet, Xabiel G. Pañeda, Claudia Acebedo, Jose Luis Arciniegas, Sergio Cabrero, David Melendi, y Roberto García, «Adaptación de una aplicación de E-Learning A T-LEARNING», presentado en V Congreso Iberoamericano de Telemática. CITA 2009.

[16] L. Graham, «Gestalt theory in interactive media design», *J. Humanit. Soc. Sci.*, vol. 2, n.º ^ s1, 2008.

[17] «Recommendation ITU-R BT.500-12: Methodology for the subjective assessment of the quality of television pictures», International Telecommunication Union, vol.12, 2009.

NAPA: An algorithm to auto-tune unicast reliable communications over DDS

Juan J. Martin-Carrascosa, Jose M- Lopez-Vega, Javier Povedano-Molina,
Juan J. Ramos-Muñoz, Juan M. Lopez-Soler
Signal Theory, Telematics, and Communications Department
ETSI Informática y Telecomunicación
University of Granada
SPAIN

***Abstract*: This paper proposes NAPA (Non-supervised Adaptative Publication Algorithm) a framework for auto-tuning unicast reliable communications over DDS. We provide the NAPA design rationale, and some implementation details. After the experimental conducted evaluation, we demonstrate how using the subscriber's feedback, as NAPA does, the publisher can vary its sending rate in order to improve the overall performance in terms of end-to-end latency and throughput in DDS applications.**

Keywords: dds; throughput; latency; tuning; middleware;

I. INTRODUCTION

This paper focuses on the publish-subscribe interaction model. In the publish-subscribe model, the publish-subscribe service decouples the information producers (publishers) from information consumers (subscribers). Publishers update a shared information space and subscribers indicate what data are they interested in. It's the publish-subscribe service who delivers the desired information from publishers to subscribers.

Publish-subscribe systems can be classified according to the mechanism they use to choose what the events of interest for the different entities are. They can be topic-based (events classified according to a label), content-based (events classified according to their content) or type-based (event classified according to their structure).

Data Distribution Service (DDS) [1] is a middleware specification adopted by the Object Management Group (OMG) [4] aimed to standardize data-centric publish/subscribe communications in distributed scenarios. DDS was specified in 2004 and that specification includes the advances developed by different companies until the moment. This specification defines an Application Programming Interface (API) designed for data distribution in real-time using publish-subscribe model.

Over the last few years, DDS has been deployed in many different contexts ranging from mission critical systems to healthcare systems or financial systems. All these scenarios have in common that different remote entities exchange data from different sources in a well controlled environment and with certain guarantees like reliability and determinism.

Publish/subscribe communication systems are able to de-couple in time and space the publishers and subscribers. The existence of projects like PSIRP [5] and PURSUIT[6] evidence the potential benefits of this model. These projects are aimed to define a publish-subscribe based Internet that can be considered a plausible alternative (even complementary) to the current design.

DDS defines a virtual data space –typically implemented as a distributed cache memory- where applications can share information just by writing or reading data identified by a name (topic), a type and optionally a key. Using this virtual data space reduces the difficulty implementing communications between system nodes, what eases the designing of distributed systems.

DDS is based on a data-centric model (where data is not opaque to the middleware) and provides a rich set of Quality of Service (QoS) that define the requirements of communications on each different scenario.

DDS specification defines two different interface levels and a layer for interoperability.

The **Real-time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol (DDS-RTPS)** interoperability layer. This layer allows different implementations of DDS to interoperate. It defines the discovery protocol, data representation format and message format. This layer was specified by the OMG in order to provide interoperability between the different implementations of DDS.

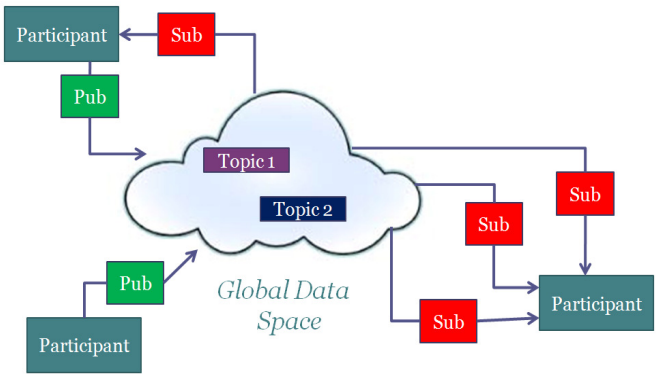


Fig 1. An overview of DDS entities.

The DCPS layer defines the concept of Data-space, Topic (group of data of same type), Publishers (data producers) and Subscribers (data consumers) (see Fig. 1). Also, this layer introduces the support of QoS Policies, group of settings that determines the behavior of the middleware and releases the application developers of certain tasks such as communication reliability.

DDS scenarios may vary considerably. In this regard, system administrators usually need to tune the middleware and nodes forming the full system in order to get better performance in terms of throughput and latency.

Although manual tuning may improve the performance achieved, tuned parameters' sensibility and scenario's variability (network variations, number of nodes and CPU load in nodes) reduce the effectiveness of the tuning. This issue could even discourage system administrators from performing any adjustment at all.

In this paper we propose an algorithm for dynamically tuning reliable communications over DDS. In particular, this algorithm adjusts data publishing rate according to subscriber's feedback (Acknowledge messages).

Regarding the performance and evaluation, to the author's knowledge there aren't any benchmarks universally accepted for evaluating real-time scenarios. However, some initiatives are gaining popularity for the case of real-time system benchmarking. Two of these famous benchmarks are SPECjms2007 [7] and STAC-M2 [8]. Nevertheless, these benchmarks are for MOM (Message Oriented Software), not for data-centric middleware.

In addition to these, the authors have already published other works related to DDS and its performance and evaluation. Most related publications are "A content-aware bridging service for publish/subscribe environments" [9] and "Performance evaluation of Publish/Subscribe middleware technologies for ATM (air traffic management) systems" [10].

The remainder of this paper is organized as follows. In Section 2, we elaborate about the reasons that motivate researching on this topic. Section 3 describes the proposed algorithm design. In Section 4 we explain the Implementation details. In Section 5 we show the results obtained when evaluating our algorithm. Finally, in Section 6 the main conclusions of this paper are shown.

II. MOTIVATION

By definition, in reliable communications involved nodes do their best to provide data with no errors, typically by resending lost samples. The additional generated traffic reduces the available bandwidth for the main communication and increases the latency both in the resent samples and the following ones. This is mainly due to two effects of sample resending: first, the increase of buffer waiting time; and secondly, the blocking of the publisher while it waits to receive the delayed data acknowledgments.

Losses are not the only reason of transmission blocking in reliable communications. In the DDS middleware, publishers have a size-limited send window that blocks communication when it is full. Since DDS does not removes samples from the window until the subscriber has acknowledged them, publishers get blocked when they send data faster than subscribers can receive and process it.

For this reason, sending data as fast as possible is not the optimal behavior, due to it can cause getting the publisher blocked. It means that those samples --being ready to be sent-- experiment an increased latency due to the incurred buffer waiting time. Note that latency is not only affected by the time spent in the link (transmission and propagation), but also the incurred time between different communication layers.

These are the reasons why there is a known need of tuning communication between publishers and subscribers: if publishers send data at the maximum rate that subscribers allow, resends' traffic will be reduced, as well as time spent in buffers.

The effect of this additional traffic is shown in Fig. 2. This Figure depicts throughput and one-way latency in function of the elapsed time between consecutive sent data, in a 1 to 1 reliable communications. In this case we use 100kB messages. As it can be seen, waiting enough time between consecutive samples may result in a better performance than sending data as fast as possible. However, if the publisher waits too much time, throughput will get worse although latency is reduced considerably.

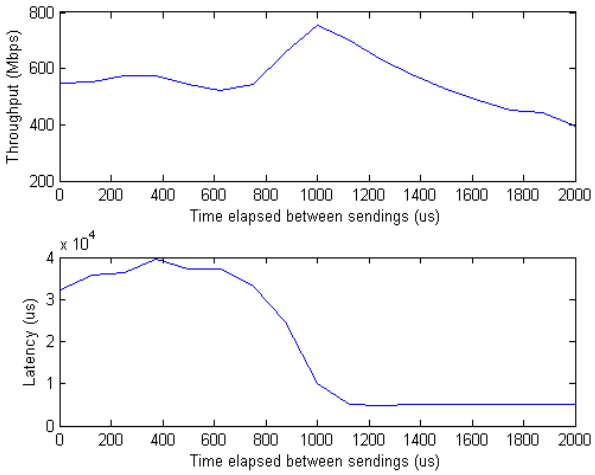


Fig 2. Performance *versus* inter-packet elapsed time.

In Figure 2 there is a range of elapsed time values that provides the best trade-off, that is, better throughput and latency. However, this range of value is dynamic and depends on sample data size, network status, CPU usage, etc.

This paper studies these DDS performance issues and particularly proposes an auto-tuning algorithm for making the system to work in the optimal operation point.

III. ALGORITHM DESIGN

The purpose of using reliable communications is to ensure that the subscriber receives all the samples (in order, with no errors either losses). Analyzing results shown in the previous section, we can enunciate the following statements:

1. As the inter-packet elapsed time is reduced, subscriber can potentially receive them faster than it can process. In this case, it starts rejecting new incoming samples and it will ask for retransmissions. As a consequence, the throughput gets lower and latency will accordingly increase.
2. For large inter-packet elapsed times, the publisher will be sending at a lower rate than the subscriber can receive. Throughput is decreased due that low rate, but latency is smaller because the system is more relaxed and there is no need to wait so much time in buffers.
3. In the correct operation point, publisher sends samples at the same rate that the subscriber can process. This makes throughput be better because retransmissions are not needed and latency gets minimized because there is no congestion in the communication path.

Now that the effect of varying the time elapsed between packets is characterized, we analyze what are the requirements that must accomplish the tuning algorithm. An algorithm that tunes the communications must consider the following points:

- The publisher should send data in such a way that the subscriber never gets empty.
- The publisher should avoid filling its sending window, so it does not get blocked.

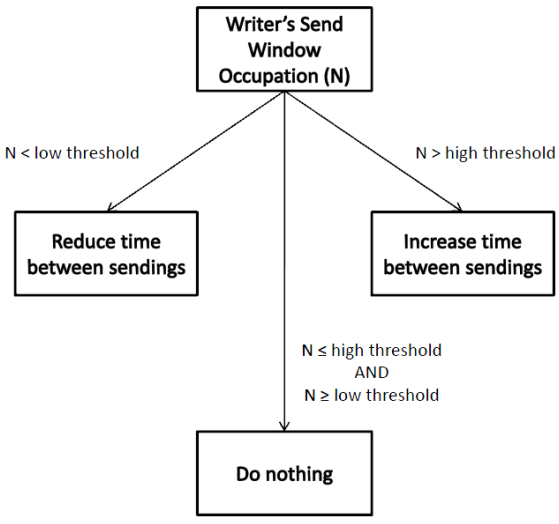


Fig 3. High level view of NAPA.

When the communication is reliable (by setting DDS QoS `reliable = reliability`), samples are kept in the sending window until the subscriber acknowledges them. This makes the sending window to be used as subscriber's feedback in the publisher's side. In terms of the publisher's sending window, according to the previous rationale:

- Sending window occupation should be highly enough to involve continuous transmission.
- Sending window should never get full.

These both are the two conditions that define the proposed algorithm behavior, hereafter referred to as Non-supervised Adaptative Publication Algorithm (NAPA).

Assuming the existence of an optimal local operation point, NAPA varies the time elapsed between consecutive data (T) as a function of the sending window occupation (N). As shown in Figure 3:

1. If N < `low_threshold`, decrease T.
2. If N > `high_threshold`, increase T.
3. If `low_threshold` ≤ N ≤ `high_threshold` do nothing.

Where `low_threshold`, and `high_threshold` (referred to as Acceptance Range) define the interval where the sending window occupation is expected to be in order to work in an optimal way.

To estimate the best values for the thresholds, we will follow two different approaches:

1. **Low_threshold**: The goal of this value is to modify the publisher's sending rate to have at least one unacknowledged sample in the sending window, so it does not get empty. For this reason, `low_threshold` is set equal to 1 for all the experiments in this paper.
2. **High_threshold**: The goal of this value is to reduce the publisher's sending rate when the publisher is being faster than the reception subscriber's capacity. To estimate the proper value for this variable, we are going to analyze the message passing diagram between publisher and subscriber.

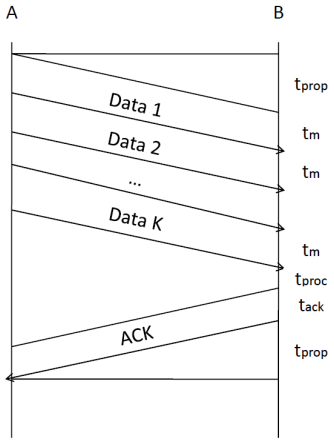


Fig 4. Time elapsed until first acknowledge message is received in the DDS Writer (A) when the DDS Reader (B) acknowledges samples in group of K samples.

Fig. 4 shows the elapsed time between different events that occur during the message passing. First, let´s estimate the size of the sending window (W) that allows the publisher to send data continuously:

$$W\ t_m\ \geq\ RTT_k$$

$$RTT_k = K\ t_m + 2\ t_{prop} + t_{proc} + t_{ack}$$

$$RTT_k = (K-1)t_m + RTT_1$$

$$W\ \geq \frac{RTT_k}{t_m} = \frac{RTT_1 C}{size_m} + (K-1)$$

where

- W: Sending window size.
- t_m: Time spent to put a message into the wire.
- RTT_k: Round-Trip Time measured when the subscriber needs to receive k messages to acknowledge.
- t_{prop}: Propagation time between publisher and subscriber.
- t_{proc}: Processing time in the subscriber.
- t_{ack}: Time spent to put an ack-message in the wire.
- C: Capacity of the network that connects publisher and subscriber.
- $size_m$: Size of the message.
- K: Number of messages that the subscriber needs to receive before sending an ACK. DDS defines this configuration parameter to save bandwidth.

After defining the minimum sending window size that is needed to have continuous transmission, `high_threshold` of the Acceptance Range must be determined. If we chose a value much higher than the defined by the above expressions, we would have bursts in the communication. In order to avoid that behavior, we chose the value defined by the following equation:

$$W = \frac{RTT_1 C}{size_m} + (K-1)$$

Given that the bandwidth, the message size and K are known values, only the RTT estimation is needed to estimate W. This can be statically done at the beginning of the communication or periodically in the transmission, what would modify the Acceptance Range and would get a better adaptation in dynamic operation scenarios.

IV. IMPLEMENTATION

For NAPA algorithm implementation, we adopted the following decisions:

- *RTT* is measured before the communication proceeds.
- The obtained value for the `high_threshold` (*W*) remains static for the session.
- To have full control, we need to spend time between sending consecutive samples without involving the CPU. To do this, elapsed time are expressed as the number of repetitions (`LoopCounter`) of a worthless operation. Time between consecutive samples will be modified indirectly just by increasing or decreasing `LoopCounter`. Note that this approach spends just a few microseconds in every execution, what provides a better granularity in comparison with the use of Sleep functions (which involves the CPU).
- The elapsed time between consecutive samples will not be modified every sent sample. Instead of that, we set an algorithm execution period.
- The elapsed time between consecutive samples will be modified as a function of the message size, a gain factor and a stability factor.
- Aiming at better adaptation speed as well as having higher precision, the gain factor will be dynamically adapted, starting at a high value and decreasing it with time.

Fig. 5 shows the NAPA implementation diagram flow:

1. At the beginning of the transmission, *RTT* is measured in order to estimate *W*.
2. NAPA modifies the `LoopCounter` once in each control period. During the transmission:
   a. If it is time for `LoopCounter` updating, compare the current sending window occupation with the Acceptance Range, and modify it consequently.
   b. If it is not time for updating it, do nothing.
3. Repeat `LoopCounter` times the worthless operations.
4. Send the message.
5. If we have sent all the messages, go to end. If not, back to step (2).

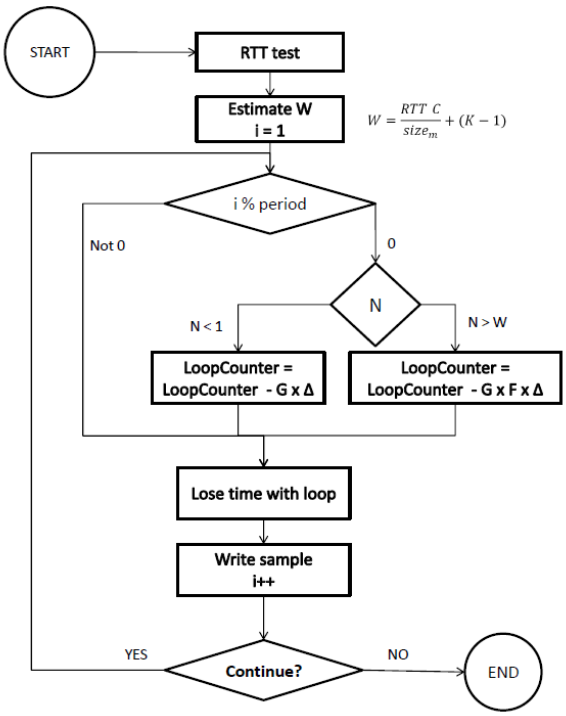


Fig 5. NAPA flow diagram.

We developed a NAPA prototype to evaluate our design and its performance improvement in comparison with non-using the proposed auto-tuning algorithm.

NAPA was implemented at the application level using the application RTIPerftest [2] as communications infrastructure. RTIPerftest is a tool used for analyzing communication performance within scenarios based in RTI Connext DDS [3].

RTIPerftest provides the features needed to measure latency and throughput, as well as the communication infrastructure needed to send data between two systems. There are several command-line options, including those to specify whether the application will act as the publisher or subscriber.

Several copies of the application can be executed (typically 1 publisher and 1 or more subscribers): The publisher application publishes throughput data and subscribes to latency echoes. The subscriber application subscribes to the throughput (in which the echo requests are embedded) and publishes the latency echoes (see Fig. 6).

Latency results are measured in the publisher and throughput results are estimated in the subscriber. RTIPerfTest includes many options to test almost every type of scenario. Among other it is possible to change data size, to specify QoS settings, different transport as well as disable acknowledgements, specify IP addresses for static discovery, activate batching, etc.

We adopted this tool for NAPA evaluation because of it could be easily done using the RTI Connext DDS API (specifically the C++ API).

Nevertheless, note that NAPA design is implementation-independent, as it only uses the sending window occupation as input to estimate the optimal sending speed. Consequently, NAPA can be implemented using any other DDS implementation.

RTIPerftest was modified to include NAPA functionality. It was compiled using gcc version 4.4.3 whereas the DDS implementation was RTI DDS 4.5d.

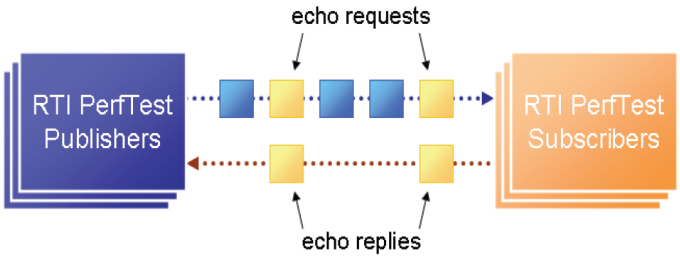


Fig 6. RTIPerfTest overview

V. EVALUATION

To evaluate the performance of NAPA, we made a set of experiments in a controlled LAN environment. Specifically, we measured the performance in terms of throughput and latency in a 1 to 1 reliable communication.

The evaluation environment was composed of two Core i5 at 2.66 GHz machines (lab01 and lab02) running Linux Kernel 2.6.32_22 x86_64 (Ubuntu 10.04) and the RTI DDS 4.5d middleware. These machines were connected by a 24-port Gigabit switch with VLAN support.

The experimental setup used in the evaluation of the NAPA algorithm were the following:

- Message size: from 5kB to 200kB.
- Reliable communication, one publisher to one subscriber via UDPv4.
- Gain factor starting at 1 and reduced to 0.2 after 30 seconds.
- Acknowledge (ACK) messages sent every 10 samples received.

Fig. 7 shows how NAPA improves the throughput for a wide range of message sizes. This is due to, as explained before, the number of retransmissions is reduced. The noticeable throughput reduction for using a data sizes slightly greater than 64kB is due to the size limit imposed by UDP packets: Note that form these message sizes it starts to use Asynchronous Writing in order to support bigger data sizes. NAPA reduces the performance loss when writing asynchronously and gets a better throughput for the rest of sizes.

Regarding the latency impact (Fig. 8), we see how one-way latency is decreased in almost an order of magnitude when applying NAPA. This reduction is the most important and noticeable result achieved by NAPA algorithm, because minimizing latency with a high level of throughput is considered one of the main goals of any real-time middleware.

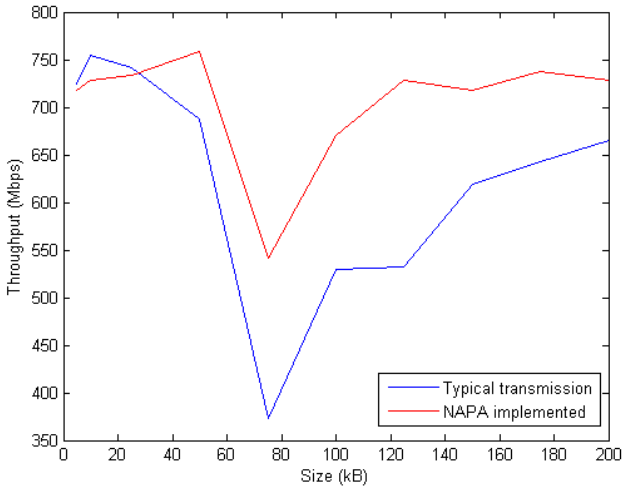


Fig 7. Throughput comparison between using and non-using NAPA.

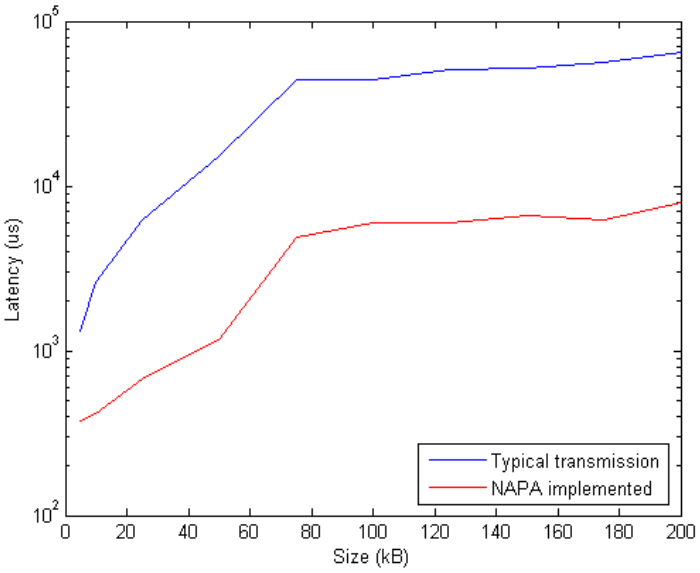


Fig 8. Latency comparison between using and non-using NAPA.

VI. CONCLUSIONS

In this paper we have presented NAPA, a dynamic auto-tuning algorithm for data-centric publish/subscribe systems.

Our algorithm is focused on avoiding publisher blocking and subscriber starvation problems by dynamically adjusting middleware parameters according to system conditions.

We have demonstrated that our algorithm effectively improves the performance of DDS-based systems both in terms of samples latency and overall throughput.

As future work, we are interested in including more dimensions in NAPA applicability:

- To apply NAPA in multicast scenarios. NAPA can be directly applied to 1 to many scenarios. DDS standard specifies that samples are removed from the send window in the publisher side when all the subscribers have acknowledged them. So, there won't be any significant change in the algorithm in order to be applied in multicast scenarios.
- To study the effect of applying NAPA in secure communications, where CPU usage is increased in the nodes due to secure protocols.
- To apply NAPA in disadvantage networks, that is in those with high loss communication. This investigation would show if NAPA improves performance when the nature of losses is not the communication congestion (overloading the subscriber writing faster than it can process).
- To include NAPA algorithm in the core DDS implementation to facilitate the auto-tuning t any application.

We are also interested in analyzing the performance improvement when increasing the NAPA complexity:

- By replacing the gain factor reduction model (linear) for a higher order model.
- By redesigning the "losing time between consecutive samples" method so it considers context switching. With the actual implementation, while the publisher application doesn't have the CPU the losing time loop doesn't advance, although in this cases time is going on what reduces its accuracy.

ACKNOWLEDGEMENTS

We would like to thank Gerardo Pardo-Castellote for his support and guidance during the investigation related to this tuning algorithm.

This research was partially founded by Spanish Ministry of Education (Collaboration Grant 2012-2013).

REFERENCES

[1] Data-Distribution Service for Real-Time Systems (DDS). v1.2. Tech. Rep., OMG. http://www.omg.org/cgi-bin/doc?formal/07-01-01.pdf.

[2] Real-Time Innovations. RTI Performance Test. Available at: http://na2.salesforce.com/_ui/selfservice/pkb/PublicKnowledgeSolution/d?orgId=00D3000000065k0&id=50140000000LQkK&retURL=%2Fsol%2Fpublic%2Fsolutionbrowser.jsp%3Fcid%3D02n400000004kPY%26orgId%3D00D3000000065k0&ps=1

[3] Real-Time Innovations. RTI Connext DDS. Available at: http://www.rti.com/products/dds/index.html

[4] OMG. Object Management Group, 2013.http://www.omg.org/

[5] Vladimir Dimitrov and Ventzislav Koptchev. PSIRP project – publish subscribe internet routing paradigm: new ideas for future internet. In Proceedingsof the 11th International Conference on Computer Systems and Technologiesand Workshop for PhD Students in Computing on International Conferenceon Computer Systems and Technologies, CompSysTech '10,pages 167–171, NewYork, NY, USA, 2010. ACM. ISBN 978-1-4503-0243 2. doi: 10.1145/1839379.1839409. http://dxhttp://dx.doi.org/10.1145/1839379.1839409

[6] PURSUIT. Publish Subscribe Internet Technology (PURSUIT) project site.Technical report, 2010. http://fp7pursuit.ipower.com/PursuitWeb/wp-content/uploads/2011/03/PURSUIT_fact_sheet.pdf

[7] Standard Performance Evaluation Corporation. Specjms2007 homepage, 2007. http://www.spec.org/jms2007/

[8] Securities Technology Analisis Center. Stac-m2 homepage. http://www.stacresearch.com/m2

[9] J. M. Lopez-Vega, J. Povedano-Molina, G. Pardo-Castellote, and J. M. Lopez-Soler, "A content-aware bridging service for publish/subscribe environments,"Journal of Systems and Software, vol. 86, no. 1, pp. 108-124, Jan. 2013. [Online]. http://dx.doi.org/10.1016/j.jss.2012.07.033

[10] J. M. Lopez-Soler, J. M. Lopez-Vega, J. Povedano-Molina, and J. J. Ramos-Munoz, "Performance evaluation of Publish/Subscribe middleware technologies for ATM (air traffic management) systems," in Workshop on Real-time, Embedded and Enterprise-Scale Time-Critical Systems, 2012.

Evaluaciones subjetivas de servicios streaming adaptativos vs no-adaptativos

Alberto Álvarez, Laura Pozueco, Sergio Cabrero, Xabiel G. Pañeda, Roberto García, David Melendi, Gabriel Díaz Orueta*.
Departamento de informática,
Universidad de Oviedo
Campus de Viesques, Gijón, Asturias, España.
*Universidad Nacional de Educación a Distancia (U.N.E.D)
{alvarezgalberto, pozuecolaura.uo, cabrerosergio, xabiel, garciaroberto, melendi}@uniovi.es,
*gdiaz@ieec.uned.es

***Resumen*- El análisis subjetivo de sistemas streaming adaptativos es un proceso clave para optimizar algoritmos que permitan una adaptación basada en medidas de calidad de la experiencia (QoE). En este trabajo abordamos el estudio comparativo de un sistema streaming adaptativo frente a un sistema streaming tradicional (no adaptativo) desde el punto de vista subjetivo. Se evaluará en qué situaciones y condiciones un sistema adaptativo mejora la calidad percibida por el usuario y cuáles son los umbrales de tolerancia a pérdidas que marquen el inicio del proceso de adaptación. Para ello se plantean diferentes situaciones de disponibilidad de ancho de banda en la red y diferentes decisiones de adaptación. Los resultados del estudio, en el que han participado 75 usuarios, resuelven cuestiones clave para el diseño de sistemas adaptativos y muestran que la adaptación mejora la experiencia de usuario en la mayoría de las condiciones evaluadas.**

***Palabras Clave*- medidas de calidad subjetivas, scalable video coding (SVC), experiencia de usuario (QoE)**

I. INTRODUCCIÓN

La creciente demanda de los servicios de vídeo en Internet es una realidad hoy en día. Sin embargo, este tipo de servicios no está exento de problemáticas relacionadas con la calidad percibida por el usuario en función de las condiciones en la red.

En entornos tipo *best-effort*, la tecnología *Scalable Video Coding* (SVC) se ha posicionado como una alternativa a tener en cuenta para implementar diseños de adaptación de los contenidos transmitidos. Sin embargo, la construcción de estrategias de adaptación para sistemas de vídeo streaming aún presenta interrogantes en lo referente a las preferencias de usuario en los cambios de calidad [1]. Cuándo y en qué situaciones un sistema adaptativo mejora la calidad percibida por el usuario son todavía cuestiones controvertidas y que plantean dos tendencias opuestas en el campo de los servicios de vídeo en entornos *best-effort*: los sistemas adaptativos frente a los sistemas no adaptativos.

Surge así la motivación de realizar un estudio subjetivo que compare diferentes decisiones de adaptación, empleando la tecnología SVC, con un servicio streaming no adaptativo. Bajo diferentes condiciones de ocupación de red, se pregunta a los usuarios acerca del grado de preferencia, si lo hay, hacia uno de los dos sistemas en diferentes circunstancias.

Para comparar el comportamiento de los dos sistemas de transmisión de vídeo, emplearemos la metodología de evaluación subjetiva denominada SCACJ (*Stimulus Comparison Adjectival Categorical Judgement*) [2]. En este método, los dos estímulos (vídeos) que se quieren comparar se presentan simultáneamente.

Cada par de vídeos de los dos sistemas evaluados se generan bajo las mismas condiciones de disponibilidad en la red. El vídeo correspondiente al sistema no adaptativo mantendrá la misma calidad durante toda la reproducción de los contenidos, mientras que el vídeo correspondiente al sistema adaptativo realizará cambios en la calidad transmitida para ajustarse a las condiciones de disponibilidad de ancho de banda. Después de la reproducción de los contenidos se pregunta al usuario cuál de los dos estímulos considera que ha visto mejor.

Para llevar a cabo los experimentos, fue necesario desarrollar una herramienta software específica y generar un conjunto de secuencias que permitan evaluar diferentes decisiones de adaptación bajo diversas condiciones de ocupación en la red.

Un total de 75 usuarios, con edades comprendidas entre los 23 y los 65 años, evaluaron 45 pares de secuencias de diferentes contenidos.

Los resultados muestran que el sistema adaptativo mejora la experiencia de usuario en la mayoría de las situaciones. Sin embargo, bajo ciertas circunstancias de pérdidas aisladas en la red, los algoritmos de adaptación no suponen una mejora apreciable en la calidad percibida por los participantes frente a un sistema streaming estándar. El análisis en detalle de la información extraída de los resultados puede ser empleado en la construcción de algoritmos adaptativos óptimos. Por otro lado, los usuarios con cierta experiencia en el visionado de contenido multimedia y la población más joven (menores de 35 años) evalúan más positivamente el sistema de adaptación en la mayoría de los casos. No obstante, nuestros resultados subjetivos muestran que los usuarios acostumbrados a ver vídeos a través de Internet también son más críticos en el proceso de evaluación que los usuarios que únicamente ven la televisión.

El resto del artículo está organizado como sigue: la Sección II repasa los trabajos relacionados en el campo de este estudio. La Sección III proporciona una descripción de los experimentos subjetivos llevados a cabo, los objetivos

que perseguimos en la realización del estudio y los detalles de la metodología de evaluación subjetiva, así como el hardware y el software empleado para llevar a cabo los experimentos. La Sección IV describe en detalle el conjunto contenidos desarrollados y la población que ha participado en el estudio. Los principales resultados se discuten en la Sección V. Finalmente, las conclusiones y los trabajos futuros se resumen en la Sección VI.

II. Trabajos Relacionados

La ITU-T recomienda un conjunto de metodologías para la evaluación subjetiva de vídeo y sistemas multimedia [2] [3]. Las evaluaciones subjetivas son claves para estudiar la calidad percibida para nuevos codecs, nuevos sistemas de distribución o, en general, para evaluar los efectos de las degradaciones en el vídeo [4].

Los codecs escalables y las estrategias de escalabilidad han sido el núcleo de algunos estudios subjetivos. El trabajo en [5] proporciona un resumen completo del estado del arte referente a estudios subjetivos y objetivos empleando diferentes técnicas de streaming escalable, incluyendo SVC.

La mayoría de los estudios subjetivos están relacionados con evaluaciones de comportamiento de codecs, incluyendo así la evaluación de diferentes capas de calidad [6]. Oelbaum et al. [7] presentan un estudio subjetivo formado por 20 usuarios y 12 secuencias de vídeo diferentes. Los resultados muestran que el códec H.264/SVC ofrece una calidad comparable con el códec de H.264/AVC (*Advanced Video Coding*) con un ligero incremento de la sobrecarga y la complejidad del decodificador. Niedermeier et al. [8] también llevan a cabo análisis subjetivos del comportamiento del códec SVC, comparándolo con Xvid y codecs AVC. Emplean para ello 5 secuencias diferentes con una población de 21 personas. Los autores en [9] también comparan el funcionamiento de SVC con AVC, pero en un contexto móvil. Evalúan 4 contenidos diferentes en experimentos subjetivos con 15 participantes.

También en un contexto móvil, Eichhorn y Ni [10] presentan un estudio subjetivo investigando los efectos de la escalabilidad multidimensional de SVC con 6 secuencias de partida y 30 usuarios. Adoptan la metodología DSCQS (*Double Stimulus Continuous Quality Evaluation*). Concluyen que las preferencias en el escalado y las dimensiones de escalabilidad seleccionadas son dependientes del contenido, tal y como hemos corroborado en los resultados de nuestro propio estudio.

Otros trabajos proponen nuevas metodologías para los estudios subjetivos. Lee et al. [11] llevan a cabo evaluaciones subjetivas de dos códecs escalables con SSCQS (*Single Stimulus Continuous Quality Scale)* y comparación por pares (PC, *Paired Comparison*) de diferentes opciones de escalabilidad para bitrates similares. Emplean para ello 3 secuencias diferentes que son evaluadas por 16 usuarios. Proponen además un método de interpretación de los resultados en los estudios de comparación por pares. Nuestro estudio incluye una comparación similar acerca de la preferencia en cuanto a la estrategia adaptativa.

Staelens et al. [12] proponen una nueva metodología que mide el impacto de la degradación sufrida en películas completas usando SVC. Su propuesta incluye la entrega del DVD con los contenidos de la película a 38 hogares, abarcando más de 100 sujetos. Después de visionar los contenidos, se realiza un cuestionario a los participantes. El trabajo presentado por estos autores también incluye una comparación de esta metodología novedosa con la metodología estándar (SS ACR: *Single Stimulus, Absolute Category Rating*). Concluyen que los usuarios acostumbrados al visionado de vídeo online son más tolerantes a los saltos de calidad. En nuestro trabajo, observamos que dichos usuarios experimentados son más conscientes, en general, de los cambios en la calidad que presenta el sistema adaptativo. Tanto en el estudio llevado a cabo por Staelens como en el nuestro propio (siguiendo una metodología estándar), se detecta una preferencia hacia las degradaciones en el plano de la calidad frente a las degradaciones en el plano temporal.

Los autores en [13] llevan a cabo un estudio subjetivo con 28 usuarios para evaluar el impacto de la red y de los parámetros de codificación en la calidad visual, usando cancelación de errores para codificaciones basadas en SVC. La metodología adoptada en este estudio es una metodología estándar ACR (*Absolute Category Rating*).

Otros estudios se centran en diferentes alternativas a SVC para llevar a cabo la adaptación de los contenidos. Un ejemplo de ello lo encontramos en el trabajo propuesto en [14], empleando la tecnología DASH (*Dynamic Adaptive HTTP Streaming*) en test subjetivos formados por 24 participantes y 11 secuencias de vídeo diferentes. Los resultados muestran que los usuarios prefieren cambios graduales en la calidad de los contenidos frente a los cambios abruptos.

A la luz del estado del arte actual podemos concluir que todavía existen situaciones que precisan de evaluaciones subjetivas para cubrir ciertos aspectos relacionados con la calidad percibida por los usuarios en entornos de vídeo adaptativo.

Nuestro trabajo incluye una metodología de evaluaciones subjetivas diferente, no empleada anteriormente con SVC. Por otro lado, las secuencias de vídeo empleadas en los test de usuario incluyen diferentes patrones de error y estrategias de adaptación en el plano temporal y de calidad. La disponibilidad de una población extensa y variada (mucho mayor del mínimo de 16 participantes recomendado por [2]) nos permite clasificar nuestros participantes en grupos de acuerdo a la edad o a la experiencia con vídeo, pudiendo extraer diferentes conclusiones relacionadas con estas categorías.

III. Descripción de los Experimentos Subjetivos

Los servicios transmisión de vídeo en Internet son muy sensibles a las variaciones en las condiciones de red y situaciones de congestión o pérdidas. Por esta razón es necesario disponer de un sistema que adapte el formato de los contenidos a las condiciones de transmisión [15]. SVC hace posible esta idea de manera factible, mediante sus tres opciones de escalabilidad: espacial (diferentes resoluciones), temporal (diferentes frecuencias de frames) y de calidad (diferentes calidades en cuanto a bits por píxel). La combinación de la tecnología SVC con algoritmos de estimación de la congestión permite construir un sistema adaptativo que sea capaz de ajustar los contenidos a las condiciones de red en cada momento. Cuando se detecta una situación de congestión, se espera que cualquier sistema

adaptativo reduzca el bitrate de la transmisión del vídeo. En una tecnología por capas como SVC, esto significa que las capas superiores (de mejora) se eliminen. Por otro lado, cuando no hay congestión, el bitrate debería incrementarse, aumentando el número de capas que se envían al cliente.

El estudio de calidad de la experiencia que llevaremos a cabo tiene como objetivo global comparar un sistema de transmisión de vídeo streaming convencional (a partir de ahora podrá ser referenciado como "sistema de referencia o sistema no adaptativo") con la filosofía expuesta de adaptación dinámica de contenidos en tiempo real (sistema adaptativo). Se pretende así estudiar la percepción de los usuarios frente a diferentes decisiones de adaptación.

A. Objetivos del experimento

A continuación se describen los diferentes objetivos establecidos para evaluar diversos factores y cuestiones relacionados con los sistemas adaptativos. Cada objetivo pretende evaluar el proceso de adaptación y la percepción del usuario frente a los cambios en una única dimensión de escalabilidad como consecuencia de diferentes condiciones de disponibilidad en la red.

- **Objetivo I**: obtener la mejor opción de adaptación cuando la red presenta situaciones de congestión severas. Se pretende estudiar cuál es el impacto en los usuarios en cuanto a la reducción de niveles temporales o niveles de calidad para compensar las pérdidas en la red.
- **Objetivo II**: estimar el umbral de pérdidas idóneo a partir del cual se debería lanzar el proceso de adaptación.
- **Objetivo III**: obtener la preferencia de los usuarios frente a una secuencia de vídeo con pérdidas y una secuencia que ha sido adaptada en la dimensión temporal reduciendo severamente los frames por segundo.
- **Objetivo IV**: en situaciones de disponibilidad de ancho de banda, evaluar la existencia de diferencias subjetivas cuando a los contenidos se añaden capas de calidad frente a mantener la calidad inicial.
- **Objetivo V**: evaluar la percepción de los usuarios en el incremento dinámico de niveles temporales cuando se compara con un sistema no adaptativo que mantiene el frame rate constante.

La Tabla 1 muestra un resumen con las principales características de los objetivos propuestos para este estudio. En dicha tabla se detalla el tipo de escenario y la adaptación llevada a cabo. También se incluye información acerca del número de secuencias generadas para la evaluación de cada objetivo por parte de los participantes en el experimento.

Tabla I
RESUMEN DE LOS OBJETIVOS

Objetivo	Tipo de escenario	Tipo de adaptación	Número de secuencias
I	congestionado	Reducir capas de calidad o temporal	6
II	congestionado	Reducir capas temporales	16
III	congestionado	Reducir capas temporales	6
IV	no congestionado	Incrementar capas de calidad	8
V	no congestionado	Incrementar capas temporales	12

Los contenidos de vídeo empleados en los test de usuario (descritos en la Sección IV.A) se generan de acuerdo a las directrices de los objetivos planteados, cubriendo así los principales aspectos en la evaluación de sistemas adaptativos desde el punto de vista de percepción de calidad recibida por el usuario.

B. Metodología subjetiva

La ITU recomienda un conjunto de metodologías para realizar evaluaciones subjetivas de vídeo y sistemas multimedia [2], [3]. Las diferentes metodologías difieren en aspectos tales como la configuración del experimento, la existencia o no de una señal de referencia o la evaluación de secuencias individuales o por pares. Para los requerimientos de nuestro experimento, la metodología seleccionada para realizar las pruebas de evaluación subjetiva ha sido, tal como sugieren en [2], SCACJ (*Stimulus Comparison Adjectival Categorial Judgment*). En la metodología SCACJ, los observadores evalúan la existencia de diferencias entre un par de secuencias (o estímulos) que se presentan de manera simultánea. En nuestro caso, esas secuencias se corresponden con los vídeos generados por un sistema streaming adaptativo y un sistema streaming tradicional, bajo las mismas condiciones de ocupación de red. Los usuarios votan de manera intuitiva hacia el lado en el que consideren que han visto la secuencia mejor, indicando en qué medida la prefieren frente al otro vídeo. El grado de diferencia percibida entre los dos sistemas se evalúa a través de las siguientes categorías: "*mucho mejor*", "*mejor*", "*ligeramente mejor*" o "*la misma*".

Durante la fase de procesado y análisis de los datos se traducirá la elección de los usuarios a una escala MOS (*Mean Opinion Square*) comparativa. La Fig. 1 muestra la categoría CMOS (*Comparison Mean Opinion Square*) propuesta para el sistema de votación de los estímulos mostrados. Este sistema de votación asume siete categorías de puntuación, desde -3 a +3, indicando cuál de los dos estímulos se elige y por cuánto más se prefiere. Valores negativos de CMOS indican una inclinación hacia el sistema de referencia (no adaptativo), mientras que los valores positivos del CMOS equivalen a una preferencia hacia el sistema adaptativo.

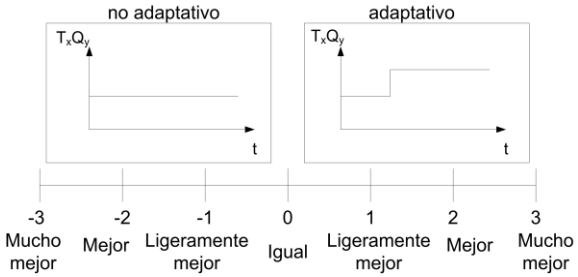


Fig. 1. Escala CMOS.

Después de una sesión de entrenamiento para cada usuario, en la que se familiarizará con la metodología de la prueba y el sistema de votación, los tests comienzan con la cumplimentación de información de contacto e información

personal referente a la edad, género, educación, experiencia con la visualización de vídeo (diferenciando entre usuarios que ven únicamente la televisión, que ven vídeos en Internet o que ven vídeos en Internet en alta definición) y los dispositivos empleados para ver vídeo (ordenadores, televisores, Tablets, Smartphones). Después, se presentan un conjunto de imágenes Ishihara [16] para medir la percepción al color de los usuarios. A continuación, el núcleo del test se compone de 45 pares de secuencias, cada par de secuencias de 19 segundos de duración, intercalando los periodos de votación entre ellas (Fig. 2). Los usuarios pueden ver los estímulos (los pares de secuencias) tantas veces como deseen.

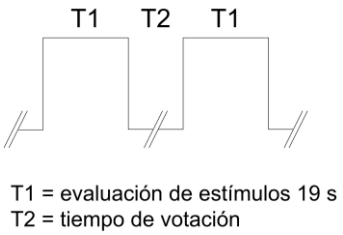


Fig. 2. Procedimiento del test.

La duración total del test se mantiene en torno a los 20 minutos, de acuerdo a las recomendaciones de la ITU.

Para evitar efectos de curvas de aprendizaje o la influencia del cansancio de los usuarios en las mismas secuencias finales, el orden de presentación de los pares de estímulos para cada usuario es aleatorio. También es aleatoria la posición en la pantalla del vídeo correspondiente al sistema referencia (no adaptativo) y al sistema adaptativo para cada par de secuencias, de manera que el usuario no sabe qué vídeo se corresponde con cada uno de los sistemas mencionados.

Fig. 3. Pantalla de visualización del estímulo.

Fig. 4. Interfaz de votación.

Tabla II
DETALLES DEL MONITOR

Monitor LCD	Philips Led Model 236V3L
Tamaño diagonal	23 pulgadas
Resolución	1920x1080 (Full HD)
Contraste	5000000:1
Tiempo de respuesta	5 ms
Interfaz	D-Sub, DVI & HDMI
Ángulo de visión	170/160 grados

Tabla III
DETALLES DEL HARDWARE

Placa base	ASUS P8H61-M LE-USB3
Procesador	Intel Core i7
Tarjeta gráfica	ATI HD6570 1GB DDR3 PCI-E PowerColor
RAM	8GB DDR3
SSD	128 GB Series 830 Notebook Kit Samsung
Sistema operativo	Windows 7 Home Premium 64-bit

C. *Equipo y entorno, software y hardware*

Para realizar estos tests de usuario con la metodología elegida, fue necesario desarrollar una herramienta software específica. El software se desarrolló en Qt, usando *Phonon*, un framework multiplataforma multimedia que permite el uso de contenido de audio y vídeo en aplicaciones Qt. El aspecto de la aplicación desarrollada se diseñó con una interfaz limpia y fondo neutro gris, de acuerdo a las recomendaciones de la ITU-T, Fig. 3 y Fig.4.

Por otro lado, el equipo hardware empleado deberá ser capaz de presentar las secuencias generadas por pares simultáneos y en formato 'crudo' (esto es, decodificados), tal y como se especifica en [2]. Para ello se empleó un ordenador de última generación, con disco duro SSD y con un monitor de 23 pulgadas. Los detalles del equipo hardware se encuentran en la Tabla 2 y Tabla 3. El equipo se colocó en un entorno tranquilo, con baja iluminación (70-100 lx), tal y como se recomienda en [2]. La distancia entre el participante y el monitor se mantiene entre 1.5 y 2 metros.

IV. MATERIAL PARA LA REALIZACIÓN DE LOS EXPERIMENTOS

Para llevar a cabo los tests subjetivos descritos en apartados anteriores, será necesario generar diferentes secuencias de vídeo que evalúen los objetivos propuestos en la Sección III.A.

Además de los contenidos generados, un segundo elemento clave para la realización de los tests subjetivos son los usuarios. En esta sección también se describe brevemente la población que ha participado en las pruebas.

A. *Contenido*

Cada par de estímulos o vídeos incluidos en la evaluación subjetiva están compuestos por una secuencia no adaptada y una secuencia adaptada. La secuencia no adaptada se corresponde con un vídeo recibido a través de un sistema streaming tradicional. Por otro lado, la secuencia adaptada pertenece a un sistema streaming que dispone de técnicas de adaptación de los contenidos en función de la capacidad de la red.

Existen muchos modelos propuestos para construir sistemas de vídeo streaming adaptativos. Sin embargo, todos ellos comparten, a grandes rasgos, su comportamiento frente a situaciones de congestión, disminuyendo el bitrate, o situaciones de disponibilidad en la red, mejorando la calidad de los contenidos que se transmiten al cliente. Para generar los contenidos de este experimento, tomaremos como referencia el sistema propuesto en [17], donde el servidor realiza cambios en los niveles de escalabilidad cada 5 segundos, con el objetivo de ajustar la tasa de transmisión al ancho de banda disponible.

A partir del sistema de adaptación citado, los contenidos generados para el estudio subjetivo realizarán cambios en los niveles temporales o de calidad transcurridos 5 segundos del inicio de la reproducción. En cuanto a los contenidos pertenecientes al sistema no adaptado, éstos mantendrán el bit rate que se transmite durante toda la duración de la secuencia. Por tanto, durante los primeros 5 segundos, ambas secuencias son iguales.

Para este estudio, los pares de secuencias que se generan únicamente consideran un tipo de escalabilidad, es decir, la secuencia que se corresponde con el sistema adaptativo va a realizar la adaptación bien sea en el nivel temporal o en el nivel de calidad, pero nunca mezclando ambos tipos de escalabilidad.

Se procesaron diferentes vídeos origen (a los que denominaremos *tractor*, *factory*, *marathon* y *touchdown*) de diferentes contenidos para obtener 45 pares de secuencias diferentes. Para la sesión de entrenamiento de los usuarios se usó una secuencia adicional distinta. Los índices de complejidad espacial y temporal (*Spatial Index*, SI; *Temporal Index*, TI) para los cuatro contenidos de origen se muestran en la Tabla 4. Para la secuencia de *marathon* se proporcionan dos valores de complejidad temporal (TI), uno perteneciente al valor con cambios de escena y el segundo valor sin cambios de escena, como se indica en [3]. Las secuencias de *touchdown* y *tractor* tienen índices de complejidad similar, ambas bajos. La secuencia *factory* tiene un índice de complejidad temporal elevado y la secuencia *marathon* tiene la complejidad espacial más alta entre el conjunto de vídeos. La Fig. 5 presenta una captura de pantalla de cada uno de los contenidos originales empleados. Los contenidos se eligieron intentando cubrir diferentes valores de complejidad temporal y espacial, con el fin de estudiar la dependencia del contenido del vídeo con las diferentes preferencias de adaptación de los usuarios.

Fig. 5. Capturas de pantalla de los materiales del test

Tabla IV
DETALLES DEL MATERIAL DE TEST

	SI	TI	Detalles
Factory	21.2556	55.3439	854x480@30 FPS, 570 frames 19''
Tractor	17.8137	23.9409	854x480@25 FPS, 475 frames 19''
Marathon	23.9810	68.16 (31.8 sin cambios de escena)	854x480@50 FPS, 950 frames 19''
Touchdown	18.0624	27.0181	854x480@30 FPS, 570 frames 19''

Los cuatro vídeos de contenido original se codifican en SVC empleando el software JSVM[1]. Todas las secuencias fueron generadas con 5 niveles temporales y 4 niveles de calidad usando el esquema CGS para este último (*Coarse Grain Scale*). Después, se empleó la herramienta software SVEF [18] para generar las secuencias procesadas que se mostrarán en la realización del test subjetivo. Dichas secuencias incluirán pérdidas o adaptaciones en alguno de los niveles temporales o de calidad. Hemos modificado el subsistema de emulación de la transmisión de SVEF para incluir un modelo de pérdidas representado por un proceso de Bernoulli con la probabilidad de pérdidas como parámetro de entrada [19].

Para poder estudiar cada uno de los objetivos de evaluación descritos en la Sección III.A, cada una de las secuencias generadas cubre uno o más aspectos de los objetivos propuestos, alcanzando la cifra total antes mencionada de 45 pares de secuencias.

Para el objetivo I, se generaron 6 pares de secuencias que estimarán la diferencia percibida por los usuarios ante el hecho de disminuir una única capa de calidad o varias capas temporales para ajustarse a una disminución repentina en el ancho de banda disponible. Los diferentes ratios de paquetes perdidos propuestos para encontrar el umbral de tolerancia a pérdidas de los usuarios en el objetivo II son: 1%, 3%, 5% y 10%. Para este segundo objetivo se crearon un total de 16 pares de secuencias. Para medir la diferencia entre un sistema no adaptativo y un sistema adaptativo en el nivel temporal con pérdidas en la red (objetivo III), se proponen 6 pares de secuencias diferentes. Para los objetivos IV y V (escenarios en los que no existen pérdidas y se añaden capas de calidad o niveles temporales respectivamente) se crearon 8 y 12 secuencias respectivamente.

La Tabla 5 resume las características, en cuanto a tasa de frames y tasa de bits, de las diferentes capas escalables de los contenidos de vídeo empleados en los tests. Como se observa, solo se usaron las combinaciones temporales (desde T0 a T4) y de calidad (desde Q0 a Q3) que resultan interesantes para el estudio. Así mismo, la Tabla 6 especifica las características de los pares de vídeos utilizados en la evaluación subjetiva, indicando la capa y el porcentaje de pérdidas (si lo hubiese) para la secuencia de referencia y la

[1]http://www.hhi.fraunhofer.de/en/fields-of-competence/image-processing/research-groups/image-video-coding/svc-extension-of-h264avc/jsvm-reference-software.html

acción de adaptación llevada a cabo en la secuencia adaptada. Nótese que ambas secuencias parten siempre de las mismas condiciones y que algunas de las secuencias generadas se emplean en varios objetivos.

Las secuencias resultantes se decodifican con las herramientas de JSVM para obtener secuencias en crudo que serán usadas finalmente en los tests de usuario.

B. *Población*

Un total de 75 participantes formaron parte del estudio subjetivo. El porcentaje de hombres/mujeres es de 76/24% respectivamente. La edad de la población está comprendida entre 23 y 66 años, siendo la media de 37.01 con una desviación estándar de 11.56. Del total de los participantes, el 49% estaba por debajo de los 35 años.

De los candidatos, el 17.3% declararon que solían ver vídeos en la televisión únicamente. El 48% eran consumidores habituales de vídeo por Internet y el 34.7% declaró que regularmente veían vídeos con contenido en alta definición en la red. De entre los participantes que veían contenido de vídeo en Internet, el dispositivo más popular resultó ser el PC (55.8%), seguido por el Smartphone (29.8%) y el Tablet (14.4%).

V. Resumen De Los Resultados

Los datos obtenidos de los experimentos subjetivos se procesan para llevar a cabo un análisis de los resultados. La Fig. 6 resume el valor medio del CMOS para cada par de secuencias. Los valores positivos del CMOS indican la preferencia hacia el sistema adaptativo y los valores negativos de CMOS incidan una preferencia hacia el sistema no adaptativo. Analizando la Fig.6 y sin entrar en detalles, podemos adelantar una primera conclusión, y es que, en la mayoría de las situaciones analizadas, los usuarios se decantan por el sistema adaptativo de vídeo.

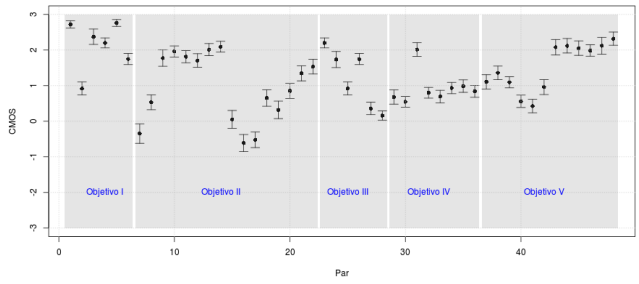


Fig. 6. Resultados CMOS agrupados por objetivos

Si clasificamos los resultados en función de la edad de los participantes (mayores y menores de 35 años, límite de edad que divide aproximadamente a la mitad a la población), se observa que la población joven (por debajo de los 35 años) muestra puntuaciones subjetivas menos moderadas que el resto. La población de mayor rango de edad normalmente puntúan con valores más próximos a la indiferencia entre el sistema adaptativo y el no adaptativo (CMOS=0), Fig. 7.

Nuestros resultados subjetivos también muestran que los usuarios con experiencia en vídeo por Internet son más críticos que los usuarios que únicamente ven la televisión y sus votaciones evalúan más positivamente la adaptación en las situaciones en las que se prefiere este sistema (Fig. 8). Al igual que en el análisis anterior, los usuarios menos experimentados, y que únicamente ven contenido multimedia a través de la televisión, evalúan el sistema adaptativo con valores más comedidos.

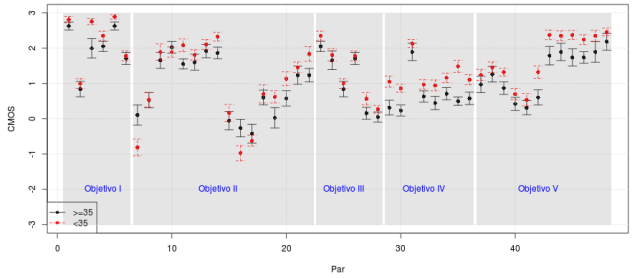


Fig. 7. Resultados CMOS en función de la edad

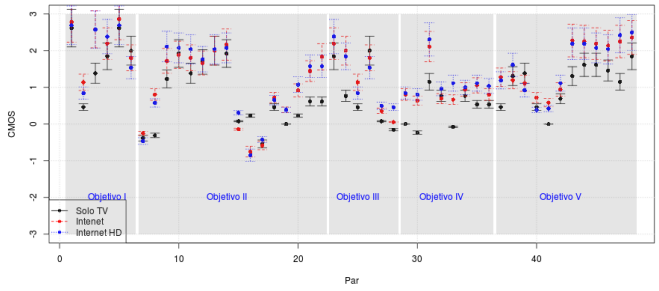


Fig. 8. Resultados CMOS en función de la experiencia con contenido multimedia

En un análisis más detallado de los resultados, donde se tiene en cuenta la naturaleza de los pares de vídeos evaluados (ver Tabla 6), se extraen los resultados que se detallan a continuación. Para el objetivo I, cuyo cometido era evaluar la preferencia en la disminución de varios niveles temporales o un único nivel de calidad, podemos concluir que, los cambios en calidad son más claramente aceptados que los cambios temporales.

Por otro lado, los algoritmos adaptativos normalmente definen un umbral de pérdidas para lanzar el proceso de adaptación. Basándose en los resultados subjetivos analizados en el objetivo II, podemos establecer que el umbral de tolerancia a pérdidas se situaría en torno al 3%, pero con consideraciones especiales con relación a las condiciones iniciales de frame rate. Por ejemplo, en secuencias con menor tasa de frames por segundo, los usuarios no aprecian tan claramente las degradaciones ocurridas a causa de la congestión en la red y, por tanto, el umbral de pérdidas puede situarse en valores más elevados.

En cuanto al objetivo III, es necesario tener en cuenta que los resultados están condicionados por la técnica de cancelación de error utilizada, que en este caso consiste en copiar el frame anterior. Por esta razón, ante pérdidas severas en la red, los usuarios apenas diferenciarán la secuencia afectada por las pérdidas (del sistema no adaptativo) y la secuencia que ha sido adaptada en el nivel temporal mediante una reducción del frame rate. En este caso, la adaptación no resulta tan ventajosa como en otros escenarios planteados.

En cuanto al objetivo IV, la preferencia se inclina ligeramente hacia el sistema adaptativo, aunque la mayoría de

los usuarios genera votaciones de 0 y 1 en la escala CMOS, no apreciándose claras mejorías entre un sistema y otro.

Por último, en el objetivo V, el sistema adaptativo siempre se prefiere cuando se incrementan los niveles temporales. La media de los valores CMOS obtenidos para la totalidad de la población es siempre positiva.

VI. Conclusiones

En este trabajo comparamos el comportamiento de un sistema de transmisión de vídeo adaptativo con un sistema tradicional (no adaptativo) en términos subjetivos. Se llevaron a cabo un elevado número de test, empleando la metodología SCACJ, incluyendo una población variada de 75 participantes. Para ello fue necesario desarrollar una herramienta software específica para la realización de los test subjetivos y generar un total de 45 pares de secuencias de diferentes características. El análisis de los resultados de los test subjetivos nos permiten establecer conclusiones referentes a la percepción de la calidad por parte del usuario en sistemas de transmisión streaming adaptativos, siendo éstos generalmente preferidos frente a los sistemas no adaptativos.

Cuando hay ancho de banda disponible en la red, la preferencia se inclina hacia el sistema adaptativo, de la misma forma que cuando hay pérdidas elevadas en la red el sistema adaptativo es percibido con mejor calidad con respecto a un sistema no adaptativo. Sin embargo, cuando hay poca congestión en la red, la tendencia no es tan clara, e incluso puede ser invertida. Con un ratio de pérdidas bajo, los usuarios pueden optar por la secuencia de referencia con pérdidas frente a la versión que ha sido adaptada. Además, la población parece preferir una reducción en calidad antes que la reducción en niveles temporales.

Los trabajos futuros derivados de este estudio están relacionados con la mejora de los algoritmos adaptativos empleando métricas derivadas de la calidad de la experiencia (QoE). Un análisis más exhaustivo de los datos puede arrojar conclusiones útiles para el desarrollo de nuevos algoritmos de adaptación. Por otro lado, los experimentos subjetivos se podrían reenfocar a la evaluación de la calidad de un único estímulo, de mayor duración, perteneciente a un sistema adaptativo, de manera que la evaluación de los saltos de calidad sea continua, en tiempo real y sin interrupciones.

Agradecimientos

Este trabajo está financiado por la Universidad de Oviedo y el Principado de Asturias a través del proyecto SV-PA-13-ECOEMP-75.

Referencias

[1] N. Cranley, P. Perry, y L. Murphy, «User perception of adapting video quality», *International Journal of Human-Computer Studies*, vol. 64, n.º 8, pp. 637–647, Ago. 2006.

[2] «Recommendation ITU-R BT.500-12: Methodology for the subjective assessment of the quality of television pictures», International Telecommunication Union, vol. 12, 2009.

[3] «Subjective Video Quality Assessment Methods for Multimedia Applications», ITU-T, Rec. P.910, 2008.

[4] J. Rückert, O. Abboud, T. Zinner, R. Steinmetz, y D. Hausheer, «Quality Adaptation in P2P Video Streaming Based on Objective QoE Metrics», en *NETWORKING 2012*, vol. 7290, pp. 1-14.

[5] J.-S. Lee, F. De Simone, T. Ebrahimi, N. Ramzan, y E. Izquierdo, «Quality assessment of multidimensional video scalability», *IEEE Communications Magazine*, vol. 50, n.º 4, pp. 38 -46, Abr. 2012.

[6] J.-S. Lee, F. De Simone, N. Ramzan, Z. Zhao, E. Kurutepe, T. Sikora, J. Ostermann, E. Izquierdo, y T. Ebrahimi, «Subjective evaluation of scalable video coding for content distribution», en *Proceedings of the international conference on Multimedia*, New York, NY, USA, 2010, pp. 65–72.

[7] T. Oelbaum, H. Schwarz, M. Wien, y T. Wiegand, «Subjective performance evaluation of the SVC extension of H.264/AVC», en *15th IEEE International Conference on Image Processing, 2008*, pp. 2772 - 2775.

[8] F. Niedermeier, M. Niedermeier, y H. Kosch, «Quality Assessment of the MPEG-4 Scalable Video CODEC», en *Image Analysis and Processing – ICIAP 2009*, vol. 5716, pp. 297-306.

[9] Y. Pitrey, M. Barkowsky, P. Le Callet, y R. Pepion, «Subjective quality assessment of MPEG-4 Scalable Video Coding in a mobile scenario», en *2010 2nd European Workshop on Visual Information Processing (EUVIP)*, 2010, pp. 86 -91.

[10] A. Eichhorn y P. Ni, «Pick your layers wisely - a quality assessment of H.264 scalable video coding for mobile devices», en *Proceedings of the 2009 IEEE international conference on Communications*, Piscataway, NJ, USA, 2009, pp. 5446–5451.

[11] J.-S. Lee, F. De Simone, y T. Ebrahimi, «Subjective Quality Evaluation via Paired Comparison: Application to Scalable Video Coding», *IEEE Transactions on Multimedia*, vol. 13, n.º 5, pp. 882 -893, Oct. 2011.

[12] N. Staelens, S. Moens, W. Van den Broeck, I. Mariën, B. Vermeulen, P. Lambert, R. Van de Walle, y P. Demeester, «Assessing Quality of Experience of IPTV and Video on Demand Services in Real-Life Environments», *IEEE Transactions on Broadcast*, vol. 56, n.º 4, pp. 458 -466, Dic. 2010.

[13] Y. Pitrey, U. Engelke, M. Barkowsky, R. Pepion, y P. Le Callet, «Subjective quality of SVC-coded videos with different error-patterns concealed using spatial scalability», en *2011 3rd European Workshop on Visual Information Processing (EUVIP)*, 2011, pp. 180 -185.

[14] R. K. P. Mok, X. Luo, E. W. W. Chan, y R. K. C. Chang, «QDASH: a QoE-aware DASH system», en *Proceedings of the 3rd Multimedia Systems Conference*, New York, NY, USA, 2012, pp. 11–22.

[15] J. Lloret, A. Canovas, J. Tomas, y M. Atenas, «A network management algorithm and protocol for improving QoE in mobile IPTV», *Computer Communications*, vol. 35, n.º 15, pp. 1855-1870, Sep. 2012.

[16] S. Ishihara, *Tests for colour-blindness: 38 Plate Edition*. Tolyo, Japan: Kanehara Suppan Co. Ltd., 1968.

[17] L. Pozueco, X. G. Pañeda, R. García, D. Melendi, y S. Cabrero, «Adaptable system based on Scalable Video Coding for high-quality video service», *Computers & Electrical Engineering*, vol. 39, nº 3, pp. 775-789, Abr. 2013.

[18] A. Detti, G. Bianchi, C. Pisa, F. S. Proto, P. Loreti, W. Kellerer, S. Thakolsri, y J. Widmer, «SVEF: an open-source experimental evaluation framework for H.264 scalable video streaming», en *IEEE Symposium on Computers and Communications, 2009*, pp. 36-41.

[19] S. Salsano, F. Ludovici, y A. Ordine, «Definition of a general and intuitive loss model for packet networks and its implementation in the Netem module in the Linux kernel», Technical report.-University of Rome «Tor Vergata», 2009.

Tabla V
RESUMEN DE LOS PARÁMETROS DE LOS VÍDEOS

FACTORY		TRACTOR		MARATHON		TOUCHDOWN	
T0Q3	1.875fps, 1183.3 kbps	T0Q3	1.5625 fps, 1504 kbps	T1Q3	6.25 fps, 4043 kbps	T2Q3	7.5 fps, 3215 kbps
T1Q3	3.75 fps, 1821 kbps	T1Q3	3.125 fps, 2102 kbps	T2Q3	12.5 fps, 5688 kbps	T3Q3	15 fps, 4188 kbps
T2Q3	7.5 fps, 2673 kbps	T2Q3	6.25 fps, 2721 kbps	T3Q3	25 fps, 7474 kbps	T4Q1	30 fps, 1287.5 kbps
T3Q3	15 fps, 3679 kbps	T3Q3	12.5 fps, 3458 kbps	T4Q0	50 fps, 820 kbps	T4Q2	30 fps, 2787 kbps
T4Q0	30 fps, 712 kbps	T4Q0	25 fps, 517.4 kbps	T4Q2	50 fps, 4609 kbps	T4Q3	30 fps, 5212 kbps
T4Q1	30 fps, 1299.3 kbps	T4Q2	25 fps, 2348 kbps	T4Q3	50 fps, 8735 kbps		
T4Q2	30 fps, 2708 kbps	T4Q3	25 fps, 4341 kbps				
T4Q3	30 fps, 4716 kbps						

Tabla VI
RESUMEN DE LOS PARES

Par	Objetivo	Contenido	Secuencia de referencia	Secuencia adaptada	Par	Objetivo	Contenido	Secuencia de referencia	Secuencia adaptada
1	I	*Tractor*	T4Q3, 40%PLR	T4Q3->T4Q2	24	III	*Tractor*	T4Q3, 30%PLR	T4Q3->T2Q3
2, 25	I,III	*Tractor*	T4Q3, 40%PLR	T4Q3->T1Q3	27	III	*Factory*	T4Q3, 70%PLR	T4Q3->T0Q3
3	I	*Factory*	T4Q3, 40%PLR	T4Q3->T4Q2	28	III	*Tractor*	T4Q3, 60%PLR	T4Q3->T0Q3
4, 23	I,III	*Factory*	T4Q3, 40%PLR	T4Q3->T2Q3	29	IV	*Touchdown*	T4Q1	T4Q1->T4Q2
5	I	*Marathon*	T4Q3, 40%PLR	T4Q3->T4Q2	30	IV	*Factory*	T4Q1	T4Q1->T4Q2
6, 26	I,III	*Marathon*	T4Q3, 40%PLR	T4Q3->T1Q3	31	IV	*Marathon*	T4Q0	T4Q0->T4Q2
7	II	*Tractor*	T4Q3, 1%PLR	T4Q3->T3Q3	32	IV	*Tractor*	T4Q0	T4Q0->T4Q2
8	II	*Marathon*	T4Q3, 1%PLR	T4Q3->T3Q3	33	IV	*Factory*	T4Q1	T4Q1->T4Q3
9	II	*Touchdown*	T4Q3, 3%PLR	T4Q3->T3Q3	34	IV	*Touchdown*	T4Q1	T4Q1->T4Q3
10	II	*Marathon*	T4Q3, 3%PLR	T4Q3->T3Q3	35	IV	*Factory*	T4Q0	T4Q0->T4Q3
11	II	*Touchdown*	T4Q3, 5%PLR	T4Q3->T3Q3	36	IV	*Tractor*	T4Q0	T4Q0->T4Q3
12	II	*Tractor*	T4Q3, 5%PLR	T4Q3->T3Q3	37	V	*Tractor*	T1Q3	T1Q3->T2Q3
13	II	*Tractor*	T4Q3, 10%PLR	T4Q3->T3Q3	38	V	*Marathon*	T1Q3	T1Q3->T2Q3
14	II	*Factory*	T4Q3, 10%PLR	T4Q3->T3Q3	39	V	*Touchdown*	T2Q3	T2Q3->T3Q3
15	II	*Touchdown*	T3Q3, 1%PLR	T3Q3->T2Q3	40	V	*Factory*	T2Q3	T2Q3->T3Q3
16	II	*Factory*	T3Q3, 1%PLR	T3Q3->T2Q3	41	V	*Marathon*	T3Q3	T3Q3->T4Q3
17	II	*Tractor*	T3Q3, 3%PLR	T3Q3->T2Q3	42	V	*Touchdown*	T3Q3	T3Q3->T4Q3
18	II	*Factory*	T3Q3, 3%PLR	T3Q3->T2Q3	43	V	*Marathon*	T1Q3	T1Q3->T3Q3
19	II	*Touchdown*	T3Q3, 5%PLR	T3Q3->T2Q3	44	V	*Tractor*	T1Q3	T1Q3->T3Q3
20	II	*Factory*	T3Q3, 5%PLR	T3Q3->T2Q3	45	V	*Tractor*	T2Q3	T2Q3->T4Q3
21	II	*Tractor*	T3Q3, 10%PLR	T3Q3->T2Q3	46	V	*Touchdown*	T2Q3	T2Q3->T4Q3
22	II	*Factory*	T3Q3, 10%PLR	T3Q3->T2Q3	47	V	*Factory*	T1Q3	T1Q3->T4Q3
					48	V	*Marathon*	T1Q3	T1Q3->T4Q3

Análisis del comportamiento de los clientes finales en una arquitectura interdominio de provisión de QoS extremo a extremo

Fernando Fernández-Valdés Pedrosa, Manuel Fernández Veiga, Jose Carlos López Ardao, Cándido López García.
Departamento de Enxeñería Telemática,
Universidad de Vigo
36310 Vigo, España
fernando@det.uvigo.es, mveiga@det.uvigo.es, jardao@det.uvigo.es, candido@det.uvigo.es

***Abstract*—Consideramos el problema de la provisión de calidad de servicio (QoS) extremo a extremo en redes interdominio, como Internet. Actualmente, existen propuestas que afrontan esta problemática desde distintas perspectivas, y aquí destacamos como en topologías jerárquicas es posible alcanzar una diferenciación proporcional extremo a extremo mediante una arquitectura que combine un mecanismo de diferenciación en cuanto a pérdidas en los ISPs (Internet Service Providers) de acceso y un mecanismo que garantice un ancho de banda a agregados de flujos en los niveles superiores. En este contexto multidominio y empleando esta arquitectura, afrontamos el estudio de cómo se comportan los clientes finales para incrementar el beneficio total de la sociedad. Ante la existencia de distintas clases de servicio por las que enviar tráfico, los usuarios determinarán qué cantidad de tráfico enviar por cada una de ellas para maximizar su utilidad; para ello se tendrá en consideración los distintos precios de las clases y la capacidad máxima disponible para el agregado de todos los flujos de los clientes. Los resultados obtenidos a partir de este análisis nos permitirán determinar el interés real que pueda tener una población de clientes en la implantación de una arquitectura como la propuesta; así bien, también nos permitirán observar alteraciones sobre el funcionamiento esperado, lo que nos proporcionará un punto de partida para mejorar dicha arquitectura con el fin de implementar un sistema eficiente de calidad de servicio extremo a extremo en entornos interdominio.**

***Index Terms*—interdominio, QoS, diferenciación proporcional**

I. INTRODUCCIÓN

La provisión de calidad de servicio extremo a extremo en una red es un problema ampliamente estudiado en la literatura, donde se proponen diversos sistemas de diferenciación de servicio: absoluta (IntServ), relativa (DiffServ) y proporcional [1] (solución de compromiso entre las dos anteriores); y múltiples implementaciones para proveer dicha diferenciación. Estas soluciones generalmente son aplicables a redes bajo un mismo dominio administrativo (AS). Sin embargo, extender estas soluciones de provisión de QoS extremo a extremo a tráfico que atraviesa múltiples ASs, como sucede en Internet, es un problema que actualmente permanece sin resolver de una manera eficiente.

Existen trabajos que afrontan esta problemática desde diversas perspectivas. Algunas propuestas asumen una cooperación entre ISPs [2], [3] donde los Sistemas Autónomos (ASs) intercambian información interna de sus redes. La mayor parte de este tipo de soluciones se basan en la creación de alianzas de ISPs que comparten información. Sin embargo, estas suposiciones no parecen realistas desde el punto de vista de que cada ISP tiene sus propios intereses y no suelen estar interesados en revelar información interna. En contraste a estas soluciones cooperativas, existen soluciones no cooperativas [4], [5], [6] que tratan de representar el comportamiento egoísta de los ISPs, quienes pretenden maximizar sus beneficios. Estas soluciones suelen basarse en la negociación de parámetros para proveer una diferenciación absoluta extremo a extremo mediante la reserva de recursos, lo que conlleva una mayor complejidad y una cooperación entre todos los ISPs en la ruta

Para evitar la complejidad y las suposiciones de las propuestas anteriores, vamos a centrar nuestro estudio en una arquitectura [7] que permite alcanzar una diferenciación proporcional extremo a extremo en topologías jerárquicas; por simplicidad, una topología de dos niveles. Un nivel de acceso (o ISPs externos) que implementa un mecanismo de diferenciación proporcional en cuanto a pérdidas, y que provee clases de servicio proporcionales a los usuarios finales (las fuentes de tráfico). Y el nivel superior de la jerarquía, que está constituido por un único ISP central que provee conectividad a los ISPs externos y que garantiza un ancho de banda a agregados de flujos. Entendiendo como agregado al conjunto de flujos que comparten determinadas características y que reciben un trato común. Esta arquitectura permite proveer calidad de servicio extremo a extremo, implementando dos mecanismos de QoS distintos en cada uno de los ISPs, lo que representa la independencia entre ISPs.

Esta arquitectura es modelada matemáticamente en este documento contribuyendo de esta manera a la creación de un marco de trabajo para analizar y estudiar desde distintas perspectivas el sistema de provisión de calidad de servicio extremo a extremo propuesto. El modelo matemático al que se llega nos permite plantear diversos problemas para analizar tanto el comportamiento de los clientes finales, como el comportamiento de los ISPs externos y también el del ISP central.

Aunque este modelo de la arquitectura permite afrontar el estudio de problemas de muy diversa índole, como un primer paso se propone el estudio del sistema desde la perspectiva de los usuarios finales. Así, mediante un problema de optimización en el que un ISP externo ofrece distintas clases de servicio, proporcionales en cuanto a pérdidas, a los usuarios

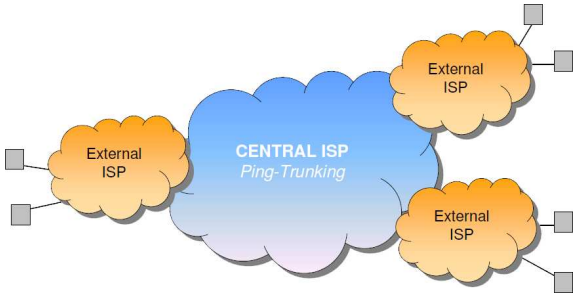


Fig. 1. Arquitectura del sistema.

finales; éstos decidirán en base a su utilidad cuánto tráfico enviar por cada una de las clases disponibles, asumiendo un mayor coste por aquellas clases con menor probabilidad de pérdidas. Los resultados obtenidos a partir de este estudio permiten analizar el interés real y el comportamiento de los clientes finales al usar esta arquitectura, permitiéndonos observar la viabilidad de este modelo de cara a ser implantado en entornos reales como Internet.

El resto del documento queda estructurado de la siguiente manera. En la sección 2, profundizamos en la arquitectura del sistema de provisión de calidad de servicio extremo a extremo, presentando brevemente los mecanismos de QoS que utiliza. En la sección 3, describimos matemáticamente el modelo de la red. A continuación, en la sección 4, se presente el problema concreto que se va a estudiar, detallando el análisis de este problema en la sección 5. Las propiedades para la resolución del problema se presentan en la sección 6. Finalmente, la sección 7 recoge las conclusiones del documento y las líneas de trabajo futuro.

II. ARQUITECTURA DEL SISTEMA

Las contribuciones de este documento están apoyadas sobre una arquitectura concreta [7], con las propiedades que se describen a continuación, y que es capaz de proveer calidad de servicio extremo a extremo a través de redes interdominio. Vamos a considerar una topología de red jerárquica de dos niveles compuesta por un ISP central que provee tránsito a los demás ISPs, y donde los ISPs del nivel inferior proveen servicio a los usuario finales como la que se muestra en la Fig. 1. Esta topología simplificada es justificable en base a estudios como el de la Cooperative Association for Internet Data Analysis (CAIDA) [8]. Este estudio determina que la distancia media, en número de ASs, en una topología interdominio es menor que 4, y que el 62% de rutas entre ASs sólo tiene 3 saltos.

Además, sólo se contempla una mínima cooperación y comunicación entre ISPs adyacentes. Esta restricción representa la existencia de acuerdos bilaterales en Internet [9]. Por último, para reflejar la independencia entre sistemas autónomos se propone el uso de dos mecanismos diferentes de QoS: Ping-Trunking en el ISP central y un mecanismo de diferenciación proporcional en cuanto a pérdidas basado en un marcado probabilístico de los paquetes en el nivel inferior de ISPs.

A. Mecanismos de QoS

Esta sección hace una breve introducción a la organización general de nuestro sistema, al igual que a los mecanismos específicos de QoS empleados en la arquitectura que posteriormente se modela.

1) Ping-Trunking [10]: es un esquema de control para tráfico IP que surge como una mejora a *TCP Trunking* [11]. Ping-Trunking permite ajustar la tasa de transmisión de cada agregado en base a una conexión de control, consiguiendo de esta manera aplicar distintos algoritmos de control de congestión a los agregados. En nuestra arquitectura, se implementa Ping-Trunking en el ISP central con Vegas como algoritmo de control. Este esquema proporciona la capacidad de repartir el ancho de banda entre los agregados de una manera no equitativa; más concretamente en función de los parámetros podremos establecer una diferenciación proporcional en throughput. De forma que el ISP central pueda ofrecer clases proporcionales para los agregados de tráfico de los distintos ISPs externos.

2) Proportional loss differentiation [12]: se usa en los ISPs de acceso. La clave de este mecanismo es una estrategia de marcado probabilístico de paquetes fundamentada en dos suposiciones: la existencia de dos clases internas de paquetes bien diferenciadas en cuanto a su probabilidad de pérdidas (*Premium* y *Best-effort*) y la existencia de un algoritmo de clasificación de paquetes en los nodos de ingreso que asocie los paquetes de las clases externas (proporcionales) con paquetes de las clases internas. No es difícil demostrar como bajo estas suposiciones es posible alcanzar una diferenciación proporcional en cuanto a la probabilidad de pérdida de paquetes. Esta propiedad permite a los ISPs externos que implementan el mecanismo ofertar distintas clases de servicio proporcionales en pérdidas a los clientes finales.

En [7], se demuestra como una correcta combinación de estos dos mecanismos de QoS asociados a través de contratos de servicio y una mínima cooperación entre los ISPs que los implementan permiten conformar una arquitectura de red capaz de proveer calidad de servicio extremo a extremo en un entorno interdominio.

III. MODELO DE RED

En esta sección, se modelan de forma matemática las características de la arquitectura de nuestro sistema, para crear de esta forma un marco de estudio que permita profundizar en los comportamientos reales sobre la red.

A. El ISP central

Hemos mencionado con anterioridad que nuestra red es una topología jerárquica de dos niveles en la que por simplicidad el nivel superior está conformado por un único ISP central, ISP_{PT}, que implementa Ping-Trunking y que proporciona conectividad y servicio a los ISPs externos.

El ISP_{PT} ofrece T clases de servicio proporcionales en cuanto a throughput a los ISPs externos $(1, 2, ..., k, ..., T)$, siendo la clase T la más prioritaria y la clase 1 la de referencia. Los ISPs de accesos contratarán una clase u otra en función de las necesidades de sus agregados de tráfico. En este modelo se considera un agregado, al grupo de flujos con mismo ISP origen y mismo ISP destino. De esta forma, la proporcionalidad entre clases queda definida por la constante de proporcionalidad α_k, tal que el ancho de banda garantizado del que dispone el agregado de flujos de un ISP externo que

contrata la clase k, C_k, queda determinado por:

$$C_k = \alpha_k \cdot C_1 \quad (1)$$

siendo C_1 la capacidad que reciben los agregados de la clase de referencia en ese momento dado.

Respecto a la constante de proporcionalidad, α_k, se verifica que:

$$\alpha_1 = 1 \quad (2)$$

$$\alpha_1 < \alpha_2 < ... < \alpha_k < ... < \alpha_T \quad (3)$$

De forma que la capacidad garantizada a los agregados de clase 2 es α_2 veces mayor que la capacidad garantizada a la clase 1, y así sucesivamente.

La capacidad de referencia garantizada C_1 en un determinado instante va a depender del número de ISPs cliente que contratan cada una de las distintas clases. Sea S_k el número de contratos de la clase k en un momento dado y C_{PT} la capacidad que puede repartir el ISP_{PT}, podríamos determinar C_1 como:

$$C_1 = \frac{C_{PT}}{\sum_{k=1}^{T} \alpha_k \cdot S_k} \quad (4)$$

El ISP central, establece unas tarifas para las distintas clases y capacidades que pueden contratar los ISPs externos $\vec{Q} = (q_1, q_2, ..., q_k, ..., q_T)$.

Todo esto nos permite modelar la relación y los contratos de servicio entre un ISP externo y el ISP central. De manera que el ISP_A, un ISP externo concreto, al contratar la clase de servicio $k = A$ recibirá un ancho de banda garantizado igual a C_A, por un precio q_A.

B. Los ISPs de acceso

Siguiendo el razonamiento anterior, también se modelan las relaciones contractuales existentes entre los ISPs externos y los clientes finales, quienes actúan como fuentes de tráfico. Por simplicidad en el análisis vamos a basar nuestro modelado en un único ISP, el ISP_A, lo que sin pérdida de generalidad es extensible al resto de ISPs externos.

El ISP_A ofrece M clases de servicio proporcionales en cuanto a pérdidas $(1, 2, ..., j..., M)$ a los usuarios finales. Siendo la clase M la más prioritaria y la clase 1 la de referencia. Nuevamente, la proporcionalidad entre clases queda definida por la constante de proporcionalidad β_j, tal que la probabilidad de pérdidas de la clase j, L_j, queda determinada por:

$$L_j = \beta_j \cdot L_1 \quad (5)$$

siendo L_1 la probabilidad de pérdidas de la clase 1.

Respecto a la constante de proporcionalidad, β_j se verifica que:

$$\beta_1 = 1 \quad (6)$$

$$\beta_1 > \beta_2 > ... > \beta_j > ... > \beta_M > 0 \quad (7)$$

De forma que la probabilidad de pérdida de paquetes de la clase 1 es la más elevada. Recordamos que esto era posible gracias a que internamente el ISP_A diferencia notablemente dos clases de paquetes (*Premium* y *Best-effort*) y emplea una política de descarte prioritario en los routers internos en base a estas dos clases.

Al igual que el ISP_{PT} establece un vector de precios para las clases de agregados que pueden contratar los ISPs externos, el ISP_A también establece unas tarifas fijas para las distintas clases proporcionales en cuanto a pérdidas, que los clientes tendrán que pagar para transmitir tráfico por cada clase, $\vec{P} = (p_1, p_2, ..., p_j, ..., p_M)$.

C. Los clientes finales

En base a lo expuesto respecto a los ISP de acceso podemos concluir que un cliente final que quiera transmitir tráfico a través de nuestra arquitectura de provisión de calidad de servicio interdominio, enviará tráfico por las distintas clases ofrecidas por el ISP_A y pagará por ello en función de sus necesidades en cuanto a la probabilidad de pérdida de paquetes.

Nuevamente, y sin pérdida de generalidad, vamos a modelar a los clientes finales de un único ISP, seguiremos contemplando el ISP_A; aunque el modelo es igualmente aplicable a cualquiera de los demás ISPs externos.

Nuestro modelo de red considera la existencia de una población fija de clientes para cada ISP, de forma que el ISP_A tendrá una población de clientes de tamaño N: $1, 2, ..., i, ..., N$; realmente sería N_A puesto que cada ISP tendrá una cantidad de potenciales clientes distinta (por simplicidad en la notación usamos N). Veremos como esta suposición de población fija no acarrea ningún problema en los estudios sobre el modelo propuesto, ya que se contempla la posibilidad de que existan clientes que no transmitan tráfico a la red. E igualmente podemos considerar N arbitrariamente grande, representando que un ISP podría dar acceso y proveer servicio a un grupo grande de potenciales clientes.

Cada uno de los usuarios i tiene una función de utilidad distinta, que representa su grado de satisfacción respecto al servicio recibido. De forma que $U_i(x_i)$ representa la utilidad de cliente i; que es función del tráfico cursado del cliente, x_i. Esta función pretende modelar que un cliente estará más o menos satisfecho en base al tráfico propio que logre ser cursado por la red.

La forma de la función de utilidad no va a quedar especificada en nuestro modelo, sino que se pretende que para el análisis de los problemas baste con tomar alguna suposición sobre esta función. Generalmente asumiremos que las funciones de utilidad de los clientes son continuas, cóncavas y no decrecientes. Estas propiedades veremos que resultan útiles al plantear y solucionar problemas sobre este modelo de red. Sin embargo, parece razonable asumir estas características en una función de utilidad:

- La utilidad de los clientes podemos entenderla como una función creciente en base a que a mayor cantidad de tráfico cursado, mayor será el grado de satisfacción del usuario.
- Además, aunque sea creciente es razonable que el aumento marginal del grado de satisfacción de un cliente sea menor cuanto mayor tráfico curse, es decir, el aumento de la satisfacción al aumentar el tráfico cursado por un usuario 1Mbps es menor si pasa de 100Mbps a 101Mbps que si el incremento es de 1Mbps a 2 Mbps. Esto implica que la segunda derivada de la función de utilidad es negativa y por consiguiente es una función cóncava.

En nuestro modelo, frente a x_i que representa el tráfico cursado del cliente i, y_i representa el tráfico ofrecido del mismo cliente.

Un cliente puede transmitir su tráfico por distintas clases de las que oferta en este caso el ISP_A, de forma que x_{ij} (y_{ij}) es el tráfico cursado (ofrecido) por el cliente i a través de la clase j.

$$x_i = \sum_{j=1}^{M} x_{ij} \quad ; \quad y_i = \sum_{j=1}^{M} y_{ij} \tag{8}$$

En una arquitectura como la que estamos presentando en este documento, la relación entre el tráfico ofrecido y el tráfico cursado queda determinada mediante la probabilidad de pérdidas de cada una de las clases por las que se cursa tráfico.

$$x_{ij} = y_{ij} \cdot (1 - L_j) \tag{9}$$

Teniendo en cuenta que al implementar Ping-Trunking con Vegas como algoritmo de control [10] se logra que la probabilidad de pérdidas en el ISP_{PT} sea despreciable y próxima a cero. Se puede afirmar que la probabilidad de pérdidas de la clase j es prácticamente proporcional, en base a las clases definidas por el ISP_A. De forma que la Ec. 9 podría escribirse en base a la función de pérdidas de la clase de referencia, L_1 y la constante de proporcionalidad β_j.

$$x_{ij} = y_{ij} \cdot (1 - \beta_j \cdot L_1) \tag{10}$$

La probabilidad de pérdida de la clase de referencia, es una función, $L(y)$ que va a depender de la carga total del ISP_A, y, puesto que sobre la probabilidad de pérdida de paquetes de la clase 1, al ser la menos prioritaria, va a influir todo el tráfico cursado por todos los clientes, por todas las clases.

$$x_{ij} = y_{ij} \cdot (1 - \beta_j \cdot L(\sum_i \sum_j y_{ij})) \tag{11}$$

Al igual que procedíamos con la función de utilidad, no vamos a concretar la forma de la función de pérdidas en la red del ISP_A. Sin embargo, bajo el estudio de los distintos problemas podremos tomar distintas consideraciones respecto a esta función. Más allá de las características generales de cualquier función de probabilidad de pérdida de paquetes, que determinan que $L(y)$ es creciente y con valores comprendidos entre 0 y 1.

IV. DESCRIPCIÓN DEL PROBLEMA

El modelo de red descrito anteriormente nos permite adquirir un marco de trabajo sobre el que poder definir muy diversos problemas para analizar distintos comportamientos sobre la arquitectura interdominio de provisión de QoS extremo a extremo propuesta en [7]. Pese a que en un futuro se plantea formular problemas desde el punto de vista del ISP central y desde los ISP de acceso; como trabajo preliminar se propone analizar el comportamiento de los clientes finales en este sistema.

Por tanto, el primer problema que se expone en este documento y con el que queremos estudiar el comportamiento de la arquitectura de Ping-Trunking y Diferenciación proporcional en cuanto a pérdidas, recoge la problemática desde el punto de vista del beneficio global de todos los usuarios finales (clientes del ISP externo). Y para ello vamos a crear una simplificación sobre el modelo de red descrito anteriormente.

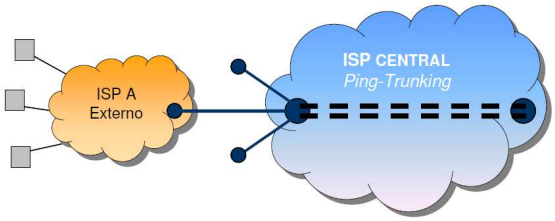


Fig. 2. Arquitectura del problema de análisis del comportamiento de los clientes finales.

En nuestro problema vamos a centrarnos en un único ISP externo, el ISP_A, esto significa que no tenemos que hacer un análisis pormenorizado de los demás ISPs de acceso, sólo teniendo que preocuparnos por modelar y contemplar aquellas características de los ISPs que afecten al comportamiento del ISP_A. En nuestra arquitectura, y bajo la suposición de que los ISPs no compiten por los clientes finales, la única interacción existente reside en que los ISPs externos conectados al mismo nodo de ingreso que el ISP_A y que transmiten hacia el mismo destino, van a limitar el ancho de banda del agregado de A. Por ello, el modelo simplificado que definimos para este problema considera esto sólo como carga en la red de Ping-Trunking. Es decir, vamos a estudiar la arquitectura cuando al ISP_A tiene un ancho de banda limitado, fijo y garantizado, C_A (Fig. 2).

Nuestro objetivo en este problema es estudiar cómo tienen que actuar los clientes para maximizar el beneficio total de la sociedad formada por todos los usuarios finales. El beneficio de un cliente en el modelo de este problema, Fig. 2, queda determinado por el grado de satisfacción de cada cliente (utilidad) $U_i(x_i)$, y por el coste que pagan los clientes al ofrecer tráfico por cada una de las clases existentes en el ISP_A. Un cliente final tiene pagarle al ISP de acceso por la cantidad tráfico que introduce en la red, es decir, el tráfico ofrecido por cada una de las clases (y_{ij}). De esta forma, el beneficio social del cliente i se puede expresar mediante la Ec. 12.

$$U_i(x_i) - \sum_j^M (p_j \cdot y_{ij}) \tag{12}$$

Ante este escenario nos interesaría llegar a obtener los valores de tráfico ofrecido de cada usuario que permiten maximizar el beneficio total de la sociedad, entendiendo este como la suma de los beneficios sociales de todos los clientes del ISP_A. Para ello, concretamos este problema como un problema de optimización en el que pretendemos maximizar la función objetivo (Ec. 13).

$$maximizar \quad \sum_i^N [U_i(x_i) - \sum_j^M (p_j \cdot y_{ij})] \tag{13}$$

Este problema de maximización está sujeto a las condiciones expuestas en las Ec. 14-17.

$$x_{ij} = y_{ij} \cdot (1 - \beta_j \cdot L(\sum_i \sum_j y_{ij})) \quad (14)$$

$$x_i = \sum_j x_{ij} \quad (15)$$

$$y_i = \sum_j y_{ij} \quad (16)$$

$$\sum_i x_i \leq C_A \quad (17)$$

Muchas condiciones se obtienen directamente del modelo de red propuesto en la sección anterior; bastaría hacer una mención extra a la Ec. 17, que simplemente establece una restricción sobre el tráfico total cursado, indicando que tiene que ser menor o igual que la capacidad total disponible por el ISP_A.

V. ANÁLISIS DEL PROBLEMA

El problema de optimización que queremos resolver expuesto en las Ec. 13-17, pretende alcanzar unos valores para los y_{ij} de forma que se obtengan los valores óptimos de tráfico ofrecido de cada usuario por cada una de las clases proporcionales en cuanto a pérdidas. Para ello resulta interesante reescribir la función objetivo en función del tráfico ofrecido.

$$max \sum_i^N [U_i(\sum_j^M y_{ij} \cdot [1 - \beta_j \cdot L(\sum_i \sum_j y_{ij})]) - \sum_j^M (p_j \cdot y_{ij})] \quad (18)$$

E igualmente reescribiríamos las condiciones del problema, que quedarían simplificadas en una sola.

$$\sum_i^N \sum_j^M y_{ij} \cdot [1 - \beta_j \cdot L(\sum_i \sum_j y_{ij})] \leq C_A \quad (19)$$

Para resolver este problema de optimización, nos interesaría llegar a un sistema de optimización convexa (en nuestro caso cóncava por ser un problema de maximización). La principal ventaja de los problemas de optimización convexa es que un óptimo local es un óptimo global, lo que permite que existan métodos eficientes para encontrar la solución al problema.

Para que nuestro problema sea de optimización cóncava, la función objetivo y la restricción (por ser una desigualdad) tienen que ser cóncavas. Y procedemos a estudiar qué condiciones tienen que cumplir nuestras funciones de utilidad (U_i) y nuestra función de pérdidas (L) para que nuestro problema sea de este tipo.

Por simplicidad en la notación, suponemos en todo el desarrollo $y = \sum_i^N \sum_j^M y_{ij}$.

Inicialmente, vamos a analizar la función de pérdidas; ya se comentó que una función de pérdidas es creciente en función de la carga de la red y que está acotada entre 0 y 1. Además, típicamente las funciones de pérdidas son inicialmente convexas (la carga de la red y las pérdidas son bajas), pero tienen un punto de inflexión donde pasan a ser cóncavas tendiendo a una probabilidad de pérdidas igual a 1. Ante esta situación, para nuestro análisis vamos a suponer que la carga total ofrecida al sistema es lo suficientemente baja como para que las pérdidas sean bajas y podamos suponer $L(y)$ convexa.

Partiendo de la hipótesis de que $L(y)$ es convexa en el rango de funcionamiento, se estudiará la convexidad del problema aplicando propiedades de las funciones convexas (cóncavas):

- La combinación lineal de funciones convexas (cóncavas) con factores positivos es otra función convexa (cóncava).
- Si una función f es convexa, entonces la función $-f$ es cóncava.
- $f(x)$ es cóncava $\Leftrightarrow f''(x) \leq 0$

En base a estas características es fácilmente demostrable que la función $m(y_{ij})$ de la Ec. 20 es cóncava.

$$m(y_{ij}) = \sum_j^M y_{ij} \cdot [1 - \beta_j \cdot L(y)] \quad (20)$$

Otra propiedad de convexidad que resulta muy interesante para nuestro análisis hace referencia a la composición de funciones. Sea $n(y_{ij}) = U(m(y_{ij}))$. Para que $n(y_{ij})$ sea cóncava es suficiente que se cumplan las siguientes condiciones:

1) $m(y_{ij})$ es cóncava
2) $U(x)$ es cóncava y no decreciente

La primera condición ya se comprobó que es cierta. Así que basta con definir las funciones de utilidad $U_i(x_i)$ como funciones cóncavas y no decrecientes para alcanzar la concavidad de $n(y_{ij})$ y también la de la función objetivo del problema de optimización.

Por tanto, tomando las suposiciones de $L(y)$ convexa y las $U_i(x_i)$ cóncavas y no decrecientes, es suficiente para demostrar que la función objetivo y la restricción del problema de optimización son cóncavas y por tanto el problema es de optimización convexa.

VI. RESOLUCIÓN DEL PROBLEMA

Para resolver el problema de optimización que se ha propuesto y se ha estudiado, se utilizan las condiciones de Karush-Kuhn-Tucker (KKT). Estas condiciones son necesarias para que una solución sea óptima. Y aunque estas condiciones suelen ser necesarias pero no suficientes, en el caso de que el problema sea convexo, entonces las condiciones KKT son también suficientes. De forma que cualquier punto que cumpla las condiciones KKT será óptimo.

Esta es la razón del interés anterior en definir las funciones $L(y)$ y $U_i(x_i)$ de forma que permitiesen alcanzar un problema de optimización cóncavo. Además, para poder aplicar las condiciones de KKT necesitamos que la función objetivo y la restricción sean diferenciables, y para ello basta con asumir que $L(y)$ y $U_i(x_i)$ son diferenciables.

Previamente a utilizar las condiciones de KKT tenemos que verificar que el problema de optimización cóncavo que proponemos tiene solución, y para ello empleamos la condición de Slater que impone que las restricciones de desigualdad tienen que ser desigualdades estrictas. Comprobamos que la Ec. 21 no se cumple para la igualdad.

$$0 < C_A - \sum_i^N \sum_j^M y_{ij} \cdot [1 - \beta_j \cdot L(\sum_i \sum_j y_{ij})] \quad (21)$$

Suponiendo que se cumpliese la igualdad llegaríamos a:

$$L(y) = \frac{y - C_A}{\sum_{i=1}^{N}\sum_{j=1}^{M} y_{ij} \cdot \beta_j} \quad (22)$$

Sin embargo, en base a que ya habíamos indicado que las derivadas parciales de la función de pérdidas son iguales se llega, desarrollando, a que se tiene que cumplir $y = C_A$ y por tanto, $L(y) = 0$. Para que esto se pueda cumplir y debido a que la función de pérdidas es monótonamente creciente, se tendría que cumplir $y = y_{ij} = 0 \neq C_A$, lo que es imposible. Quedando demostrado que la restricción del problema es una desigualdad estricta.

Una vez desarrolladas, las condiciones KKT quedarían:

$$\sum_{i}^{N}\sum_{j}^{M} y_{ij} \cdot [1 - \beta_j \cdot L(\sum_{i}\sum_{j} y_{ij})] \leq C_A \quad (23)$$

$$\lambda \geq 0 \quad (24)$$

$$C_A - \sum_{i}^{N}\sum_{j}^{M} y_{ij} \cdot [1 - \beta_j \cdot L(\sum_{i}\sum_{j} y_{ij})] = 0 \quad (25)$$

$$\begin{aligned} 0 = \tfrac{\partial R}{\partial y_{ab}} = \textstyle\sum_i \{U_i'(\sum_j^M y_{ij} \cdot [1 - \beta_j L(y)]) \cdot \\ \cdot [-\textstyle\sum_j \beta_j \cdot y_{ij} \cdot L'(y)]\} + \\ + U_a'(\textstyle\sum_j y_{aj} \cdot [1 - \beta_j L(y)]) \cdot [1 - \beta_b L(y)] - p_b + \\ + \lambda \cdot L'(y) \cdot \textstyle\sum_i \sum_j y_{ij} \cdot \beta_j - \lambda + \lambda \cdot \beta_b \cdot L(y) \end{aligned} \quad (26)$$

donde R es la función de Langrange del problema de optimización. Y donde $L'(y)$ es la derivada parcial de $L(y)$ respecto a cualquiera de los tráficos ofrecidos y_{ij}. $L'(y) = \partial L(y)/\partial y_{ij}$.

Llegado a esta situación bastaría resolver este sistema de ecuaciones formado por todas las derivadas parciales representadas en la Ec. 26 y por la Ec. 25. Y comprobar si el resultado hallado verifica las condiciones de las Ec. 23 y 24. En caso de alcanzar una solución válida esta es una solución óptima al problema.

Hay que considerar dos aspectos a la hora de plantearse resolver el problema propuesto, por una parte hay que tener en cuenta que si la pretensión fuese obtener soluciones concretas, tendríamos que definir una función de utilidad ($U(x)$) y una función de pérdidas ($L(y)$) concretas; ya que en este documento sólo se profundizó en las propiedades que tenían que cumplir para alcanzar una solución óptima. Por otra parte, no podemos olvidar que en el planteamiento del problema se tomaron determinadas suposiciones que hay que verificar. Así, hay que comprobar que el resultado de problema de optimización se ajusta al régimen de funcionamiento en el que la probabilidad de pérdidas es baja y donde la función $L(y)$ se podía aproximar por una función convexa.

Este documento, una vez presentado el mecanismo de resolución del problema, no tiene como fin último alcanzar una solución concreta, sino que se pretende estudiar el comportamiento de los clientes de la forma más genérica posible. De ahí que se ha pretendido analizar, en la medida de lo posible la arquitectura de QoS extremo a extremo sin especificar funciones de utilidad concretas. Estos análisis preliminares nos han permitido concluir que las derivadas de las funciones de utilidad de los distintos clientes en el punto de equilibrio (optimización) son iguales, independientemente de la forma de la función de utilidad de los clientes.

$$U_a'(\sum_{j}^{M} y_{aj} \cdot [1 - \beta_j \cdot L(y)] = U_c'(\sum_{j}^{M} y_{cj} \cdot [1 - \beta_j \cdot L(y)] \quad (27)$$

Es decir, que aunque la utilidad percibida por los distintos clientes puede ser diferente. La utilidad marginal (la derivada de la utilidad) es la misma para todos. Ninguno de los usuarios tiene una capacidad de mejora mayor que la de otro. Con lo que se puede decir que la solución al problema se basa en un reparto justo.

VII. CONCLUSIONES

En este documento afrontamos el estudio de una arquitectura de provisión de calidad de servicio extremo a extremo en redes interdominio, como Internet. El análisis de esta arquitectura se afronta en dos pasos, en primer lugar se aporta un modelo de red como marco de referencia para el estudio del sistema desde distintos enfoques y bajo distintas hipótesis que queramos plantear. En segundo lugar, se planteó bajo este modelo de red un problema inicial concreto con el que se quiere analizar el comportamiento de los clientes finales y prever cómo actuarán para incrementar el beneficio total de la sociedad. Los resultados preliminares muestran que bajo ciertas suposiciones asumibles, de convexidad en la utilidad de los usuarios y en la función de pérdidas, es posible alcanzar un mecanismo de resolución del problema planteado. Siguiendo esta línea de trabajo parece interesante plantearse para un futuro cercano nuevos problemas sobre la misma arquitectura pero desde otros puntos de vista, como podría ser la competencia entre los ISP por el ancho de banda del ISP central, etc. Las conclusiones de este documento junto a un trabajo futuro sobre esta arquitectura de provisión de QoS extremo a extremo nos permitirán determinar el interés real de los clientes y los ISPs en la posible implantación de esta arquitectura; así bien, también permitirán detectar posibles deficiencias que sirvan como punto de partida para mejorar la arquitectura y proveer calidad de servicio extremo a extremo en entornos interdominio de una manera más eficiente.

AGRADECIMIENTOS

Este trabajo ha sido financiando por el Ministerio de Economía y Competitividad, mediante el proyecto TEC2009-12135.

REFERENCES

[1] C. Dovrolis and P. Ramanathan, "Case for relative differentiated services and the proportional differentiation model," *IEEE Network*, vol. 13, no. 5, pp. 26–34, Sep. 1999.

[2] N. Kumar and G. Saraph, "End-to-end QoS in interdomain routing," in *International Conference on Networking and Services (ICNS'06)*, Silicon Valley, CA, Jul. 16–18, 2006, p. 82.

[3] M. P. Howarth *et al.*, "End-to-end quality of service provisioning through inter-provider traffic engineering," *Computer Communications*, vol. 29, no. 6, pp. 683–702, Mar. 2006.

[4] R. Ma *et al.*, "Internet economics: the use of shapley value for ISP settlement," *IEEE/ACM Transactions on Networking*, vol. 18, no. 3, pp. 775–787, Jun. 2010.

[5] R. Ma, D. Chiu, J. Lui, V. Misra, and D. Rubenstein, "On cooperative settlement between content, transit, and eyeball internet service providers," *IEEE/ACM Transactions on Networking*, vol. 19, no. 3, pp. 802–815, Jun. 2011.

[6] K. Suksomboon, P. Pongpaibool, Y. Ji, and C. Aswakul, "PC-nash: QoS provisioning framework with path-classification scheme under nash equilibrium," *Computer Journal*, vol. 54, no. 6, pp. 931–943, Jun. 2011.
[7] F. Fernández-Valdés Pedrosa, M. Fernández Veiga, C. López García, and A. Suárez González, "Decoupling losses for end-to-end bandwidth guarantees in interdomain traffic," in *26th IEEE Intl. Conf. on Advanced Information Networking and Applications (AINA 2013)*, Barcelona (Spain), 2013.
[8] P. Mahadevan *et al.*, "Lessons from three views of the internet topology," Cooperative Associationo for Internet Data Analysis (CAIDA), Tech. Rep. CAIDA-TR-2005-02, Aug. 2005.
[9] L. Gao, "On inferring autonomous system relationships in the internet," *IEEE/ACM Transactions on Networking*, vol. 9, no. 6, pp. 733–745, Dec. 2001.
[10] S. Herrería-Alonso, M. Fernández-Veiga, M. Rodríguez-Pérez, A. Suárez-González, and C. López-García, "Edge-to-edge proactive congestion control for aggregated traffic," *Computer Communications*, vol. 29, no. 7, pp. 801–811, Apr. 2006.
[11] H. T. Kung and S. Y. Wang, "TCP trunking: design, implementation and performance," in *International Conference on Network Protocols (ICNP'99)*, Toronto, Canada, Oct./Nov. 1999, pp. 222–231.
[12] P. J. Argibay-Losada, A. Suárez-González, C. López-García, and M. Fernández-Veiga, "A new design for end-to-end proportional loss differentiation in IP networks," *Computer Networks*, vol. 54, no. 7, pp. 1389–1403, Jun. 2010.

Dimensionado dinámico de buffers para flujos de tráfico diferenciados no elásticos

Andrés Vázquez-Rodas, Luis J. de la Cruz Llopis, Mónica Aguilar Igartua y Emilio Sanvicente Gargallo.
Departamento de Ingeniería Telemática
Universitat Politècnica de Catalunya
C/ Jordi Girona 1. Módulo C3. Campus Nord UPC. Barcelona. España.
{andres.vazquez,luis.delacruz,monica.aguilar,e.sanvicente}@entel.upc.edu

***Resumen*- El dimensionado del tamaño de los buffers de almacenamiento de paquetes en los equipos de red es un aspecto fundamental debido a sus consecuencias directas sobre la calidad de servicio observada por los usuarios finales. Dicho tamaño debe ser el más pequeño posible que cumpla con unos determinados requisitos respecto a algún parámetro de prestaciones de la red (caudal, tiempo extremo a extremo, probabilidad de pérdida de paquetes, etc.). En este artículo se propone un mecanismo de dimensionado que permite mantener la probabilidad de pérdida por debajo de un umbral determinado y que se adapta dinámicamente a las variaciones de carga en la red. El mecanismo, basado en una aproximación de máxima entropía, permite además el autodimensionado de buffers por parte de cada equipo, sin necesidad de la intervención de equipos especiales, y puede utilizarse también cuando se desea diferenciar diferentes flujos de tráfico y pedir para ellos distintas prestaciones.**

***Palabras Clave*- Buffers, máxima entropía, diferenciación de tráfico.**

I. INTRODUCCIÓN

Los buffers de almacenamiento de paquetes son elementos cruciales en los distintos equipos que conforman una red de comunicaciones. Su impacto es muy importante en diferentes parámetros de prestaciones de las redes, como la utilización de los canales de transmisión, la probabilidad de pérdida de paquetes, el tiempo extremo a extremo o el caudal de la red. En muchas ocasiones, la reducción en el coste de fabricación de las memorias y un intento no siempre apropiado de reducir la probabilidad de pérdida de paquetes, ha propiciado un excesivo tamaño de buffers. Este fenómeno, conocido como *bufferbloat* [1], tiene como principal consecuencia que los usuarios experimenten excesivos retardos independientemente de su tecnología de acceso y del ancho de banda disponible [2].

Un tamaño de buffer pequeño es también extremadamente apreciado en el diseño y construcción de conmutadores de paquetes *all-optical* [3][4]. Sin embargo, si dicho tamaño se hace excesivamente pequeño, se puede provocar un crecimiento indeseado de la probabilidad de pérdidas de paquetes, así como reducir la utilización de los enlaces cuando se utilizan protocolos de transporte con control de congestión por ventana (como por ejemplo TCP) [5].

Por otra parte, la diferenciación de tráficos permite la asignación de distintos grados de servicio a diferentes flujos de tráfico, con lo que la cantidad de memoria necesaria para cada uno de ellos puede ser diferente. Como puede observarse, el correcto dimensionado de buffers no es un aspecto sencillo y es por tanto el objetivo de diversos trabajos de investigación [5][6][7].

En este artículo se plantea el dimensionado de buffers de forma dinámica en los equipos de red, de forma que se adapte a las variables condiciones de trabajo del equipo en cada momento. El objetivo es asignar en cada momento el tamaño de buffer mínimo que cumpla con unos requisitos preestablecidos en cuanto a probabilidad de pérdida de paquetes. La adaptación la deberá realizar el equipo por sí solo y evitando una innecesaria sobrecarga en el procesador central.

El resto del artículo está organizado como se expone a continuación. En la siguiente sección se presentan algunos trabajos relacionados con la temática bajo estudio. En la sección III se presenta el algoritmo que se utilizará para el dimensionado de los buffers, que como se verá está basado en la obtención de parámetros elementales de trabajo y la aplicación de una aproximación de máxima entropía. La validación del mecanismo propuesto se presenta en la sección IV mediante la exposición de resultados obtenidos por simulación. Finalmente, y como es preceptivo, en la sección V se resumen las conclusiones y se presentan las futuras líneas de investigación que se derivan de este trabajo.

II. TRABAJOS RELACIONADOS

El dimensionado del tamaño de buffers puede realizarse de dos formas principales: sólo una vez en la etapa de diseño del equipo o permitiendo una adaptación dinámica. Un ejemplo del primer tipo se presenta en [8], donde los autores modelan cada nodo como una cola M/M/1/B y utilizan la teoría de grandes desviaciones para dimensionar el tamaño del buffer. Por otra parte, diversos autores proponen mecanismos de asignación dinámica. Por ejemplo en [9], donde los autores justifican la necesidad de la asignación dinámica con objeto de garantizar un caudal elevado y un tiempo extremo a extremo razonablemente bajo en redes de área local inalámbricas. Su propuesta es una adaptación de la clásica regla del producto “ancho de banda – retardo” (*Bandwidth-Delay Product*, BDP), la cual está basada en el mecanismo de control de congestión del protocolo TCP [5]. La adaptación consiste en ir actualizando el tiempo medio de servicio de los paquetes, ya que al trabajar sobre redes inalámbricas este tiempo depende del número de retransmisiones necesarias por paquete, el cual a su vez depende del estado de carga de la red. En la misma línea, en [10] se propone un mecanismo de dimensionado con objeto de reducir los tiempos de espera en cola de flujos TCP multisalto sobre redes mesh inalámbricas, a la vez que se

mantiene una alta utilización de los canales. La idea principal es considerar un único buffer pero distribuido sobre un determinado número de equipos que contienden por el acceso dentro de un mismo dominio de colisión.

Cuando la investigación se lleva a cabo para servicios no elásticos ofrecidos estrictamente en tiempo real sobre redes IP, los flujos de tráfico UDP son los que han de ser mayoritariamente considerados. Nótese que no todos los clásicos servicios en "tiempo real" entran dentro de esta categoría. Por ejemplo, en la gran mayoría de servicios de vídeo bajo demanda actuales, las secuencias de vídeo han sido previamente codificadas y almacenadas. Este hecho, junto con un elevado ancho de banda para la transmisión y una gran cantidad de memoria disponible en los receptores, permite enviar el vídeo a una tasa mayor de la necesaria para su reproducción e ir almacenándolo en el receptor. De este modo, es posible aplicar técnicas de retransmisión frente a errores en la transmisión, con lo que se podría decir que el servicio de vídeo bajo demanda se ha convertido en un servicio de transmisión de ficheros. Actualmente, por tanto, los servicios ofrecidos estrictamente en tiempo real son aquellos en los que la información ha de ser consumida prácticamente en el instante de tiempo en que es generada, y en estos casos las retransmisiones en caso de error no tienen sentido, pues la información ya no es útil tras el retardo que la retransmisión supone, y además hay que dejar paso a las informaciones siguientes. El más claro ejemplo de este tipo de servicios son las conversaciones interactivas entre dos usuarios de la red. Como se ha dicho, en este entorno los protocolos no fiables del tipo UDP han de ser considerados. Para estos flujos UDP, uno de los aspectos más importantes a tener en cuenta, por su directa repercusión en la calidad de servicio percibida por el usuario, es la probabilidad de pérdida debida al desbordamiento de los buffers en los equipos de red.

Por otra parte, en el momento de asignar flujos de tráfico a buffers de espera, se pueden escoger entre dos posibilidades principales. La primera consiste en poner todos los tráficos en la misma cola independientemente de su naturaleza. Sin embargo, la tendencia actual es hacia la diferenciación de servicios, ofreciendo diferentes calidades a cada uno de ellos. En este caso, un módulo clasificador separa los diferentes flujos colocándolos en diferentes colas, y a continuación un módulo *scheduler* decide cuál de ellas se atiende en cada momento. En este trabajo se ha considerado esta segunda opción, de modo que los flujos UDP transportando tráfico no elástico dispondrán de sus buffers por separado.

De este modo, resumiendo, en este artículo se aporta una nueva posibilidad para el dimensionado dinámico de buffers para flujos de tráfico en tiempo real estricto, cuyos requisitos son los siguientes:

- Se ha de asignar siempre el menor tamaño posible. De esta forma se evita el efecto de *bufferbloat*, y se dispone de memoria libre para asignar a otros canales. Es decir, un equipo de red con varios canales de transmisión podrá repartir de forma más eficiente su memoria disponible en función de las condiciones variables de carga en cada uno de los canales.
- Se ha de garantizar una probabilidad de pérdida máxima, que ha de poder ser configurable. Esta probabilidad de pérdida vendrá determinada por la naturaleza de cada flujo de tráfico y por la calidad de servicio que el usuario final espera recibir.
- El algoritmo se debe poder ejecutar de forma aislada en cada dispositivo, es decir, los equipos deben poder autoconfigurar el tamaño de sus buffers sin intervenciones de otros equipos de red. De esta forma, el mecanismo que se proponga podrá ser utilizado en cualquier entorno, al no ser necesarios equipos especiales con funcionalidades de las que dependan el resto de equipos. Considérese por ejemplo el caso de redes de área extendida formadas por equipos heterogéneos de distintos fabricantes y transmitiendo por canales tanto alámbricos como inalámbricos. El requerimiento de un equipo central junto con los nuevos protocolos necesarios para el intercambio de información relacionada con el dimensionado dinámico de buffers, pondría serias dificultades prácticas a la hora de poner en marcha dichos mecanismos. Además, se debería tener en cuenta también la sobrecarga de tráfico introducida, ya que al realizarse una adaptación dinámica a las condiciones de trabajo de la red, los protocolos mencionados deberían generar regularmente nuevos mensajes.

Para conseguir estos requisitos, el mecanismo propuesto se basa en la obtención, dinámicamente, de la probabilidad de pérdida en un equipo en función de la carga y del tamaño del buffer. A partir de aquí, tomando un valor concreto para la probabilidad de pérdida deseada, se calcula el tamaño de buffer. A continuación se resume el algoritmo utilizado.

III. Aproximación para la obtención del tamaño necesario del buffer vía máxima entropía

Como se ha comentado, el mecanismo propuesto en este trabajo para el dimensionado de buffers tiene como objetivo principal asignar el tamaño de buffer mínimo que cumple con un requisito predeterminado de probabilidad de pérdida. Un estudio analítico de dicha probabilidad de pérdida en un sistema de transmisión (buffer más canal de transmisión) se puede hacer a partir de la obtención de las probabilidades de los estados en una cola G/G/1/K, pero restringiéndonos a los instantes en que efectivamente se producen llegadas de paquetes. La obtención exacta de dichas probabilidades es un problema de difícil solución y aplicabilidad, ya que presupone el conocimiento exacto de las funciones de densidad de probabilidad del tiempo entre llegadas y del tiempo de servicio. La dificultad aumenta cuando se desea trabajar dinámicamente a lo largo del tiempo, con lo que dichas funciones de probabilidad van a ir cambiando.

La propuesta que se hace en este trabajo es la de hacer que los equipos de red tomen unas medidas elementales (utilización del canal y número de unidades en el sistema, ambos únicamente en los instantes de llegada de paquetes), y a partir de ahí aplicar una hipótesis de máxima entropía para obtener las probabilidades de los estados del sistema condicionadas al hecho de que hay una llegada de un paquete. De hecho, no es necesario encontrar todas las probabilidades, ya que la única que será de interés es la probabilidad de que el sistema esté completamente ocupado cuando hay una llegada (es decir, la probabilidad de pérdida). Como es obvio, al proporcionar las probabilidades de los estados tomando como base únicamente dos parámetros medidos, estamos dando más información de la que tenemos

y por tanto se trata de una aproximación que será necesario contrastar por medio de simulaciones.

Sean ρ_a y N_a la utilización del canal y el número medio de unidades en el sistema, ambos medidos únicamente en los instantes de llegada de los paquetes, y sean a_i, $i=0,1,2,..,K$, las probabilidades de que en el sistema haya i paquetes en los instantes de llegada. Desde el pionero trabajo de C. Shannon [11] la incertidumbre de una variable aleatoria que puede tomar los valores x_1, x_2, x_3, … con probabilidades p_1, p_2, p_3, … se mide a través de su entropía, la cual viene dada por la expresión [12]:

$$\sum_{i=1}^{\infty} p_i \ln \frac{1}{p_i} \tag{1}$$

En el caso que nos ocupa, el valor de a_0 es conocido:

$$a_0 = 1 - \rho_a \tag{2}$$

y por tanto se trata de maximizar:

$$\sum_{i=1}^{K} a_i \ln \frac{1}{a_i} \tag{3}$$

pero estando sujetos a las condiciones que nos proporcionan los valores medidos:

$$\sum_{i=1}^{K} a_i = \rho_a$$
$$\sum_{i=1}^{K} i \cdot a_i = N_a \tag{4}$$

La solución del problema planteado puede encontrarse en [13], donde se obtienen las probabilidades de los estados tanto para colas finitas como infinitas y se hace un estudio detallado de diferentes casos de interés. Para el caso concreto que nos ocupa, la probabilidad de pérdida P_L viene dada por:

$$P_L = a_K = \alpha \beta^K \tag{5}$$

donde β se obtiene numéricamente de la expresión [13]:

$$\frac{1}{1-\beta} \frac{1-\left[(K+1)-K\beta\right]\beta^K}{1-\beta^K} = \frac{N_a}{\rho_a} \tag{6}$$

y α es igual a [13]:

$$\alpha = \rho_a \frac{1-\beta}{\beta} \frac{1}{1-\beta^K} \tag{7}$$

Por lo tanto, para obtener el valor del tamaño del buffer que satisface una probabilidad de pérdida determinada, no hay más que despejar en la Ec. (5), teniendo en cuenta que el tamaño del buffer (Q) es el número máximo de elementos en el sistema (K) menos uno:

$$Q = \log_\beta \left(\frac{P_L}{\alpha} \right) - 1 \tag{8}$$

IV. Resultados

En esta sección se presentan los resultados obtenidos por medio de simulaciones tras la aplicación del algoritmo presentado en diversos escenarios. Las simulaciones se han llevado a cabo con una adaptación de un simulador de sistemas de transmisión orientado a la evaluación de algoritmos de *scheduling* [14][15].

A. Secuencias de test

Para conducir las simulaciones, se prepararon varias secuencias de test provocando variaciones de la carga del sistema con el paso del tiempo. El perfil de una de dichas secuencias se muestra en la Fig. 1, donde se puede observar cómo se provoca una variación en la utilización del canal entre 0.4 y 0.8. Para obtener cada uno de dichos niveles de utilización, se han mezclado cuatro tráficos diferentes con objeto de simular unas condiciones de trabajo lo más realistas posibles. Para cada uno de dichos tráficos se han tomado diferentes distribuciones, tanto para el tiempo entre llegadas de paquetes como para el tamaño de los mismos. En la Tabla I se presentan dichas distribuciones. Los valores concretos de los parámetros de cada una de las distribuciones se han variado para conseguir los diferentes niveles de carga deseados.

Tabla I
Variables aleatorias utilizadas para la generación de tráficos

Tráfico	Tiempo entre llegadas	Longitud de los paquetes
1	Exponencial truncada	Pareto truncada
2	Uniforme	Gamma
3	Determinista	Uniforme
4	Gamma	Pareto truncada

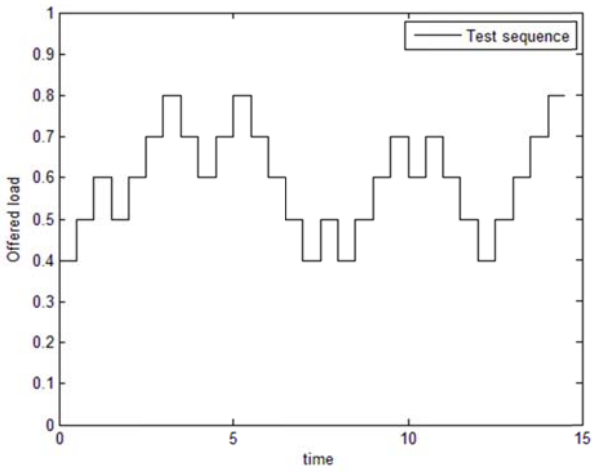


Fig. 1. Secuencia de test para las simulaciones.

B. Suavizado de los parámetros de entrada

Como se ha visto en la sección III, el mecanismo de adaptación del tamaño del buffer se basa en los valores medidos por el propio equipo de red de ρ_a y N_a. En una implementación práctica, estos valores no se deben obtener únicamente de medidas instantáneas, sino que hay que promediarlos (suavizarlos) para evitar oscilaciones que impedirían el funcionamiento deseado. La opción adoptada en este trabajo es la de realizar una media móvil ponderada exponencialmente (Exponentially Weighted Moving Average, EWMA):

$$\rho_a = w \cdot s_\rho + (1-w)\rho_a'$$
$$N_a = w \cdot s_N + (1-w)N_a' \tag{9}$$

donde ρ_a' y N_a' son los valores previos, s_ρ y s_N las muestras actuales y ρ_a y N_a los nuevos promedios que se utilizarán como entrada de las Ecs. (6) y (7). Por otra parte, el valor de

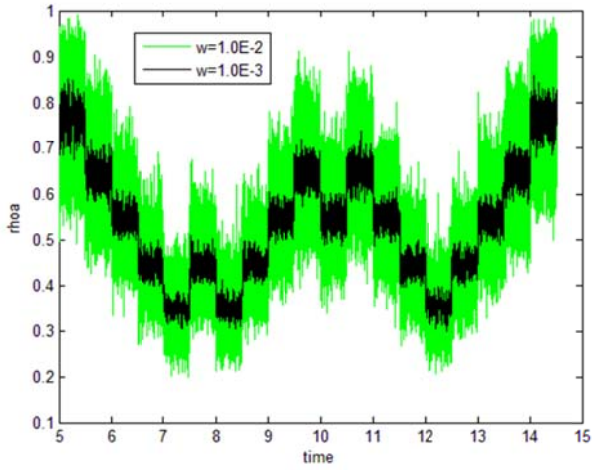
w ($w \in [0,1]$) determina si se da más importancia o menos a la muestra actual respecto de la historia pasada, de forma que cuanto mayor es su valor menos se suaviza y más rápido se sigue la evolución del parámetro en cuestión. En el entorno de este trabajo interesa suavizar lo máximo posible, pero sin perder demasiado la evolución del parámetro, lo cual podría llevarnos a no cumplir los objetivos deseados en cuanto a mantener acotada la probabilidad de pérdida de paquetes.

Para la secuencia de test bajo estudio, se realizaron diversas simulaciones con objeto de encontrar el valor mínimo de w que permite cumplir con el requisito de la probabilidad de pérdidas. En la Tabla II se resumen los valores obtenidos para distintos requisitos de P_L y para distintos valores de w. Como puede observarse, con un valor de w de 10^{-4} los requisitos de P_L aún se cumplen. Sin embargo, para 10^{-5} las pérdidas obtenidas superan a las deseadas en la mayoría de los casos. Este efecto queda también patente en la Fig. 2 (dividida en dos subfiguras). En ella se muestra la evolución temporal del valor suavizado de ρ_a para diferentes valores de w y para un valor de $P_L=10^{-3}$. Por motivos de claridad se muestran solo los diez últimos segundos de dicha evolución. Como puede observarse en la Fig. 2a, para valores de w de 10^{-2} y 10^{-3} las fluctuaciones de ρ_a son muy elevadas. En el otro extremo, para valores de 10^{-5} y 10^{-6} (Fig. 2b) no se sigue adecuadamente la evolución de la variación de la carga. El valor $w=10^{-4}$ vuelve a mostrarse como el más adecuado para seguir dicha variación suavizando a su vez lo máximo posible.

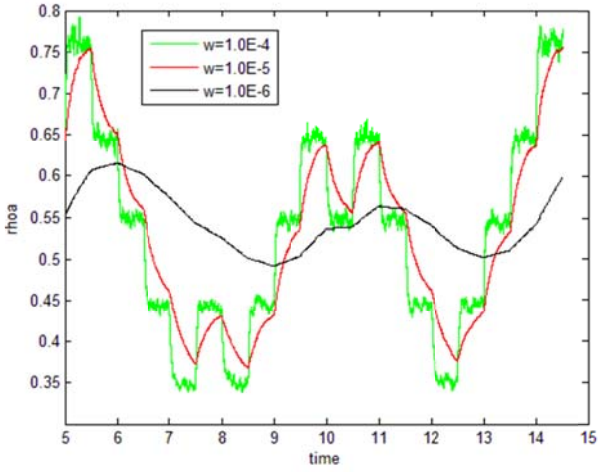
En la Fig. 3 se muestra la evolución del tamaño del buffer Q (en paquetes) para $P_L=10^{-3}$ y diferentes valores de w, obtenido aplicando la expresión de la Ec. (8) (En realidad la expresión da como resultado un valor decimal, y, como es lógico al tratarse del tamaño del buffer en paquetes, se toma el valor entero inmediatamente superior). Como era de esperar, las variaciones de tamaño son más acusadas cuanto mayor es el valor de w, pero para los valores inferiores no se cumplen los requisitos de P_L (como se ha mostrado en la Tabla II). Finalmente, en la Fig. 4, una vez adoptado el valor de trabajo $w=10^{-4}$, se muestra la evolución del tamaño del buffer para distintos requisitos de probabilidad de pérdida. Como puede comprobarse, a mayor requisito de probabilidad de pérdida mayor es el tamaño de buffer necesario.

Tabla II
P_L OBTENIDA EN FUNCIÓN DE W Y DE LA P_L REQUERIDA

	P_L requerida		
w	10^{-3}	10^{-4}	10^{-5}
10^{-3}	$5.66 \cdot 10^{-4}$	$2.62 \cdot 10^{-5}$	$2.38 \cdot 10^{-7}$
10^{-4}	$8.07 \cdot 10^{-4}$	$7.96 \cdot 10^{-5}$	$8.58 \cdot 10^{-6}$
10^{-5}	$9.27 \cdot 10^{-4}$	$1.18 \cdot 10^{-4}$	$1.57 \cdot 10^{-5}$
10^{-6}	$1.35 \cdot 10^{-3}$	$2.34 \cdot 10^{-4}$	$4.36 \cdot 10^{-5}$



a) $w=10^{-2}$ y 10^{-3}.



b) $w=10^{-4}$,10^{-5} y 10^{-6}.

Fig. 2. Suavizado del parámetro ρ_a.

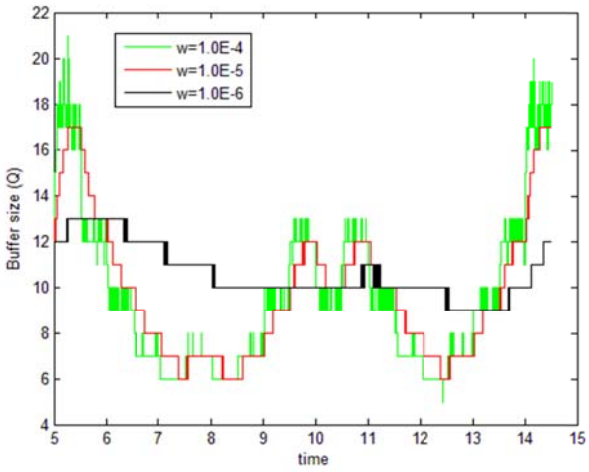


Fig. 3. Evolución del tamaño del buffer para distintos valores de w y $P_L=10^{-3}$.

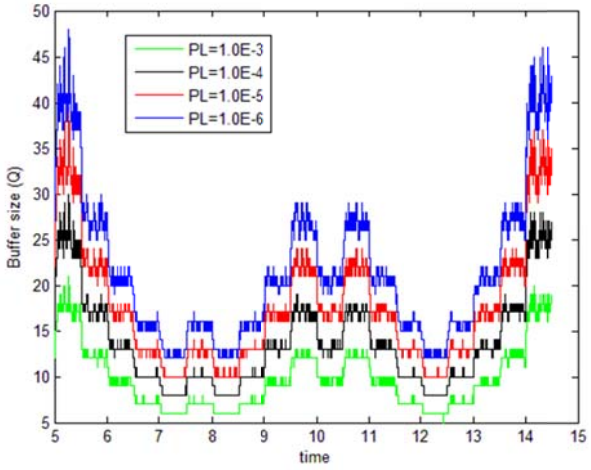


Fig. 4. Evolución del tamaño del buffer para distintos valores de P_L.

C. *Minimización de la sobrecarga introducida*

Como se ha visto con los experimentos anteriores, el equipo de red bajo estudio sería capaz de adaptar la cantidad de memoria que asigna a cada canal de transmisión en función de la carga y del requisito de probabilidad de pérdida. Para ello, cada vez que recibe un nuevo paquete que ha de retransmitir, realiza los cálculos necesarios y adapta el tamaño del buffer. Obsérvese que para poder aplicar la expresión de la Ec. (8) es necesario conocer el valor de α, el cual a su vez se obtiene del valor de β, y para la obtención de este último es necesaria la aplicación de métodos numéricos. Sin lugar a dudas, esta forma de proceder introduce una elevada sobrecarga en el dispositivo que podría resultar en retardos añadidos en la retransmisión de los paquetes.

Con objeto de reducir al máximo esta sobrecarga, en este apartado se presentan los resultados obtenidos tras instaurar unos umbrales para que se ponga en marcha el mecanismo de adaptación. Se han considerado dos umbrales diferentes, uno de bajada y otro de subida (Th_{DW} y Th_{UP}). Es decir, para cada paquete recibido el equipo actualiza el valor del promedio de ρ_a y N_a (esto no introduce una sobrecarga apreciable), pero el valor actualizado de ρ_a deberá diferir más de un determinado umbral respecto a su valor en el instante en que se realizó la última adaptación, tanto para aumentar como para reducir el tamaño del buffer. De este modo los cálculos numéricos necesarios según la Ec. (6) solo serán realizados cuando la variación de carga en el equipo sea realmente significativa. Esta forma de proceder disminuirá drásticamente la tasa de ejecuciones del algoritmo, permitiendo su implementación en dispositivos reales.

Para el ajuste de los valores de los umbrales se han realizado numerosas simulaciones. Además, se ha trabajado tanto con valores absolutos como con valores relativos para los umbrales (por ejemplo, que la utilización se incremente en 0.1 frente a la referencia anterior -valor absoluto- antes de incrementar el tamaño del buffer, o que lo haga en un 5% -valor relativo-). De todos los experimentos realizados se presentan los resultados que condujeron a la elección final de valores para los umbrales de subida y de bajada. En ambos casos fueron valores absolutos. Para el umbral de bajada, se adoptó un valor de 0.075, el cual asegura no disminuir el tamaño del buffer fácilmente, con objeto de mantener la probabilidad de pérdida acotada. Una vez ajustado este valor, se realizaron nuevas simulaciones para el ajuste del umbral de subida, obteniéndose los valores de la Tabla III.

Tabla III
P_L OBTENIDA EN FUNCIÓN DEL UMBRAL DE SUBIDA Y DE LA P_L REQUERIDA

	P_L requerida			
Th_{UP}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
0.01	$6.47\cdot10^{-4}$	$7.44\cdot10^{-5}$	$8.35\cdot10^{-6}$	$4.47\cdot10^{-7}$
0.05	$8.47\cdot10^{-4}$	$9.87\cdot10^{-5}$	$1.07\cdot10^{-5}$	$1.19\cdot10^{-6}$
0.1	$1.11\cdot10^{-3}$	$1.48\cdot10^{-4}$	$2.22\cdot10^{-5}$	$3.34\cdot10^{-6}$
0.15	$1.88\cdot10^{-3}$	$2.98\cdot10^{-4}$	$4.79\cdot10^{-5}$	$8.82\cdot10^{-6}$

Como se puede observar en la tabla, al incrementar el valor del umbral ponemos más difícil la adaptación del sistema a un incremento de carga y, por tanto, la probabilidad de pérdida crece. El valor máximo para el umbral que nos permite mantener acotada la probabilidad de pérdida por debajo de la requerida en todos los casos es 0.01. Utilizando este valor se obtiene la evolución para el tamaño del buffer que se muestra en la Fig. 5 para diferentes probabilidades de pérdida requeridas. Como puede observarse, comparando con la Fig. 4, se han eliminado ejecuciones innecesarias del algoritmo, evitando de esta forma la indeseada sobrecarga del equipo de red.

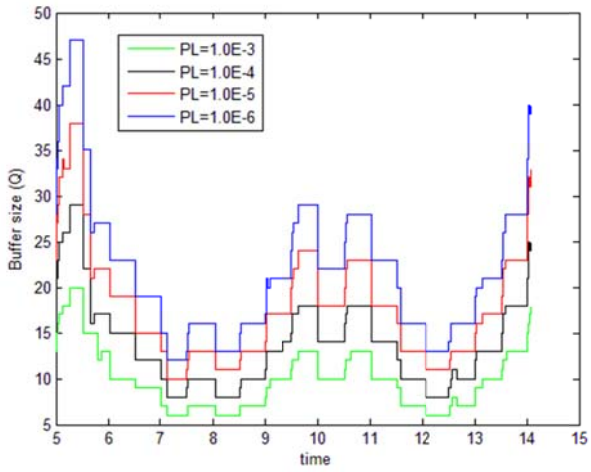


Fig. 5. Evolución del tamaño del buffer aplicando umbrales de subida y bajada, para distintos valores de P_L.

En concreto, para las simulaciones presentadas en las figuras, el valor del número de ejecuciones del algoritmo descendió desde 6499628 cuando no se aplicaron los umbrales (es decir, una ejecución por llegada de paquete), a 213. Además, este valor fue el mismo para los diferentes casos de probabilidad de pérdida estudiados. Promediando temporalmente, estos resultados equivalen a pasar de una tasa de 448225 a 15 ejecuciones por segundo. Nótese que el drástico descenso es debido fundamentalmente a una situación inicial en la que el número de ejecuciones es desmesuradamente elevado.

Por otra parte, se analizó el número de ejecuciones del algoritmo que provocaba realmente un cambio en el tamaño del buffer. Es decir, en ocasiones la ejecución del algoritmo puede llevar a obtener un valor para el tamaño del buffer que sea el mismo que ya tenía. Este hecho nos da información sobre si los umbrales se han escogido adecuadamente. Si la tasa de ejecuciones es mucho mayor que la tasa de cambios reales de tamaño, el valor de los umbrales se podría hacer más grande para reducir el número de ejecuciones, y viceversa. Sin embargo, hay que tener en cuenta que los

valores no podrán ser muy similares, pues en este caso podríamos perder actualizaciones necesarias que nos llevarán a no cumplir el objetivo de mantener la probabilidad de pérdida acotada. En la Fig. 6 se han representado los valores de la tasa media de ejecuciones y la tasa media de cambios de tamaño para diferentes probabilidades de pérdida. Como puede observarse, la tasa de cambios efectivos en el tamaño de buffer crece al hacer más fuerte el requisito de probabilidad de pérdida.

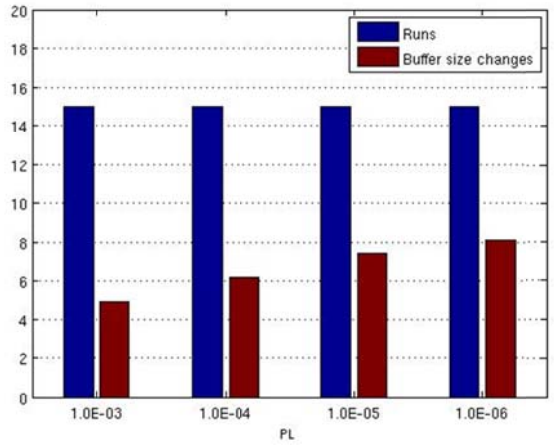


Fig. 6. Tasa de ejecuciones y tasa de cambios en el tamaño del buffer, para distintos valores de P_L.

D. Diferenciación de tráficos

A continuación se presentan los resultados obtenidos cuando se considera la posibilidad de ofrecer diferentes grados de servicio a diferentes flujos de tráfico. En concreto, uno de los flujos de tráfico será el correspondiente a la secuencia de test utilizada en los apartados anteriores, al que se añaden otros tres flujos con subidas y bajadas de carga a lo largo del tiempo diferentes entre ellos. Cada uno de dichos flujos se ha escalado para que produzca una cuarta parte del total de la carga ofrecida al sistema. En conjunto, la evolución temporal de la utilización del canal queda como se muestra en la Fig. 7. Nótese que esta utilización global es la misma que perciben los cuatro tráficos dado que comparten el canal.

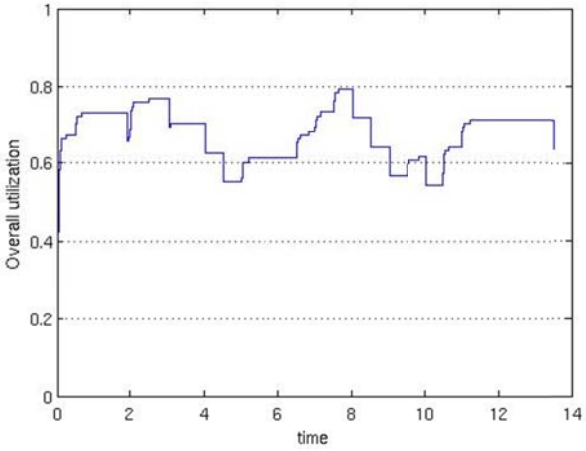


Fig. 7. Utilización global del canal por los cuatro flujos de tráfico.

En una primera simulación, se ha pedido la misma probabilidad de pérdida para los cuatro flujos. La Tabla IV resume los valores de P_L obtenida para cada uno de ellos y para diferentes valores de P_L requerida. Como puede observarse, la probabilidad de pérdida obtenida se encuentra en todos los casos por debajo de la deseada, comprobándose por tanto que el mecanismo presentado continúa ofreciendo resultados correctos cuando se tratan diferentes flujos por separado.

En la Fig. 8 se muestra el número de unidades en el sistema (promediado) que observa cada uno de los flujos a lo largo de la simulación, para el caso concreto de tener una probabilidad de pérdida requerida igual a 10^{-6}. Estos valores sí que difieren para cada uno de los tráficos, ya que se toman en cada cola por separado y por tanto reflejan la distinta evolución de la carga provocada por cada uno de ellos. Por su parte, en la Fig. 9 se presenta la evolución del tamaño del buffer asignado a cada uno de los flujos. Esta evolución es asimismo diferente para cada tráfico, ya que se adapta a las condiciones de cada uno de ellos.

Tabla IV
P_L OBTENIDA PARA FLUJOS DE TRÁFICO DIFERENCIADOS EN FUNCIÓN DE LA P_L REQUERIDA (IDÉNTICA PARA TODOS LOS FLUJOS)

	P_L requerida			
Flujo	10^{-3}	10^{-4}	10^{-5}	10^{-6}
1	$3.86 \cdot 10^{-4}$	$2.78 \cdot 10^{-5}$	$2.31 \cdot 10^{-6}$	$1.54 \cdot 10^{-7}$
2	$5.21 \cdot 10^{-4}$	$4.51 \cdot 10^{-5}$	$5.54 \cdot 10^{-6}$	$4.62 \cdot 10^{-7}$
3	$3.71 \cdot 10^{-4}$	$2.69 \cdot 10^{-5}$	$3.85 \cdot 10^{-6}$	$1.54 \cdot 10^{-7}$
4	$5.00 \cdot 10^{-4}$	$2.49 \cdot 10^{-5}$	$2.46 \cdot 10^{-6}$	$6.15 \cdot 10^{-7}$

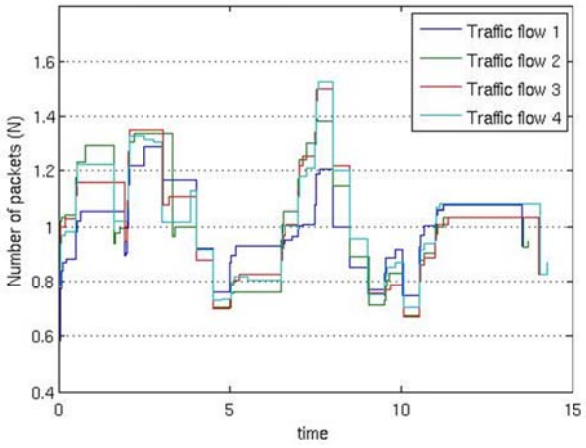


Fig. 8. Promedio del número de paquetes en el sistema.

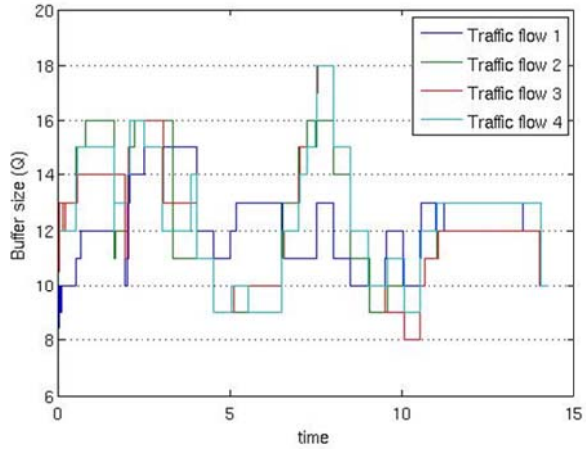


Fig. 9. Tamaño de buffer para cada uno de los flujos de tráfico.

El siguiente paso en la tanda de simulaciones ha sido comprobar que el mecanismo funciona correctamente cuando se solicitan diferentes grados de servicio (diferentes probabilidades de pérdida) a cada uno de los flujos de tráfico. En concreto, se han solicitado probabilidades de pérdida que van desde 10^{-3} hasta 10^{-6}. En la Tabla V se muestran los resultados obtenidos, comprobándose de nuevo el correcto funcionamiento. En este caso, se ha añadido también el valor del tiempo de permanencia (T) en el sistema (espera más transmisión) para cada uno de los flujos. Se muestra como dicho tiempo es muy parecido para todos los tráficos, independientemente de la probabilidad de pérdida solicitada. Esto es así debido a que las probabilidades de pérdida son pequeñas, con lo cual prácticamente todos los paquetes son admitidos en los buffers en todos los casos y por tanto no se aprecia en exceso el efecto de un buffer finito. Obsérvese como para la probabilidad de pérdida más grande, 10^{-3}, sí que se aprecia un valor más pequeño de T como corresponde a un buffer de tamaño menor. Por otra parte, en las Fig. 10 y Fig. 11 se presenta la evolución del número de paquetes en cola y del tamaño del buffer asignado a cada uno de los tráficos respectivamente. Al igual que en la simulación anterior, ha de tenerse en cuenta que los incrementos y decrementos de carga son diferentes para cada uno de los flujos, y que por tanto los incrementos y decrementos en el tamaño de buffer asignado no tienen por qué estar sincronizados. Además se observa como los tráficos con menor probabilidad de pérdida deseada son los que tienen asignados mayores tamaños de buffer a lo largo del tiempo.

E. Diferentes políticas de servicio

Para finalizar con la presentación de resultados, se incluyen los obtenidos cuando se aplican diferentes políticas de servicio (*schedulers*). Si bien los resultados teóricos presentados en el apartado III se han obtenido para una política de servicio FCFS (*First Come First Served*) [13], se encontró interesante estudiar lo que ocurre cuando se utiliza otro tipo de *scheduler*, que ofrezca algún tipo de prioridad en el servicio a unos tráficos frente a otros. Se realizaron simulaciones para tres tipos de *schedulers*: NPP (*Non Preemption Priority*), WRR (*Weighted Round Robin*) y DRR (*Deficit Round Robin*). La idea consistía en combinar la solicitud de distintas probabilidades de pérdida para distintos flujos de tráfico, como se ha hecho al final del apartado anterior, con una política de servicio que ofrezca prioridades diferentes en la cola de espera. En la Tabla VI se presentan los resultados obtenidos con NPP. El flujo de tráfico de mayor prioridad es el 1 y el de menos el 4. Obsérvese que en la simulación 1 se asigna más prioridad al tráfico al que se pide menor P_L, y en la simulación 2 es a la inversa. En ambos casos, los tráficos prioritarios satisfacen la P_L deseada, mientras que los menos prioritarios no lo hacen. Además, se incluye el valor de T en ambos casos y para cada uno de los tráficos. Como es lógico, los tráficos más prioritarios obtienen un valor de T menor. Una conclusión interesante es que, comparando ambas simulaciones, el valor de T vuelve a no depender de la P_L solicitada, sino solo de la prioridad asignada. De esta forma, si se desea satisfacer requisitos tanto de P_L como de T, en una primera aproximación se puede trabajar con ambos parámetros por separado.

Como se ha comentado, también se han realizado simulaciones similares utilizando como *schedulers* WRR y DRR. Los resultados obtenidos ofrecen conclusiones similares a las expuestas para NPP. Aun así, queda como futura línea de trabajo el análisis detallado del mecanismo propuesto cuando se utilizan diferentes políticas de servicio.

Tabla V
P_L Y T OBTENIDOS PARA FLUJOS DE TRÁFICO DIFERENCIADOS EN FUNCIÓN DE LA P_L REQUERIDA (DIFERENTE PARA CADA FLUJOS)

	P_L requerida			
	Flujo 1 10^{-3}	Flujo 2 10^{-4}	Flujo 3 10^{-5}	Flujo 4 10^{-6}
P_L	$3.86\cdot10^{-4}$	$4.43\cdot10^{-5}$	$3.84\cdot10^{-6}$	$6.15\cdot10^{-7}$
T	$1.17\cdot10^{-6}$	$1.21\cdot10^{-6}$	$1.22\cdot10^{-6}$	$1.22\cdot10^{-6}$

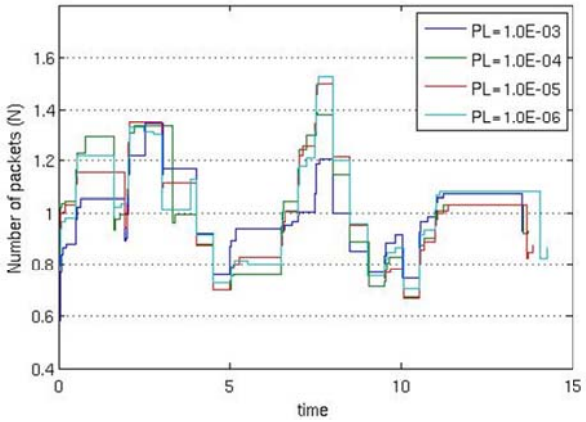


Fig. 10. Promedio del número de paquetes en el sistema.

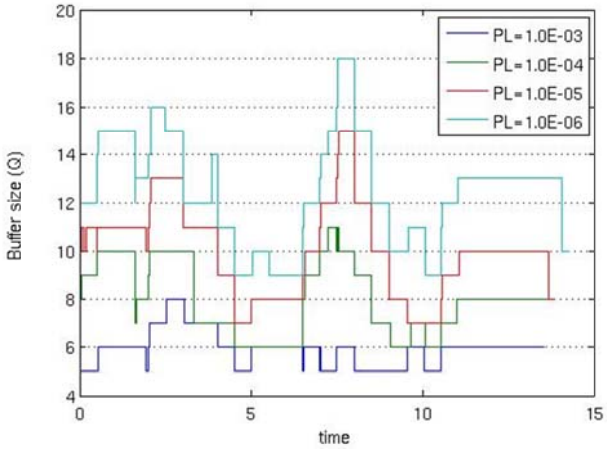


Fig. 11. Evolución del tamaño del buffer con distinta probabilidad de pérdida para cada uno de los flujos de tráfico.

Tabla VI
P_L Y T OBTENIDOS PARA FLUJOS DE TRÁFICO DIFERENCIADOS EN FUNCIÓN DE LA P_L REQUERIDA (DIFERENTE PAIRA CADA FLUJOS) Y DE LA PRIORIDAD ASIGNADA (SCHEDULER NPP).

SIM 1	P_L requerida			
	Flujo 1 10^{-6}	Flujo 2 10^{-5}	Flujo 3 10^{-4}	Flujo 4 10^{-3}
P_L	$1.65\cdot10^{-7}$	$1.00\cdot10^{-5}$	$1.44\cdot10^{-4}$	$1.35\cdot10^{-3}$
T	$5.89\cdot10^{-7}$	$6.92\cdot10^{-7}$	$8.69\cdot10^{-7}$	$1.20\cdot10^{-6}$

SIM 2	P_L requerida			
	Flujo 1 10^{-3}	Flujo 2 10^{-4}	Flujo 3 10^{-5}	Flujo 4 10^{-6}
P_L	$4.11\cdot10^{-4}$	$6.69\cdot10^{-5}$	$2.00\cdot10^{-5}$	$4.44\cdot10^{-6}$
T	$5.88\cdot10^{-7}$	$6.91\cdot10^{-7}$	$8.69\cdot10^{-7}$	$1.21\cdot10^{-6}$

V. Conclusiones

El dimensionado de buffers en equipos de interconexión de red es un aspecto crítico por sus repercusiones inmediatas en la calidad de servicio que perciben los usuarios finales. Si bien el coste económico de la memoria va decreciendo y su integración es más sencilla, está demostrado que un exceso de memoria puede ser incluso perjudicial por el incremento en el retardo que puede añadir. Por otra parte, asignar la justa cantidad de memoria a un canal de transmisión permitirá aprovechar la memoria en otro canal que necesite mayor cantidad en un momento determinado.

En este trabajo se ha propuesto un mecanismo que asigna dinámicamente el tamaño mínimo de buffer para flujos de tráfico que han de ser transmitidos y consumidos en tiempo real estricto. Dicho tamaño mínimo deberá garantizar que no se sobrepasa una probabilidad de pérdida máxima, que podrá asignarse independientemente a cada flujo de tráfico en función de su naturaleza. Además, el algoritmo se puede ejecutar independientemente en cada equipo de red que lo necesite. De esta forma, dichos equipos serán capaces de autoconfigurar el tamaño de sus buffers sin necesidad de intervención de ningún otro dispositivo.

El correcto funcionamiento del mecanismo propuesto ha sido comprobado mediante simulaciones realizadas bajo distintas condiciones en cuanto a carga del dispositivo y a la calidad de servicio requerida. Asimismo, con objeto de evitar una posible sobrecarga de trabajo en el procesador central, se ha comprobado que no es necesario ejecutar el algoritmo con la llegada de cada nuevo paquete, sino que es posible establecer unos umbrales de activación.

Por otra parte, también se ha planteado la posibilidad de ofrecer diferentes probabilidades de pérdida a diferentes flujos de tráfico que comparten un mismo canal de transmisión. Al igual que en los casos anteriores, las simulaciones han dado como resultado que efectivamente el mecanismo propuesto ofrece resultados correctos, asignando a cada uno de los flujos el mínimo tamaño de buffer necesario para garantizar su propia probabilidad de pérdida máxima.

Finalmente, se ha hecho una primera incursión en la posibilidad de combinar el mecanismo propuesto con la utilización de diferentes *schedulers*, con objeto de buscar no sólo una probabilidad de pérdida diferente para distintos flujos, sino también un diferente tiempo de permanencia en el sistema. Las primeras simulaciones indican que es posible trabajar con ambos parámetros por separado, lo cual es muy conveniente para facilitar la tarea de auto configuración de los equipos. Sin embargo, el análisis detallado en este entorno queda como futura línea de trabajo.

Una línea de trabajo adicional que se ha comenzado a poner en marcha es la tarea de implementación del mecanismo propuesto en dispositivos reales, para lo cual se evaluarán dos alternativas diferentes. La primera de estas alternativas consiste en modificar directamente el código fuente de los controladores de las tarjetas de red, de tal manera que el atributo "*tx_queue_len*" (máximo número de tramas que pueden ser admitidas en la cola de transmisión interna del dispositivo), configurado por defecto con un valor fijo, se ajuste dinámicamente con la utilización del mecanismo propuesto. Un punto de partida para este fin será el de utilizar y adaptar la librería DQL (Dynamic Queue Limit) desarrollada por investigadores de Google [16][17] e introducida en el kernel de Linux versión 3.3. Esta librería implementa un mecanismo para limitar dinámicamente el tamaño de la cola de transmisión del hardware de una tarjeta de red.

La segunda alternativa que se evaluará es la de la implementación de la propuesta en enrutadores que operen con un sistema operativo que permita una completa configuración y personalización. Para este fin se utilizará la distribución GNU/Linux para sistemas embebidos OpenWrt [18].

Agradecimientos

Este trabajo se ha realizado con el soporte de los proyectos TAMESIS (TEC2011-22746) y CONSEQUENCE (TEC2010-20572-C02-02), y con el programa de becas del gobierno de Ecuador SENESCYT 2010 y de la Universidad Politécnica Salesiana.

Referencias

[1] J. Gettys and K. Nichols, "Bufferbloat: dark buffers in the internet", Communications of the ACM, vol. 55, n. 1, pp., 57-65, 2012.

[2] C. Kreibich, N. Weaver, B. Nechaev and V. Paxson, "Netalyzr: illuminating the edge network", Proc. of the 10th ACM SIGCOMM conference on Internet measurement (IMC '10). ACM, New York, NY, USA, pp. 246-259, 2010.

[3] N. Beheshti, Y. Ganjali, R. Rajaduray, D. Blumenthal and N. McKeown, "Buffer sizing in all-optical packet switches", Optical Fiber Communication Conference, 2006 and the 2006 National Fiber Optic Engineers Conference. OFC 2006, Paper OThF8, 2006.

[4] A. Vishwanath, V. Sivaraman and G.N. Rouskas, "Anomalous Loss Performance for Mixed Real-Time and TCP Traffic in Routers With Very Small Buffers", IEEE/ACM Transactions on Networking, vol.19, no.4, pp.933-946, 2011.

[5] C. Villamizar and C.Song, "High performance TCP in ANSNET", SIGCOMM Computer Communication Review, vol. 24, no. 5, pp.45-60, 1994.

[6] G. Appenzeller, I. Keslassy, and N. McKeown, "Sizing router buffers", SIGCOMM Computer Communication Review, vol. 34, no.4, pp.281-292, 2004.

[7] N. Beheshti, Y. Ganjali, M. Ghobadi, N. McKeown, and G. Salmon, "Experimental study of routerbuffer sizing", Proceedings of the 8th ACM SIGCOMM conference on Internet measurement (IMC '08), ACM, New York, pp. 197-210 , 2008.

[8] V. Mahendran, T. Praveen, and C. S. R. Murthy, "Buffer dimensioning of delay-tolerant network nodes - a large deviations approach", Proceedings of the 13th international conference on Distributed Computing and Networking (ICDCN 2012), LNCS 7129, pp. 502-512, Springer-Verlag, Berlin, 2012.

[9] T. Li; D. Leith, and D. Malone, "Buffer Sizing for 802.11-Based Networks", IEEE/ACM Transactions on Networking , vol.19, no.1, pp. 156-169, 2011.

[10] K. Jamshaid, B. Shihada, L. Xia, P. Levis, "Buffer Sizing in 802.11 Wireless Mesh Networks", 2011 IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 272-281, 2011.

[11] C. Shannon and W. Weaver, "The Mathematical Theory of Communication", University of Illinois Press, 1972.

[12] T.M. Cover and J.A. Thomas, "Elements of Information Theory", John Wiley, 1991.

[13] Emilio Sanvicente, Luis J. de la Cruz y Mónica Aguilar, "Buffer Dimensioning for the G/G/1 Queue via Maximum Entropy", Internal Report, Dpt. of Telematics Engineering, Universitat Politécnica de Catalunya, Biblioteca, Doc. n. 1400837095, 2012.

[14] Luis J. de la Cruz y Emilio Sanvicente, "Scalev: Herramienta Software para la Evaluación de Algoritmos de Scheduling", En Actas de las VI Jornadas de Ingeniería Telemática JITEL 2007, pp. 237-244, ISBN 978-84-690-6670-6, 2007.

[15] Scalev website: http://scalev.upc.es.

[16] T. Herbert, "bql: Byte queue limits," Patch posted to the Linux kernel network development mailing list, Nov 2011. [Online]. Available: http://article.gmane.org/gmane.linux.network/213308/

[17] J. Corbet, "Network transmit queue limits," LWN Article, August 2011. [Online]. Available: https://lwn.net/Articles/454390/

[18] OpenWrt website [Online]. Available: https://openwrt.org/

Evaluación de rendimiento de Bluetooth Low Energy en sistemas de posicionamiento en interiores

David Contreras Bárcena y David Sánchez de la Torre
Departamento de Sistemas Informáticos
Universidad Pontificia de Comillas
Alberto Aguilera, 23 28015 Madrid
davidcb@upcomillas.es, dsanchezdelatorre@gmail.com

***Resumen*- Los sistemas de posicionamiento en interiores o Local Positioning Systems (LPS) están en pleno auge, tanto desde el punto de vista comercial como científico. Son muchas las tecnologías inalámbricas utilizadas, pero las que concentran un mayor número de aplicaciones son precisamente las más cercanas al usuario: WiFi y Bluetooth. Estas dos tecnologías son las elegidas por su simplicidad, coste e integración en los dispositivos móviles. La aparición de la nueva especificación de Bluetooth, denominada Low Energy (BLE) y la aparición de nuevos dispositivos que la incorporan, abren la puerta a nuevas soluciones LPS basadas en esta tecnología inalámbrica. Por este motivo, este artículo evalúa la viabilidad de BLE en escenarios de posicionamiento en interiores. Además, se define un marco de trabajo que permita entender y migrar los sistemas LPS anteriores basados en otras tecnologías a BLE. Los experimentos realizados demuestran que mediante una correcta configuración de los dispositivos BLE se pueden obtener unos excelentes resultados en términos de tiempo de descubrimiento y en consumo.**

***Index Terms*- Bluetooth Low Energy, Local Positioning System, discovery time, indoor positioning**

I. INTRODUCCIÓN

La tecnología hoy en día, gracias a las posibilidades de interconexión, está alcanzando un nivel de inmersión en nuestra sociedad prácticamente total. La comunicación existente entre, no sólo las personas, sino con todo lo que nos rodea (conocido como el Internet de las cosas) está superando las previsiones más optimistas. Sin embargo, hay un ámbito donde esta comunicación e interacción hombre-máquina no está cumpliendo con las expectativas: los sistemas de posicionamiento en interiores. Saber cómo llegar a una tienda en un centro comercial, crear sistemas de guiado a personas con discapacidad dentro del metro de una gran ciudad, en definitiva, migrar la tecnología de GPS al interior de edificios e infraestructuras, está todavía lejos de ser una realidad.

La aparición de nuevas tecnologías de comunicaciones como Bluetooth Low Energy (BLE) debe ser un paso adelante para ser capaces de ofrecer este tipo de soluciones con plenas garantías. Esta tecnología inalámbrica evolucionada a partir del estándar Bluetooth, ha supuesto cambios en el protocolo original para reducir el consumo de energía y tiempos de respuesta para poder utilizarla en aplicaciones antes imposibles por su alto consumo como: sensores biomédicos, cerraduras de puertas, soluciones *wearable*, etc.

Hoy en día, son muchos los sistemas de posicionamiento en interiores existentes basados en Bluetooth, Zigbee, Wi-Fi, UWB, etc. Con este artículo se pretende analizar y evaluar el funcionamiento y rendimiento de BLE para que estos sistemas puedan migrar y utilizar esta tecnología.

El artículo se estructura de la siguiente forma. En el capítulo II se describe el funcionamiento de la especificación BLE. En el capítulo III se realiza una revisión de los sistemas de posicionamiento existentes, basados en tecnologías inalámbricas en general y Bluetooth estándar. En el capítulo IV se comentan los resultados obtenidos después de pruebas experimentales y por último, se resaltan las conclusiones del artículo.

II. BLUETOOTH LOW ENERGY

Bluetooth Low Energy (BLE) es una tecnología inalámbrica que trabaja en la frecuencia sin licencia de 2.4GHz, en concreto entre las frecuencias 2402MHz y 2480MHz definiendo un total de 40 canales de 2MHz cada uno. Para las funciones búsqueda de dispositivos utiliza los canales 37 (2402Mhz), 38 (2426Mhz) y 39 (2480Mhz). El resto de las frecuencias (37 canales) quedan libres para el envío de datos.

La Tabla I muestra las diferencias existentes entre la versión clásica de Bluetooth (orientada al uso doméstico) y la nueva especificación de bajo consumo (orientada a entornos de control/sensores). Esta especificación de BLE no está diseñada para la transmisión de grandes volúmenes de información, sino que intenta maximizar el tiempo de vida de los dispositivos y proporcionar tiempos de descubrimiento realmente reducidos.

Tabla I
COMPARATIVA TEÓRICA DE BLUETOOTH Y BLE

Características	Bluetooth	BLE
Velocidad efectiva	2,1 Mbps	0,26Mbps
Consumo	100%	1%-5%
Latencia de envío datos	100ms	3ms

Esta tecnología se caracteriza por tener cinco estados en la capa de enlace (Fig. 1): *standby*, *scanning*, *advertising*, *initiating* y *connection*. Además, BLE permite realizar acciones básicas como es la recepción de paquetes de búsqueda y la posible petición de más información básica sin necesidad de estar conectado. Este funcionamiento responde a la necesidad de envío esporádico de información de sensores, por ejemplo.

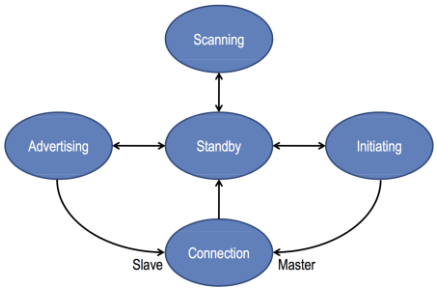


Fig. 1. Representación de los estados definidos por BLE. El estado de *Advertising* permite envío de paquetes para ser encontrado por el dispositivo que se encuentre en estado *Scanning*.

Para el caso que nos preocupa, escenarios de posicionamiento en interiores, los dos estados más interesantes son aquellos que intervienen en la búsqueda de dispositivos (dispositivo móvil intentando localizar balizas de posicionamiento, por ejemplo): *advertising* y *scanning*.

A. *Estado de Advertising*

El objetivo principal de este estado es que un dispositivo (*scanner*) detecte a otros dispositivos (*advertiser*) con necesidad de transmisión o detección. Existen cuatro tipos de paquetes de *advertising* en función del tipo de búsqueda que se desee realizar. El dispositivo con el rol de *advertiser* enviará un paquete cada T_{adv} segundos (Fig. 2). En cada evento de *advertising* se enviarán estos paquetes utilizando los tres canales destinados al efecto (37, 38 y 39). Con el fin de evitar interferencias con otros *advertiser* que pudieran estar sincronizados casualmente en el envío de los paquetes, se añade, al finalizar cada evento de *advertising*, un tiempo aleatorio que no debe exceder de 10ms.

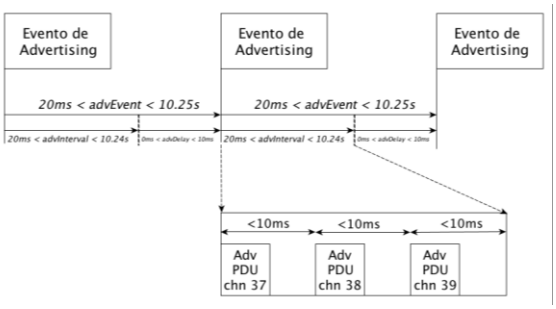


Fig. 2. Esquema de funcionamiento del estado de *Advertising*.

Los tipos de paquetes existentes que pueden ser enviados por un *advertiser* son:

- ADV_IND (Connectable Undirected Advertising Event): una vez enviado este paquete, el *advertiser* recibe un paquete del *scanner* del tipo SCAN_REQ solicitando más información. Se responderá con un paquete SCAN_RSP en el mismo canal de *advertising*. A continuación el *scanner* puede solicitar la conexión con un paquete CONNECT_REQ.
- ADV_DIRECT_IND (Connectable Undirected Advertising Event)**:** cuando el *advertiser* envía este paquete, recibirá un CONNECT_REQ del *scanner*.
- ADV_NONCONN_IND (Non-connectable Undirected Event)**:** cuando el *advertiser* envía este paquete es porque no acepta conexiones.
- ADV_SCAN_IND (Scannable Undirected Event): realiza la misma función que un paquete ADV_IND, pero no permite conexiones.

B. *Estado de Scanning*

Este estado complementa al estado de *advertising* en el proceso de descubrimiento de dispositivos en el rango. El dispositivo que entra en este modo (*scanner*) escuchará las peticiones de detección o conexión enviadas por el *advertiser*. El *scanner* escuchará durante un tiempo denominado $T_{scanWindow}$ en cada canal de los definidos para este fin y de forma secuencial, durante cada período de tiempo definido en $T_{scanInterval}$ (Fig. 3). Este intervalo de escaneo no puede exceder de 10,24seg.

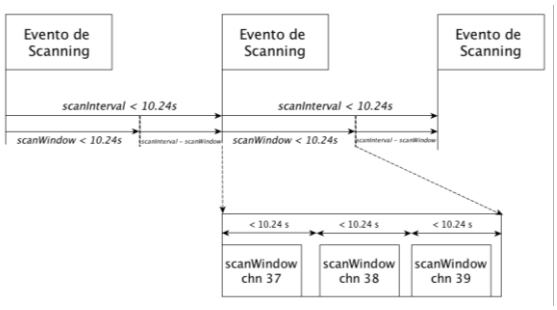


Fig. 3. Esquema de funcionamiento del estado de *Scanning*.

Existen dos tipos de modo dentro de este estado:

- Pasive Scanning: el *scanner* sólo recibirá paquetes, pero no contestará con ningún paquete.
- Active Scanning: dependiendo del tipo de paquete de *advertising*, el *scanner* contestará al dispositivo configurado como *advertiser*.

Una ventaja de Bluetooth Low Energy es que en los paquetes de *advertising* del tipo ADV_IND, ADV_NONCONN o ADV_SCAN_IND pueden viajar datos de hasta 31 bytes. De esta forma, se puede llegar a programar el sistema LPS para que las balizas envíen información asociada al mismo mediante los perfiles GATT en el mismo paquete de *advertising*. Este hecho supone una gran ventaja respecto a la versión previa de Bluetooth ya que permite transferencia de información reducida (como información de sensores) sin requerir la conexión entre los dispositivos.

Como se puede extraer de todo lo anterior, los diferentes modos y parámetros existentes en la especificación BLE permiten establecer múltiples configuraciones de descubrimiento que serán analizadas más adelante.

III. TRABAJOS RELACIONADOS

Recientemente, muchos trabajos han intentado resolver el problema de estimación de la localización en interiores de diferentes formas mediante la utilización de redes inalámbricas. A continuación se clasificarán y resumirán algunas de las más importantes aportaciones.

En primer lugar se citarán algunos sistemas de referencia que utilizan distintos tipos de tecnologías. Uno de los primero sistemas fue el sistema basado en tecnología de infrarroja denominada Active Badge System [1]. El sistema Cricket [2], propuesto por el MIT, es otro de los trabajos de referencia cuando se habla de los sistemas LPS. En esta

ocasión el sistema está basado en emisores de ultrasonidos y de radiofrecuencia (RF). LandMarc [3] está basado en RFID y comienza a plantear los problemas derivados del posicionamiento basado en la medición de la intensidad de la señal. El sistema MoteTrack [4] está basado en RF y fue desarrollado en la Universidad de Hardvard. Prácticamente todos los presentan errores de posicionamiento de unos 2 ó 3 metros, lo cual explica la complejidad en la estimación de la posición en interiores, donde las diferentes perturbaciones que presenta la señal (*multipath*, reflexión, refracción, etc.) convierte esta solución en una tarea compleja.

Una de las soluciones que se han tomado para reducir esta complejidad ha sido mediante el procesamiento de la señal para eliminar el *multipath* y la utilización de métodos para eliminar el problema de *cross-correlation*, en el que tenemos que eliminar la señal más fuerte para poder recoger las señales más débiles [5][6].

Muchos de los sistemas propuestos tienen como punto de partida en un indicador que mide la fuerza de señal, denominado RSSI. A partir de este valor se suelen emplear diferentes técnicas como son las que se agrupan en las basadas en *range-based* o *range-free*. Los primeros requieren de una fase de entrenamiento previa en la que se almacenan previamente los valores RSSI en diferentes posiciones para a continuación mediante diferentes modelos se pueda reproducir con los datos obtenidos en tiempo real.

Dentro de los algortimos basados en range-based se encuentra una técnica muy empleada en posicionamiento y combinada con WiFi o Bluetooth, denominada *finger-printing* [8]. Se basa en la utilización del indicador de fuerza de la señal (RSSI) de cada uno de los puntos de acceso para crear un mapa en toda la infraestructura. Estas técnicas se suelen combinar con otros tipos de sensores (acelerómetros, por ejemplo) y la aplicación de filtros (Kalman) para eliminar el ruido de la señal y predecir el movimiento del objeto a realizar el *tracking*. También se utilizan otras técnicas de post-procesado como las redes neuronales, la aplicación de filtros de partículas, mediante el método de Monte Carlo [13], filtros Butterworth o Chebyshev, modelos estadísticos de Markov [11] o modelos bayesianos [12].

Dentro del grupo de los sistemas denominados *range-free* encontramos aquellos que no necesitan una fase de entrenamiento almacenando datos en diferentes lugares, lo cual nos da una mayor flexibilidad a la hora de utilizar el sistema en lugares donde los datos sin embargo no nos posiciona en un punto en el sistema, sino que nos da una zona en la que podríamos encontrarnos [10].

IV. RESULTADOS

Como se ha discutido en el apartado anterior, son muchos los trabajos propuestos con diferentes tecnologías de comunicaciones y técnicas de procesado que reducen los desajustes de la principal medida que utilizan: el RSSI (indicador de la fuerza de la señal). A continuación se procederá a evaluar si Bluetooth Low Energy es una tecnología que permita mejorar los resultados obtenidos en el contexto de las soluciones de posicionamiento en interiores (LPS).

Para demostrar la validez de BLE en este tipo de soluciones se han realizado experimentos en entornos reales, con el fin de proporcionar unos resultados aprovechables para futuros desarrollos LPS. Para la realización de estos experimentos se ha trabajado con los siguientes dispositivos y software:

- 4 dongles Bluegiga BLED112 con chip TI C2540.
- 2 dongles Texas Instrument C2540.
- 1 sniffer TI BLE.

Para el procesamiento y cálculo de los retardos producidos en el envío de los paquetes, se han embebido dentro del dongle BLE de Bluegiga programas codificados en C que permiten gestionar la recepción de los paquetes recibidos en el *scanner*, gracias a la librería BGLib que proporciona el fabricante.

De todos los modos de descubrimiento y tipos de paquetes descritos en el apartado II, se utilizarán aquellos que simplifiquen el proceso de búsqueda y no requieran conexión. En todos los paquetes de tipo *advertsing*, se incluye el valor del indicador de fuerza de la señal recibida (RSSI), por lo que se no sería necesario entrar en un estado de conexión para generar una infraestructura de un sistema de posicionamiento en interiores basado en este indicador. Este estado implicaría realizar una tarea más costosa en tiempo y consumo. Cabe destacar también, que se han utilizado los tres canales disponibles (37, 38 y 39) destinados para el proceso de *advertising*.

En los experimentos realizados se han llevado a cabo un gran número de pruebas obteniendo los tiempos medios de descubrimiento entre un dispositivo cumpliendo el rol de *scanner* y otro de *advertiser*. Con el fin de evaluar el proceso de búsqueda de BLE, se estudiará el impacto de los parámetros definidos en la especificación: $T_{advertising}$, $T_{scanWindow}$ y $T_{scanInterval}$ en el proceso de descubrimiento de dispositivos. Por tanto, se evaluarán dos métricas críticas para cualquier sistema de posicionamiento en interiores: el tiempo de búsqueda de un dispositivo (baliza) y el coste asociado en términos de consumo.

A. Evaluación del estado de Advertising

Para evaluar el impacto de estado de *advertising* en el descubrimiento, se ha modificado el intervalo de *advertising* (T_{adv}). En este primer análisis realizado se ha configurado el *scanner* para que esté escuchando paquetes durante todo el tiempo ($T_{scanWindow}=T_{scanInterval}$), estableciéndose en 1000ms. De esta manera, se aislará el efecto de ambos tiempos de *scanning*. Como se muestra en la Fig. 4 el tiempo de descubrimiento del *scanner* es proporcional a la frecuencia de generación de paquetes de *advertising*.

Analizando los resultados obtenidos en los experimentos, llama la atención cómo para $T_{adv}\leq$200ms, el tiempo de descubrimiento se mantiene constante en 191ms (línea azul con cuadrados). Después de profundizar en este hecho, se ha comprobado cómo la pila BLE implementada en los *dongles* utilizados en los experimentos admite sólo los 5 primeros paquetes recibidos, desechando el resto. Por este motivo, el tiempo de descubrimiento satura en 200ms ($T_{scanWindow}/nºpaquetesBuffer$; 1000ms/5paq=200ms). La justificación de la función de *buffer* en los dispositivos es debido a que las aplicaciones generalistas que hacen uso de la pila, sólo desean conocer la presencia o no de dispositivos durante el intervalo de *scanning* y no la frecuencia con la que es detectado. El comportamiento de BLE sin tener en cuenta

la comentada funcionalidad de *buffer* se muestra en la Fig. 4 mediante la línea roja discontinua.

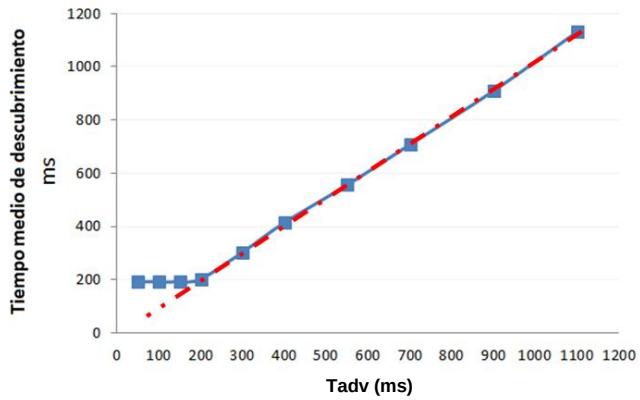


Fig. 4. Tiempo de descubrimiento en función del T_{adv} definido en el *advertising*. Se representan los valores medios de un conjunto de 100 pruebas para cada experimento.

B. Evaluación del estado de Scanning

Teniendo en cuenta el sincronismo obligatorio que debe haber en el proceso de búsqueda en BLE, el valor óptimo del intervalo de *advertising* (T_{adv}) debe ser ajustado en función del valor de escucha de los paquetes de *advertising*, determinado por la ventana de *scanning* ($T_{scanWindow}$). En el experimento anterior (Fig. 4) el *scanner* estaba en un proceso continuo de escucha. Como se puede intuir y más adelante se demostrará, este hecho afecta directamente en el consumo. Por este motivo y para el analizar el impacto del $T_{scanWindow}$, se ha variado desde 0 a 1000ms, manteniendo el valor del $T_{scanInterval}$=1000ms. El valor de T_{adv} se ha establecido en 200ms. Como muestra la Fig. 5 se observa que para un valor de $T_{scanWindow}$=1000ms, se obtiene un tiempo medio de descubrimiento de 191ms, confirmando la validez del experimento. El retardo en el proceso de búsqueda crece exponencialmente a medida que la relación entre el $T_{scanInterval}$ y $T_{scanWindow}$ es menor, llegando a alcanzar valores de descubrimiento inviables para escenarios de posicionamiento en interiores.

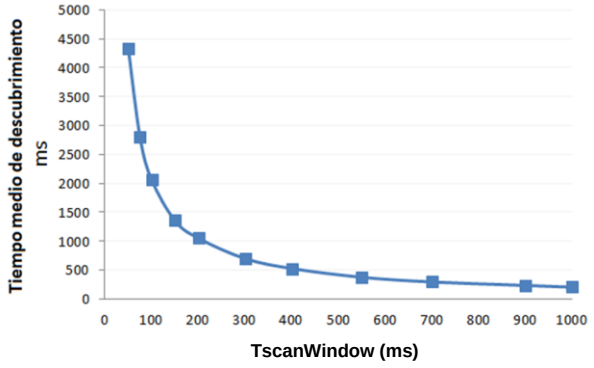


Fig. 5. Tiempo de descubrimiento en función del $T_{scanWindow}$ con un $T_{scanInterval}$=1000ms y un T_{adv}=200ms. Se representan los valores medios de un conjunto de 100 pruebas para cada experimento.

C. Evaluación conjunta del estado

Después de analizar los resultados anteriores y conociendo las restricciones en la pila de los dispositivos BLE, la elección del intervalo ($T_{scanInterval}$) y la ventana de *scanning* ($T_{scanInterval}$) son críticos para las soluciones LPS. Por este motivo, se busca maximizar el tiempo de búsqueda y la resolución de muestreo de obtención de paquetes de *advertising*. Con este objetivo, se realiza el siguiente experimento: obtención del tiempo de descubrimiento medio variando conjuntamente los valores de T_{adv}, $T_{scanInterval}$ y $T_{scanWindow}$ de igual forma. Como se observa en la Fig. 6, a medida que se reduce la ventana y el intervalo de *scanning*, los tiempo de descubrimiento son más sensibles al intervalo de *advertising*. Este hecho demuestra que aunque $T_{scanInterval}$ sea igual $T_{scanWindow}$ influye proporcionalmente en el tiempo de descubrimiento respecto al valor que posean. A pesar de significar la igualdad de los valores, que el *scanner* está escuchando peticiones de descubrimiento durante todo el período, el resultado experimental arroja valores muy relevantes y beneficiosos para los escenarios de posicionamiento en interiores.

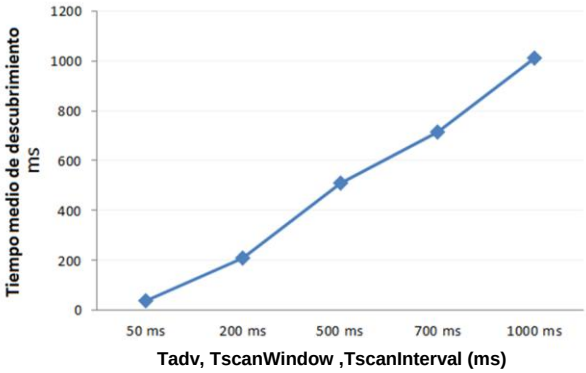


Fig. 6. Tiempo de descubrimiento en función del T_{adv}, $T_{scanInterval}$ y $T_{scanWindow}$. Los valores de todos estos parámetros son idénticos.

D. Consumo

Como se puede intuir y demuestran Liu y Chen en [8], el consumo del módulo de radio en estado de envío/recepción es del doble que en espera. Por este motivo, establecer una configuración que se ajuste a las necesidades de cada escenario puede resultar crítico.

Así, se definen tres perfiles de rendimiento en función de los requisitos de retardo de la aplicación de posicionamiento a desarrollar, mediante el establecimiento de diferentes valores para cada uno de los parámetros, como se resume en la Tabla II. En la columna "Consumo relativo" se muestra el consumo de los modos propuestos respecto al modo exhaustivo. Para el cálculo de esta relación se ha tenido en cuenta el tiempo de transmisión (T_{adv}) y recepción ($T_{scanWindow}$ y $T_{scanInterval}$) de los dispositivos durante un instante de tiempo. Analizándolo se observa la relación lineal entre el consumo y el tiempo de descubrimiento. Por ejemplo, el modo relajado consumirá 12,5 veces menos que el exhaustivo, con un retardo en el descubrimiento ~10 veces mayor.

Tabla II
PERFILES DE BÚSQUEDA

Modo	Consumo relativo	T_{adv}	$T_{scanWindow}$	$T_{scanInt.}$	$T_{descub.}$.
Exhaustivo	100%	50ms	50ms	50ms	**56ms**
Medio	20%	200ms	1000ms	1000ms	**191ms**
Relajado	8%	200ms	400ms	1000ms	**550ms**

Los resultados obtenidos nos muestran un escenario optimista en la utilización de BLE en sistemas de posicionamiento en interiores. En contextos *range-free*, con un perfil de búsqueda exhaustivo se obtienen unos valores medios de descubrimiento de 56ms, unos valores de descubrimiento excelentes y muy por debajo de los resultados ofrecidos por otras tecnologías inalámbricas. Bluetooth clásico, por ejemplo, proporciona tiempos de descubrimiento entre 3 y 10 segundos en función del número de dispositivos en el rango y unos consumos del orden de 20 veces mayor. Este hecho puede proporcionarnos una perspectiva del bajo consumo del modo relajado. Para evaluar la viabilidad de BLE en otros contextos LPS, como *range-based* utilizando el RSSI, se deberá profundizar en la obtención y procesamiento de este valor, tal y como se describe en el siguiente apartado.

E. RSSI

El valor del RSSI es uno de los más utilizados por los autores [5][9][14] y a su vez, uno de los que más controversia genera dada la poca precisión que se obtiene en interiores [8]. Por otro lado, también se ha demostrado que es a partir de los 3 metros de distancia donde se produce realmente la pérdida de precisión en la medida. Por este motivo, en este trabajo nos centraremos en su comportamiento del RSSI en distancias inferiores a 3 metros (Fig. 7).

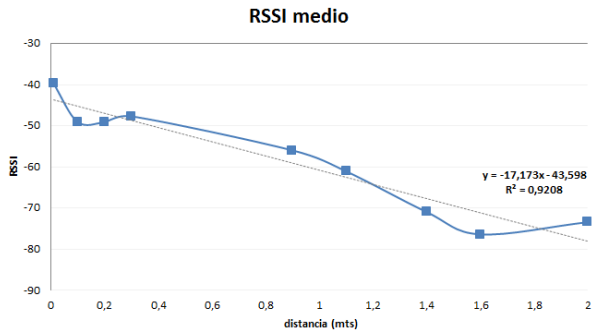


Fig. 7. Valores medios del RSSI para diferentes distancias.

Observando los valores medios de la señal, se aprecia una tendencia lineal inversa del RSSI en función de la distancia (Fig. 7), lo cual representa unos resultados bastantes aceptables. Analizando la regresión lineal realizada, en el peor de los casos obtendríamos un error de precisión de 20cm.

Sin embargo, si se analizan en profundidad los valores individuales del RSSI obtenidos para una posición estática (Fig. 8), se aprecian variaciones en el RSSI de 10dBm, en el mejor de los casos, pero de 55dBm en los casos peores (media=70dBm;desviación típica=4,63). Este hecho, trasladado al sistema de posicionamiento creado anteriormente mediante una regresión lineal, nos induciría a un nivel de error de 2 metros, coincidiendo con la resolución del sistema (Tabla II).

Como se ha descrito en el capítulo anterior, uno de los puntos fuertes de BLE es la alta la frecuencia de recepción de paquetes, y por ende, de los valores RSSI, pudiendo obtener un valor cada 56ms, lo que permite tener una frecuencia de unos 17 valores RSSI o paquetes ADV por segundo. Esta alta tasa de paquetes de *advertising* recibidos por el *scanner* permite añadir un post-procesado a este valor que mitigue la dispersión ofrecida en la obtención de este valor.

El filtro utilizado para mejorar los resultados es el de Butterworth. Este es un filtro del tipo casual que permite una transición de paso banda, de forma que en caso de encontrar una fluctuación en la señal, esta sería ignorada y en el caso de reducirse la potencia de la señal, se producirá un descenso gradual. Para la creación del filtro se han establecido los parámetros n=2 (orden del filtro) y Wn=0,007 (frecuencia de corte).

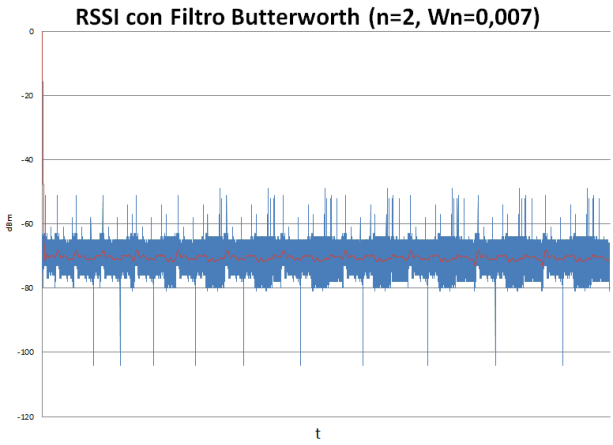


Fig. 8. Valores individuales del RSSI entre *advertiser* y scanner a una distancia de 1 metro en estático. En azul, el valor RSSI sin procesar. En rojo, tras la aplicación de un filtro Butterworth.

Como se muestra en la Fig. 8, tras la aplicación del filtro a esta señal, se obtiene una precisión mucho mayor (media=69dBm;desviación típica=0,76), la cual permite reducir la oscilación del RSSI de 55 dBm a 5,7dBm en el peor de los casos. El único inconveniente de este filtro está en el número de muestras que requiere para estabilizar los valores, 143 en este caso. Con la frecuencia alcanzada en los experimentos BLE significa que requiere de 8 segundos para obtener unos óptimos resultados con el tiempo de descubrimiento de 56ms (Tabla III).

Tabla III
COMPARACIÓN RSSI VS RSSI-FILTRADO

Modo	Media	Desv.T.
RSSI	70dBm	4,63dBm
FILTRADO	69dBm	0,76dBm

V. CONCLUSIONES

En este trabajo se ha demostrado de una forma experimental cómo los tiempos de descubrimiento obtenidos hacen de BLE una alternativa muy recomendable para las soluciones de posicionamiento en interiores. Además, la alta frecuencia de recepción de paquetes recibidos en BLE permite aplicar filtros que minimicen la distorsión del valor

del RSSI en interiores, convirtiendo este parámetro en un buen indicador de posicionamiento. Muchos sistemas de posicionamiento que utilizaban el indicador RSSI como base de la localización, podrán mejorar sus resultados migrando sus sistemas a BLE y así beneficiarse de los excelentes tiempos de descubrimiento que obtiene y de las recomendaciones de consumo y rendimiento que se plasman en este artículo. También han quedado reflejadas las grandes diferencias que existen entre los datos teóricos ofrecidos por la especificación y los resultados experimentales extraídos de este estudio experimental.

Bluetooth Low Energy, se presenta como una tecnología novedosa en el campo de soluciones LPS, por lo que debe ser explorada en profundidad, analizando el comportamiento del dispositivo con rol de *scanner* en dispositivos comerciales. En este trabajo se han podido modificar todos los parámetros de la especificación libremente, pero este hecho está limitado cuando hablamos de teléfonos inteligentes, como es el iPhone 4S/5/5S, con soporte BLE. También se deberá evaluar el impacto del número de canales *advertising* en el proceso de descubrimiento.

REFERENCIAS

[1] R. Want, A. Hopper, V. Falcão, and J. Gibbons, "The active badge location system," *ACM Transactions on Information Systems*, vol. 10, no. 1, pp. 91–102, 1992.

[2] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket location-support system," *Proceedings of the 6th annual international conference on Mobile computing and networking MobiCom 00*, vol. 2000, no. August, pp. 32–43, 2000.

[3] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "LANDMARC: Indoor Location Sensing Using Active RFID," *Wireless Networks*, vol. 10, no. 6, pp. 701–710, Nov. 2004.

[4] K. Lorincz and M. Welsh, "MoteTrack: a robust, decentralized approach to RF-based location tracking," *Personal and Ubiquitous Computing*, vol. 11, no. 6, pp. 489–503, 2006.

[5] G. Giaglis and A. Pateli, "On the potential use of mobile positioning technologies in indoor environments," pp. 413–429, 2002.

[6] G. Dedes and A. Dempster, "Indoor GPS Positioning, Challenges and Opportunities," *Proceedings of the IEEE Semiannual Vehicular Technology Conference*, 2005.

[7] D. Cho, C. Park, and S. Lee, "An assisted GPS acquisition method using L2 civil signal in weak signal environment," *Journal of Global Positioning Systems*, vol. 3, no. 1, pp. 25–31, 2004.

[8] W. Xiao, W. Ni, and Y. K. Toh, *Integrated Wi-Fi fingerprinting and inertial sensing for indoor positioning*, no. September. IEEE, 2011, pp. 1–6.

[9] Y. Wang, S. Shi, X. Yang, and A. Ma, "Bluetooth Indoor Positioning using RSSI and Least Square Estimation."

[10] J. Wang, R. V. Prasad, X. An, and I. G. M. M. Niemegeers, "A study on wireless sensor network based indoor positioning systems for context-aware applications," no. January 2010, pp. 53–70, 2012.

[11] Y. Zang, J. Wang, L. Ling, and P. Lu, "The Hybrid HMM for RSS-based Localization in Wireless Sensor Networks," *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)*, no. Iccsee, pp. 2211–2216, 2013.

[12] D. Madigan and E. Einahrawy, "Bayesian indoor positioning systems," *... 2005. 24th Annual ...*, 2005.

[13] R. Szumny and J. Modelski, "Neural Networks in Indoor Positioning Based on Power Delay Profile System," *Computer as a Tool, 2005. EUROCON ...*, vol. 00, pp. 1726–1729, 2005.

[14] A. Parameswaran, "Is RSSI a reliable parameter in sensor localization algorithms-an experimental study," 2009.

[15] J. Liu and C. Chen, "Energy Analysis of Neighbor Discovery in Bluetooth Low Energy Networks," *Nokia*.

Propuesta de modelo con redes de Petri estocásticas para optimización de una sonda de análisis de tráfico de datos

Luis Zabala, Armando Ferro, Alberto Pineda.
Networking, Quality and Security (NQaS) Research Group. Departamento de Ingeniería de Comunicaciones.
Universidad del País Vasco-Euskal Herriko Unibertsitatea (UPV/EHU).
Escuela Técnica Superior de Ingeniería de Bilbao. Alameda Urquijo s/n. 48013 Bilbao.
luis.zabala@ehu.es, armando.ferro@ehu.es, alberto.pineda@ehu.es.

***Abstract*- Packet capturing and analysis in high-speed networks, like 1-10 Gigabit Ethernet, is a challenging task, especially when applications do not permit packet loss. In this environment, the use of multiprocessor and multicore systems, as well as the parallelization of applications, is aimed at improving the performance. However, the monitoring application may even experience performance penalties when adapted to multiprocessor architectures. After observing certain anomalies in a real traffic monitoring system that runs on a multiprocessor platform, this paper presents an analytical model for that type of systems. The model, which is based on generalized stochastic Petri nets, evaluates the efficiency of the traffic capturing and analysis system depending on the hardware/software platform features.**

***Keywords* – traffic analysis system, generalized stochastic Petri nets, multiprocessor, multicore**

I. INTRODUCCIÓN

Los sistemas de monitorización de tráfico se han convertido en elementos clave dentro de la infraestructura de Internet y de las redes de datos en general. Aspectos como la seguridad, la calidad de servicio o QoS (Quality of Service), el seguimiento del tráfico, etc. están relacionados con este tipo de sistemas. Si, además, se trata de redes de alta velocidad, los requisitos de rendimiento adquieren una especial relevancia. En estos entornos donde se generan condiciones de carga de tráfico alta, el rendimiento de estos sistemas de monitorización depende, en gran medida, de las políticas y los mecanismos que gestionan cómo se ejecutan y planifican las diferentes tareas. En todo momento, el objetivo es garantizar que parámetros de rendimiento como throughput, latencia o disponibilidad del sistema sean aceptables.

Diferentes subsistemas están involucrados en el procesamiento de paquetes: la tarjeta de red y su driver, los procedimientos de captura de paquetes del sistema operativo, la aplicación de monitorización, etc. Es suficiente que uno de estos subsistemas tenga problemas de rendimiento para que conlleve una pérdida de paquetes o un resultado negativo del proceso completo. Los últimos avances en buses de sistema, tarjetas de red, procesadores multinúcleo, etc. han hecho posible la captura de tráfico en redes Gigabit o Multi-Gigabit Ethernet utilizando hardware convencional [1][2]. Sin embargo, esto último no es una tarea sencilla, puesto que se debe afinar la configuración y se requiere una optimización de los componentes hardware y software implicados en la captura de paquetes. Aunque ya existen varios estudios de rendimiento de la captura de paquetes como [3][4], no sólo es necesario evaluar el rendimiento en captura, sino que también es interesante ver cómo afecta la carga que puede tener la fase de análisis o la aplicación de monitorización en el conjunto del sistema.

Dentro de esta línea, el grupo de investigación NQaS (Networking Quality and Security) ha propuesto varias sondas de tráfico como son Adviser [5] y Ksensor [6], sometidas a distintas cargas de análisis. Mientras que Adviser es un sistema multiprocesador con un diseño en espacio de usuario, Ksensor dispone de una arquitectura, también multiprocesadora, pero que trabaja a nivel de kernel.

Este trabajo se centra en la sonda Ksensor. Primeramente, se presenta un análisis de los resultados que se han obtenido en la sonda Ksensor. Dichas observaciones han tenido lugar en distintos escenarios (variando número de procesadores, tasas de tráfico de red, cargas de análisis). Se han hecho medidas de rendimiento sobre Ksensor tales como throughput de paquetes capturados, throughput de paquetes analizados, tiempos de ejecución de hilos de captura y análisis, etc. Se han detectado ciertas anomalías en algunas de esas medidas. Por ello, se pretende proponer, en un futuro próximo, mejoras de diseño de la sonda Ksensor. En dicho proceso de mejora de rendimiento, se considera interesante el uso del modelado. Es por ello que este artículo presenta un modelo analítico basado en redes de Petri estocásticas generalizadas, que representa el comportamiento de un sistema de captura y análisis de tráfico de datos multiprocesador y estima los parámetros de rendimiento de interés con las condiciones actuales de Ksensor.

El resto del artículo está estructurado de la siguiente forma. La sección II introduce la arquitectura de Ksensor. En la sección III, se presentan los resultados experimentales de rendimiento observados en la sonda Ksensor. La sección IV proporciona el modelo de red de Petri que representa al sistema real. En la sección V, se expone la forma de resolver el modelo y evaluarlo. Finalmente, la sección VI expone las conclusiones y el trabajo futuro.

II. ARQUITECTURA DE KSENSOR.

En el trabajo previo [6] se propone la sonda Ksensor para monitorización pasiva de tráfico en redes de alta densidad.

Dicha sonda está diseñada e implementada para Linux y funciona a nivel de kernel.

Ksensor tiene un diseño multihilo para aprovechar las arquitecturas multiprocesador. Sin embargo, se han realizado determinadas pruebas que muestran un problema de rendimiento en arquitecturas de más de dos procesadores.

A. *Arquitectura de Ksensor.*

Como ya se ha introducido, Ksensor es una sonda pasiva de análisis de tráfico que funciona a nivel de kernel implementada para Linux.

En la Fig. 1 se puede observar su arquitectura. En primer lugar, cabe destacar que sólo hay dos partes del sistema que funcionan a nivel de usuario. Por un lado, el módulo Parser que es el encargado de realizar la configuración de la sonda. Por otro lado, el OPM (Offline Processing Module) que es el encargado de gestionar los resultados. La comunicación entre el espacio de usuario y el espacio de kernel se realiza a través del módulo Driver que genera un dispositivo virtual. El resto del sistema funciona a nivel de kernel.

A nivel de kernel se pueden observar tres módulos: el motor de captura, el motor de procesado de paquetes y el mapa de memoria. El motor de captura se encarga de capturar los paquetes de las tarjetas de red. El motor de procesamiento, por su parte, se encarga de realizar el análisis pertinente. El módulo de mapa de memoria es una porción de memoria compartida que contiene la lógica de análisis que aplica el módulo de procesamiento sobre los paquetes y una serie de variables.

El diseño de Ksensor está basado en hilos de kernel para adaptar el funcionamiento de dicha sonda a sistemas multiprocesador y aprovechar las características de estos sistemas para obtener un mejor rendimiento. En la Fig. 2 se pueden observar las instancias de ejecución de Ksensor para un sistema de dos procesadores.

Ksensor ejecuta dos tareas básicas. Por un lado, captura paquetes y, por otro, los procesa en base a la lógica que se almacena en la memoria compartida. La captura la realiza a través de la softirq de red y, por tanto, hace uso de los mecanismos del sistema operativo. Por tanto, hay un hilo que se encarga de capturar los paquetes y que se corresponde con la interrupción software del sistema. El hilo sólo lo ejecuta un procesador dejando los demás libres para el resto de tareas.

Por otra parte, para el procesado, Ksensor crea tantos hilos de análisis como procesadores tenga el sistema y ejecuta cada uno de los hilos en un procesador diferente.

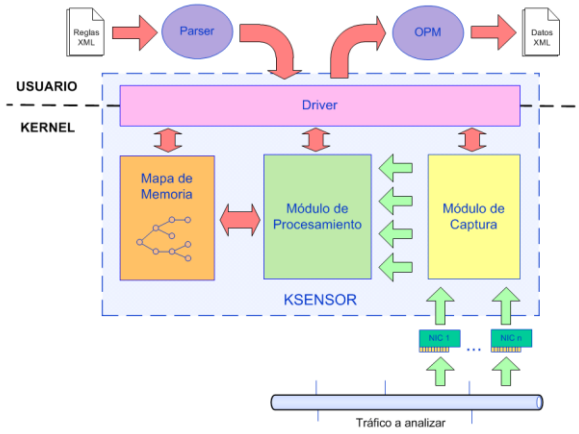


Fig. 1. Arquitectura de Ksensor.

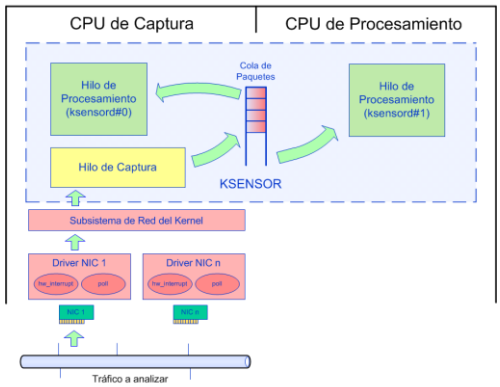


Fig. 2. Instancias de ejecución de Ksensor.

El funcionamiento básico de la sonda es el siguiente. La interrupción software se encarga de capturar los paquetes y almacenarlos en la cola de paquetes que se observa en la Fig. 2. Hay una única cola de paquetes en la que se almacenan todos los paquetes recibidos por Ksensor para ser analizados. Las instancias de análisis obtienen los paquetes de dicha cola y los analizan en base a la lógica almacenada en la memoria compartida. Como todas las instancias de análisis tienen acceso a la memoria compartida y, por tanto, a la misma lógica de análisis, no importa qué instancia analice cada paquete.

B. *Sistema de captura de Ksensor*

Por su importancia a la hora de entender el problema, en este apartado se va a explicar con un poco más de detalle el sistema de captura de paquetes que utiliza Ksensor.

La etapa de captura de Ksensor es una modificación de aquélla que emplea el kernel. El proceso de captura resumido se puede observar en la Fig. 3 para un sistema de dos procesadores.

Cuando un paquete llega a la tarjeta de red, éste se almacena en la memoria de la tarjeta. Después se copia a un buffer mediante DMA sin involucrar a la CPU. Y finalmente, se deposita el paquete en una cola común, denominada cola de análisis, de la que se alimentan los hilos de análisis. Para depositar el paquete en la cola común se hace uso de los mecanismos del subsistema de red del sistema operativo. Para ello, se ejecuta una interrupción software denominada softirq que realiza un polling sobre cada interfaz de red para extraer los paquetes. Es dentro de dicho polling donde se introducen los paquetes en la cola. Esta cola de paquetes es un recurso compartido al que tienen acceso varios hilos de kernel.

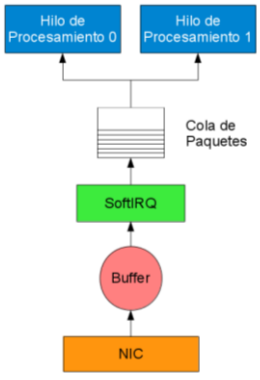


Fig. 3. Diagrama de captura de Ksensor.

Por ello y para evitar condiciones de carrera, el acceso a dicha cola está controlado por un mecanismo que permite el acceso a la cola a un hilo únicamente.

Al tratarse de un diseño para un sistema multiprocesador, se ha activado un hilo de ejecución por CPU que se encarga de extraer los paquetes de la cola y de analizarlos.

Sin embargo, tan solo una de las CPUs puede estar asociada a la tarjeta de red [7] y realizar el proceso de captura anteriormente descrito. Esto conlleva que uno de los procesadores del sistema deba repartir sus recursos entre tareas de captura y de análisis. En Ksensor dicha CPU es la denominada como cpu0, mientras que el resto de procesadores realizan tareas de análisis únicamente.

Si la tasa de llegada de paquetes es elevada, puede que Ksensor no sea capaz de procesarlos todos, en cuyo caso, cuando la cola de análisis se llena, los paquetes recibidos con posterioridad son descartados.

III. Realización de pruebas y formulación del problema.

A. *Entorno de pruebas*

En el presente trabajo se han realizado una serie de experimentos con la sonda en determinadas condiciones para obtener parámetros de rendimiento de la misma.

Para realizar los experimentos se hace uso de una arquitectura de pruebas que permite la automatización de la configuración, ejecución y recogida de datos de las pruebas. Dicha arquitectura ha sido diseñada e implementada en el grupo de investigación NQaS y ha sido presentada en el trabajo previo [8].

En la Fig. 4 se observa el esquema de red utilizado en la arquitectura de pruebas. El esquema de red se divide en dos subredes: una de gestión que se utiliza para las configuraciones y otra de captura que es la utilizada para las pruebas propiamente dichas. Conectados a esas dos subredes hay cuatro equipos. El equipo gestor es el que se encarga de enviar las configuraciones y recibir y dar formato a los resultados. El equipo inyector se encarga de inyectar tráfico sintético en la red para simular la transferencia de información de una red real. Para realizar dicha inyección se hace uso de una tarjeta Endace DAG 4.3GE [9]. Otro equipo es el que ejecuta la sonda, en este caso, Ksensor. Y, por último, el equipo receptor recibe el tráfico.

Para realizar las pruebas no se utilizan algoritmos de análisis reales. Se han implementando unas secciones de código que realizan un consumo de procesamiento fijo por paquete para facilitar los cálculos de rendimiento.

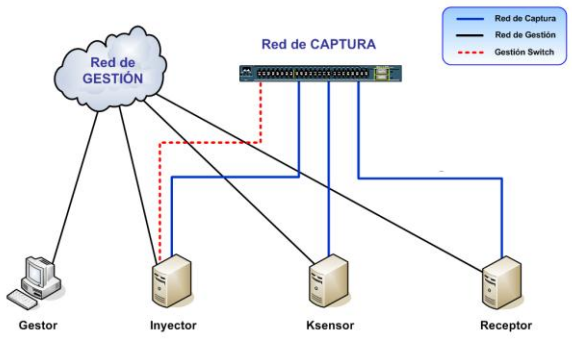


Fig. 4. Implementación real de la arquitectura de pruebas.

Se implementan cuatro posibles cargas de análisis: null, 1k, 5k y 25k. La carga denominada null no realiza ningún consumo salvo el consumo fijo de procesamiento básico del paquete. La carga denominada 1k, además del procesamiento fijo, implementa una carga de 1000 ciclos de procesamiento. Por su parte, la carga 5k realiza 5000 ciclos de procesamiento por paquete además del procesamiento fijo. Por último, la carga denominada 25k implementa una sección de código que consume 25000 ciclos de procesamiento por paquete además del consumo por procesamiento fijo.

Para este trabajo se han realizado pruebas con uno, dos y cuatro procesadores activados para una misma máquina.

B. *Análisis de resultados y formulación del problema.*

En este apartado se presentan los resultados obtenidos en las pruebas. En las Fig. 5 y 6 se pueden ver las gráficas que muestran los resultados. Como se puede observar, cada figura está compuesta por tres gráficas, una para 1 procesador, otra para 2 y otra para 4. Cada gráfica, por otra parte está formada por cuatro series de datos, una por cada carga de análisis. Cada uno de los puntos de las series de datos indica el valor medio del parámetro obtenido tras una prueba de cuatro minutos a la tasa indicada.

El throughput de captura indica el número de paquetes por segundo que captura la sonda en cada una de las pruebas a diferentes tasas.

Por otra parte, el tiempo medio de polling indica el número medio de ciclos que emplea el sistema de captura de la sonda en realizar un polling a la interfaz de red. En cada polling el sistema extrae un número determinado de paquetes denominado quota y lo introduce en la cola de análisis. Los paquetes los extrae y los introduce en la cola de uno en uno.

En cuanto a los resultados observados para throughput de captura, lo más llamativo es que el rendimiento de captura va disminuyendo cuando sube el número de procesadores. Se observa también que dicha disminución de rendimiento, que se traduce en un menor número de paquetes capturados por segundo, es dependiente de la carga de análisis. En contra de lo que cabría esperar, el rendimiento es inferior cuanto menor es la carga de análisis.

Como se ha explicado anteriormente, la cola de análisis es un recurso compartido controlado por un bloqueo que impide el acceso a la misma a más de un hilo. Los hilos, tanto de captura como de análisis, tienen que competir para acceder a dicha cola. Cuanto menor es la carga de análisis, menor es el tiempo que los hilos de análisis emplean por paquete. Esto implica que los hilos de análisis tienen una mayor frecuencia de acceso a la cola de análisis. Esto provoca un mayor número de intentos de accesos por segundo. De esta manera, es más probable que el hilo de captura quede bloqueado esperando poder acceder a la cola de análisis. Así se emplea más tiempo en capturar cada paquete y se capturan menos paquetes.

Esto se comprueba en las gráficas de la Fig. 6. Se observa que el tiempo medio de polling es mayor cuantos más procesadores haya y cuanto menor sea la carga de análisis.

Por tanto, el principal problema que se observa es que la existencia de una única cola hace que los hilos gasten mucho tiempo de procesamiento esperando a poder acceder a dicha cola.

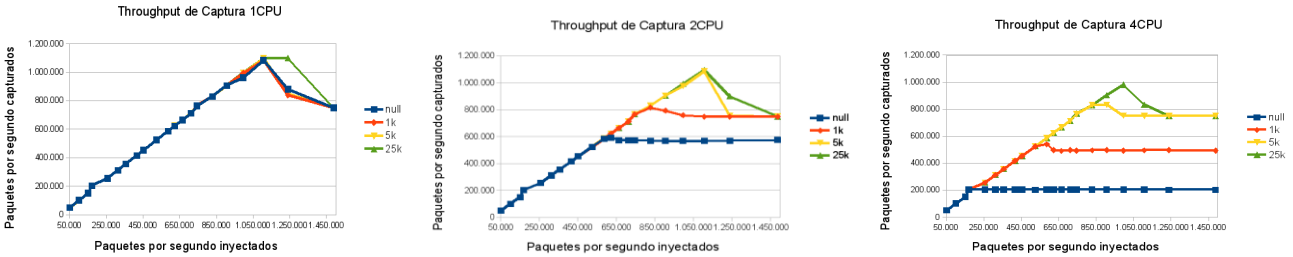


Fig. 5. Throughput de captura para 1, 2 y 4 procesadores.

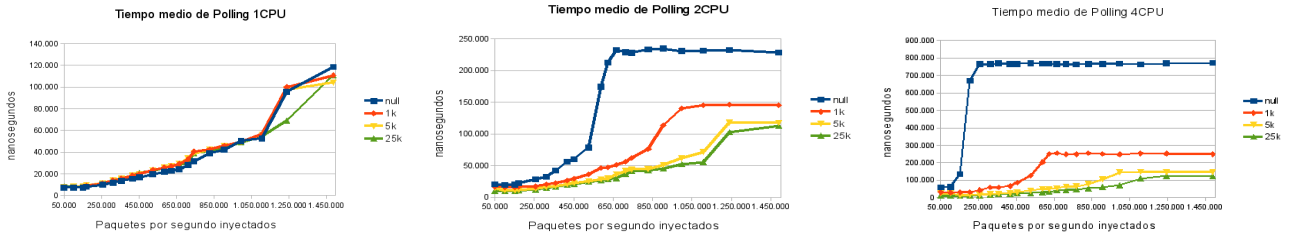


Fig. 6. Tiempo medio por polling para 1,2 y 4 procesadores.

IV. Modelado de Ksensor mediante redes de Petri

Con objeto de analizar más en detalle el comportamiento de la sonda de de tráfico, en esta sección, se va a proponer un modelo basado en redes de Petri para representar a dicho sistema de captura y análisis el sistema. El desarrollo del modelo tiene dos objetivos: por un lado, que el modelo represente fiablemente al sistema Ksensor descrito anteriormente y, por tanto, pueda evaluar su rendimiento en términos de throughput; por otro lado, que el mismo modelo pueda utilizarse para estimar rendimientos futuros de Ksensor. Estos rendimientos futuros son los que se espera obtener tras aplicar ciertas mejoras de diseño. La elección de las redes de Petri como herramienta de modelado viene dada por la gran expresividad que ofrecen y por el procedimiento de análisis relativamente sencillo.

A. *Redes de Petri*

Las redes de Petri son una técnica de modelado matemático para la descripción de sistemas discretos distribuidos [10][11][12][13]. Desarrolladas originalmente en [14], sus conceptos se han desarrollado, extendido y aplicado en diferentes áreas como son sistemas de fabricación, lenguajes de programación, protocolos y redes, estructuras hardware, sistemas embebidos, sistemas en tiempo real, evaluación de rendimiento, investigación operativa, sistemas biológicos, ingeniería de software [15], etc.

Una red de Petri es un tipo particular de grafo bipartido dirigido donde los nodos que lo componen pertenecen a dos clases distintas (lugares y transiciones), y los arcos del grafo únicamente pueden conectar nodos de distinta clase. Una red de Petri se define en base la quíntupla (P, T, F, W, M) donde:

- $P=\{p_1, p_2,\ldots, p_{np}\}$ es el conjunto de n_p lugares, representados como círculos en el grafo.
- $T=\{t_1, t_2,\ldots, t_{nt}\}$ es el conjunto de n_t transiciones, representadas como barras.
- F es un conjunto de arcos que determinan las relaciones entre los lugares y las transiciones.
- W es una función de peso que asigna un determinado peso a cada arco que relaciona lugares y transiciones.
- $M=\{m_1, m_2,\ldots, m_{np}\}$ es el estado. Cada estado asigna a cada lugar un número entero no negativo que representa el número de fichas ("tokens") en dicho lugar. Estas fichas se representan como puntos en cada lugar del grafo. Si se llama Z a una estructura de red de Petri, Z=(P, T, F, W), y se define un estado inicial M_0, se refiere como (Z, M_0) a la red de Petri con dicho estado inicial.

En el modelado del comportamiento de sistemas dinámicos, el estado de una red de Petri se ve modificado de acuerdo a las siguientes reglas:

1. Una transición t se dice que está activa si cada uno de los lugares p de entrada a t dispone al menos de w(p,t) fichas, donde w(p,t) es el peso del arco de p a t.
2. Cuando una transición activa t se dispara, retira $w(p_i,t)$ fichas de cada lugar de entrada p_i a t, y añade $w(p_j,t)$ a cada lugar de salida p_j de t.

El disparo de una transición de la red de Petri puede modificar su estado. Se define el conjunto alcanzable como el conjunto de todos los estados alcanzables a través de cualquier secuencia de disparo de transiciones a partir del estado inicial M_0.

En el modelo que se presenta en este trabajo, se utilizan un tipo concreto de redes de Petri: las redes de Petri estocásticas generalizadas o GSPN (Generalized Stochastic Petri Nets). Estas redes provienen de las redes de Petri estocásticas o SPN (Stochastic Petri Nets), que introducen el concepto de tiempo, de forma que es posible obtener parámetros de rendimiento en términos de tiempo, algo que siempre resulta útil. La introducción del término "generalizadas" se debe a que no solo se utilizan transiciones temporizadas, que representan actividades que requieren cierto tiempo para su realización, sino que también aparecen transiciones inmediatas, como mecanismo para representar condiciones lógicas. Ésta es una de las características clave que permiten realizar el modelado con un nivel de detalle y expresividad elevado, sin hacer más complejo el proceso.

Las transiciones temporizadas se caracterizan por su tasa de servicio, μ por ejemplo, mientras que las transiciones inmediatas se caracterizan por un determinado peso, ω. Dado

que estas últimas se utilizan principalmente en bifurcaciones, su función es la de determinar la probabilidad de tomar una determinada rama de ejecución u otra. Dadas dos transiciones inmediatas en paralelo (condición de bifurcación) caracterizadas por sus pesos ω_1 y ω_2, la probabilidad de seguir por la rama asociada a la transición 1 es $\omega_1/(\omega_1+\omega_2)$, mientras que la probabilidad de seguir por la segunda rama es $\omega_2/(\omega_1+\omega_2)$.

B. Modelo para la sonda de tráfico

El modelo que se propone en este trabajo es la red de Petri con el estado inicial que se ve en la Fig. 7. Corresponde a un sistema de monitorización de tráfico con arquitectura multiprocesador. En concreto, muestra el ejemplo de una sonda con 4 procesadores, uno de los cuales (cpu0) se dedica a tareas de captura y análisis, mientras que los otros tres, (cpu1, cpu2 y cpu3) se dedican en exclusiva a la fase de análisis.

El modelo está compuesto por lugares y transiciones que, según la función que representan, pueden agruparse en:

- Elementos sobre la disponibilidad de procesadores.
- Elementos de la llegada de paquetes al sistema.
- Elementos relacionados con la softirq que se ejecuta en el procesador cpu0.
- Elementos de la fase de análisis del procesador cpu0.
- Elementos relacionados con la fase de análisis del resto de procesadores (cpu1-cpu3).
- Elementos de control de buffers finitos y del acceso al recurso compartido que es la cola de análisis.

A continuación, se procederá a describir cada uno de estos grupos.

C. Disponibilidad de los procesadores del sistema

En primer lugar, se presentan los lugares que representan estados en los que los procesadores del sistema (cpu0, cpu1, cpu2, cpu3) están disponibles. Es decir, cuando haya una ficha en esos lugares, se indica que el correspondiente procesador está disponible.

Tabla I
ELEMENTOS QUE MODELAN LA DISPONIBILIDAD DE PROCESADORES

Lugar	Descripción
P3_Cpu0Available	Disponibilidad del procesador cpu0
P15_Cpu1Available	Disponibilidad del procesador cpu1
P19_Cpu2Available	Disponibilidad del procesador cpu2
P23_Cpu3Available	Disponibilidad del procesador cpu3

La tabla I muestra el listado de lugares que entran en esta clasificación. En este trabajo se entiende que un procesador está disponible siempre que no esté ejecutando ni un hilo de captura ni un hilo de análisis.

D. Llegada de paquetes al sistema

Esta parte del modelo está compuesta por los lugares y transiciones listados en la tabla II. El lugar "*P1 CaptureBuffer"* representa al buffer donde se almacenan los paquetes que provienen de la tarjeta de red. Esta llegada de paquetes al buffer se produce con una tasa λ que, en el modelo, corresponde a la transición temporal *"T1 PackArrival"*. Siempre que haya fichas en el lugar "*P2 Counter"*, estará activa la transición *T1* y habrá llegada de paquetes al buffer con tasa λ. En cambio, si se agotan las fichas en el lugar *P2*, esta situación modela el estado de bloqueo del buffer de captura ya que éste habrá llegado a su máxima capacidad (en el ejemplo, 512 paquetes).

En situación de bloqueo, se produce el rechazo de paquetes. En el modelo, esto no conlleva ningún movimiento de fichas, pero sí es posible medir el flujo de los paquetes rechazados λP_B (paquetes/seg) siendo P_B la probabilidad de bloqueo que equivale a la probabilidad de que no haya ninguna ficha en el lugar *P2*. En consecuencia, el lugar *P2* es un contador que controla la ocupación del buffer de captura. Se inicializa con tantas fichas como el número máximo de paquetes que admite el buffer. Cada vez que se produce el disparo de la transición T1 (llegada de un paquete) se decrementa en uno el contador *P2*. Por el contrario, cuando dispara la transición *"T2 SoftirqPoll"*, aumenta en uno.

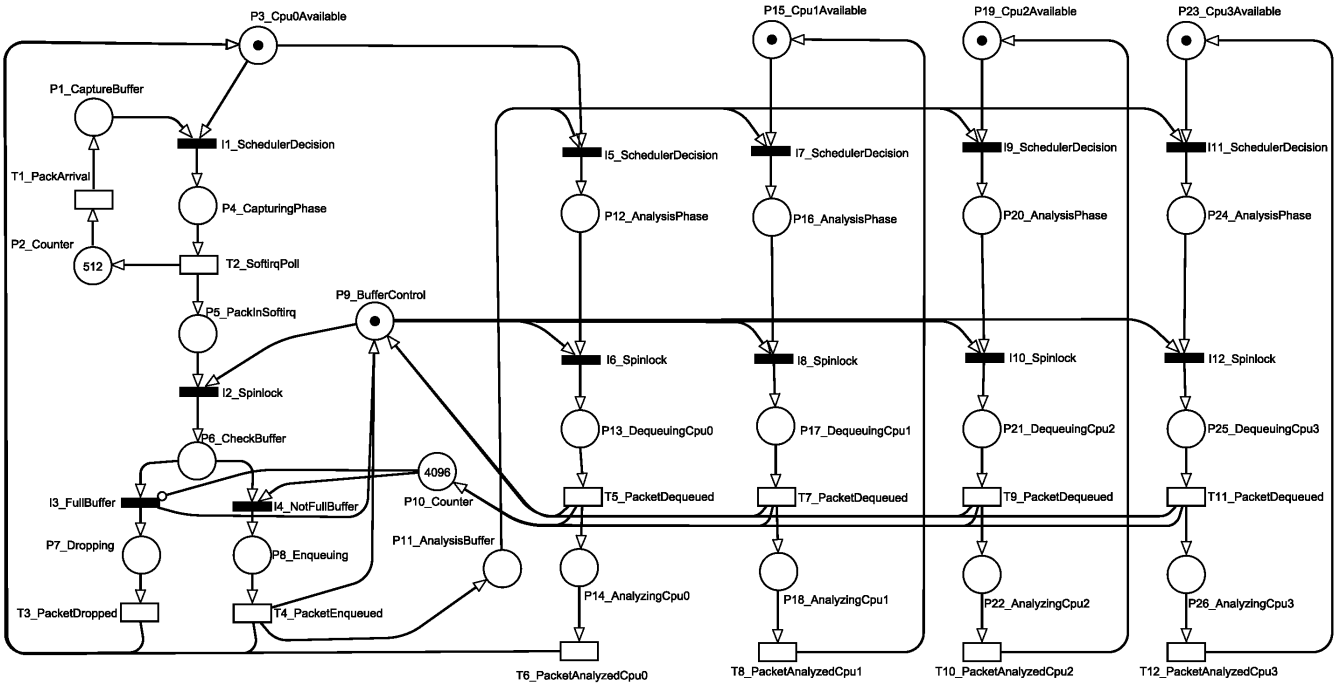


Fig. 7. Modelo de redes de Petri para el sistema de captura y análisis de tráfico.

Tabla II
ELEMENTOS QUE MODELAN LA LLEGADA DE PAQUETES AL SISTEMA

Lugar	Descripción
P1_CaptureBuffer	Buffer de captura con capacidad máxima de 512 paquetes.
P2_Counter	Control de espacio disponible en buffer.

Transición	Descripción
T1_PackArrival	Transición temporal que modela la llegada de paquetes con tasa λ.

E. Ejecución de softirq (fase de captura de paquetes)

Esta parte del modelo representa la ejecución de la softirq o hilo de captura que tiene lugar en el procesador cpu0. Básicamente está compuesta por la extracción de paquetes almacenados en el buffer DMA, el acceso al recurso compartido que constituye la cola de análisis y la posterior introducción de esos paquetes "capturados" en la cola de análisis. Si el buffer de análisis está lleno, el paquete capturado será descartado ("packet dropped"). Los lugares y transiciones del modelo relacionados con la softirq están detallados en la tabla III.

En el modelo de la Fig. 7, el hilo de captura comienza con el disparo de la transición inmediata *"I1 SchedulerDecision"*. Esto se producirá si se dan dos condiciones: por un lado, debe estar disponible la cpu0 (ficha en *P3*) y por otro debe haber al menos un paquete en el buffer DMA (presencia de alguna ficha en *P1*). Mencionar que *I1* puede entrar en conflicto con la transición inmediata *I5*, que, como se explicará más adelante, está relacionada con la ejecución del hilo de análisis por parte de la cpu0. Esto ocurrirá si se dan las condiciones para activar al mismo tiempo las dos transiciones. Esta condición de bifurcación del lugar *P3* se resuelve con la asignación de pesos ω_{I1} y ω_{I5}, para *I1* e *I5* respectivamente, cuyos valores dependen del planificador del sistema. Así, la probabilidad de que una ficha salga de *P3* y active *I1* será $\omega_{I1}/(\omega_{I1}+\omega_{I5})$, mientras que $\omega_{I5}/(\omega_{I1}+\omega_{I5})$ será la de activar *I5*.

El siguiente elemento de la softirq es el lugar *"P4 CapturingPhase"* que, cuando hay una ficha en él, indica que la cpu0 está en la primera parte del hilo de captura, esto es, en el polling extrayendo un paquete del buffer DMA. La transición temporal *"T2_SoftirqPoll"* representa el tiempo que lleva esa operación de extracción. *T2* se activará siempre que haya ficha en *P4* y tiene dos salidas: por un lado, una ficha pasa al lugar *"P5 PackInSoftirq"* para continuar la ejecución de la softirq; por otro lado, una ficha pasa al contador *P2* para incrementar su valor en uno ya que se ha acabado la operación de extracción de paquete, se ha liberado su espacio de memoria y, por tanto, hay una posición libre nueva en el buffer P1.

A continuación, el hilo de captura debe acceder a la cola de análisis para introducir en ella el paquete extraído del buffer DMA. Éste es un acceso a un recurso compartido, que se producirá si se activa la transición inmediata *"I2_Spinlock"*. Esto se producirá si se dan dos condiciones: que haya ficha en *P5* y en *"P9_BufferControl"*. Si no se dan esas dos condiciones a la vez, la ficha permanecerá en espera en P5. Como se explicará más adelante, *P9* es un lugar cuya función es asegurar que sólo se permita el acceso de un hilo (bien sea de captura o de análisis) al recurso compartido.

Tabla III
ELEMENTOS QUE MODELAN LA SOFTIRQ (FASE DE CAPTURA DE PAQUETES)

Lugar	Descripción
P4_Capturing Phase	Cpu0 en el inicio de la fase de captura, extrayendo paquete del buffer DMA.
P5_PackInSoftIRQ	Paquete extraído y pendiente de ser introducido en la cola de análisis.
P6_CheckBuffer	Cpu0 comprobando si hay espacio disponible en la cola de análisis (operación dentro de la sección crítica).
P7_Dropping	Descarte de paquete, dado que no hay espacio en la cola de análisis
P8_Enqueuing	Introducción de paquete en la cola de análisis, ya que sí hay espacio para él (operación dentro de la sección crítica).

Transición	Descripción
I1_SchedulerDecision	Transición inmediata que representa el arranque del hilo de captura por decisión del planificador del sistema.
T2_SoftirqPoll	Tiempo de extracción de paquete del buffer DMA.
I2_Spinlock	Transición inmediata que controla el acceso del hilo de captura a la sección crítica de manera única.
I3_FullBuffer	Transición inmediata que comprueba si está lleno el buffer de análisis.
I4_NotFullBuffer	Transición inmediata que comprueba si no está lleno el buffer de análisis.
T3_PacketDropped	Tiempo de descarte de un paquete capturado en el polling de la softirq.
T4_PacketEnqueued	Tiempo de encolado o de introducción de paquete en el buffer de análisis.

La ejecución de la sección crítica por parte del hilo de captura de la cpu0 comienza con el lugar *"P6_CheckBuffer"*, para comprobar si hay o no hay espacio disponible para un nuevo paquete en la cola de análisis. A *P6* le sucede una condición de bifurcación con las transiciones inmediatas *"I3 FullBuffer"* e *"I4 NotFullBuffer"*. No hay conflicto entre *I3* e *I4* porque si una se cumple la otra no y viceversa. Ambas transiciones dependen del estado del contador "P10 Counter" que controla el estado del buffer de análisis. Si este buffer está lleno, se activa *I3*, se sale de la sección crítica, pasa una ficha al lugar P9 y otra al lugar *"P7 Dropping"*. Éste representa a la operación de descarte de paquete capturado y la transición temporal *"T3 PacketDropped"* modela el tiempo que lleva esa operación de descarte. Si, por el contrario, el buffer de análisis no está lleno y se activa *I4*, se pasará al lugar "P8 Enqueuing" donde se realiza la operación de encolado o introducción de paquete en la cola de análisis.

Finalmente, la transición temporal *"T4 PacketEnqueued"* representa el tiempo que lleva la operación de encolado. Cuando acaba *T4*, una ficha que representa el paquete capturado pasa al lugar que representa al buffer de análisis que es el *"P11 AnalysisBuffer"*, otra ficha pasa al lugar *P9* para indicar que ha terminado el acceso a la sección crítica y una tercera ficha pasa al lugar *P3* para indicar que acaba la parte del hilo de captura relacionada con este paquete.

F. Recurso compartido y acceso al mismo

En este sistema se dispone de un recurso compartido que es el buffer de análisis. En el modelo, este elemento fundamental está representado por el lugar "*P11 AnalysisBuffer*". En él entran fichas provenientes de la transición *T4* del hilo de captura y salen fichas a través de las transiciones *I5*, *I7*, *I9* ó *I11* de los hilos de análisis.

Tabla IV
ELEMENTOS QUE MODELAN EL ACCESO AL RECURSO COMPARTIDO

Lugar	Descripción
P11_AnalysisBuffer	Recurso compartido. Buffer de análisis con capacidad para 4096 paquetes.
P10_Counter	Control de espacio disponible en el recurso compartido.
P9_BufferControl	Control de acceso a la sección crítica del recurso compartido.

Sin embargo, no menos importante es el mecanismo de acceso al recurso compartido, de modo que se asegure la integridad de los datos. Dentro de la red de Petri, este mecanismo de control se implementa con el lugar denominado *"P9 BufferControl"*. Éste determina qué hilo de captura o análisis accede a la sección crítica y evita que los lugares de la operación de encolado (*P6* y *P8*) y los de desencolado (*P13*, *P17*, *P21* y *P25*) contengan fichas simultáneamente. Un hilo que accede a la sección crítica "coge" la ficha de P9 y bloquea al resto de los hilos que intenten acceder. Cuando termina de ejecutar la sección crítica, "devuelve" la ficha colocándola de nuevo en el lugar P9 y permite que otros hilos accedan al recurso compartido.

Por último, dentro de este grupo, se encuentra el lugar *"P10 Counter"* que controla el espacio disponible en el buffer de análisis. En el ejemplo, la capacidad máxima del buffer de análisis es 4096. Si este buffer está vacío, el contador *P10* tendrá 4096 fichas y, si el buffer está lleno, ocurrirá lo contrario: no habrá ninguna ficha en *P10*. Como se ha explicado anteriormente, *P10* se utiliza para comprobar las condiciones de las transiciones *I3* e *I4*. El valor de este contador se decrementa con la introducción de paquetes en la cola de análisis y su valor se incrementa cada vez que hay un desencolado de paquete por parte de los hilos de análisis.

La tabla IV recoge los elementos de la Fig. 7 que pertenecen al grupo de este subapartado.

G. Fase de análisis en el procesador cpu0

El hilo de análisis de la cpu0 se inicia cuando se dispara la transición inmediata *"I5 SchedulerDecision"*. *I5* disparará cuando haya paquetes para analizar en el buffer de análisis y la cpu0 esté disponible. Como ya se ha explicado anteriormente, *I5* puede entrar en conflicto con *I1* y esto se resuelve con la asignación de pesos ω_{I1} y ω_{I5}.

Tras la activación de *I5*, una ficha pasa al lugar *"P12 AnalysisPhase"*. Éste simplemente indica que la cpu0 ha comenzado la ejecución del hilo de análisis.

El siguiente paso es el acceso al recurso compartido para proceder con el desencolado de un paquete. Dicho acceso se dará si se activa la transición inmediata *"I6 Spinlock"*. Para ello, además de la ficha de *P12* también debe haber otra ficha en *P9* que controla el acceso al recurso compartido. Si eso sucede, se pasa al lugar *"P13 DequeuingCpu0"* que modela la operación de desencolado dentro de la sección crítica. La transición temporal *"T5 PacketDequeued"* representa el tiempo que lleva la operación de desencolado. Cuando termina esta operación salen tres fichas de la transición T5: una hacia el lugar *"P14 AnalyzingCpu0"* para seguir con el tratamiento del paquete; una segunda hacia el lugar P9, de forma que se habilita el permiso para accesos futuros al recurso compartido; una tercera hacia el contador P10, ya que se ha extraído un paquete del buffer de análisis y es necesario actualizar dicho contador.

Tabla V
ELEMENTOS QUE MODELAN LA FASE DE ANÁLISIS DE CPU0

Lugar	Descripción
P12_AnalysisPhase	Hilo de análisis iniciado en cpu0.
P13_DequeuingCpu0	Desencolado de paquete por cpu0 (operación dentro de sección crítica).
P14_AnalyzingCpu0	Análisis de paquete por cpu0.

Transición	Descripción
I5_SchedulerDecision	Arranque de hilo de análisis en cpu1 (si hay paquete pendiente de analizar).
I6_Spinlock	Acceso de cpu1 al recurso compartido (cola de análisis) de forma controlada.
T5_PacketDequeued	Tiempo de desencolado de paquete.
T6_PacketAnalyzedCpu0	Tiempo de análisis de paquete.

Para acabar el hilo de análisis, se tienen el lugar *"P18 AnalyzingCpu1",* que representa a la operación propiamente de análisis de un paquete, y la transición temporal *"T6 PacketAnalyzedCpu0"* que es el tiempo que se emplea en analizar cada paquete. Cuando termina la transición *T6*, una ficha pasa de *T6* al lugar P3 y la cpu0 volverá a estar disponible para ejecutar otra vez el hilo de análisis o el de captura según lo que disponga el planificador.

La tabla V detalla los elementos explicados en este subapartado.

H. Fase de análisis en el resto de procesadores

El resto de procesadores (cpu1, cpu2, cpu3, en el ejemplo) se dedican únicamente a tareas de análisis. Los lugares y transiciones de los hilos de análisis de cada uno de estos procesadores son análogos a los de la tabla V y son los siguientes de la Fig.7:

- I7, P16, I8, P17, T7, P18 y T8 para el hilo de análisis de la cpu1.
- I9, P20, I10, P21, T9, P22 y T10 para el hilo de análisis de la cpu2.
- I11, P24, I12, P25, T11, P26 y T12 para el hilo de análisis de la cpu3.

Cabe mencionar que es posible que haya conflicto entre las transiciones inmediatas I5, I7, I9 e I11 a la hora de acceder al recurso compartido. Estos conflictos se resuelven según la asignación de los pesos ω_{I5}, ω_{I7}, ω_{I9} y ω_{I11}. Dado que, en el sistema real, los cuatro hilos de análisis compiten en igualdad de condiciones, la asignación de estos pesos será $\omega_{I5}=\omega_{I7}=\omega_{I9}=\omega_{I11}$.

V. EVALUACIÓN DEL MODELO

A. Resolución del modelo: análisis vs simulación

El modelo propuesto es una red GSPN con un estado inicial M_0, al que se puede asociar un proceso estocástico semi-markoviano en tiempo continuo, con un espacio de estados finito. Su resolución puede plantearse de manera analítica reduciendo el modelo GSPN a una red SPN sin transiciones inmediatas. A continuación, debido a que los sistemas SPN son isomórficos a una cadena de Markov de tiempo continuo, se puede analizar el modelo de manera tradicional. Además, ya existen algoritmos que construyen automáticamente el generador infinitesimal de la cadena de Markov isomórfica. A pesar de eso, cuando la red de Petri tiene un espacio de estados muy grande (el espacio de estados crece exponencialmente) resulta inviable aplicar

algoritmos analíticos o numéricos y se recurre a la simulación. En nuestro caso, por esa misma razón, también hemos utilizado la opción de la simulación para evaluar el modelo. Existen numerosas herramientas de simulación de redes de Petri. Entre ellas, hemos elegido TimeNET [16] debido a que este software permite introducir en las transiciones temporizadas tanto distribuciones exponenciales (que es lo habitual) como deterministas.

B. *Resultados obtenidos del modelo*

Tal y como se ha mencionado, utilizando el software TimeNET e introduciendo los parámetros de entrada del modelo (tiempos para las transiciones temporales y pesos para las transiciones inmediatas) se ha evaluado el modelo y se han obtenido resultados de throughput de captura, throughput de análisis por CPU, tasa de pérdidas en DMA, tasa de pérdidas en el buffer de análisis y utilización de CPU en captura y análisis. Indicar que los parámetros de entrada introducidos se han obtenido de datos experimentales [8].

La conclusión de los resultados obtenidos es la siguiente. El modelo de red de Petri que se presenta en este trabajo tiene una buena respuesta para bajas tasas de recepción de paquetes por parte de la sonda. A medida que la tasa de datos aumenta, resulta más complicado el ajuste de algunos parámetros de entrada del modelo. En concreto, los pesos ω_{I1} y ω_{I5} de las transiciones inmediatas *I1* e *I5* deben ser asignados correctamente para modelar el procedimiento de budget de la softirq. Con tasas no altas, se modela fácilmente asignando $\omega_{I1}=\omega_{I5}$, ya que nunca se agota el budget. Por el contrario, en el caso de tasas altas, la asignación debe tener en cuenta la proporción existente entre el número de paquetes tratados en la softirq y el número de paquetes analizados entre el final de una softirq y el inicio de la siguiente. Tomando medidas experimentales de estos parámetros de la sonda real, se ha asignado valores a los pesos ω_{I1} y ω_{I5} y, finalmente, se ha conseguido ajustar el modelo para el régimen de tasas altas de datos. La Fig. 8 muestra un ejemplo donde se pueden comparar throughputs de captura obtenidos mediante el modelo y mediante la sonda real.

VI. Conclusiones

Este artículo plantea un modelo basado en redes de Petri que representa una sonda de tráfico de datos. El modelado con redes de Petri es satisfactorio ya que nos permite introducir diferentes interacciones que tenemos en el sistema real como son: procesamiento secuencial y paralelo, concurrencia, existencia de recursos limitados, exclusión mutua en acceso a recurso compartido.

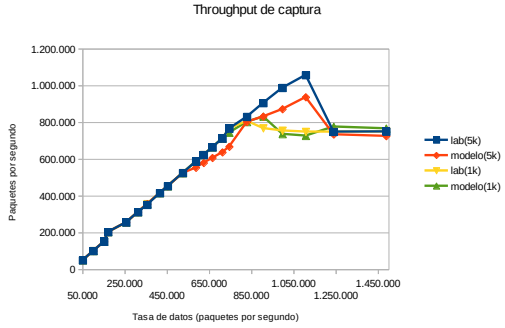


Fig. 8. Resultados de throughputs obtenidos mediante el modelo y en la sonda real para el caso de 2 CPUs y cargas de análisis de 1k y 5k.

Dado que la red de Petri planteada tiene un espacio de estados muy grande, se ha optado por evaluar el modelo mediante simulación. Aunque ha habido dificultades para ajustar ciertos parámetros de entrada del modelo (ω_{I1} y ω_{I5}) que están relacionados con el planificador del sistema, al final, se han obtenido unos resultados aceptables.

Como trabajo futuro se plantea la introducción de mejoras en la sonda Ksensor tales como la actualización del kernel Linux de modo que se puedan utilizar características nuevas de la captura de paquetes como son GRO (Generic Receive Offload) y RPS (Receive Packet Steering), la disminución del tiempo de acceso a la sección crítica o la mejora del proceso de desencolado. Así mismo se espera que el modelo propuesto sea válido para estimar el rendimiento de la sonda con estas nuevas modificaciones.

Agradecimientos

El trabajo que aquí se presenta está realizado en el marco del proyecto "VM.@T-Máquinas virtuales para el análisis de tráfico en redes de alta capacidad" financiado por el Gobierno Vasco en la convocatoria SAIOTEK 2012.

Referencias

[1] F. Schneider, J. Wallerich, A. Feldmann, “Packet Capture in 10-Gigabit Ethernet Environments Using Contemporary Commodity Hardware”. En PAM 2007. Louvain-la-neuve, Bélgica, Abril 2007.

[2] L. Rizzo, L. Deri, A. Cardigliano, “10 Gbit/s line rate packet processing using commodity hardware: survey and new proposals”. Online: http://luca.ntop.org/10g.pdf (2012).

[3] A. Fiveg, “Ringmap Capturing Stack for High Performance Packet Capturing”. De http://wiki.freebsd.org/AlexandreFiveg, 2010.

[4] F. Fusco F., L. Deri, "High Speed Network Traffic Analysis with Commodity Multi-core Systems". En IMC 2010, Melbourne, Australia, Noviembre 2010.

[5] A. Ferro, F. Liberal, A. Muñoz, I. Delgado, A. Beaumont, “Software architecture based on multiprocessor platform to apply complex intrusion detection techniques”. En CCST’05, Las Palmas, Octubre 2005.

[6] A. Muñoz, A. Ferro, F. Liberal, J. Lopez, “A kernel-level monitor over multiprocessor architectures for high-performance network analysis with commodity hardware”. En SensorComm 2007. Valencia, Octubre 2007.

[7] C. Benvenuti. “Understanding Linux Network Internals”. O'Reilly Media, 2005.

[8] A. Pineda, L. Zabala, A. Ferro, “Network Architecture to Automatically Test Traffic Monitoring Systems”. En MIC-CSP2012, Barcelona, Abril, 2012.

[9] Endace DAG Cards Enterprise Network Monitoring Tools, http://www.endace.com (2013).

[10] A. Bobbio, “System modeling with Petri nets. Systems Reliability Assessment”, Ed. Springer, pp. 103-143, 1990.

[11] G. Balbo, J.M. Colom, G. Rozenberg., “Introductory tutorial on Petri nets”. En 21st International Conference on Application and Theory of Petri Nets, Aarhus, Dinamarca, 2000.

[12] L.K. John, L. Eeckhout, “Performance evaluation and benchmarking”. CRC Press, 2006.

[13] T. Murata, “Petri nets: Properties, analysis and applications”. Proceedings of the IEEE, Vol. 77, nº 4, pp. 541-580, 1989.

[14] C.A. Petri, “Kommunikation mit Automaten”. Dissertation. Bonn: Institut für Instrumentelle Mathematik, Schriften des IIM Nr. 2, 1962.

[15] S.M. Halawani, Z.M. Sidek, "Visualization of Aho Corasick Algorithm Using Z-eves and Petri Net". En European Journal of Scientific Research, vol. 45, pp. 37-46, 2010.

[16] A. Zimmermann, "Modeling and evaluation of stochastic Petri nets with TimeNET 4.1". En VALUETOOLS 2012. Cargèse, Francia, Octubre 2012.

Comparativa entre distribuciones α-estables para modelar tasas de transferencia obtenidas a partir de registros de SNMP y NetFlow

Matteo Stoppa[1], Jorge E. López de Vergara[1],
Federico Simmross-Wattenberg[2], José Luis García-Dorado[1]
[1]Escuela Politécnica Superior,
Universidad Autónoma de Madrid
28049 Campus de Cantoblanco, Madrid.
[2]ETSI Telecomunicación,
Universidad de Valladolid,
47011 Campus Miguel Delibes, Valladolid.
ing.stoppamatteo@gmail.com, jorge.lopez_vergara@uam.es, fedsim@tel.uva.es, jl.garcia@uam.es.

***Resumen*— Este trabajo evalúa los parámetros de una distribución α-estable para modelar el tráfico en una red a partir de la información agregada generada por el protocolo Simple Network Management Protocol (SNMP) y los flujos de red generados por el protocolo NetFlow de Cisco. Además, se presenta una comparación entre la información almacenada por los dos protocolos, los procesos necesarios para efectuar esta comparación, así como el cálculo de los errores entre las muestras disponibles y la distribución calculada a partir de los resultantes parámetros, el error entre las distribuciones empíricas de cada traza y finalmente un error conjunto con la finalidad de ver cuál de los dos protocolos proporciona informaciones que mejor se adaptan a un modelo estadístico de tipo α-estable. Como conclusión, se observa que es posible obtener resultados semejantes, incluso con registros muestreados de NetFlow. Esto permite aprovechar este protocolo para estudiar las desviaciones del comportamiento habitual del tráfico de la red, reduciendo la carga que se pueda introducir en el *router*.**

***Palabras Clave*— Distribución α-estable, SNMP, NetFlow**

I. INTRODUCCIÓN

La gestión de red siempre ha sido una tarea muy compleja y un campo de investigación abierto. Además, a medida que crece el tráfico en la red este trabajo se puede volver más difícil. También hay que considerar la posibilidad de tener que enfrentarse a anomalías o ataques que intentan violar la privacidad de datos sensibles o causar interrupciones de servicio. En este último caso, la gestión debería comprender un sistema de monitorización con el objetivo de detectar rápidamente la anomalía/intrusión para poder resolver el problema.

Con el avance tecnológico y la mayor potencia de cálculo y almacenamiento de los equipos de red, aumenta la disponibilidad de información que es posible tener en cuenta para las tareas de monitorización y gestión de redes. Inicialmente, los equipos han venido utilizando el protocolo SNMP (*Simple Network Management Protocol*) [1] para obtener esta información por parte de un gestor. No obstante, dicha información suele entregarse de manera agregada (e.g., bytes que han entrado o salido por una interfaz de red). En los últimos años se han planteado otras posibilidades, como NetFlow [2], que proporciona un gran volumen de información del tráfico que atraviesa la red, agregando la información en flujos.

NetFlow es un protocolo abierto desarrollado por Cisco para recoger datos de tráfico IP, que está incluido en los *routers* y en los conmutadores de Cisco y de otros fabricantes. NetFlow permite obtener información relativa al tráfico de red como un flujo de datos con origen, destino y protocolo en común. Por cada flujo NetFlow, se registra la fecha y hora de inicio y fin, los puertos y direcciones IP del remitente y del destinatario, el tipo de protocolo utilizado por el tráfico, el tipo de servicio proporcionado y las interfaces de red. De esta forma, la monitorización puede hacer uso de una información más detallada respecto a la que se puede obtener mediante SNMP.

El uso de NetFlow permite incluso ampliar de forma notable el conjunto de anomalías y ataques que se pueden detectar. Utilizando la información de SNMP se pueden detectar solo ataques que afectan de forma evidente al número de bytes que pasan por la red. Por contra, en un sistema basado en flujos de red se puede combinar la información del número de bytes con otros datos, tales como el número de flujos y la media de bytes y paquetes por flujo, así como las direcciones IP y puertos involucrados en dichos flujos. De esta manera, con técnicas como las que se encuentran descritas en [3], se pueden detectar varias clases de ataques distintos, aunque esto tenga un coste computacional más elevado a la hora de utilizar los datos, pero siempre inferior al estudio del tráfico a nivel de paquete y cargas útiles. Afortunadamente los equipos en los que se realizan los algoritmos de detección no son los mismos que los dispositivos de red, con lo cual pueden ser bastante más potentes, aunque tampoco hay que infravalorar el tiempo de ejecución del estudio de los datos por cada una de las ventanas temporales en las que se divida la monitorización, que podría llegar a resultar demasiado largo para un sistema efectivamente viable.

Para modelar información relativa al ancho de banda consumido en un enlace a partir de los registros de NetFlow, cara a detectar tráfico anómalo, se va a usar un modelo estadístico, concretamente una distribución α-estable, el cual, como se puede ver en [4], tiene la ventaja de adaptarse bien a la alta variabilidad del tráfico de red, y permite identificar y distinguir cuándo el tráfico sigue un patrón normal o anómalo (por ejemplo, debido a un ataque de denegación de servicio) a partir de los parámetros que caractericen la distribución en cada momento. Como a lo largo del tiempo la cantidad de

datos que pasan por la red varía sensiblemente, será muy importante utilizar ventanas de tiempo en las cuales los parámetros del modelo se puedan considerar estacionarios y volver a calcular dichos parámetros para cada ventana de tiempo. Una vez calculados los parámetros será también posible poder comparar los resultados obtenidos con los encontrados a partir de registros de tráfico agregado en la misma red y en el mismo periodo temporal. De esta forma se podrá determinar la eventual mejora debida al uso de un conjunto de información más detallada.

El resto de este artículo se estructura de la siguiente manera: en la sección siguiente se da una visión general sobre las distribuciones α-estables. A continuación se presentan las características de los registros de SNMP y NetFlow empleados en la comparación. Posteriormente se explica el método empleado para sincronizar los registros. Tras ello, se muestra la necesidad de filtrar la serie temporal obtenida con los registros de NetFlow para obtener mejores resultados. Después se evalúan los parámetros estadísticos en ambos casos, así como los errores obtenidos. Finalmente se presenta un conjunto de conclusiones y se indican líneas de continuación.

II. Distribuciones α-estables

Las distribuciones α-estables se pueden ver como un superconjunto de la distribución gaussiana y surgen como solución al teorema del límite central cuando se admite la posibilidad de que los momentos de segundo orden no existan (es decir, cuando se considera que la varianza puede ser infinita) [5]. En términos de sucesos reales, es obvio que éste nunca será el caso; sin embargo, en múltiples disciplinas, tan dispares como la hidrología, la física de partículas o las telecomunicaciones, se observa que un modelo de varianza infinita se adapta mucho mejor a los datos que otros modelos existentes con varianza finita. Este fenómeno se suele denominar "alta variabilidad" o "efecto Noah" (Noé). El tráfico de red agregado es un ejemplo de este tipo de sucesos [6].

Esta familia de distribuciones ha sido descrita con detalle en la literatura [7]. No obstante, se mencionan aquí algunas de sus propiedades de especial interés para este trabajo.

Las distribuciones α-estables están caracterizadas por cuatro parámetros: α, β, γ y δ (aunque algunos autores denominan a estos últimos σ y μ). α puede variar en el intervalo (0,2] y determina la forma de la curva: desde gaussiana, cuando α=2, hasta una distribución degenerada cuando α→0. β pertenece al intervalo [-1,1] y determina la asimetría de la función de densidad de probabilidad: -1 indica asimetría total hacia la izquierda, 0 simetría y +1 asimetría total hacia la derecha. γ y δ son los parámetros análogos a la desviación típica y la media de las gaussianas, respectivamente (de ahí que algunos autores les den este mismo nombre) pero γ nunca coincide con la desviación típica, ni siquiera en el caso α=2, mientras que δ coincide con la media solamente en caso de que ésta exista (lo cual sucede cuando α>1). Estos cuatro parámetros, forma, asimetría, dispersión y localización, confieren a las distribuciones α-estables una gran flexibilidad, pero su capacidad para adaptarse a multitud de fenómenos reales proviene no tanto de los cuatro grados de libertad sino de su estrecha relación con el teorema del límite central, al igual que ocurre con las gaussianas. En particular, en el caso del tráfico de red agregado, se puede comprobar [6] que la familia α -estable permite no sólo modelar el tráfico de red mejor que otros modelos frecuentemente utilizados, sino también distinguir anomalías de reconocido interés para los administradores, como las inundaciones y los *flash crowds*, analizando la evolución temporal de sus parámetros. Las figuras 1 y 2 muestran algunos ejemplos de funciones de densidad de probabilidad α-estables para diversos valores de α y β respectivamente.

III. Comparación entre registros de SNMP y NetFlow

Durante el trabajo se han considerado los datos de subida y bajada procedentes del *router* de la Universidad de Valladolid recogidos a través de SNMP y NetFlow durante el periodo de tiempo que va del 4 de junio del 2007 al 30 de julio de 2008 para los datos de SNMP y del 1 de septiembre de 2007 al 31 de diciembre del 2008 para los flujos de NetFlow. Las muestras se tomaron de manera independiente, siendo obtenidas por parte de un sistema de monitorización para el caso de SNMP, y generadas directamente por el

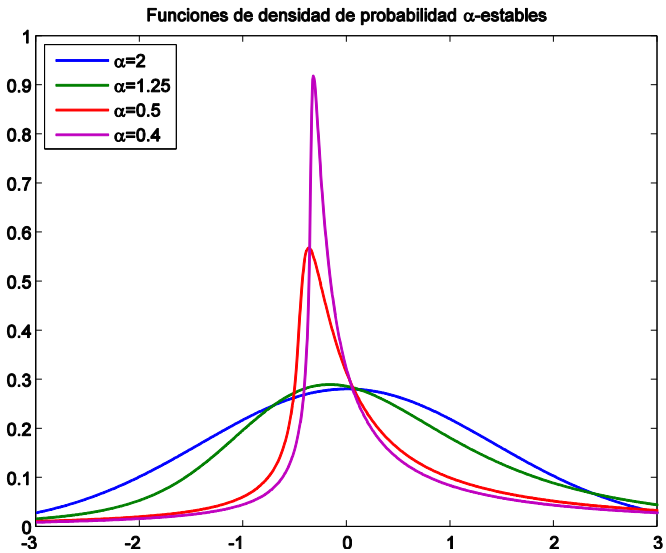


Fig. 1. Funciones de densidad de probabilidad α-estables para distintos valores de α.

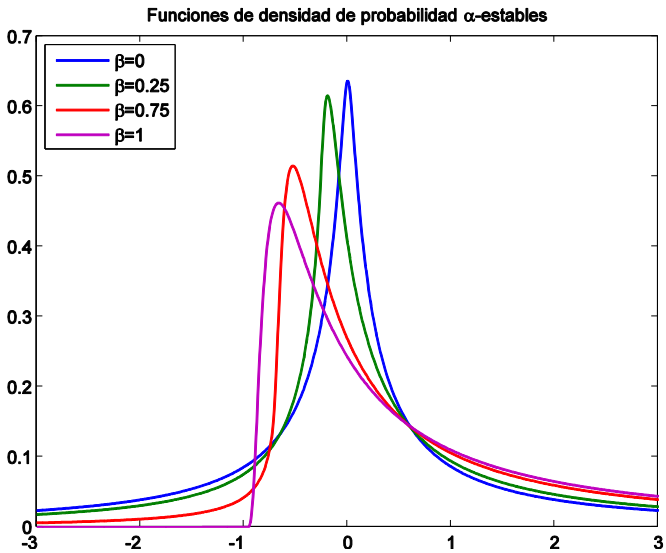


Fig. 2. Funciones de densidad de probabilidad α-estables para distintos valores de β.

router para el caso de NetFlow. Al ser dichas muestras independientes será necesario sincronizarlas posteriormente.

Para poder comparar los registros claramente se necesita evaluarlos durante un periodo común, por lo que se ha considerado un periodo entre el 1 de septiembre del 2007 al 30 de julio del 2008. Además, los protocolos utilizados no almacenan los datos relativos al tráfico de red de la misma forma, pues en el caso de SNMP sólo se ha obtenido la información del contador temporal y la suma de bytes totales en el instante de muestreo, mientras que la información disponible con NetFlow es más extensa, como ya se apuntaba anteriormente. A continuación se pueden encontrar información más detallada para cada uno de los dos tipos de datos a comparar:

- Registros SNMP. El sistema de monitorización en la Universidad de Valladolid fue configurado para sondear de manera periódica de SNMP a la tabla de interfaces del *router*, y con los datos obtenidos generar series temporales formadas por dos campos: el primero almacena el valor del contador temporal con resolución de microsegundo y con muestras recogidas cada 5 segundos; el segundo campo almacena el valor del contador de bytes en el instante de muestreo.
- Registros NetFlow. Estos registros guardan más información que los primeros, ya que por cada flujo transmitido se almacenan la fecha y la hora (4 campos) de inicio de la transmisión, la fecha y la hora de fin de la transmisión (con resolución de milisegundos), protocolo de nivel 4, dirección IP (4 campos) y puerto de origen, tipo de servicio, dirección y puerto de destino, otros dos campos de información de servicio y finalmente un campo para el número de paquetes y uno con el número de bytes [8]. Para reducir la dimensión de la matriz resultante se ha decidido omitir los campos de la información de servicio, así como juntar los campos de la hora transformando todo a escala de milisegundos. De esta forma la matriz pasa de 26 a 16 columnas, ahorrando espacio de almacenamiento, carga computacional y en consecuencia tiempo de elaboración. También hay que tener en cuenta la tasa de muestreo de los registros NetFlow, los cuales no contienen toda la información del tráfico sino que se limita, en nuestro sistema de captura, a una muestra cada 100 paquetes para reducir el coste computacional en los dispositivos de red. En este trabajo comprobaremos empíricamente el impacto que dicho muestreo tienen en el cálculo de tasas de transmisión. Como el instante inicial y la forma de almacenar los datos en ambos casos es distinto, para sincronizar los flujos, en los registros de SNMP inicialmente se han aislado las 7 semanas y 4 días de diferencia que hay entre las dos para luego buscar la mejor sincronización encontrando el mínimo valor de error cuadrático medio, como vamos a ver en la sección siguiente.

IV. Sincronización de los registros

Para comparar los registros generados a partir de ambos protocolos hay que transformar sus muestras en cantidades homogéneas y sincronizarlas temporalmente. Los registros tienen bases de tiempo distintas debido a que en el caso de SNMP es el gestor que ha realizado las peticiones quien realiza la marca temporal, mientras que en el caso de NetFlow la marca temporal la establece el propio reloj del *router* que los ha exportado. Cabe mencionar igualmente que ambos registros se han obtenido de dos fuentes independientes, por lo que no hubiera sido posible establecer a priori ninguna sincronización de los equipos implicados.

De dichos registros se va a generar la serie temporal que representa la evolución de la tasa de transmisión de datos a lo largo del tiempo. Esto se consigue en 3 simples pasos:

- Transformar el formato de los ficheros de los registros para poderlos importar directamente en una matriz con la herramienta de importación de Octave [9], importando el tipo de fichero en ASCII. De hecho con esta importación los elementos de la matriz tienen que estar separados por un espacio, mientras que las líneas tienen que estar separadas por una alimentación de línea (el carácter 0x0A, LF).
- Importar las matrices y calcular la misma variable para ambos tipos de registros, en este caso específico se trata de la tasa de transmisión en función de los intervalos de tiempo, como se indica en [10]. En este momento se pueden crear varias matrices con intervalos cada 5, 10, 15, 20, 30 segundos y más para poder evaluar también como varía el error cuadrático medio en función a la dimensión del intervalo. Como el objetivo es la comparación de la información entre los dos protocolos no se han considerado intervalos inferiores a los 5 segundos, pues la serie temporal de SNMP fue obtenida usando dicho intervalo.
- Sincronizar los registros. Para encontrar la misma referencia temporal se ha operado de la siguiente manera: a partir de las fechas de inicio del almacenamiento (4 de junio y 1 de septiembre) y del periodo de transmisión de los contadores (5 segundos), se ha partido el fichero de registros de SNMP en dos, uno con las primeras 7 semanas y 4 días y el otro que empieza por la tarde del 31 de agosto con el resto del fichero. Después, teniendo en cuenta que el primer flujo de NetFlow empieza a las 00:03:44 del 1 de septiembre, en una primera fase (aislando un día y medio de SNMP) se han comparado las posiciones del máximo absoluto y de unos máximos relativos para conocer la magnitud del desplazamiento restante. Finalmente, a partir del valor más frecuente se ha refinado el proceso calculando el error cuadrático medio para los valores de desplazamiento en un intervalo bastante ancho entre -20 y 20 muestras de diferencia, también para comprobar que el valor encontrado en la primera fase no hubiese sido afectado por el ruido. El error mínimo corresponde a la máxima semejanza de los registros.

Después de haber sincronizado los registros, como conocemos el tiempo absoluto se han ajustado también el final y el principio de los ficheros de los datos de SNMP para dividirlos justo a la medianoche del 1 de septiembre.

V. Filtrado de la serie temporal de NetFlow

La Fig. 3 muestra la tasa de transmisión del enlace calculada mediante ambos mecanismos de medida a lo largo de un día con muestras cada 5 segundos. Como puede observarse, la serie temporal obtenida a partir de NetFlow tiene mucho ruido respecto a la obtenida por SNMP. Para

estudiar este ruido, a partir de los registros se ha calculado la FFT (*Fast Fourier Transform*) de ambas series temporales, calculando así la densidad de potencia en el dominio transformado. Los resultados se pueden ver en la Fig. 4. Para apreciar la diferencia y resaltar los picos de alta frecuencia, se omiten las primeras dos muestras de la densidad de potencia. Además siendo las señales reales, su transformada es simétrica por lo que se muestran sólo las frecuencias positivas.

Como se puede ver, la serie temporal obtenida a partir de los registros de NetFlow está caracterizada por la presencia de componentes espectrales de alta frecuencia con un considerable nivel de energía, lo que se traduce en una variabilidad más alta en el dominio del tiempo. Estas componentes son las que generan el ruido y añaden un valor de error cuadrático medio muy alto. Dado este hecho, para mejorar los resultados que se pueden obtener a la hora de extraer los parámetros de una distribución estadística se ha procedido a filtrar la serie temporal obtenida a partir de los registros de NetFlow. De esta manera se consigue una similitud mayor con la serie temporal obtenida por SNMP.

La forma en que hay que definir el filtro no es trivial, pues tiene que eliminar el ruido de alta frecuencia pero al mismo tiempo no puede ser un filtro paso bajo, porque al atenuar mucho la banda de alta frecuencia, eliminaría también la información relativa a la alta variabilidad del tráfico de red, quitando a la distribución α-estable su característica principal, y como consecuencia empeorando los resultados de la extracción de los parámetros.

Comparando bien la densidad de potencia de las dos series temporales, lo más destacable es que las componentes de ruido se concentran alrededor de 6 frecuencias fijas y que según los cálculos serían las que se encuentran en correspondencia en los índices 1441, 2881, 4320, 5760, 7200 y 8640 (1/12, 1/6, 1/4, 1/3, 5/12 y 1/2 de la frecuencia de muestreo respectivamente) del vector de densidad de potencia.

Además se ha comprobado que el ruido se encuentra con las mismas características a lo largo de todos los días del periodo considerado y no se limita al día considerado en el ejemplo.

Los resultados que se encuentran en el dominio de las frecuencias se reflejan en el dominio del tiempo, donde se puede comprobar que cada minuto (12 muestras) la tasa de flujos que el *router* está almacenando en el fichero baja, probablemente como consecuencia de alguna tarea periódica configurada en el mismo *router*. A continuación se han efectuado otras pruebas para ver si estas componentes pueden de alguna forma depender de la limitación temporal de la serie temporal o de efectos de *aliasing*. En el primer caso se ha aplicado una ventana de Hamming (0,54 + 0,46*sin(2πt/NT)) en el dominio temporal para eliminar por completo el primer lóbulo secundario en el dominio transformado. El resultado de esta operación no ha modificado la intensidad del ruido respecto a la de la señal. En el segundo caso se han cambiado la longitud de los intervalos de agregación de los flujos de NetFlow considerando intervalos de 2,5 y 10 segundos. En este caso las densidad de potencia calculada igualmente presentaba ruido pero con sólo 3 componentes en el caso de intervalos de 10 segundos y 12 componentes en el de 2,5 segundos.

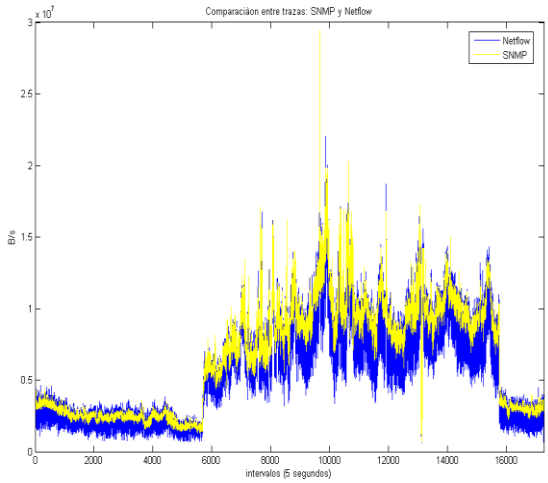


Fig. 3. Ejemplo de series temporales de SNMP (en amarillo) y NetFlow (en azul) a lo largo de un día.

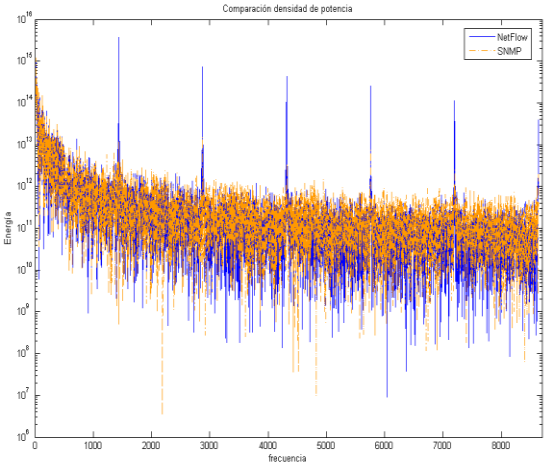


Fig. 4. Densidad de potencia de la serie temporal de SNMP (en naranja) y NetFlow (en azul)

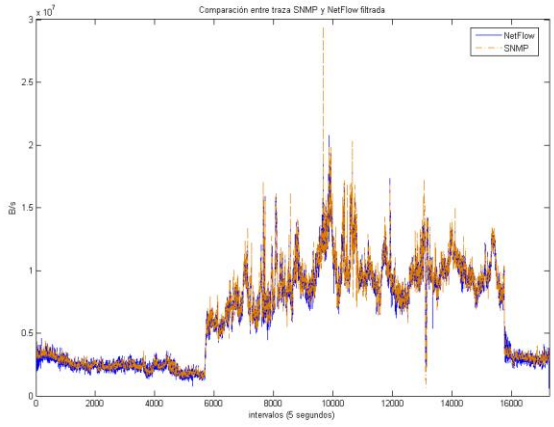


Fig. 5. Ejemplo de serie temporal de SNMP (en naranja) y NetFlow filtrada (en azul) a lo largo de un día.

Aprovechando esta característica del ruido se han definido 6 filtros Notch, cada uno de los cuales centrado en la frecuencia de un armónico. Para fijar la banda de cada filtro se han encontrado los puntos en los cuales el valor de la función de densidad sube de 3 dB (el doble) y ésta resulta ser de aproximadamente 81 muestras para los primeros 5 filtros y 40 para el último. Una vez definidos los filtros se pasa a filtrar la serie temporal obtenida a partir de los registros de NetFlow.

Para filtrar la serie temporal se han utilizado dos funciones distintas; la primera aplica a la vez numerador y denominador del filtro IIR (*Infinite Impulse Response*) a la función como en una operación normal de filtrado, mientras que la segunda, para proporcionar una fase plana, aplica el numerador en el sentido creciente del tiempo y el denominador en sentido inverso. Aunque la segunda función es más compleja, a la hora de extraer los parámetros, genera unos valores menos parecidos, especialmente para anchura y valor medio y como consecuencia un peor ajuste entre distribución teórica y empírica. Por esta motivación se ha preferido utilizar la primera función para la operación de filtrado.

En la Fig. 5. se puede ver la gráfica comparada entre la serie temporal de SNMP y la de NetFlow después del filtrado. Como se puede observar las dos series temporales después del filtrado (así como la densidad de potencia) se parecen más y como consecuencia también el error cuadrático medio ha bajado en un orden de magnitud.

VI. Evaluación de los parámetros

Para extraer los parámetros de la distribución α-estable se ha utilizado Matlab, en concreto la función "stblfit", basada en el método de Koutrouvelis que se encuentra en el paquete STBL_CODE [11], que comprende todas las funciones relativas a esta distribución.

En primer lugar, para la extracción de los 4 parámetros se necesitan ventanas temporales en las cuales el tráfico de red se pueda considerar estacionario. Exactamente como en [4], se ha elegido una duración de media hora para cada ventana. Como las series temporales tienen una resolución de 5 segundos, la longitud de las ventanas asegura un buen nivel de estacionariedad así como un número suficiente de muestras por cada ventana (1800 segundos/5 segundos por muestra = 360 muestras), de forma que se puede redefinir bien el modelo, bajando el valor del error entre las funciones de distribución acumulada de la ventana con respecto a la distribución calculada a partir de los 4 parámetros extraídos.

En segundo lugar hay que corregir la pérdida de sincronía con la serie temporal de SNMP que se genera en consecuencia de la derivade los relojes y de errores en la secuencia de los contadores, como puede ocurrir cuando se pierden mensajes de NetFlow o SNMP. Para mantener la referencia temporal se han vuelto a sincronizar ambas series temporales cada 12 horas. Como a veces se pueden encontrar ventanas en las cuales faltan muestras de una o de las dos trazas, el cálculo de los parámetros así como el de los errores ha sido ignorado en dichas ventanas, ya que no serían de ninguna utilidad para evaluar las características del sistema.

En las Fig. 6-8 se puede ver un ejemplo de la diferencia entre los parámetros de una distribución α-estable, estimados a partir de la serie temporal de SNMP y de la de NetFlow.

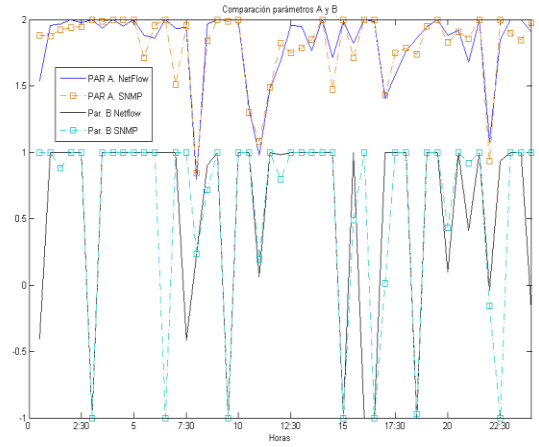


Fig. 6. Ejemplo de parámetros α y β para SNMP (en naranja y cian) y NetFlow filtrada (en azul y negro) a lo largo de un día.

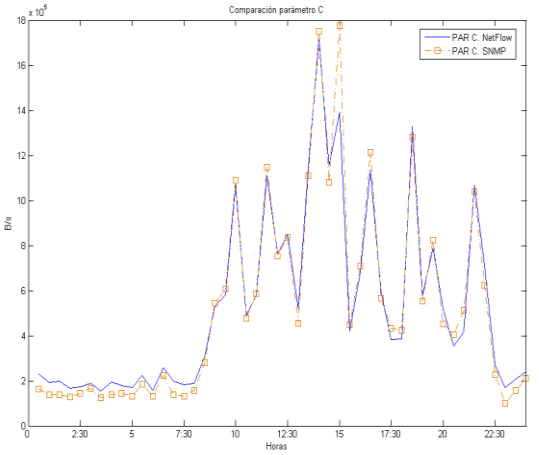


Fig. 7. Ejemplo de parámetro γ para SNMP (en naranja) y NetFlow filtrada (en azul) a lo largo de un día.

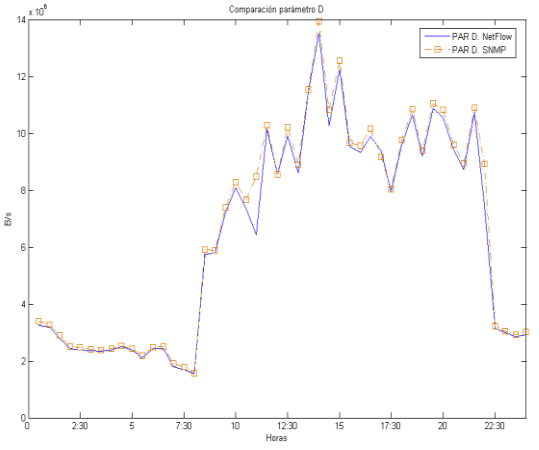


Fig. 8. Ejemplo de parámetro δ para SNMP (en naranja) y NetFlow filtrada (en azul) a lo largo de un día.

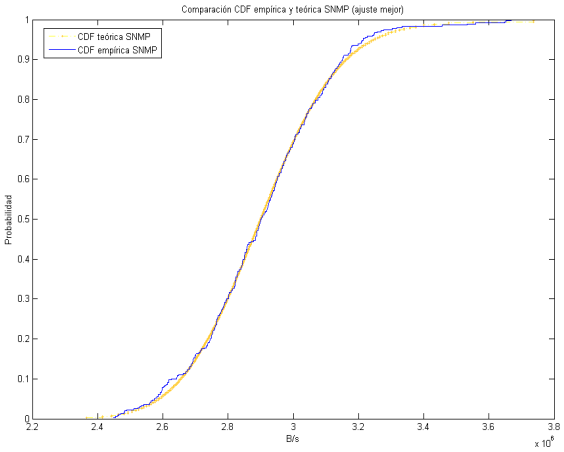


Fig. 9. Ejemplo de comparación entre la CDF teórica (en amarillo) y empírica (en azul) de SNMP en una ventana donde SNMP consigue un mejor ajuste.

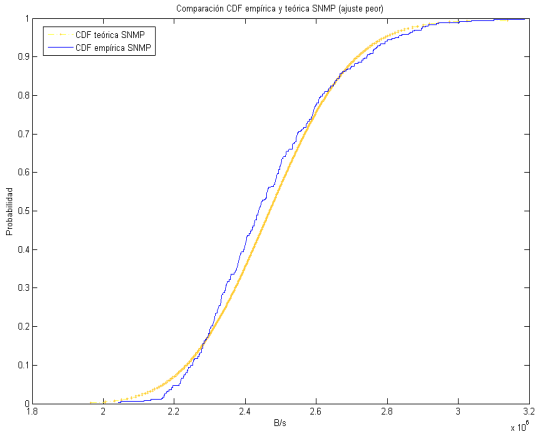


Fig. 11. Ejemplo de comparación entre la CDF teórica (en amarillo) y empírica (en azul) de SNMP en una ventana donde SNMP consigue un peor ajuste.

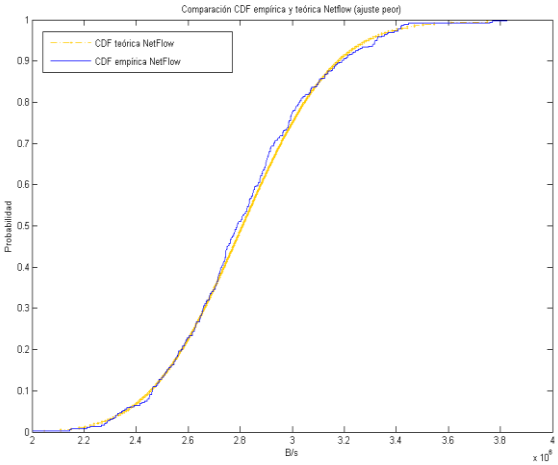


Fig. 10. Ejemplo de comparación entre la CDF teórica (en amarillo) y empírica (en azul) de NetFlow en la misma ventana de Fig. 9.

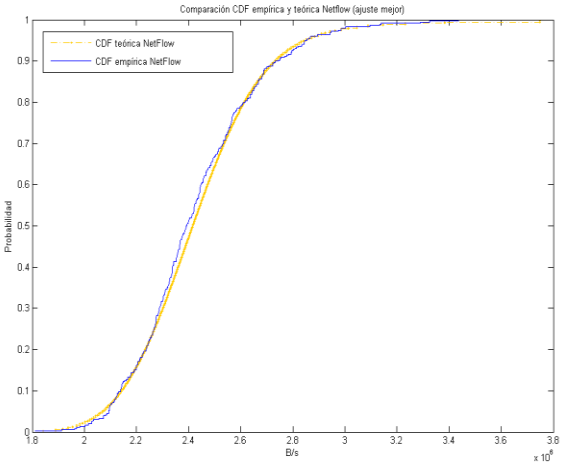


Fig. 12. Ejemplo de comparación entre la CDF teórica (en amarillo) y empírica (en azul) de NetFlow en la misma ventana de Fig. 11.

En las Fig. 9-12 se puede ver un ejemplo de ajuste entre las funciones de distribución acumulada estimadas (a partir de los parámetros extraídos) y empíricas (a partir de las muestras de la ventana) para SNMP y NetFlow. Se han elegidos dos casos, uno donde la serie temporal de SNMP proporciona una menor distancia entre las funciones y otro donde es la de NetFlow la que minimiza la diferencia. En cada caso la diferencia entre el error de ambas series temporales está por debajo del 5% en la mayoría de las ventanas.

VII. Evaluación de los errores

Para calcular los errores, entre varias alternativas [5] se ha elegido la máxima diferencia entre la función de distribución de probabilidad acumulada generada a partir parámetros extraídos, y la generada directamente a partir de las muestras de la ventana. Como quedó dicho en párrafos precedentes, el cálculo del error no ha sido efectuado para ventanas cuyas muestras son todos ceros o que contengan un bajo número de muestras distintas a cero pues no garantizarían un resultado fiable.

Estos errores están calculados independientemente por cada serie temporal, SMNP y NetFlow, para tener una idea de la diferencia entre los parámetros de ambas. Además se ha añadido el cálculo del error comparado, es decir la máxima diferencia entre las distribuciones de probabilidad obtenidas a partir de las muestras de las dos series temporales.

En la Tabla I se resumen los resultados de media y desviación estándar de los errores encontrados a lo largo de 1344 ventanas que abarcan 28 días completos. La longitud del periodo de tiempo intenta mejorar la estadística del cálculo de los errores, de forma parecida a la encontrada en [12].

Como se puede ver en la Tabla I el valor medio de los primeros dos errores descritos es muy parecido. Igualmente, la máxima diferencia entre las distribuciones de probabilidad de ambos protocolos presenta un valor bastante bajo,

Tabla I
Valores mínimos, máximos y medios de los errores

Error	Media	Desviación estándar
NetFlow	0,0741	0,0708
SNMP	0,0778	0,0678
Error comparado	0,0118	0,0533

reflejando el hecho que tras la sincronización y el filtrado, los parámetros estimados para la distribución α-estable de SNMP y de NetFlow son suficientemente parecidos y, por tanto, la sincronización se ha realizado correctamente.

VIII. CONCLUSIONES

Como se ha podido ver a lo largo del artículo, para extraer características del tráfico de red, se puede utilizar un modelo estadístico. Dentro de la gran variedad de modelos disponibles en literatura, el uso de una distribución que es capaz de tener en cuenta la característica de alta variabilidad del tráfico, como la distribución α-estable, es una elección que asegura un buen nivel de ajuste a pesar del protocolo utilizado para obtener los datos.

En el trabajo presentado se han considerado dos protocolos distintos: SNMP y NetFlow. El primero facilita la información del tráfico con dos contadores incrementales, uno para el tiempo y el otro para los bytes, mientras que el segundo no sólo proporciona esta misma información a través de campos donde guarda la hora de inicio y fin de la transmisión junto al número de paquetes y bytes transmitidos, sino que consigue también otro tipo de información que podría resultar muy valiosa para la gestión y la seguridad en la red. Dada la gran cantidad de datos generados, el *router* muestrea el tráfico creando registros NetFlow que tienen en consideración solo 1 paquete de cada 100.

Después de una elaboración previa, poco costosa a nivel computacional, para homogenizar la información contenida en los registros obtenidos con ambos protocolos, se han calculados los parámetros de la distribución y los errores relativos de ajuste tanto para SNMP como para NetFlow. Lo más destacable de los resultado obtenidos es notar como, tras realizar adecuadamente una sincronización y un filtrado, con los registros de NetFlow se pueden obtener valores similares a los obtenidos con SNMP con un margen de error muy pequeño, ocurriendo además que la tasa de muestreo de paquetes prácticamente no tiene influencia en los parámetros estimados.

La ventaja principal de este resultado es, por tanto, la posibilidad de llegar a resultados similares con una simple configuración inicial del *router* y sin tener que cargar el *router* ni la red con peticiones SNMP periódicas (cada 5 segundos para trabajar en la misma escala de tiempos) y con aproximadamente el 1% de los flujos disponibles por efecto del muestreo. En [4] se muestra que un tiempo de muestreo de 5 segundos para la serie temporal de SNMP añadía una carga del *router* no superior al 5%. Es interesante notar como si se quisiera reducir este tiempo (por ejemplo para disminuir la longitud de la ventanas de análisis o para aumentar el número de muestras por cada ventana) la carga del *router* para gestionar las peticiones de SNMP subiría bastante respecto a una menos importante subida del coste computacional durante la interpolación de la serie de NetFlow. Esta fuerte dependencia de la carga del *router* y el intervalo de muestreo hace que pueda ser preferible utilizar NetFlow en lugar que SNMP cuando se necesita un periodo de muestreo muy pequeño.

Además utilizando toda la información disponible en los flujos de NetFlow, se podría construir una herramienta muy efectiva para la gestión y sobre todo la seguridad de la red, pues se podrían detectar distintas clases de ataques a través de la búsqueda de patrones que los caracterizan. En [3] se describen varias técnicas para detectar ataques de distintas categorías, tales como denegación de servicio, gusanos o escaneos, pudiéndose encontrar una huella de dichos ataques en la información almacenada en los registros de NetFlow.

Como trabajo futuro se plantea estudiar si los armónicos de alta frecuencia se encuentran también en registros de NetFlow generados en otros *routers* de RedIRIS, o bien es un caso particular del *router* en estudio. Esto permitiría saber si es posible utilizar los mismos filtros utilizado en este trabajo, o si por el contrario sería necesario definir filtros distintos para cada *router* según el comportamiento en frecuencia de los registros del tráfico. Igualmente puede resultar interesante realizar una comparación con la información que se puede obtener de agentes RMON (*Remote network MONitoring*) [13], desplegados también en muchos de los *routers* disponibles en el mercado.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el Ministerio de Economía y Competitividad dentro del proyecto PackTrack (TEC2012-33754).

REFERENCIAS

[1] D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks". IETF RFC 3411, diciembre de 2002.

[2] C. Gates, M. Collins, M. Duggan, A. Kompanek, M. Thomas, "More NetFlow Tools: For Performance and Security". Proceedings of LISA '04: Eighteenth Systems Administration Conference, pp. 121-132, Atlanta, noviembre de 2004

[3] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, B. Stiller, "An Overview of IP Flow-based Intrusion Detection", IEEE Communications Surveys & Tutorials, vol. 12, no. 3, pp. 343-356, 2010.

[4] F. J. Simmross Wattenberg. "Detección de anomalías en el tráfico agregado de redes IP basada en inferencia estadística sobre un modelo α–estable de primer orden", Tesis Doctoral, Universidad de Valladolid. Julio de 2009.

[5] G. R. Arce, "Nonlinear Signal Processing. A Statistical Approach", John Wiley and sons, New Jersey, NJ, USA, 2005.

[6] F. Simmross-Wattenberg, J. I. Asensio-Pérez, P. Casaseca-de-la-Higuera, M. Martín-Fernández, I. A. Dimitriadis, C. Alberola-López, "Anomaly detection in network traffic based on statistical inference and α-stable modeling". IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 4, pp. 494-509, 2011.

[7] G. Samorodnitsky and M. S. Taqqu, Stable non–Gaussian random processes. Stochastic models with infinite variance. Boca Raton, CA, USA: Chapman & Hall, 1994.

[8] G. R. Upadhaya. "NetFlow, Flow-tools tutorial". AfNOG Tutorials 14 May 2006, Nairobi, Kenya.

[9] J. Schmidt Hansen, "Gnu Octave Beginner's Guide", Packt Publishing Ltd, 2011.

[10] J. L. García-Dorado, J. E. López de Vergara, J. Aracil, V. López, J. A. Hernández, S. López-Buedo, L. de Pedro, "Utilidad de los flujos netFlow de RedIRIS para análisis de una red académica", Jornadas Técnicas RedIRIS 2007, Mieres, Asturias, 19-23 de noviembre de 2007. Publicado en el Boletín de RedIRIS, no.82-83, abril de 2008.

[11] MathWorks. "Alpha-Stable distributions in MATLAB". [Fecha de consulta Abril 2013]. Disponible en http://math.bu.edu/people/mveillet/html/alphastablepub.html

[12] J.L. García Dorado, J. A. Hernández, J. Aracil, J. E. López de Vergara, F. J. Montserrat, E. Robles, T. P. de Miguel. "On the Duration and Spatial Characteristics of Internet Traffic Measurement Experiments", IEEE Communications Magazine, vol. 46, no. 11, pp. 148-155, noviembre de 2008.

[13] S. Waldbusser, R. Cole, C. Kalbfleisch, D. Romascanu, "Introduction to the Remote Monitoring (RMON) Family of MIB Modules", IETF RFC 3577, agosto de 2003.

Monitorización y Análisis de los Recursos Compartidos en la Red BitTorrent

Rafael A. Rodríguez-Gómez, Gabriel Maciá-Fernández, Pedro García-Teodoro
CITIC - Departamento de Teoría de la Señal, Telemática y Comunicaciones,
E.T.S. de Ingenierías Informática y de Telecomunicación, Universidad de Granada
C/Periodista Daniel Saucedo Aranda s/n, E-18071, Granada
{rodgom, gmacia, pgteodor}@ugr.es

***Resumen*—BitTorrent es el protocolo de distribución de contenidos basado en P2P más extendido en la actualidad, y mediante él se distribuyen recursos de todo tipo, unos dentro de la legalidad y otros no tanto. Conocer las características representativas de los recursos compartidos en esta red puede ser crucial de cara a la detección temprana del intercambio de recursos de tipo específico, como pueden ser: recursos utilizados para distribuir *malware* o con *copyright*, entre otros. En este trabajo se hace uso de una técnica de monitorización que permite recoger información de la evolución temporal de la compartición de 1/256 del total de recursos compartidos en toda la red BitTorrent. Para ello, una gran cantidad de nodos *sybil* han sido introducidos en la red, presentándose como vecinos de una zona particular y recabando la información dirigida a ella. La monitorización de la red se ha llevado a cabo durante 3 meses y como resultado se ha conseguido información de más de 70.000 recursos. Dicha información se ha analizado tomando como base cuatro características: (*i*) dispersión geográfica, (*ii*) popularidad, (*iii*) duración de la compartición y (*iv*) disponibilidad. Confiamos en que los resultados de este análisis pueden derivar en herramientas y procedimientos de interés acerca de la compartición de recursos en BitTorrent.**

***Palabras Clave*—Compartición de recursos; P2P; BitTorrent**

I. INTRODUCCIÓN

Es conocido que las redes de compartición de recursos mediante Peer-to-Peer (P2P) son utilizadas en ocasiones para distribuir contenidos fuera de la legalidad, como puede ser contenidos con *copyright*. De igual forma, estas redes son también un foco enorme de infección y distribución de *malwares* de todo tipo. Incluso existen *botnets* que utilizan estas redes como mecanismo de comunicación entre sus nodos [1].

De entre todos los protocolos de compartición de archivos mediante P2P, BitTorrent es el más extendido en la actualidad. De hecho, el tráfico derivado de su uso oscila entre un 43% y un 70% de todo el tráfico de Internet dependiendo de la zona geográfica [2]. Recientemente, BitTorrent ha comenzado a utilizar una característica de *trackers* distribuidos. Así, un cliente de la red puede descubrir qué nodos almacenan una copia o una parte de un archivo gracias a un algoritmo de tabla de *hash* distribuida (DHT). Concretamente, BitTorrent utiliza una implementación de Kademlia denominada Mainline.

Dado el uso que se les da a las redes de compartición de archivos mediante P2P, es deseable disponer de estudios que detallen el comportamiento de la compartición en ellas. En especial en BitTorrent, al ser ésta la más utilizada. Estos estudios pueden arrojar luz sobre el comportamiento general de estas redes, lo que podrá repercutir en su mejora. Asimismo, pueden servir como punto de partida para posibles detecciones de ciertos tipos de recursos.

Con este objetivo en mente, en este trabajo se presenta: (*i*) un método de monitorización de Mainline tomado de [3] y [4] y, tras ello, (*ii*) un análisis inicial de los resultados de dicha monitorización.

En primer lugar, la monitorización se basa en dos módulos: (*i*) *crawling* y (*ii*) *sniffing*. El módulo de *crawling* envía constantemente mensajes tipo `find_node` a los nodos de una zona para que éstos le devuelvan la lista de nodos que poseen. Es capaz de extraer 1/256 del total de nodos activos en la red, lo que puede ser realizado en menos de 2,5 segundos.

El módulo de *sniffing* toma como entrada los nodos que componen una determinada zona de la red que se corresponde con la salida del módulo anterior. En esta zona inserta como vecinos una enorme cantidad de nodos *sybils* que recogen todos los mensajes que tienen como destino la zona monitorizada. En resumen, este módulo es capaz de recopilar la información de qué usuarios comparten en cada instante todos los recursos asociados a la zona monitorizada.

En segundo lugar, el análisis de la monitorización se ha llevado a cabo estudiando 4 características.

1) Dispersión geográfica. Número de continentes desde los que se comparte un recurso dado.

2) Popularidad. Relacionada con el número máximo de usuarios que comparten un recurso determinado durante un cuanto de tiempo.

3) Duración de la compartición. Tiempo transcurrido desde el primer instante hasta el último en el que un recurso es anunciado en la red.

4) Disponibilidad. Proporción del tiempo en el que es posible descargar el recurso con respecto a la duración de su compartición.

El resto del artículo se estructura como sigue. En la Sección

II se presentan una serie de trabajos relacionados con el campo abordado. Los conceptos básicos de BitTorrent y Mainline necesarios para la comprensión del presente trabajo se exponen en la Sección III. El proceso de monitorización es descrito en la Sección IV, mientras que el análisis de la información conseguida en la misma se indica en la Sección V. Finalmente, las conclusiones y algunas líneas de posibles trabajos futuros se presentan en la Sección VI.

II. TRABAJOS RELACIONADOS

Existen multitud de trabajos destinados a estudiar el comportamiento de la red BitTorrent, y más concretamente a estudiar los recursos compartidos en ella. Algunos de estos estudios se basan en simulaciones, como puede ser el trabajo de Bharambe et al. [5] en el que los autores ponen de manifiesto que BitTorrent es casi óptimo en cuanto a utilización de ancho de banda de subida y tiempo de descarga. También encontramos en [6] un trabajo en el que se demuestra la escalabilidad de BitTorrent. De hecho, hoy por hoy se siguen implementando módulos para simular BitTorrent [7]. En esta misma línea también encontramos trabajos más teóricos enfocados en el modelado de la red, como es el caso de Liao et al. en [8]. Estos estudios son útiles para comprender el comportamiento de BitTorrent pero es necesaria una monitorización de los escenarios reales para complementar los resultados obtenidos en simulación.

También existe una gran cantidad de trabajos en la línea del estudio de desarrollos reales. En [9] Andrade et al. presentan un estudio de la demanda y suministro de los recursos en BitTorrent. En este estudio se utiliza la información de 3 *trackers aluvion*, *bitsoup* y *etree*, recogiendo datos de alrededor de 15.000 archivos durante 68 días como máximo. Meulpolder et al. aseguran en [10] que el rendimiento experimentado por los usuarios que descargan en comunidades privadas de BitTorrent es claramente superior al experimentado en las comunidades públicas; así como difiere enormemente la proporción entre semillas y *leechers* y la duración de la compartición de las semillas. La principal deficiencia encontrada en estos trabajos es que basan la recolección de información en la información que poseen los *trackers*. Ésta no es una información global ni precisa de la red ya que un *tracker* posee información desactualizada y no recoge la información de los nodos que se comunican de forma totalmente distribuida. Esta deficiencia es, por tanto, nuestra principal motivación para realizar el presente trabajo.

El presente trabajo pretende abordar el estudio de la compartición de recursos en BitTorrent desde una perspectiva diferente a todos los estudios anteriores. En nuestro caso se estudia una implementación real del protocolo pero no nos basamos en los datos que los *trackers* de BitTorrent facilitan en sus páginas web, sino que recabamos la información mediante una monitorización real de la compartición de los nodos que la componen. Adicionalmente, en este trabajo se estudian más recursos que en sus predecesores, concretamente 1/256 del total de los compartidos en BitTorrent. El tiempo durante el que se lleva a cabo esta monitorización es elevado para poder abarcar realmente el ciclo de vida de estos archivos.

III. CONCEPTOS GENERALES DE BITTORRENT

El protocolo BitTorrent se basa en los archivos *torrent*, que contienen información acerca de los archivos compartidos y el *tracker* asociado. El *tracker* es la máquina encargada de coordinar la distribución de este archivo, facilitando información acerca de qué nodos contienen una copia o una parte del archivo buscado.

Recientemente el protocolo BitTorrent contempla otro modo de funcionamiento. Es un modo completamente distribuido que no requiere de la existencia de *trackers*. Se utiliza una tabla de *hash* distribuida (DHT) para almacenar la correspondencia entre recursos y los nodos que los comparten. Se podría decir que cada nodo se convierte en un *tracker*. Este nuevo protocolo se basa en una implementación de Kademlia [11] llamada Mainline [12].

En Mainline cada nodo posee un identificador global único generado aleatoriamente de 160 bits de longitud. Este identificador es generado la primera vez que un cliente nuevo inicia la aplicación de BitTorrent correspondiente. Éste será siempre el identificador de este cliente a menos que la aplicación de BitTorrent sea completamente desinstalada o se elimine su fichero de preferencias. Así que podemos suponer el ID de nodo como un identificador único por cliente incluso en la circunstancia de que este cliente cambie de dirección IP.

Adicionalmente, cada recurso compartido en la red Mainline posee un identificador único con la misma longitud que el identificador de nodo, 160 bits. Este identificador se genera como resultado de una función *hash* del recurso compartido.

Para comparar la "cercanía" de dos identificadores de nodo o un identificador de nodo y un identificador de recurso se utiliza una métrica de distancia. Esta métrica de distancia es la operación XOR y es simétrica de modo que la distancia entre A y B es la misma que la distancia entre B y A. Se asume que valores menores de esta métrica implican identificadores más cercanos.

De forma genérica, los usuarios con identificadores cercanos al identificador de un recurso son los encargados de almacenar la información de qué nodos de la red poseen una copia o una parte de este recurso. Así, si un nodo pretende encontrar nodos para un *torrent* en particular, utiliza la distancia XOR para comparar el identificador del recurso asociado al *torrent* con los identificadores de los nodos de su tabla de rutas. Después contacta con aquellos nodos con un identificador más cercano al identificador del recurso y les solicita una lista de nodos que estén compartiendo el recurso buscado. Si los nodos contactados poseen esta información se la envían en respuesta. En otro caso, los nodos contactados deben responder con los nodos de su tabla de ruta con un identificador más cercano al identificador del recurso buscado. El nodo original solicita iterativamente la misma petición a nodos cada vez más cercanos al identificador del

recurso hasta obtener la respuesta buscada.

A. Principales mensajes de Mainline

A continuación presentamos los principales mensajes en Mainline. Para una información más detallada puede consultarse el borrador [12]:

- `ping` comprueba si un nodo continúa estando activo. El nodo receptor del mensaje también aprende la existencia del nodo que lo originó.

- `find_node` solicita información de un nodo n al nodo más cercano al identificador de nodo buscado, ID_n. El nodo que responde a este mensaje envía una lista con la IP, puerto e identificadores de nodo más cercanos a ID_n en su tabla de ruta.

- `get_peers` pide información sobre un archivo f con identificador de archivo ID_f. Este mensaje sigue un procedimiento que funciona de forma iterativa. En cada iteración del proceso, cada salto, los nodos responden al mensaje con las direcciones IP, puertos e identificadores de nodo de los nodos más cercanos a ID_f. En el último salto del proceso los nodos devuelven una lista con las direcciones IP, puertos e identificadores de nodo de los nodos que poseen una copia del recurso buscado, f.

- `announce_peer`. Un nodo anuncia con este mensaje que posee un archivo (o una parte de él) con un identificador de recurso ID_f. Un nodo envía estos mensajes a los k nodos con identificadores más cercanos a ID_f. El valor de k oscila de 3 a 8 dependiendo de la implementación del cliente de BitTorrent. Estos k nodos más cercanos han sido previamente encontrados con un mensaje del tipo `get_peers`. El nodo que envía este mensaje es responsable de reenviarlo cada cierto periodo de tiempo para evitar que su entrada en la lista de nodos que poseen el archivo expire.

IV. MONITORIZACIÓN DE BITTORRENT

El proceso de monitorización se compone de dos módulos principales: (*i*) *crawling* de la red y (*ii*) *sniffing* de los mensajes de una zona. A continuación se describen brevemente ambos módulos.

A. Crawling

Este módulo se basa en el trabajo realizado en [3] y posteriormente adaptado a Mainline en [4].

El *crawler* se implementa en base a dos hebras asíncronas: una encargada de enviar mensajes de tipo `find_node` y la otra encargada de recibir y procesar las respuestas. Una lista con los nodos descubiertos es compartida por ambas hebras. La hebra encargada de recibir las respuestas añade los nodos extraídos a la lista. Mientras tanto, la otra hebra recorre la lista constantemente enviando 16 mensajes `find_node` a cada nodo de ella. El valor del identificador de nodo de cada mensaje es diferente en cada una de las 16 solicitudes. Una premisa importante es que cada identificador escogido debe pertenecer a una sección diferente del árbol de rutas de los nodos. De esta forma se minimiza el solapamiento del conjunto de nodos recibido en cada respuesta.

Con este módulo se puede recoger la información de toda la red Mainline en sólo 8 minutos. Pero también es posible realizar un *crawling* de una zona específica de la red con un prefijo determinado, en nuestro caso de 8 bits. Esto quiere decir, encontrar todos los nodos activos en la red con los mismos primeros 8 bits de identificación de nodo. Este proceso, que es capaz de extraer 1/256 del total de nodos activos en la red, puede ser realizado en menos de 2,5 segundos.

B. Sniffing

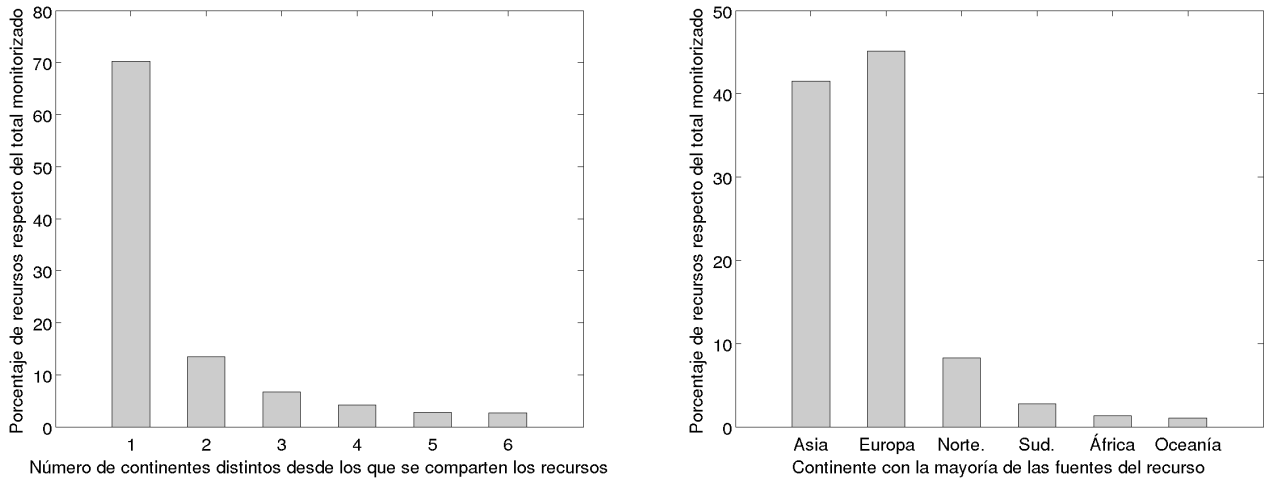
Este módulo se basa en el presentado en [4], adaptado a nuestro caso particular. Así, se lleva a cabo la recopilación de los nodos que en cada instante comparten recursos asociados a una zona concreta de la red Mainline. Para esto se incluyen en la DHT una gran cantidad de nodos *sybils* con identificadores de nodo cercanos a todos los nodos activos en esa zona. Esta información es facilitada por el módulo anterior.

Sea n un nodo de la zona a monitorizar e ID_n su identificador de nodo. Este módulo inserta 256 *sybils* cuyos identificadores de nodo coinciden en los primeros 47 bits de ID_n. Esto hace que la probabilidad de que exista un nodo en la DHT de Mainline con un identificador más cercano a ID_n sea extremadamente reducida. Los identificadores de nodo de los *sybils* se generan variando los bits en el intervalo 48-56 (8 bits) y como resultado se obtienen 256 identificadores de nodo diferentes.

El proceso de inclusión de estos *sybils* como nodos de la DHT se basa en notificar de la existencia de los *sybils* a los nodos reales con identificadores de nodo cercanos al nodo objetivo n. Estos nodos serán los que posteriormente propagarán esta información a otros nodos en la DHT, ya que nuestros *sybils* formarán parte de su tabla de ruta. Este proceso puede detallarse como sigue a continuación:

Primero, se descubren los nodos dentro de la zona a monitorizar utilizando el módulo de *crawling*. Tras esto, se envían mensajes del tipo `ping` con el identificador de nodo fuente igual a los *sybils* correspondientes a todos los nodos activos en dicha zona. De esta forma, se realiza un ataque de polución a las tablas de ruta de los nodos reales en esta zona insertando todos nuestros *sybils* como sus vecinos. Hecho esto, para alcanzar a cualquier nodo de la zona monitorizada se enviará primero una solicitud a uno de nuestros *sybils* ya que son nodos muy cercanos a los nodos objetivo.

Segundo, se almacena la información de los mensajes del tipo `annonce_peers`, que son los que apuntan a los nodos que poseen realmente los recursos que se pretenden monitorizar. Para cada mensaje `annonce_peers` se



(a) (b)

Fig. 1: Dispersión geográfica de los recursos monitorizados: número de fuentes que comparten un recurso (a) y continentes que contienen la mayoría de las fuentes de los recursos (b)

almacena el identificador del recurso anunciado, la IP, el identificador del nodo origen del mensaje y una marca temporal del momento en el que llegó el mensaje.

V. ANÁLISIS DE LA MONITORIZACIÓN DE BITTORRENT

A. Entorno experimental general

Se ha llevado a cabo una monitorización de todos los recursos compartidos en BitTorrent cuyo identificador de recurso comience por los mismos 8 bits. Concretamente, los 8 bits elegidos han sido en hexadecimal "8C". Esto implica que la monitorización ha abarcado 1/256 del total de la red mundial de BitTorrent. Este es un tamaño suficiente para considerar que los recursos comprendidos en esta zona de la red de BitTorrent suponen una representación significativa del total de los recursos de toda la red.

Esta monitorización se ha realizado durante 3 meses, desde el 4 de abril hasta el 4 de julio de 2012. Durante este período de tiempo se han monitorizado un total de 71.135 archivos que han sido compartidos por cientos de millones de IPs diferentes de todos los continentes. Para cada uno de estos archivos se ha almacenado el número de IPs diferentes, número de identificadores de nodo diferentes y número de mensajes de tipo `announce_peer`, por hora.

En el resto de la sección se presenta un análisis de esta monitorización en base a las características que han sido consideradas como de una especial relevancia para el análisis de los archivos monitorizados en BitTorrent.

B. Resultados experimentales

A continuación se definen las cuatro características utilizadas en el análisis de los datos monitorizados. Estas son: (*i*) dispersión geográfica, (*ii*) popularidad, (*iii*) duración de la compartición y (*iv*) disponibilidad. Se considera que estas características pueden ser útiles para realizar un análisis inicial genérico de los datos obtenidos como resultado de la monitorización de la red BitTorrent.

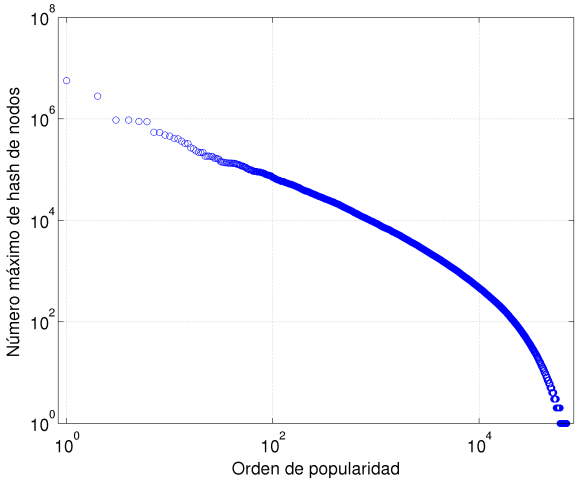


Fig. 2: Número máximo de IPs diferentes que han compartido en cuantos de una hora los recursos monitorizados.

1) Dispersión Geográfica: La **dispersión geográfica** se extrae del número diferente de continentes desde los que existen nodos compartiendo un recurso concreto. Para esto se han de conseguir las localizaciones de todos los nodos recogidos en el periodo de monitorización. Para hallar esta correspondencia se ha utilizado el módulo GeoIP de Python [13].

En la Fig. 1 se presentan los resultados más relevantes relativos a la dispersión geográfica. En la Fig. 1a podemos ver que el interés de la mayoría de los recursos está centrado en un único continente. En la Fig. 1b se muestra que entre Asia y Europa reúnen más del 80% de los recursos monitorizados. Se puede concluir que estos continentes son los más activos

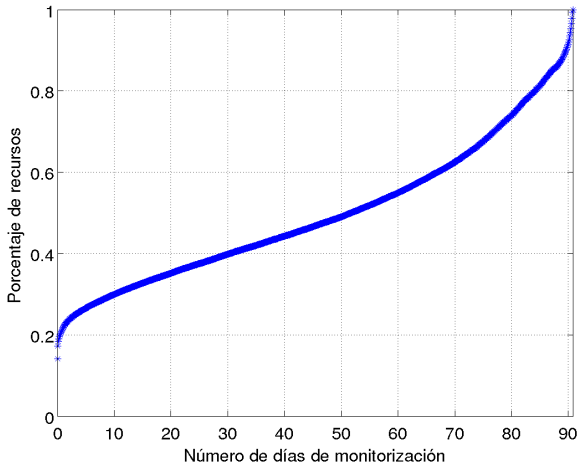


Fig. 3: Histograma acumulado de la duración de los recursos monitorizados

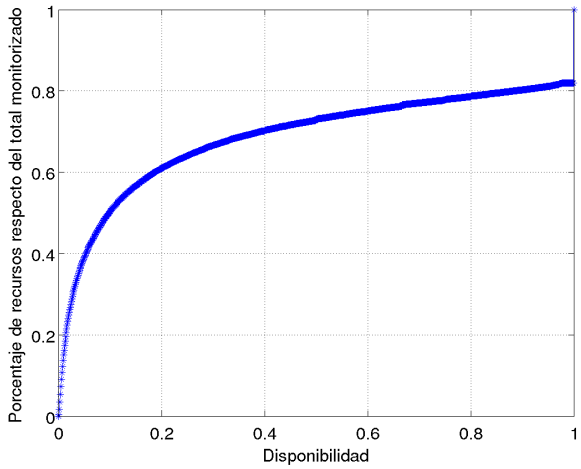


Fig. 4: Histograma acumulado de la disponibilidad de los recursos monitorizados

en el uso de BitTorrent, lo cual es coherente con [2].

2) Popularidad: La **popularidad** se ha definido en base al número máximo de usuarios diferentes que han compartido el recurso durante un cuanto de monitorización, suponiendo que un identificador de nodo diferente implica un usuario diferente. En resumen, aquí se asume que los recursos populares serán aquellos que hayan sido compartidos por un mayor número de usuarios.

En la Fig. 2 se presenta en el eje x el orden de popularidad, correspondiendo el valor 1 al recurso que ha sido compartido por más nodos en un cuanto de una hora y el último valor al recurso que ha sido compartido por menos nodos. En el eje y se presenta el número máximo de nodos que han compartido el recurso dado en una hora.

Como puede verse en esa figura, existen unos pocos recursos muy populares y una enorme cantidad de recursos con una popularidad muy reducida. Los diez recursos más populares llegan al millón de usuarios diferentes compartiéndolos en una hora. Es importante resaltar la enorme cantidad de recursos cuyo número máximo de usuarios diferentes compartiéndolos en una hora es uno; concretamente, en nuestra monitorización encontramos 27.896 recursos en esta situación.

3) Duración de la compartición: La **duración de la compartición** da cuenta del tiempo que un recurso ha sido compartido dentro del periodo de monitorización total. Para hallar este valor se restan el último y el primer instante en los que algún nodo de la red envió un mensaje de tipo `announce_peer` relativo al recurso correspondiente. Es importante aclarar que es posible que existan instantes en los que un recurso no esté siendo compartido por nadie y, sin embargo, este tiempo se sume a su duración porque en instantes posteriores algún nodo vuelva a compartirlo.

Como se muestra en la Fig. 3, más de un 20% de los recursos monitorizados tiene una duración muy reducida.

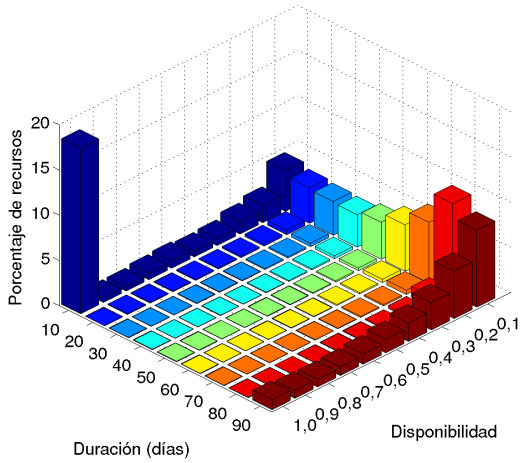


Fig. 5: Distribución de los recursos según su duración y disponibilidad

Estos son recursos que además son extremadamente poco populares, teniendo como máximo un nodo a la vez compartiéndolos.

4) Disponibilidad: Para disponer de una medida del tiempo en el que un recurso está siendo realmente compartido se define la **disponibilidad** como el tiempo durante el que este recurso puede ser descargado. Suponemos que un recurso puede ser descargado cuando existe al menos un nodo que está compartiendo este recurso. Así, la disponibilidad se calcula como la división entre el tiempo en el que un recurso dado está siendo compartido por al menos un usuario y la duración total del recurso:

$$disponibilidad_i = \frac{duracionNoCero_i}{duracion_i}$$

Los valores que puede tomar esta característica quedan definidos dentro del intervalo (0,1]. Un recurso al ser monitorizado ha sido compartido al menos por un usuario, razón por la que el cero no está excluido de los posibles

valores de la disponibilidad.

En la Fig. 4 se muestra el histograma acumulado de la disponibilidad. Alrededor de un 20% de los recursos presentan una disponibilidad cercana a 0. Estos son recursos que han sido compartidos en dos instantes muy separados en el tiempo y que en el resto del periodo de monitorización no han sido anunciados. Por tanto, son recursos que poseen muy pocos nodos en la red y sólo aparecen cuando éstos se conectan.

Por otro lado, en la Fig. 5 se presentan de forma conjunta la duración y la disponibilidad. Como podemos ver, existe cerca de un 20% de los recursos que presentan una duración muy reducida y una disponibilidad muy alta. Estos son recursos que sólo han aparecido en unas pocas horas del proceso de monitorización y que no han vuelto a ser anunciados; por esto su disponibilidad es máxima y su duración reducida. También se ve que la disponibilidad de los recursos con duración elevada es bastante reducida. Cabe destacar en este punto que en un análisis más detallado se descubre que los recursos que presentan una disponibilidad elevada son los más populares que, como se comentó en el apartado de popularidad, representan un porcentaje muy reducido de los recursos y, en consecuencia, influyen poco en las gráficas presentadas.

VI. CONCLUSIONES Y TRABAJO FUTURO

En este trabajo se utiliza un método de monitorización de la red Mainline. Este método se basa en el uso de dos módulos: *crawling* y *sniffing*. El módulo de *crawling* es capaz de conseguir la lista de nodos activos de una zona de 8 bits de la red Mainline (1/256 del total de la red) en menos de 2,5 segundos. El módulo de *sniffing*, tomando como entrada la salida del módulo de *crawling*, es capaz de almacenar todos los mensajes del tipo `announce_peer` cuyo destino sea cualquier nodo dentro de la zona monitorizada. De esta forma, la monitorización utilizada almacena una lista de los nodos que están compartiendo todos los recursos con identificadores cercanos a la zona monitorizada.

Tomando como base los datos de la monitorización de la zona con prefijo '8C' de la red Mainline durante 3 meses se ha llevado a cabo un análisis de cuatro características: (*i*) dispersión geográfica, (*ii*) popularidad, (*iii*) duración de la compartición y (*iv*) disponibilidad. Algunas de las conclusiones más reseñables derivadas de su análisis son:

- El interés de la gran mayoría de los recursos (entorno al 70%) está localizado en un único continente, aglutinando Asia y Europa más de un 80% de los recursos de la red.
- Existe una enorme cantidad de recursos (entorno a 28.000) que sólo son compartidos por un nodo durante un periodo breve de tiempo. Estos son recursos anómalos que requieren un estudio más detallado.
- La disponibilidad de la mayor parte de los recursos es inferior al 20%. Sólo los recursos populares se mantienen disponibles la mayor parte del tiempo.

Algunas líneas de trabajo que estamos abordando en este momento en relación al estudio aquí desarrollando son: extensión de la caracterización de los datos monitorizados y utilización de esta caracterización para la detección de ciertos tipos de recursos específicos.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el MICINN (Ministerio de Ciencia e Innovación) mediante el proyecto TEC2011-22579.

REFERENCIAS

[1] S. Golovanov and I. Soumenkov, "TDL4 – Top Bot," http://www.securelist.com/en/analysis/204792180/TDL4_Top_Bot, Tech. Rep., [Online; accessed 30-mayo-2013].

[2] H. Schulze and K. Mochalski, "Internet Study 2008/2009," Tech. Rep., 2009.

[3] M. Steiner, T. En-Najjary, and E. W. Biersack, "Long term study of peer behavior in the KAD DHT," *IEEE/ACM Trans. Netw.*, vol. 17, no. 5, pp. 1371–1384, Oct. 2009.

[4] M. Varvello and M. Steiner, "Traffic localization for DHT-based BitTorrent networks," in *Proceedings of the 10th international IFIP TC 6 conference on Networking - Volume Part II*, ser. NETWORKING'11, 2011, pp. 40–53.

[5] A. Bharambe, C. Herley, and V. Padmanabhan, "Analyzing and Improving a BitTorrent Networks Performance Mechanisms," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, 2006, pp. 1–12.

[6] D. Stutzbach, D. Zappala, and R. Rejaie, "The scalability of swarming peer-to-peer content delivery," in *Proceedings of the 4th IFIP-TC6 international conference on Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communication Systems*, ser. NETWORKING'05. Springer-Verlag, 2005, pp. 15–26.

[7] E. Weingärtner, R. Glebke, M. Lang, and K. Wehrle, "Building a modular BitTorrent model for ns-3," in *Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques*, ser. SIMUTOOLS '12, ICST, Brussels, Belgium, Belgium, 2012, pp. 337–344.

[8] W.-C. Liao, F. Papadopoulos, K. Psounis, and C. Psomas, "Modeling BitTorrent-like systems with many classes of users," *ACM Trans. Model. Comput. Simul.*, vol. 23, no. 2, pp. 13:1–13:25, May 2013.

[9] N. Andrade, E. Santos-Neto, F. Brasileiro, and M. Ripeanu, "Resource demand and supply in BitTorrent content-sharing communities," *Comput. Netw.*, vol. 53, no. 4, pp. 515–527, Mar. 2009.

[10] M. Meulpolder, L. D'Acunto, M. Capotă, M. Wojciechowski, J. A. Pouwelse, D. H. J. Epema, and H. J. Sips, "Public and private BitTorrent communities: a measurement study," in *Proceedings of the 9th international conference on Peer-to-peer systems*, ser. IPTPS'10, 2010.

[11] P. Maymounkov and D. Mazières, "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01, 2002, pp. 53–65.

[12] "Mainline DHT Implementation," http://bittorrent.org/beps/bep_0005.html\#dht-queries, [Online; accessed 30-mayo-2013].

[13] "GeoIP country database reader in Python," http://www.isi.edu/nsnam/ns/, [Online; accessed 30-mayo-2013].

Proporcionando Interoperabilidad a un Sistema Ubicuo de Asistencia Médica Mediante el Estándar HL7 CDA

Albert Brugués de la Torre*†, Michael Schumacher*, Josep Pegueroles-Vallés†
Stefano Bromuri*
*University of Applied Sciences Western Switzerland
Sierre, Suiza
{albert.brugues, michael.schumacher, stefano.bromuri}@hevs.ch
†Universitat Politècnica de Catalunya
Barcelona, España
{josep.pegueroles}@upc.edu

***Resumen*—La interoperabilidad entre diferentes sistemas heterogéneos es un reto tecnológico que no se tiene en cuenta en la mayoría de Sistemas Ubicuos de Asistencia Médica (SUAMs). Para poder colaborar de manera federada, los SUAMs deben adoptar el uso de estándares de e-Salud. Entre ellos, *Health Level 7* (HL7) es una solución apropiada ya que éste define los mensajes para el intercambio electrónico de datos médicos. En este artículo se describe como se ha proporcionado interoperabilidad a un sistema SUAM mediante el uso del estándar HL7. En particular se describe como se ha implementado el *Clinical Document Architecture* (CDA) para enviar datos médicos entre el lado cliente y el lado servidor del sistema, y la necesidad de incluir nuevos elementos XML en el CDA generado para poder representar toda la semántica del sistema.**

I. INTRODUCCIÓN

La asistencia médica ubicua es una disciplina científica emergente que consiste en aplicar las tecnologías de computación ubicua en el ámbito médico [1]. Varshney [2] define la asistencia médica ubicua como la *"asistencia médica a cualquiera, en cualquier momento, y en cualquier lugar eliminando la localización, el tiempo y cualquier otra restricción a la vez que se incrementa tanto la cobertura como la calidad de la asistencia médica"*.

La asistencia médica ubicua intenta modificar el modelo de los servicios médicos de los países occidentales, moviéndolos de un enfoque centralizado centrado en los médicos a un enfoque descentralizado basado en los pacientes [3]. En otras palabras, trata de cambiar un modelo reactivo en el que la gente acude al hospital porque está enferma por un modelo pro-activo y preventivo en el que la gente participa de manera activa en su bienestar, y por tanto puede proporcionar servicios de asistencia sanitaria más personalizados.

El desarrollo de Sistemas Ubicuos de Asistencia Médica (SUAMs) tiene el potencial de poder proporcionar mejores servicios sanitarios a un número de personas que va en aumento, y de reducir los costes a largo plazo de la asistencia sanitaria [4]. Sin embargo, cuando se desarrollan este tipo de sistemas existen ciertos retos tecnológicos que deben ser tenidos en cuenta como por ejemplo su escalabilidad, seguridad e interoperabilidad.

El IEEE define la interoperabilidad como *"la habilidad de dos o más sistemas o componentes para intercambiar información y poder utilizar la información que se ha intercambiado"* [7]. Sin embargo, la interoperabilidad no se tiente en cuenta en la mayoría de los SUAMs existentes, dando como resultado soluciones que son de naturaleza muy especifica, también conocidas como sistemas "cerrados" [8]. Estos sistemas no son capaces de comunicarse entre si dando lugar a la no colaboración entre ellos. Para lograr la interoperabilidad entre diferentes SUAMs es obligatorio el uso de estándares como por ejemplo los desarrollados por la organización "Health Level 7" (HL7). HL7 es un estándar de e-Salud que habilita el intercambio de información médica entre sistemas heterogéneos y organizaciones de forma consistente, ya que define las especificaciones para el formato, los tipos de datos y la estructura de los mensajes para el intercambio de dichos datos. HL7 también ha definido el *Clinical Document Architecture* (CDA). El CDA es un estándar basado en el lenguje de marcas extensible (XML), con el propósito de especificar la codificación estructura y semántica de documentos clínicos. Por otro lado, iniciativas industriales como Continua Health Alliance, con el propósito de establecer un ecosistema de sistemas de salud personales interoperables entre si, utiliza el estándar CDA para proporcionar datos de monitorización personales en forma de registros médicos.

El *Gestational Diabetes Monitoring System* (GDMMS) [9] es un SUAM basado en sistemas multiagente para la monitorización contínua de mujeres afectadas por diabetes mellitus gestacional (DMG). La plataforma de multiagentes del sistema analiza los datos fisiológicos de los pacientes y proporciona alertas cuando se detectan situaciones potencialmente peligrosas para la paciente y el feto en desarrollo. En [10] se describe la seguridad del sistema, mientras que en [11] proporciona un estudio de la escalabilidad del sistema. En este trabajo se describe como se ha proporcionado interoperabilidad al

Actas de las Jornadas de Ingeniería Telemática 2013, ISBN-13: 978-84-616-5597-7, páginas 249 - 256

sistema mediante el cumplimiento del estándar HL7.

En particular, la principal contribución de este trabajo es mostrar cómo se ha utilizado el CDA para registrar el estado de monitorización del paciente y enviar esta información del lado cliente al lado servidor del sistema. Al hacerlo se amplia la funcionalidad del sistema, permitiendo que éste pueda colaborar con otros sistemas heterogéneos que ya estén utilizando el estándar CDA.

El resto del documento está organizado de la siguiente forma: en la Sección II se proporciona una descripción del sistema GDMMS y del estándar CDA; en la Sección III se describe la integración del estándar CDA en el SUAM; en la Sección IV se revisan diferentes sistemas utilizando el estándar CDA. Finalmente en la Sección V se concluye el documento con unas conclusiones y el trabajo futuro a realizar.

II. PRELIMINARES

A. GDMMS

El propósito del sistema GDMMS es asistir el tratamiento de la DMG, un tipo de diabetes que afecta al 3%–10% de las mujeres embarazadas debido a un aumento de resistencia a la insulina. La DMG puede incrementar el riesgo de desarrollar problemas de salud en el feto, por lo tanto es importante realizar un control de los niveles de glucemia en las mujeres embarazadas.

El sistema GDMMS proporciona ayuda para la monitorización de mujeres embarazadas afectadas por DMG mediante el uso de teléfonos inteligentes basados en Android. El terminal permite a las pacientes introducir datos médicos relacionados con la DMG como por ejemplo parámetros fisiológicos, síntomas y medicación. Por otro lado, los médicos al cuidado de las pacientes pueden usar el sistema para visualizar y analizar estos datos. El sistema permite tanto a pacientes como médicos estar informados con valores históricos y recibir alertas cuando se detecten situaciones peligrosas durante el embarazo.

La Figura 1 muestra la arquitectura del sistema. Éste está formado por cinco componentes que son los siguientes:

- *Client workstation*: el lado cliente del sistema pude ser un teléfono móvil o un navegador web. El teléfono móvil permite a las pacientes del sistema enviar los datos de su monitorización al lado servidor. Por su parte, el navegador web lo utilizan los doctores para comprobar el estado de salud de sus pacientes. Ambos utilizan conexiones HTTPS y certificados digitales para el intercambio de datos.
- *Web server*: esta parte está compuesta por un *web entry gate* el cual se ocupa de las peticiones y los certificados de los clientes; y un *web server* que actúa como capa de presentación, responsable de interactuar con la *business layer* para poder atender las peticiones de los doctores.
- *Application server*: está formado por cuatro capas. El i) *security proxy* genera y envía un *token* a los clientes en su primera petición. En las peticiones sucesivas comprueba la validez del *token* (por ejemplo que no haya expirado).

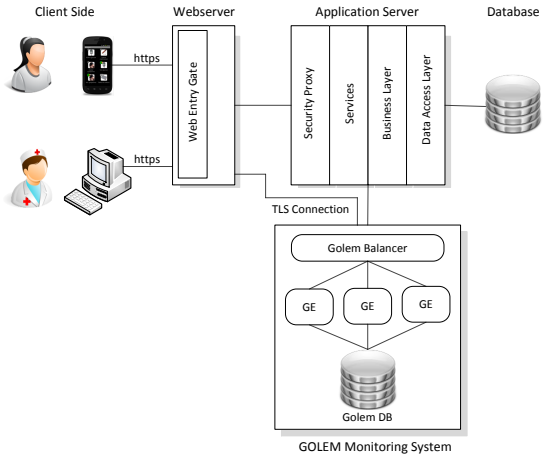


Fig. 1. Arquitectura del sistema GDMMS

La capa ii) *services* comprueba que las peticiones estén bien formadas, y las redirige a la *business layer*. La iii) *business layer* implementa la funcionalidad principal del sistema. Finalmente la iv) *data access layer* proporciona el acceso a los datos almacenados en el servidor.

- *GOLEM monitoring system*: está formado por tres componentes. El i) *GOLEM balancer* es un servicio web que recibe notificaciones de la *business layer*, que consisten en los datos médicos de la paciente. Los ii) *GOLEM environments* son contenedores que hospedan los agentes encargados de la monitorización. Cada paciente tiene asignado un agente que se ocupa analizar sus datos en base a una serie de reglas y generar así las alarmas pertinentes. La iii) *GOLEM database* por su parte almacena los agentes que durante cierto tiempo permanecen inactivos.
- *Database*: almacena toda la información de los pacientes: demográfica, valores de la monitorización y alarmas producidas.

El lector interesado puede encontrar en [12] una descripción detallada del sistema.

B. Clinical Document Architecture (CDA)

El CDA [13] es un estándar de e-Salud desarrollado por la organización internacional HL7. Este estándar especifica la estructura y semántica de un documento clínico con el propósito de intercambio. El CDA se codifica mediante XML y su contenido deriva del *Reference Information Model* (RIM) de la versión 3 de HL7. Un documento CDA incluye texto, pero también puede incluir imágenes, sonidos y otro tipos de contenido multimedia. Un documento CDA presenta las siguientes características [14]:

- Persistencia: un documento clínico continua existiendo sin alteraciones por un periodo de tiempo definido por requerimientos locales y regulatorios.
- Responsabilidad: un documento clínico debe ser mantenido por una organización a la que se asigna su cuidado.

```
<ClinicalDocument>
    <!-- CDA Header -->
    <!-- CDA Body -->
    <component>
        <structuredBody>
            <component>
                <section>...</section>
                <section>...</section>
            </component>
        </structuredBody>
    </component>
</ClinicalDocument>
```

Fig. 2. Ejemplo de documento CDA con un cuerpo estructurado

- Potencial para autenticación: un documento clínico recopila información que tiene prevista su autenticación legal.
- Contexto: un documento clínico establece un contexto para su contenido.
- Completitud: la autenticación de un documento clínico se aplica al conjunto y no se aplica a partes del documento sin el contexto completo del documento.
- Legilibilidad: un documento clínico tiene que poder ser leído por seres humanos.

El elemento raíz de todo documento CDA es `<ClinicalDocument>`. Éste está compuesto por dos partes: una cabecera y un cuerpo. La cabecera especifica el contexto del contenido del documento, mediante su identificación y clasificación, y proporciona información sobre la autenticación, el encuentro, el paciente, y los proveedores involucrados. El cuerpo contiene el informe clínico, el cual puede organizarse mediante un elemento `<NonXMLBody>` o un elemento `<structuredBody>`. El primero permite una baja adopción del estándar mediante el encapsulamiento de un cuerpo sin contenido XML. El segundo permite la definición de un cuerpo estructurado mediante el uso de XML, de tal forma que éste pueda ser interpretado por un ordenador. Un cuerpo estructurado se organiza en uno o mas componentes mediante el uso de elementos `<component>`. A su vez los componentes pueden organizarse en una o múltiples secciones mediante elementos `<section>`. Las secciones presentan riqueza expresiva, permitiendo la representación formal de actos clínicos mediante el uso de múltiples elementos `<entry>`. Estos actos clínicos pueden ser observaciones, administración de medicamentos, efectos secundarios, entre otros.

C. Vocabularios

El contenido narrativo del cuerpo del CDA se puede codificar mediante el uso de vocabularios. Estos estándares están relacionados con terminología médica, proporcionando códigos específicos a conceptos clínicos. En este trabajo se han utilizado los siguientes vocabularios:

- SNOMED CT (*Systemized Nomenclature of Medicine Clinical Terms*): proporciona una colección de términos clínicos que abarca enfermedades, hallazgos, procedimientos, microorganismos, substancias, etc.
- LOINC (*Logical Observation Identifiers Names and Codes*): se utiliza para identificar observaciones médicas de laboratorio.
- ICD-10 (*International Classification of Diseases*): este vocabulario está definido por la Organización Mundial de la Salud (OMS), y proporciona un sistema de códigos para la clasificación de enfermedades.
- ATC (*Anatomical Therapeutic Chemical Classification System*): otro vocabulario definido por la OMS para la clasificación de medicamentos.

III. INTEROPERABILIDAD EN EL GDMMS

El lado cliente del sistema GDMMS para la paciente consiste en un teléfono inteligente basado en Android. El teléfono tiene una aplicación instalada que permite a la paciente introducir una serie de datos médicos, relacionados con la DMG, que se organizan en tres categorías distintas: parámetros fisiológicos, síntomas, y medicamentos. En la Tabla I se muestran los elementos de cada categoría. A parte, la aplicación permite a la paciente comprobar y corregir los datos que han entrado. Todos los datos se almacenan cifrados en el teléfono y se envían al servidor para su procesamiento cuando el teléfono tiene conexión de red.

La información que aparece en la Tabla I se ha codificado siguiendo el estándar CDA para enviar los datos del teléfono al servidor en este formato. El teléfono crea un documento CDA que contiene todos los valores introducidos por la paciente que todavía no hayan sido enviados. Esto se ha realizado mediante la adición de un nuevo módulo al código fuente con todas las clases necesarias para generar el CDA (ver diagrama UML de clases en Figura 3). La clase CDADocument corresponde al documento clínico que se pretende enviar y contiene todos los métodos necesarios para generarlo. El resto de las clases están asociadas cada una a una plantilla XML formateada acorde a su representación en CDA. Para generar el documento clínico, los valores variables de las plantillas XML necesarias se seleccionan mediante expresiones XPath y se rellenan con su valor correspondiente.

Enviar los datos del lado cliente del sistema de forma estándar implica realizar cambios en el lado servidor, para poder procesar correctamente las conexiones. Por otro lado, un documento CDA es de naturaleza persistente y debe ser mantenido por una organización responsable de su cuidado [14]. Estas características se reflejan en el cambio de la base de datos relacional por la base de datos XML BaseX, que permite almacenar el documento clínico en su formato original. Esto implica el uso de XQuery para consultar la información contenida en los documentos CDA. A continuación se detalla la estructura de cada parte del documento CDA.

A. Cabecera del CDA

La cabecera contiene sólo los elementos obligatorios especificados por el estándar. Los elementos opcionales no se han utilizado para minimizar la cantidad de datos enviados a través de la interfaz de red del teléfono.

TABLA I
DATOS RELACIONADOS CON LA DMG CODIFICADOS EN EL CUERPO DEL DOCUMENTO CDA (NOMBRES EN INGLÉS, COMO APARECEN EN LA APLICACIÓN MÓVIL)

Physiological Parameters	Blood pressure
	Heart rate
	Blood sugar
	Weight
Symptoms	Chest pain
	Edema
	Dyspnea
	Blurred vision
	Headache
	Epigastric pain
Medicaments	Insulatard
	Huminsulin basale
	Levemir
	Novorapid
	Humalog
	Metformin

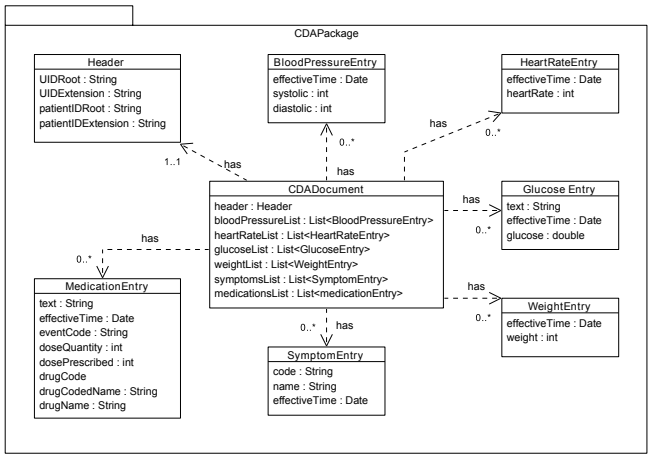


Fig. 3. Diagrama UML de las clases utilizadas para generar el documento CDA

Como se ha expresado en la Sección II la cabecera especifica el contexto del documento clínico. El conjunto mínimo de elementos que define dicho contexto son los siguientes:

- La identificación del documento, la cual se define mediante el elemento `<id>`. Este elemento XML tiene dos atributos *root* y *extension*. El atributo *root* identifica el universo del documento, y *extension* proporciona la identificación única al documento.
- El tipo de documento, especificado con el elemento `<code>`. Para este elemento se ha utilizado el código LOINC "51855-5" con nombre *"Patient Note"*, ya que su descripción se ajusta al tipo de documento generado por la aplicación: "*A patient authored note is generated by a patient, or a patient agent, acting in a non-clinical role to provide clinically relevant information.*"
- La fecha en la cual se creo el documento, definida con el elemento `<effectiveTime>`.
- El nivel de confidencialidad del documento, definido mediante el elemento `<confidentialityCode>`.
- El paciente (o pacientes) al cual pertenece el documento. Todos los datos de identificación del paciente están dentro de un elemento `<recordTarget>`. Estos pueden incluir nombre, género, dirección, entre otros. Sin embargo el único elemento obligatorio es el identificador del paciente especificado mediante un elemento `<id>`.
- El autor del documento, puede ser una persona o un dispositivo con el rol de autor. El autor se define mediante el elemento `<author>` y su elemento hijo `<assignedAuthor>`. El autor se puede especificar mediante su nombre, dirección, teléfono, correo electrónico, pero el único campo obligatorio es su identificador especificado mediante el elemento `<id>`. En este caso la paciente y el autor del documento clínico son la misma persona.
- La organización responsable de mantener el documento, definida con el elemento `<custodian>`. Aunque se puede especificar el nombre, dirección, teléfono entre otros, el único elemento obligatorio es el `<id>`.

TABLA II
CÓDIGOS LOINC UTILIZADOS PARA IDENTIFICAR LAS DISTINTAS SECCIONES DEL CUERPO (EN INGLÉS, COMO APARECEN EN EL ESTÁNDAR)

Section	**Code**	**Display name**
Physiological Parameters	8716-3	Vital signs
Symptoms	10164-2	History of present illness
Medicaments	10160-0	History of medication use

B. Cuerpo del CDA

El cuerpo del CDA generado es un cuerpo estructurado en XML, dividido en tres secciones distintas cada una codificando uno de los siguientes grupos: parámetros fisiológicos, síntomas y medicamentos. Las secciones se distinguen las unas a las otras mediante el uso de códigos LOINC aplicados a elementos `<code>` (ver Tabla II).

1) Parámetros Fisiológicos: La sección correspondiente a los parámetros fisiológicos puede tener cuatro tipos diferentes de entradas distinguidas mediante elementos `<entry>`. Cada tipo de entrada codifica un parámetro fisiológico distinto. Estos parámetros pueden ser: presión arterial, pulso, nivel de azúcar en sangre, o peso. Todos estos parámetros se codifican como observaciones utilizando el elemento `<observation>`. Una observación es un acto que puede ser visto como un procedimiento "no alterante" que da como resultado un valor [14]. Para esta sección un valor es una magnitud física de un parámetro fisiológico, aunque éste puede ser virtualmente cualquier cosa.

Cada parámetro fisiológico se identifica utilizando su correspondiente código SNOMED CT utilizando el elemento `<code>` (ver Tabla III), especifica sus unidades de medida en el atributo *unit* de elemento `<value>`, y tiene unos metadatos asociados como el tiempo en que se tomo la medida especificado en el atributo *value* del elemento `<effectiveTime>`. Las Fig. 3 y Fig. 4 muestran respectivamente la codificación de la presión arterial y el pulso. El atributo *classCode* del elemento `<observation>` define el tipo de acto que se trata, mientras que el atributo *moodCode* describe su posi-

TABLA III
CÓDIGOS SNOMED CT UTILIZADOS PARA IDENTIFICAR LOS PARÁMETROS FISIOLÓGICOS (EN INGLÉS, COMO APARECEN EN EL ESTÁNDAR)

Physiological parameter	Code	Display name
Blood pressure	251076008	Cuff blood pressure
Systolic blood pressure	271649006	Systolic BP
Diastolic blood pressure	271650006	Diastolic BP
Heart rate	364075005	Heart rate
Blood sugar	302789003	Capillary blood glucose measurement (procedure)
Weight	363808001	Body weight measure

TABLA IV
CÓDIGOS ICD-10 UTILIZADOS PARA IDENTIFICAR LOS SÍNTOMAS (EN INGLÉS, COMO APARECEN EN EL ESTÁNDAR)

Symptom	Code	Display name
Chest pain	R07.4	Chest pain, unspecified
Edema	O12.0	Gestational oedema
Dyspnea	R06.0	Dyspnoea
Blurred vision	H53.8	Other visual disturbances
Headache	R51	Headache
Epigastric pain	R10.1	Pain localized to upper abdomen

cionamiento en el tiempo. En este caso el valor *moodCode* de todos los parámetros fisiológicos es "EVN" ya que este define un acto que ya ha ocurrido.

La codificación de la presión sanguínea difiere del resto de parámetros fisiológicos ya que ésta se compone de dos valores distintos, la presión sanguínea sistólica y la diastólica. Esta relación se codifica mediante dos elementos `<entryRelationship>` dentro del elemento `<observation>`. La codificación del pulso también difiere de los otros parámetros fisiológicos ya que se mide en pulsaciones pro minuto (bpm). Este hecho se expresa mediante el elemento `<denominator>` que es un elemento hijo del elemento `<value>`.

2) Síntomas: La sección correspondiente a los síntomas puede tener seis tipos de entradas distintos, cada una codificando un síntoma distinto. Los síntomas, como los parámetros fisiológicos, se han codificado como observaciones mediante elementos `<observation>`. La identificación de los síntomas se realiza utilizando el vocabulario ICD-10 (ver Tabla IV para los códigos). En cada síntoma el elemento `<code>` hijo del elemento `<observation>` proporciona identificación del síntoma. Cada síntoma tiene unos metadatos asociados que consisten en el tiempo en que ocurrió el síntoma. La Fig. 5 muestra un ejemplo codificando el síntoma cefalea.

3) Medicamentos: La sección correspondiente a los medicamentos puede tener seis tipos de entradas distintos, cada una codificando un medicamento distinto. Todos los medicamentos de esta sección se corresponden con tipos de insulina. En esta sección los medicamentos se codifican mediante el elemento `<substanceAdministration>`. Este elemento representa la administración de una substancia particular, p. ej. un medicamento, un inmunizador o otra substancia a un paciente [14].

Cada medicamento se identifica utilizando su código ATC (ver Tabla V). A parte el elemento `<name>` proporciona el nombre del medicamento tal y como aparece en la aplicación móvil. La Fig. 6 muestra el ejemplo de codificación de un medicamento. Los metadatos asociados con un medicamento son: i) un comentario opcional relacionado con la entrada que la paciente puede escribir en la aplicación móvil y que se recoge mediante el elemento `<text>`, ii) la fecha y hora en que el medicamento fue tomado codificado mediante dos elementos `<effectiveTime>`, y iii) la dosis tomada por la paciente y la dosis prescrita por el doctor, ambas expresadas en unidades de insulina (IU).

En la aplicación móvil el tiempo en que se inyectó un bolo de insulina se especifica mediante dos elementos: un *timestamp*, y un texto que especifica cuándo se inyecto el bolo en relación a las comidas p. ej. antes del desayuno, etc. A parte, el CDA especifica que la frecuencia de las dosis se debe especificar con un elemento `<effectiveTime>` del tipo *General Timing Specification* (GTS). El tipo de dato GTS permite usar distintas operaciones como intersecciones, uniones y diferencias para expresar el tiempo como un conjunto de intervalos. La especificación del tiempo de administración del medicamento se ha codificado como la intersección de un *Time Stamp* (TS) y un *Event-Related Periodic Interval of Time* (EIVL). El tipo de dato EIVL se utiliza para representar eventos relacionados con las comidas y el dormir. El elemento `<event>` se utiliza para especificar un evento específico mediante su atributo *code*. Los códigos permitidos están predefinidos en el estándar HL7. La Tabla VI muestra los que se han usado para la aplicación.

Otra particularidad de esta entrada es que el elemento `<substanceAdministration>` sólo permite la codificación de una dosis. Sin embargo, en la aplicación móvil la paciente puede introducir tanto la dosis de insulina recetada por el doctor como la dosis real que se ha inyectado la paciente. Esto es debido a que la diabetes es una enfermedad autogestionada, y por tanto la paciente tiene cierto grado de autonomía para decidir cuál es la dosis de insulina apropiada que necesita ya que los niveles de glucosa en sangre dependen del tipo y cantidad de ingestas tomadas. Para codificar la dosis de insulina que se ha inyectado la paciente se ha utilizado el elemento `<doseQuantity>` definido por el estándar, y se ha añadido el elemento `<dosePrescribed>` para codificar la dosis prescribida por el doctor. Este es el único elemento XML que se ha tenido que definir en todo el CDA con tal de poder codificar todos los datos especificados en la aplicación móvil. El poder añadir elementos XML definidos a nivel local está permitido por el estándar ya que en su Sección 1.4 especifica "*Locally-defined markup may be used when local semantics have no corresponding representation in the CDA specification.*"

La incorporación del elemento `<dosePrescribed>` tiene implicaciones respecto a la interoperabilidad con otros sistemas. En particular, la validación de un documento CDA que contenga extensiones debe realizarse por fases [14]. En una primera fase se deben validar las extensiones, mediante el uso de XML Schema o ISO Schematron que se deben proporcionar

```
<observation classCode="OBS" moodCode="EVN">
    <code code="251076008" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED CT" displayName="Cuff blood pressure
        "/>
    <effectiveTime value="201301221746"/>
    <entryRelationship typeCode="COMP">
        <observation classCode="OBS" moodCode="EVN">
            <code code="271649006" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED CT" displayName="Systolic BP
                "/>
            <value unit="mm[Hg]" value="120" xsi:type="PQ"/>
        </observation>
    </entryRelationship>
    <entryRelationship typeCode="COMP">
        <observation classCode="OBS" moodCode="EVN">
            <code code="271650006" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED CT" displayName="Diastolic
                BP"/>
            <value unit="mm[Hg]" value="80" xsi:type="PQ"/>
        </observation>
    </entryRelationship>
</observation>
```

Fig. 3. Medida de la presión arterial codificada en el CDA

```
<observation classCode="OBS" moodCode="EVN">
    <code code="364075005" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED CT" displayName="Heart rate"/>
    <effectiveTime value="201301221746"/>
     <value xsi:type="RTO_PQ_PQ">
        <numerator value="60"/>
        <denominator unit="min" value="1"/>
    </value>
</observation>
```

Fig. 4. Medida del pulso codificada en el CDA

```
<observation classCode="OBS" moodCode="EVN">
    <code code="R51" codeSystem="2.16.840.1.113883.6.3" codeSystemName="ICD10" displayName="Headache"/>
    <effectiveTime value="201305212115"/>
</observation>
```

Fig. 5. Síntoma de dolor de cabeza codificado en el CDA

TABLA V
CÓDIGOS ATC UTILIZADOS PARA IDENTIFICAR LOS MEDICAMENTOS (EN INGLÉS, COMO APARECEN EN EL ESTÁNDAR)

Medicament	**Code**	**Display name**
Insulatard	A10AC01	insulin (human)
Huminsulin basale	A10AD01	insulin (human)
Levemir	A10AE05	insulin detemir
Novorapid	A10AB05	insulin aspart
Humalog	A10AB04	insulin lispro
Metformin	A10BA02	metformin

TABLA VI
CÓDIGOS DE EVENTOS RELACIONADOS CON EL TIEMPO UTILIZADOS PARA IDENTIFICAR LOS PERIODOS DEL DÍA (EN INGLÉS, COMO APARECEN EN EL ESTÁNDAR)

Time of the day	**Code**	**Meaning (from lat.)**
Before breakfast	ACM	ante cibus matutinus
After breakfast	PCM	post cibus matutinus
Before lunch	ACD	ante cibus diurnus
After lunch	PCD	post cibus diurnus
Before dinner	ACV	ante cibus vespertinus
After dinner	PCV	post cibus vespertinus
Later	ICV	inter cibus vespertinus

al resto de aplicaciones. Una vez se han validado las extensiones éstas se deben eliminar antes de realizar posteriores validaciones. Este proceso se puede realizar mediante el uso de hojas de estilo XSLT.

IV. TRABAJOS RELACIONADOS

Aunque en la mayoría de SUAMs la interoperabilidad no se tiene en cuenta [8], en la literatura se pueden encontrar distintos proyectos que han utilizado el estándar CDA para proporcionar interoperabilidad. Todos estos sistemas podrían interactuar con el sistema GDMMS combinándolos de distintas formas. Aunque estas integraciones no son directas, el uso del estándar CDA minimiza los esfuerzos requeridos para conseguirlo.

En [15] los autores presentan un *Home Telecare System* (HTS) que consiste en una base de datos de paciente y un sistema de informes. La base de datos amacena valores extraídos de señales vitales, mientras que el sistema de informes realiza un análisis sobre estos datos. El sistema de informes convierte primero la información a formato XML que a su vez se utiliza para generar el documento CDA. En este sistema el documento CDA generado contiene sólo constantes vitales, mientras que en el sistema GDMMS el documento CDA también contiene información sobre síntomas y mediación. Además, en el sistema GDMMS el uso del terminal móvil permite la movilidad del paciente mientras se le monitoriza. Es por ello que el sistema GDMMS podría complementar a

```
<substanceAdministration classCode="SBADM" moodCode="EVN">
    <text>optional comment related with the entry</text>
    <effectiveTime xsi:type="TS" value="201305211250"/>
    <effectiveTime xsi:type="EIVL" operator="A">
        <event code="ACD"/>
    </effectiveTime>
    <doseQuantity value="2.5" unit="IU"/>
    <dosePrescribed value="2" unit="IU"/>
    <consumable>
        <manufacturedProduct>
            <manufacturedLabeledDrug>
                <code code="A10AE05" codeSystem="2.16.840.1.113883.6.73" codeSystemName="ATC" displayName="insulin detemir
                    "/>
                <name>Levemir</name>
            </manufacturedLabeledDrug>
       </manufacturedProduct>
    </consumable>
</substanceAdministration>
```

Fig. 6. Medicamento Levemir codificado en el CDA

este sistema extendiendo sus funcionalidades. Para conseguir esta relación de inclusión la información sobre síntomas y medicación se debería enviar a la base de datos, y el sistema de informes debería incluir estas secciones en los informes CDA generados.

En [16] se presenta una *smart home healthcare system*. El objetivo de este sistema es la monitorización de pacientes que sufren alzheimer. En este sistema los datos sobre distintas actividades se captan mediante sensores de movimientos, preprocesados utilizando distintos algoritmos, y almacenados en formato XML. Cada actividad incluye información sobre el tipo de actividad, el sensor, la persona que realizó la actividad y la fecha en que se realizó la actividad. El sistema genera un documento CDA con todas las actividades realizadas por los pacientes, que se puede transmitir a todos los centros hospitalarios suscritos a la *smart home*. Este sistema y el sistema GDMMS monitorizan diferentes tipos de enfermedades, es por ello que podían tener una relación de comorbilidad combinando las funcionalidades de ambos.

Koutkias et al. [17] proponen una plataforma centrada en la gestión de la medicación para proporcionar ayuda respecto los efectos secundarios de los medicamentos. Su arquitectura se compone de dos subsistemas, uno en el lado paciente y otro en el lado medico. La parte del paciente se compone por una red de sensores corporales que mide la presión arterial y el pulso, y una unidad base móvil (UBM) que coordina la red de sensores y notifica al lado médico el estado de la monitorización. El lado médico almacena los datos de la monitorización y envía a la UBM información relacionada con la prescripción como los objetivos en cuanto a los parámetros monitorizados, efectos secundarios que pueden ocurrir, y patrones para la detección de efectos secundarios. La comunicación entre ambos subsistemas se realiza mediante XML. Del lado médico al lado paciente la información sobre la prescripción del medicamento se codifica utilizando un *schema* propio, y para el canal reverso los resultados de la monitorización se proporcionan utilizando el CDA. La funcionalidad de este sistema relacionada con los efectos secundarios se podría incluir en el sistema GDMMS, complementándolo con una relación de inclusión.

Todos los sistemas descritos tratan la interoperabilidad mediante la generación de documentos CDA que informan sobre el estado de monitorización del paciente. Sin embargo, ninguno de ellos proporciona información sobre como han seguido las especificaciones del estándar o la estructura de los documentos CDA generados.

Por otro lado, el sector industrial está más concienciado con la interoperabilidad de sistemas. En particular, HL7 y Continua han publicado conjuntamente el *Personal Healthcare Monitoring Record* (PHMR), una guía de implementación del CDA que restringe los elementos a utilizar para la cabecera y el cuerpo del CDA. El PHMR está pensado para ser implementado por dispositivos de monitorización como glucómetros, esfingomanometros, etc. que quieran transmitir de manera estandarizada los valores de sus medidas. La propuesta de CDA descrita en este artículo difiere del PHMR ya que está más orientada hacia el paciente. Esto se refleja en el hacho de que el PHMR no tiene una sección específica para síntomas, ya que los síntomas sólo pueden ser comunicados por el paciente.

V. CONCLUSIONES Y TRABAJO FUTURO

La mayoría de SUAMs que se pueden encontrar en la literatura no tienen en cuenta la interoperabilidad [8]. En este artículo se ha descrito la implementación del estándar CDA en un SUAM particular para hacerlo interoperable. En concreto se ha utilizado el CDA para producir un documento clínico el cual reporta en tres secciones distintas los parámetros fisiológicos, los síntomas, y la medicación administrada por la paciente. Los autores creemos que este trabajo puede tomarse como referencia para proporcionar interoperabilidad a futuras implementaciones de SUAMs.

Además, se concluye la necesidad de ampliar las especificaciones del CDA con tal de considerar la participación del paciente en el proceso de monitorización. Por ejemplo, en GDMMS hay dos tipos de dosis de insulina, la inyectada por la paciente y la prescrita por el doctor, mientras que en estándar CDA sólo existe un atributo para codificar dosis. Por este motivo se ha tenido que añadir el elemento `<dosePrescribed>` para modelar la dosis de insulina prescrita por el médico, y se ha utilizado el elemento `<doseQuantity>` proporcionado por el estándar

para especificar la dosis de insulina inyectada por la paciente. Se asume también que en un escenario real, se debería pedir a la organización HL7 un código para la organización encargada de la custodia del documento para poderla identificar un *ISO Object Identifier* (OID) único.

Como trabajo futuro se planea mejorar la escalabilidad del sistema, moviendo la plataforma multiagente del servidor a la parte cliente del sistema. En consecuencia, las alertas generadas por los agentes se pueden codificar como una nueva sección dentro del documento CDA que se genera actualmente en el terminal móvil.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por la Hasler Foundation y el proyecto TAMESIS (TEC2011-22746).

REFERENCIAS

[1] B. Arnrich, O. Mayora, J. Bardram, and G. Tröster, "Pervasive Healthcare Paving the Way for a Pervasive, User-centered and Preventive Healthcare Model," *Methods of Information in Medicine*, vol. 49, no. 1, pp. 67–73, 2010.

[2] U. Varshney, "Pervasive Healthcare and Wireless Health Monitoring," *Mobile Networks and Applications*, vol. 12, no. 2-3, pp. 113–127, 2007.

[3] J. E. Bardram, "Pervasive Healthcare as a Scientific Discipline," *Methods of Information in Medicine*, vol. 47, no. 3, pp. 178–185, 2008.

[4] U. Varshney, "Pervasive Healthcare," *IEEE Computer*, vol. 36, no. 12, pp. 138–140, 2003.

[5] A. B. Bondi, "Characteristics of Scalability and Their Impact on Performance," in *Proceedings of the 2nd international workshop on Software and performance*, ser. WOSP '00. New York, NY, USA: ACM, 2000, pp. 195–203. [Online]. Available: http://doi.acm.org/10.1145/350391.350432

[6] Y. Liu and F. Li, "PCA: A Reference Architecture for Pervasive Computing," in *Pervasive Computing and Applications, 2006 1st International Symposium on*, 2006, pp. 99–103.

[7] "IEEE Standard Computer Dictionary. A Compilation of IEEE Standard Computer Glossaries," *IEEE Std 610*, 1991.

[8] M. Baumgarten and M. D. Mulvenna, "Cognitive Sensor Networks: Towards Self-adapting Ambient Intelligence for Pervasive Healthcare," in *PervasiveHealth*, 2011, pp. 366–369.

[9] R. Schumann, S. Bromuri, J. Krampf, and M. I. Schumacher, "Agent Based Monitoring of Gestational Diabetes Mellitus (Demonstration)," in *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems - Volume 3*, ser. AAMAS '12, 2012, pp. 1487–1488. [Online]. Available: http://dl.acm.org/citation.cfm?id=2343896.2344074

[10] S. Bromuri, J. Krampf, R. Schumann, and M. Schumacher, "Enforcing Security in Pervasive Healthcare Monitoring Gestational Diabetes Mellitus," in *Proceedings of the Fourth International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED 2012)*. IARIA, Feb. 2012, pp. 221–226.

[11] J. Krampf, S. Bromuri, M. Schumacher, and J. Ruiz, "An Agent Based Pervasive Healthcare System: A First Scalability Study," in *Electronic Healthcare*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012, vol. 91, pp. 128–137.

[12] S. Bromuri, M. I. Schumacher, K. Stathis, and J. Ruiz, "Monitoring Gestational Diabetes Mellitus with Cognitive Agents and Agent Environments," in *IAT*, 2011, pp. 409–414.

[13] R. H. Dolin, L. Alschuler, S. Boyer, C. Beebe, F. M. Behlen, P. V. Biron, and A. S. Shvo, "HL7 Clinical Document Architecture, Release 2," *JAMIA*, vol. 13, no. 1, pp. 30–39, 2006.

[14] K. Boone, *The CDA ™ Book*. Springer, 2011.

[15] H. Garsden, J. Basilakis, B. Celler, K. Huynh, and N. Lovell, "A Home Health Monitoring System Including Intelligent Reporting and Alerts," in *Engineering in Medicine and Biology Society, 2004. IEMBS '04. 26th Annual International Conference of the IEEE*, vol. 2, Sept. 2004, pp. 3151–3154.

[16] W. A. Khan, M. Hussain, A. M. Khattak, M. Afzal, B. Amin, and S. Lee, "Integration of HL7 Compliant Smart Home Healthcare System and HMIS," in *Impact Analysis of Solutions for Chronic Disease Prevention and Management*, ser. Lecture Notes in Computer Science, 2012, vol. 7251, pp. 230–233.

[17] V. Koutkias, I. Chouvarda, A. Triantafyllidis, A. Malousi, G. D. Giaglis, and N. Maglaveras, "A Personalized Framework for Medication Treatment Management in Chronic Care," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 2, pp. 464–472, 2010.

Modelo basado en HMM para la detección de emociones a partir de interacciones durante el aprendizaje de desarrollo de software

Derick Leony*, Pedro J. Muñoz-Merino*, Abelardo Pardo†, Carlos Delgado Kloos*
* Departamento de Ingeniería Telemática,
Universidad Carlos III de Madrid
Leganés, España
{dleony, pedmume, cdk}@it.uc3m.es
† School of Electrical and Information Engineering,
University of Sydney, NSW, 2006
Australia
abelardo.pardo@sydney.edu.au

***Resumen*—Este artículo presenta un modelo para la detección de estados de ánimo durante la realización de actividades relacionadas con el desarrollo de software. La detección se realiza a partir de datos generados por el usuario al utilizar herramientas en su entorno de trabajo. El modelo se basa utilizar estos datos como observaciones de un modelo oculto de Markov para cada emoción en un conjunto seleccionado: alegría, frustración, confusión y aburrimiento. La emoción se detecta a partir de las probabilidades de generación de las secuencias de datos. En el artículo se explica en detalle el proceso de captura y normalización de datos, así como la justificación de los modelos para cada emoción. También se explica la implementación del modelo así como un ejemplo de la utilización del mismo en un entorno educativo.**

***Palabras Clave*—estado de ánimo, desarrollo de software, analítica del aprendizaje, telemática**

I. INTRODUCCIÓN

La inclusión de características afectivas en sistemas computacionales es un tema de interés desde hace casi dos décadas. Esta temática incluye dos grandes áreas: la síntesis de emociones por parte de un sistema computacional, y el reconocimiento automático de las emociones expresadas por una persona [1]. En este artículo nos centramos en el reconocimiento de emociones durante el aprendizaje de desarrollo de software. Durante la actividad del desarrollo de software, el estudiante puede percibir varios estados afectivos que afectan su rendimiento. Por ejemplo, no encontrar la causa de un error de compilación o no comprender mensajes de error puede generar un sentimiento de frustración. Esta información afectiva puede ser muy importante en sistemas de soporte al desarrollo de software, ya sea en un entorno de trabajo o en uno educativo.

Gran parte del estado del arte para la detección de emociones se ha enfocado en el estudio de factores fisiológicos y su relación con estados afectivos de la persona. Estos estudios hacen uso de sensores corporales para la medición de características como ritmo cardíaco, actividad eléctrica del corazón, conductividad de la piel y actividad bioeléctrica cerebral. Si bien la usabilidad de sensores corporales ha incrementado en los últimos años, su uso sigue implicando un alto nivel de invasión en el entorno del usuario. Los sensores corporales especialmente incómodos en entornos de trabajo como el que trata este artículo debido al posible efecto sobre la concentración de la persona.

Por otro lado, existen diversas acciones que pueden capturarse durante la creación de software. Como ejemplo pueden mencionarse eventos propios del dominio tales como una compilación con resultado erróneo o iniciar la depuración de un programa; también se pueden observar eventos genéricos como la edición de ficheros y el uso del navegador web. En este artículo proponemos un modelo para el análisis de secuencias de eventos para inferir información afectiva. El análisis se realiza mediante el uso de modelos ocultos de Markov (HMM) cuyas observaciones son los eventos generados durante la actividad de aprendizaje. La implementación de este modelo posee la ventaja de ser invisible para el usuario, por lo que no implica invasión alguna.

El articulo está organizado de la siguiente forma: La sección II incluye el estado del arte en relación al análisis de comportamiento durante el desarrollo de software y a la detección de emociones en entornos educativos. En la sección III se explica en detalle el modelo y se justifican las decisiones hechas para su definición. El artículo también incluye la descripción de la implementación del modelo y un ejemplo de su aplicación, en la sección IV. Finalmente, en la sección V presentamos las conclusiones del trabajo y el trabajo futuro relacionado con esta línea de investigación.

II. ESTADO DEL ARTE

El estudio de la computación afectiva incluye del reconocimiento, entendimiento y síntesis de emociones por parte de sistemas computarizados. En [1] Picard presenta la base teórica así como aproximaciones iniciales para la implementación de sistemas afectivos.

Respecto al área de reconocimiento de emociones, Calvo y D'Mello [2] presentan una categorización de aproximaciones y de la información a utilizar para ello. Siguiendo esta categorización, nuestro trabajo se encuentra en la dimensión de aproximaciones cognitivas para la detección de emociones. Una de las observaciones que pueden realizarse sobre la literatura es la falta de consideración de datos relacionados

con las aplicaciones que una persona utiliza en entornos informáticos. Los datos que utilizamos en nuestro estudio están en el área definida como multimodal, ya que son el resultado de acciones del usuario que describen parcialmente su comportamiento y provienen de varias fuentes.

Entre los trabajos relacionados con la detección de emociones en entornos educativos, Arroyo et al. han estudiado el uso de sensores corporales como entrada de un sistema inteligente de enseñanza (ITS por sus siglas en inglés) [3]. Las emociones de interés en este trabajo son confianza, frustración, entusiasmo e interés. Se utiliza una cámara web para analizar expresiones faciales, un ratón sensible a la presión aplicada sobre sus botones, un brazalete sensor de conductividad en la piel y una funda especial en la silla para el análisis de la postura del alumno. El estudio concluye en que la cámara web y la funda de la silla son los sensores que presentan mayor correlación con las emociones de interés. En una línea similar, D'Mello et al. han trabajado en la detección de emociones durante el uso del ITS *AutoTutor* [4], [5]. Una de sus conclusiones es que las emociones que suelen expresarse durante una actividad de aprendizaje son frustración, aburrimiento, confusión y entusiasmo; factor que utilizamos en nuestro análisis. Su trabajo también utiliza sensores e incluye el análisis de diálogo conversacional entre el ITS y el estudiante. En otro estudio, Conati y Zhou han propuesto un modelo para la detección de las emociones de estudiantes durante el uso de un juego educativo [6]. Su modelo se basa en una red dinámica de decisión y persigue la detección de tipos de personalidad, emociones y metas.

Nuestro trabajo se diferencia de los descritos anteriormente por el hecho de no utilizar sensores corporales para la captura de emociones. Además, los datos de bajo nivel que analizamos provienen de la interacción del estudiante con varias herramientas y no solamente de un ITS o de un juego educativo. También diferenciamos el trabajo al centrarnos en el dominio concreto de desarrollo de software.

III. DESCRIPCIÓN DEL MODELO

El proceso para la detección de emociones se divide en dos: la captura de eventos generados por el usuario durante el desarrollo de software y el análisis de estos datos para inferir el estado anímico. La captura de eventos se basa en el trabajo realizado previamente por Pardo y Delgado Kloos descrito en [7].

III-A. Entorno de aprendizaje y captura de eventos

Los estudiantes utilizan una máquina virtual provista con las herramientas necesarias para la realización de la asignatura. Los programas hechos durante la asignatura son entregados a través del sistema de control de versiones, ya que los profesores también tienen acceso al mismo. La máquina virtual está configurada para grabar la interacción de los estudiantes con un conjunto específico de aplicaciones. Algunas de estas herramientas son específicas para el dominio de la asignatura (compilador, depurador, depurador de memoria, línea de comandos y sistema controlador de versiones) mientras que otras son de uso genérico (editor de texto y navegador web). La figura Fig. 1 muestra una captura de pantalla del escritorio de la máquina virtual.

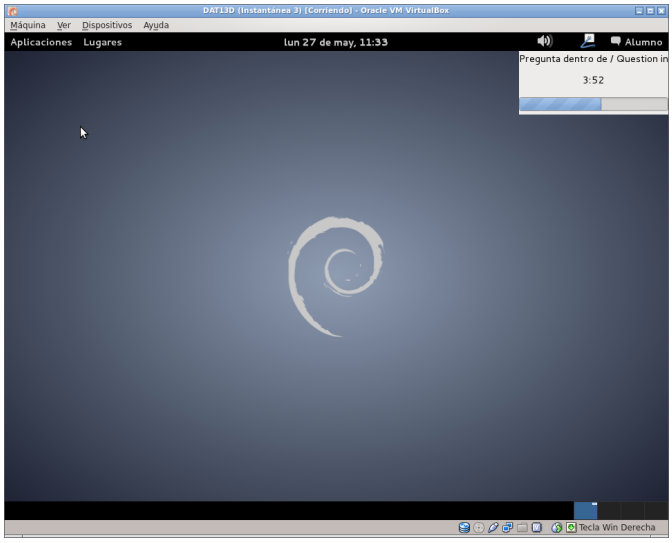


Figura 1. Captura de pantalla de máquina virtual.

La interacción con las herramientas indicadas, incluyendo la hora y el tipo de acción realizada por el estudiante se almacena en un fichero o *log*. La información almacenada en estos *logs* depende de los datos provistos por la herramienta asociada. Por ejemplo, un navegador web permite conocer la dirección web (URL) que el alumno ha accedido y este es el único dato almacenado en el *log* del navegador. Un compilador genera un informe detallado en caso de encontrar algún error en el programa compilado y la máquina virtual captura todo este informe dentro del *log* del compilador. Los *logs* se almacenan en formato de texto plano dentro de carpetas ocultas en el entorno de trabajo de los estudiantes.

Durante la realización de las prácticas de la asignatura se requiere a los estudiantes enviar su trabajo a través de un sistema controlador de versiones. Los *logs* de las herramientas utilizadas se envían junto a su trabajo al servidor central del gestor de versiones. Este proceso se repite con cada actualización hecha por los estudiantes, por lo que los *logs* de eventos capturados se almacenan de forma incremental en el servidor. El análisis de los eventos capturados puede realizarse al final de un período específico (e.g. al finalizar el curso académico) o de forma periódica (e.g. de forma diaria).

Además de los *logs* generados en la máquina virtual, también pueden obtenerse eventos provenientes de fuentes externas. En el caso del contexto educativo de este estudio contamos con los eventos generados dentro del ambiente virtual de aprendizaje, el cual es una instancia de Moodle, y con los accesos al sitio web oficial de la asignatura. Los eventos generados en Moodle pueden incluir interacciones con el curso tales como acceder a la página de la asignatura o al listado de personas matriculadas. Los eventos relacionados al servidor web de la asignatura se restringen a los registros de acceso a las páginas web.

Para analizar los eventos almacenados en el servidor central es necesario normalizar los *logs*, debido a que poseen datos relacionados a la herramienta de la que provienen. La normalización se realiza mediante el análisis léxico del contenido de los ficheros, y la información normalizada se almacena en un formato genérico. En nuestro caso, el formato genérico es

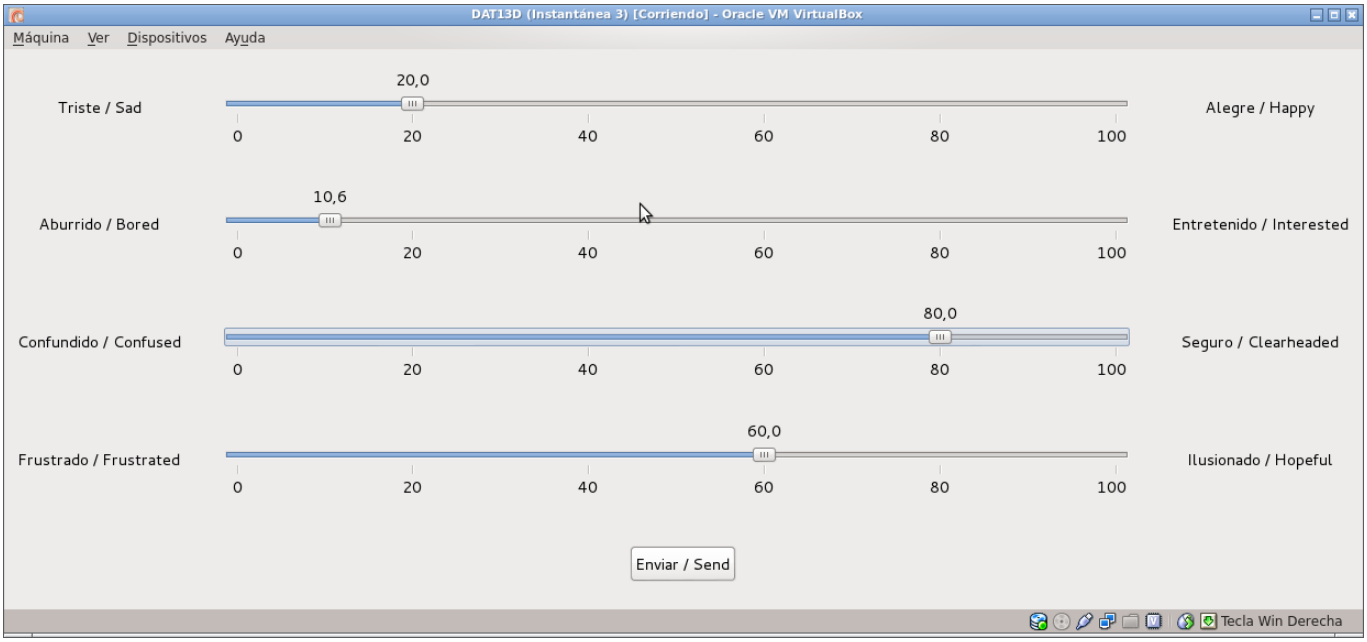


Figura 2. Formulario sobre estado anímico del estudiante.

Contextualized Attention Metadata (CAM) [8], el cual permite definir acciones de usuarios en entornos computarizados. En caso de que el lector esté interesado en más detalles sobre el proceso de captura de datos véase [7] y para experiencias relacionadas consulte [9].

Finalmente, es necesario conocer información explícita sobre el estado anímico del estudiante. Esta información permite tanto la evaluación del modelo propuesto así como un posible entrenamiento del modelo. Se adaptó la máquina virtual para poder consultar al estudiante sobre su estado anímico mediante un formulario en el que indican el nivel de las cuatro emociones de interés: alegría, frustración, aburrimiento y confusión. El formulario se muestra de forma recurrente y la frecuencia de visualización se puede configurar por el administrador de la máquina virtual. El estudiante debe modificar todos los valores de las emociones para poder enviar sus respuestas. Las respuestas a este formulario se envían al servidor central junto con los *logs* de actividad. Se muestra una captura de pantalla del formulario en la Fig. 2.

III-B. Uso de modelos ocultos de Markov para inferir emociones

Varios modelos relacionan la ocurrencia de eventos a la aparición de emociones [10], [11], [12]. Una característica común en estos modelos es la clasificación de eventos como favorables o desfavorables para alcanzar un objetivo. En el contexto de este artículo, el objetivo de un estudiante es completar una actividad de aprendizaje de desarrollo de software exitosamente. A partir de este objetivo, definimos un modelo para el análisis de secuencias de eventos y asociarlas a la emoción que posea la mayor probabilidad de generar dicha secuencia. Por ejemplo, una secuencia con mayoría de eventos contrarios al objetivo del alumno (la obtención de errores al compilar o al analizar el uso de memoria de un programa) sería clasificada con la emoción de frustración.

Dada la necesidad para detectar patrones en una secuencia de observaciones, utilizamos Modelos Ocultos de Markov (HMM). Los HMM están definidos por dos conjuntos de elementos: un alfabeto o conjunto de símbolos y un conjunto de estados. El comportamiento del modelo está definido por tres conjuntos de probabilidades: una lista de la probabilidad de cada estado de ser el estado inicial, una matriz de probabilidades de generación de cada observación, y una matriz de probabilidades de transición entre estados. Desde el exterior del HMM se tiene acceso a los símbolos generados por este, pero no a la secuencia de estados. Entre las propiedades de los HMM se encuentra la posibilidad de calcular la probabilidad de producir una secuencia de símbolos observada; esto mediante el uso del algoritmo de avance-retroceso.

Los símbolos u observaciones a utilizar en nuestra propuesta se construyen a partir de los eventos capturados previamente. Algunos símbolos se obtienen directamente del evento generado en la máquina virtual, como es el caso del símbolo *command*. En otros casos, el símbolo en el que se traduce un evento depende de la información adicional de dicho evento (e.g. el evento de compilación puede generar el símbolo *compile-error* o *compile-ok*). En otros casos sucede lo contrario, eventos diferentes pueden generar el mismo símbolo (e.g. todos los eventos generados en el foro de Moodle generan el símbolo *observations*). La tabla I presenta un listado las observaciones tomadas en cuenta así como sus descripciones y las herramientas que las generan, ya sea dentro de la máquina virtual o desde sistemas externos monitorizados.

Nuestro modelo define cinco estados en el HMM descritos a continuación:

1. *Trabajo en actividad* (E_1). Implica trabajar fluidamente en el desarrollo de software. La mayoría de las compilaciones son exitosas y la mayor parte del trabajo se realiza en el entorno de programación. Pueden existir compilaciones erróneas aunque no en gran mayoría y con resolución rápida. Se considera que puede existir comunicación con profesores y otros estudiantes me-

Cuadro I
SÍMBOLOS OBSERVADOS EN EL MODELO.

Observación	Descripción	Herramientas que la generan
command	Instrucción introducida en la línea de comandos	Bash
forum	Cualquier interacción con el foro de la asignatura: acceder a un hilo, crear un nuevo hilo y enviar un mensaje.	Foros en LMS Moodle
compile-error	Compilación con resultado erróneo	GCC, Java
compile-ok	Compilación con resultado exitoso	GCC, Java
debugger	Interacción con la herramienta de depuración	GDB
ide	Interacción con el entorno de desarrollo	KDevelop
lms	Interacción con herramientas del ambiente virtual de aprendizaje que no sean el foro	Moodle
text-editor	Arranque o finalización del editor de texto	Kate
resource-external	Acceso a material no relacionado a la asignatura	Google Chrome, Mozilla Firefox
resource-internal	Acceso a material relacionado con la asignatura (basado en la URL del material)	Google Chrome, Mozilla Firefox
resource-search	Acceso al motor de búsqueda Google	Google Chrome, Mozilla Firefox
memory-ok	Análisis de manejo de memoria con resultado exitoso	Valgrind
memory-error	Análisis de manejo de memoria con resultado erróneo	Valgrind

diante el foro, pero no se espera la consulta de material de clase o adicional.

2. *Encuentro de dificultad* (E_2). Implica un momento de saturación del programador en el que no puede corregir rápidamente un error de compilación o ejecución. Es común ver iteraciones del uso del editor de texto y del compilador, en los intentos por solucionar el error. Debido a que este estado es exactamente el punto donde el estudiante obtiene un error, no se espera ningún tipo de interacción con herramientas diferentes al compilador y al analizador de memoria y, en menor nivel, con la línea de comandos.
3. *Búsqueda de información* (E_3). Este estado se caracteriza por el acceso a material de soporte en búsqueda de la solución al problema encontrado en el estado E_2. El estudiante en este estado suele utilizar el navegador web para buscar material relacionado al problema. Se espera un nivel alto de interacción en los foros de Moodle. Además, accede a documentos locales y a la documentación del entorno de programación. Al ser un estado de búsqueda de información, no se espera el uso de ninguna de las herramientas relacionadas al desarrollo de software en sí.
4. *Solución a dificultad* (E_4). En este estado se encuentra y aplica la solución a la dificultad descrita en el estado E_2. Generalmente se producirá un numero reducido de compilaciones exitosas y ninguna compilación errónea. Este estado no genera ningún símbolo relacionado a la consulta de información en foros o en material de la asignatura.
5. *Distracción* (E_5). Implica que el programador no está trabajando en la tarea de desarrollo de software sino en una tarea no relacionada. En este estado se observan entre otros eventos, el acceso a sitios web no relacionados al desarrollo de software. No se espera ningún tipo de eventos relacionados a las herramientas de desarrollo de software.

Cada uno de los estados en el modelo posee una probabilidad de emitir cada símbolo descrito previamente. La asignación de probabilidades depende de la descripción del estado y de las herramientas que están relacionadas al mismo.

Cuadro II
PROBABILIDADES DE EMISIÓN PARA CADA ESTADO.

Símbolo	E_1	E_2	E_3	E_4	E_5
command	0.25	0.05	0.00	0.05	0.00
forum	0.10	0.00	0.30	0.00	0.00
compile-error	0.15	0.70	0.00	0.00	0.00
compile-ok	0.10	0.00	0.00	0.50	0.00
debugger	0.05	0.00	0.00	0.05	0.00
ide	0.05	0.00	0.00	0.05	0.00
lms	0.10	0.00	0.10	0.00	0.05
text-editor	0.10	0.00	0.00	0.00	0.00
resource-external	0.00	0.00	0.10	0.00	0.95
resource-internal	0.00	0.00	0.30	0.00	0.00
resource-search	0.00	0.00	0.20	0.00	0.00
memory-ok	0.05	0.00	0.00	0.35	0.00
memory-error	0.05	0.25	0.00	0.00	0.00

La tabla II presenta las probabilidades asignadas inicialmente en nuestro modelo. Estas probabilidades pueden obtenerse mediante el entrenamiento del modelo utilizando algoritmos como Baum-Welch.

Mientras que las probabilidades de emisión de símbolos son constantes para todas las emociones, las probabilidades de transición sí varían dependiendo de la emoción del alumno. Actualmente nos enfocamos en cuatro estados anímicos que suelen observarse en experiencias de aprendizaje: alegría, frustración, confusión y aburrimiento. Aunque los últimos dos suelen clasificarse como estados cognitivos, se ha observado un nivel alto de correlación entre la ocurrencia de estos y ganancias de aprendizaje [4]. Además, es posible relacionar la confusión y el aburrimiento con el comportamiento del desarrollador de software. Por ejemplo, en este escenario un estudiante confundido intenta programar con una aproximación de prueba y error. Un estudiante aburrido tiende a hacer tareas que no están relacionadas a la asignatura, así como navegar sitios web sin relación alguna al material de clase.

En el caso de alegría, esperamos un trabajo fluido del alumno. Esto implica que la mayor parte de las transiciones tengan como destino el estado *Trabajo en actividad* (E_1) sin importar el estado origen. Es posible que el alumno encuentre un problema pero deberá encontrar la solución a este con una probabilidad relativamente alta. Se espera una ocurrencia casi nula del estado *Distracción* (E_5) porque el alumno

Cuadro III
PROBABILIDADES DE TRANSICIÓN PARA EL ESTADO ANÍMICO DE ALEGRÍA.

Estado	E_1	E_2	E_3	E_4	E_5
E_1	0.60	0.10	0.10	0.10	0.10
E_2	0.30	0.20	0.30	0.10	0.10
E_3	0.40	0.10	0.20	0.20	0.10
E_4	0.60	0.10	0.10	0.10	0.10
E_5	0.60	0.10	0.10	0.10	0.10

Cuadro IV
PROBABILIDADES DE TRANSICIÓN PARA EL ESTADO ANÍMICO DE FRUSTRACIÓN.

Estado	E_1	E_2	E_3	E_4	E_5
E_1	0.40	0.30	0.10	0.10	0.10
E_2	0.10	0.50	0.20	0.05	0.15
E_3	0.25	0.50	0.10	0.05	0.10
E_4	0.70	0.15	0.05	0.05	0.05
E_5	0.30	0.30	0.15	0.05	0.20

está motivado en la tarea de desarrollo llevada a cabo. La tabla III muestra una propuesta inicial de las probabilidades de transición para el estado anímico de alegría.

Las probabilidades de transición para el modelo de frustración se incluyen en la tabla IV. La característica principal en este caso es una probabilidad alta de trasladarse al estado *Encuentro de dificultad* (E_2). No se espera una probabilidad alta del estado *Búsqueda de información* (E_3) hacia la solución del problema debido al estado de frustración del alumno. También se considera una probabilidad mayor de permanecer en el estado *Distracción* (E_5).

Las probabilidades de transición para la confusión son similares a las de frustración por la similitud de sus causas en un entorno de desarrollo de software. La principal diferencia en la definición de sus HMM consiste en que el estudiante tiene aún más probabilidad de quedar en el estado *Encuentro de dificultad* (E_2). De nuevo no se espera gran cantidad de transiciones del estado *Búsqueda de información* (E_3) a *Solución a dificultad*, y se incrementa la posible transición hacia el estado de distracción. En este caso se realza aún más la probabilidad de que el estudiante permanezca en el estado *Distracción* (E_5). Las probabilidades de transición para la confusión se listan en la tabla V.

Finalmente, la tabla VI presenta las probabilidades de transición para el estado de aburrimiento. En este caso se espera que el estudiante al desarrollar software o buscar información relacionada a esa tarea termine realizando actividades no relacionadas. En este caso sobresale la alta probabilidad de pasar al estado *Distracción* (E_5), manteniendo una probabilidad alta de permanecer en dicho estado.

Para identificar el estado de ánimo del alumno se calcula

Cuadro V
PROBABILIDADES DE TRANSICIÓN PARA EL ESTADO ANÍMICO DE CONFUSIÓN.

Estado	E_1	E_2	E_3	E_4	E_5
E_1	0.40	0.30	0.05	0.05	0.20
E_2	0.15	0.50	0.15	0.05	0.15
E_3	0.20	0.30	0.20	0.10	0.20
E_4	0.60	0.20	0.05	0.05	0.10
E_5	0.20	0.30	0.05	0.05	0.40

Cuadro VI
TRANSICIONES ENTRE ESTADOS PARA EL ESTADO ANÍMICO DE ABURRIMIENTO.

Estado	E_1	E_2	E_3	E_4	E_5
E_1	0.40	0.10	0.10	0.10	0.30
E_2	0.10	0.20	0.20	0.10	0.40
E_3	0.15	0.20	0.20	0.15	0.30
E_4	0.40	0.10	0.05	0.05	0.40
E_5	0.20	0.10	0.05	0.05	0.60

la probabilidad de que una secuencia de eventos sea generada por el modelo de cada estado. La primera etapa de este proceso consiste en definir la longitud, l, de las secuencias de eventos a utilizar. Los eventos ya estarán traducidos a sus correspondientes símbolos en esta etapa. A continuación se construye la secuencia con los últimos l eventos generados por el alumno justo antes de iniciar el proceso de identificación. Posteriormente se calcula la probabilidad de que cada uno de los modelos de estados anímicos genere dicha la secuencia, utilizando el algoritmo de avance-retroceso. Las probabilidades obtenidas presentan valores muy bajos, lo cual es comprensible al tener en cuenta que se busca la generación de una secuencia exacta de l símbolos. El estado anímico elegido como el actual que presenta el estudiante es cuyo modelo presente una mayor probabilidad.

El proceso de detección de emociones puede verse como una transición entre niveles de información. La Fig. 3 presenta gráficamente el procesado de eventos a acciones de más alto nivel, relacionadas a estados definidos. El nivel superior está compuesto por los eventos capturados directamente en la máquina virtual, el ambiente virtual de aprendizaje y el servidor web de la asignatura. En el siguiente nivel están los símbolos construidos a partir de los eventos. Estos símbolos tienen un nivel de información apropiado para poder relacionarlos con posibles actividades relacionadas al desarrollo de software, incluidos en el siguiente nivel. En un último nivel de información se encuentra el estado anímico del estudiante, obtenido a partir de las transiciones de eventos en el tercer nivel.

IV. IMPLEMENTACIÓN DEL MODELO PROPUESTO Y UN EJEMPLO DE SU APLICACIÓN

La base de datos de eventos se almacenan en el gestor MySQL. La traducción de eventos y el proceso del modelo descrito se han implementado en el lenguaje Python. Se ha utilizao la biblioteca GHMM[1] para el soporte de HMM, incluyendo los algoritmos de avance-retroceso y Baum-Welch. Los resultados del proceso se almacenan en ficheros de texto plano para analizarlos en la fase de evaluación estadística.

Se propone un ejemplo de la ejecución del modelo propuesto con el objetivo de completar y facilitar la comprensión del mismo. Para este ejemplo se ha definido la longitud de las secuencias de eventos con el valor 20. Esto implica que deben capturarse 20 eventos para iniciar el proceso de detección del estado anímico. La tabla VII muestra una secuencia de símbolos generados a partir de eventos capturados en una actividad real de aprendizaje. Las columnas respectivas para cada emoción corresponden al logaritmo de la probabilidad

[1] http://ghmm.org/

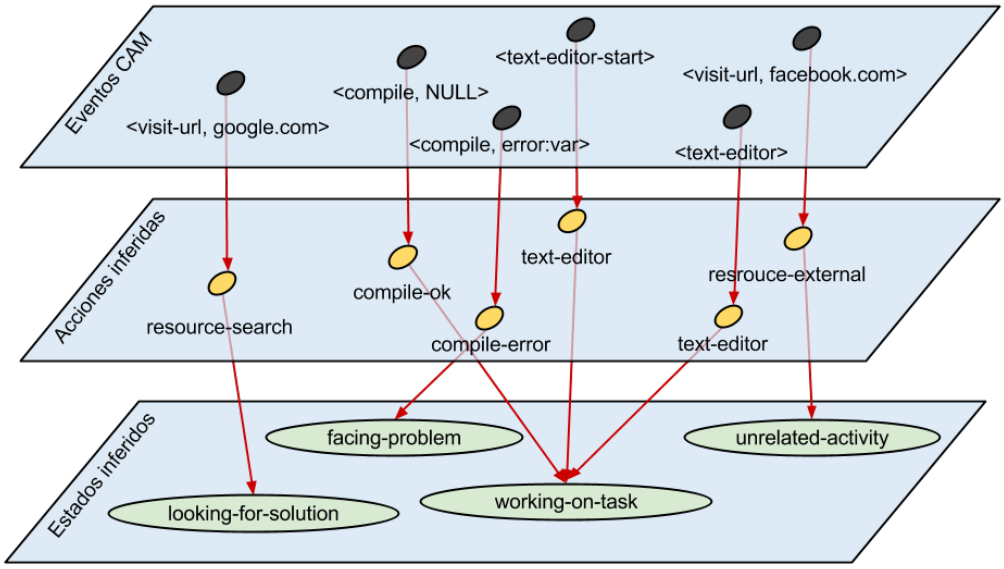


Figura 3. Niveles de información obtenida de los eventos capturados en el entorno de aprendizaje de desarrollo de software.

de que la secuencia de eventos previa sea producida por el HMM del estado anímico. Es decir,

$$log(P(S_t|H_E))$$

donde O_t es la secuencia de símbolos capturados en el momento t y H_E el HMM respectivo para la emoción E. La función logaritmo permite simplificar la presentación de los valores tan bajos de probabilidad. Como es de esperarse por la magnitud de las probabilidades, todos los valores obtenidos son negativos. La tabla resalta en negrita la emoción con el valor mayor, el cual representa la probabilidad más alta. Puede observarse que al inicio el estudiante genera una secuencia que podría parecer normal hasta ese momento, empezando por la utilización de la linea de comandos y el acceso a dos recursos relacionados con la asignatura. Con estos eventos iniciales, la probabilidad de que el estudiante sienta la emoción de alegría es mayor y esto se refleja en al ser el valor mayor entre los cuatro posibles. A continuación, el estudiante genera tres eventos de compilación errónea, seguidos de dos eventos de búsqueda de recursos y un evento de acceso a un recurso externo. Al observar los logaritmos puede apreciarse en una disminución de probabilidad en la columna de alegría, hasta llegar a la fila 9, con un punto muy menor al inicial en la fila 1. Sin embargo, las probabilidades de los otros tres estados anímicos muestran incrementos hasta llegar al punto en el que la confusión presenta la mayor probabilidad. Esto se mantiene mientras el estudiante sigue buscando la solución a la dificultad encontrada como puede apreciarse en los eventos de la fila 10 a la 14. Es hasta en la fila 15 donde se genera un evento de compilación exitosa y cambia levemente la tendencia de las emociones. Al llegar a la fila 20, ya se han generado tres eventos de compilación exitosa y es donde la probabilidad de que el estudiante presente la emoción de alegría vuelve a ser la mayor de todas. Esto se mantiene hasta el final del ejemplo, siguiendo con la lógica de los eventos debido a que reflejan interacciones normales en la actividad de aprendizaje: compilaciones y análisis de memoria mayormente satisfactorios, uso del editor de texto y del depurador.

V. DISCUSIÓN

El trabajo presentado en el artículo ha demostrado la viabilidad de implementar el modelo propuesto para la detección de emociones a partir de eventos capturados en el entorno de desarrollo de software. El hecho de que para detectar cada emoción se necesite solamente la matriz de probabilidades de transición entre estados ha facilitado la implementación. Además, esto simplifica extender el modelo a nuevos estados anímicos o cognitivos que sean de interés en un entorno de desarrollo de software.

La principal debilidad del modelo propuesto es el elevado número de variables que participan en la detección de estados anímicos. Las probabilidades de emisión de símbolos están asociadas a 5 elementos y 13 símbolos, por lo que se cuenta con 60 grados de libertad para su definición. Esto sumado a las probabilidades de transición entre los 5 estados, que implican 20 grados de libertad. Se ha intentado contrarrestar esta debilidad con un planteamiento coherente de las probabilidades iniciales, tal y como se ha explicado a lo largo del artículo. También se espera que con una cantidad adecuada de datos sea posible ajustar estas probabilidades para mejorar las predicciones hechas por el modelo.

Otra debilidad, causada por el uso de modelos ocultos de Markov, es no poder incluir información sobre el contexto en el proceso de detección. Un ejemplo es información relacionada con la ubicación del estudiante y así poder estudiar si realizar la actividad de desarrollo de software en casa o en el centro de estudios tiene algún efecto sobre el estado anímico. Otro tipo de información es temporal con la que se podría analizar si ciertas emociones son más frecuentes en horas específicas o, por ejemplo, durante el fin de semana. Al no poder incluir esta información directamente en los modelos ocultos de Markov, una posible solución sería realizar

Cuadro VII
EJEMPLO DE SÍMBOLOS GENERADOS Y EL LOGARITMO DE LA PROBABILIDAD RESPECTIVA PARA CADA EMOCIÓN.

No.	Símbolo	Alegría	Frustración	Confusión	Aburrimiento
1	command	**-53.75**	-62.49	-58.41	-57.30
2	resource-internal	**-54.56**	-62.80	-59.28	-57.86
3	resource-internal	**-54.75**	-63.35	-59.09	-57.82
4	compile-error	**-54.12**	-61.33	-57.41	-56.69
5	compile-error	**-53.02**	-59.23	-55.09	-55.39
6	compile-error	**-52.46**	-57.50	-53.49	-54.68
7	resource-search	**-53.30**	-58.13	-54.52	-55.48
8	resource-search	**-53.74**	-58.92	-54.49	-55.55
9	resource-external	-53.70	-58.57	**-53.54**	-54.28
10	compile-error	-52.92	-56.92	**-51.90**	-53.65
11	resource-search	-53.38	-57.17	**-52.22**	-53.96
12	resource-search	-53.25	-57.49	**-51.85**	-53.76
13	compile-error	-52.48	-54.93	**-50.46**	-52.76
14	compile-error	-51.42	-52.46	**-48.67**	-51.83
15	compile-ok	-50.99	-52.22	**-49.03**	-51.77
16	debugger	-51.53	-52.11	**-49.78**	-52.72
17	debugger	-52.07	-52.24	**-50.72**	-53.61
18	compile-ok	-52.47	-51.13	**-50.61**	-53.26
19	compile-error	-49.80	-49.23	**-49.11**	-52.63
20	compile-ok	**-50.38**	-51.22	-51.19	-53.36
21	debugger	**-51.93**	-53.63	-53.80	-55.23
22	memory-ok	**-53.17**	-54.67	-54.88	-56.32
23	memory-error	**-52.85**	-53.27	-54.09	-56.20
24	compile-ok	**-51.36**	-52.27	-53.92	-55.94
25	memory-error	**-52.29**	-53.68	-55.19	-56.96
26	text-editor	**-53.87**	-55.68	-56.81	-58.85
27	compile-ok	**-52.85**	-54.18	-56.32	-58.04
28	text-editor	**-52.17**	-54.66	-56.50	-57.99

experimentos en cada uno de los entornos de interés y así poder comparar los resultados obtenidos. Como línea de investigación futura se plantea la definición de un modelo que pueda incluir esta información de forma sistemática.

Otro factor a considerar es la dificultad para evaluar la detección de emociones al no contar con una fuente confiable de la emoción de la persona. En nuestro caso confiamos en la información que el propio estudiante proporcione sobre su estado anímico. Esta información puede ser errónea por dos motivos; el primero es que el estudiante no pueda identificar adecuadamente el estado en el que se encuentra. El segundo motivo es que el estudiante no pueda cuantificar el nivel del estado anímico en el formulario provisto. Para solucionar este problema, se plantea el uso de sensores solamente para evaluar la precisión de las emociones detectadas por el modelo.

Actualmente estamos trabajando en el análisis de datos obtenidos durante experimentos para evaluar el modelo. Estos experimentos se han realizado en entornos reales de aprendizaje, con estudiantes segundo curso de ingeniería. Además de utilizar los datos para la evaluación también se utilizan para realizar un entrenamiento del modelo y así ajustar las probabilidades de emisión y de transición. También se podrá analizar posibles correlaciones entre las emociones detectadas y aspectos relacionados a la actividad educativa, tales como la tasa de abandono o la ganancia de aprendizaje.

Como trabajo futuro se propone la integración de las detección de emociones con sistemas utilicen dicha información para mejorar la experiencia de aprendizaje de desarrollo de software. Un ejemplo consiste en comunicar las emociones detectadas con sistemas recomendadores de material de aprendizaje como el propuesto en [13]. Esta integración permitiría la recomendación de material de aprendizaje sin necesidad de que el estudiante informe su estado anímico ni del uso de sensores corporales.

Finalmente, otra línea futura de investigación está relacionada a la comunicación y presentación de los estados de ánimo detectados. El objetivo de es utilizar esta información como método de retroalimentación hacia el profesor y los mismos estudiantes sobre el estado anímico de un grupo específico de estudiantes o del grupo completo. Para esto, pueden utilizarse herramientas como las visualizaciones presentadas en [14].

AGRADECIMIENTOS

Trabajo financiado parcialmente por el proyecto EEE, “Plan Nacional de I+D+I TIN2011-28308-C03-01” y el proyecto “Emadrid: Investigación y desarrollo de tecnologías para el e-learning en la Comunidad de Madrid” (S2009/TIC-1650).

REFERENCIAS

[1] R. W. Picard, *Affective computing*. MIT press, 2000.
[2] R. A. Calvo and S. D’Mello, “Affect detection: An interdisciplinary review of models, methods, and their applications,” *Affective Computing, IEEE Transactions on*, vol. 1, no. 1, pp. 18–37, 2010.
[3] I. Arroyo, D. G. Cooper, W. Burleson, B. P. Woolf, K. Muldner, and R. Christopherson, “Emotion sensors go to school,” in *Proceeding of the 2009 conference on Artificial Intelligence in Education, July 6th-10th, Brighton, UK, IOS Press*, 2009, pp. 17–24.
[4] S. K. D’Mello, S. D. Craig, J. Sullins, and A. C. Graesser, “Predicting affective states expressed through an emote-aloud procedure from autotutor’s mixed-initiative dialogue,” *International Journal of Artificial Intelligence in Education*, vol. 16, no. 1, pp. 3–28, 2006.
[5] S. D’Mello, A. Graesser, and R. W. Picard, “Toward an affect-sensitive autotutor,” *Intelligent Systems, IEEE*, vol. 22, no. 4, pp. 53–61, 2007.
[6] C. Conati and X. Zhou, “Modeling students’ emotions from cognitive appraisal in educational games,” in *Intelligent tutoring systems*. Springer, 2002, pp. 944–954.
[7] A. Pardo and C. Delgado Kloos, “Stepping out of the box. Towards analytics outside the Learning Management System,” in *International Conference on Learning Analytics and Knowledge*, 2011.

[8] M. Wolpers, J. Najjar, K. Verbert, and E. Duval, "Tracking actual usage: the attention metadata approach," *Journal of Technology Education & Society*, vol. 10, no. 3, pp. 106–121, 2007.
[9] V. A. Romero Zaldívar, A. Pardo, D. Burgos, and C. Delgado Kloos, "Monitoring Student Progress Using Virtual Appliances : A Case Study," *Computers & Education*, vol. 58, no. 4, pp. 1058–1067, 2012.
[10] I. Roseman and A. Evdokas, "Appraisals cause experienced emotions: Experimental evidence," *Cognition and Emotion*, vol. 18, no. 1, pp. 1–28, 2004.
[11] K. R. Scherer, "Psychological models of emotion," *The neuropsychology of emotion*, vol. 137, p. 162, 2000.
[12] A. Ortony, G. L. Clore, and A. Collins, *The cognitive structure of emotions*. Cambridge university press, 1990.
[13] D. Leony, A. Pardo, H. A. Parada, and C. Delgado Kloos, "A cloud-based architecture for an affective recommender system of learning resources," in *Proceedings of the 1st International Workshop on Cloud Education Environments*. CEUR Workshop Proceedings, 2012, vol. 945, pp. 41–46.
[14] D. Leony, P. J. Muñoz-Merino, A. Pardo, and C. Delgado Kloos, "Provision of awareness of learners' emotions through visualizations in a computer interaction-based environment," *Expert Systems with Applications*, 2013.

Arquitectura Telemática para la Detección Precoz de Trastornos del Lenguaje

Martín-Ruiz, M.L.[1], Valero Duboy, M.A. [1], Torcal Loriente, C.[2], Martín Uría, J.[1], Peñafiel Puerto, M.[2]

[1]Departamento de Ingeniería y Arquitecturas Telemáticas
EUIT de Telecomunicación, Universidad Politécnica de Madrid
Carretera de Valencia, km. 7, 28031, Madrid

[2]Colegio Legamar
Ctra. Leganés-Fuenlabrada Km. 1,5. 28914 Leganés – Madrid

{marisam, mavalero}@diatel.upm.es, infantiluno@colegiolegamar.es, javier.martin.uria@alumnos.upm.es, dirección@colegiolegamar.es

***Resumen*- La investigación y desarrollo de sistemas telemáticos en e-salud se ha limitado típicamente al despliegue de soluciones centradas en el acceso a la historia clínica electrónica. El presente trabajo aborda la complejidad de diseñar un servicio telemático capaz de ayudar al pediatra de atención primaria en el proceso de decidir si derivar o no a atención especializada a un niño de hasta seis años con posibles trastornos del lenguaje. Con esta finalidad, se ha construido una ontología a partir del análisis sistemático de 21 casos de niños ya diagnosticados y se ha desarrollado una plataforma web que facilita al pediatra su labor de detección precoz. Asimismo, se ha implementado una plataforma web para el especialista que permite validar la efectividad del sistema construido. El proceso de evaluación se ha completado con 21 casos de niños, diferentes de los 21 originales y extendiéndose a 160 niños de una escuela infantil.**

***Palabras Clave*- web semántica, gestión del conocimiento, atención temprana, e-salud, servicios telemáticos**

I. Introducción

La medicina es una disciplina tradicionalmente pionera en la incorporación de las tecnologías de la información y la comunicación. Shortlife ya describe a mediados de los 70 una experiencia documentada de aplicación de las técnicas de Inteligencia Artificial (IA) en un sistema de información en el contexto de una consulta médica [1].

La gestión eficiente de información en el ámbito sanitario es una tarea compleja que puede facilitar considerablemente el seguimiento adecuado del paciente. Los pediatras que trabajan en el Sistema de Salud español son médicos de Atención Primaria (AP) que desempeñan su actividad asistencial en centros de salud donde se atiende a la población infantil entre 0 y 14 años.

El seguimiento del desarrollo neuroevolutivo del niño es tarea del Pediatra de AP (PAP), el cual adolece del tiempo y conocimiento necesario para la detección precoz de los trastornos del desarrollo. Este contexto problemático provoca que la detección de dichos trastornos sea inferior a su prevalencia real y plantea la necesidad de una solución para la identificación temprana de dicha población de riesgo [2,3]. El empleo de las tecnologías de la Web Semántica puede facilitar al PAP la difícil tarea de gestionar la información y conocimiento requerido para el seguimiento del niño.

Los procedimientos médicos existentes para la detección de trastornos neurológicos en la infancia son de difícil aplicación en la consulta del PAP [4-6]. Sin embargo, tanto la Organización Mundial de la Salud como Unicef enfatizan en la necesidad de emplearlos para una atención a la población infantil [7].

Múltiples trabajos inciden en la necesidad de la detección temprana de los trastornos neurológicos así como en la importancia del desarrollo del lenguaje como precursor de este tipo de patologías [8-11]. La Encuesta de Discapacidad, Autonomía Personal y Situaciones de Dependencia del Instituto Nacional de Estadística (INE) de 2008 refleja cómo casi un 17% de los niños que necesitan recibir un tratamiento de Atención Temprana (AT) en España no lo reciben. Esta situación manifiesta la importancia de construir sistemas de información que faciliten estas actuaciones. Dicha encuesta recoge el número de niños con limitación por grupo de deficiencia (Tablas I y II), y muestra que las deficiencias del lenguaje, ocupan el segundo lugar entre las más comunes, afectando a un mayor número de varones (27,06%).

El conjunto de patologías o alteraciones en el desarrollo, abordables mediante una solución telemática como la descrita en esta investigación, es muy amplio y heterogéneo.

Dicha complejidad sugiere centrarse en primer lugar en los trastornos del lenguaje, puesto que además son típicamente los primeros síntomas que un niño presenta en relación con un posible trastorno del desarrollo [12].

Tabla I
NIÑOS/AS CON ALGUNA LIMITACIÓN POR GRUPO DE DEFICIENCIA
(EN MILES DE NIÑOS)

	Total
Total	60,4
Deficiencias mentales	14,1
Deficiencias visuales	1,5
Deficiencias de oído	5,2
Deficiencias del lenguaje, habla y voz	12,3
Deficiencias osteoarticulares	5,5
Deficiencias del sistema nervioso	9,6
Deficiencias viscerales	11
Otras deficiencias	2,8
No consta	4,6

Tabla II
PORCENTAJE DE NIÑOS/AS CON LIMITACIÓN SEGÚN SU GRUPO DE DEFICIENCIA Y SEXO

	Ambos sexos	Varones	Mujeres
Total	100	100	100
Deficiencias mentales	25,24	25,14	25,38
Deficiencias visuales	2,6	2,7	2,46
Deficiencias de oído	9,32	8,37	10,67
Deficiencias del lenguaje, habla y voz	22,12	27,06	15,04
Deficiencias osteoarticulares	9,86	12,21	6,5
Deficiencias del sistema nervioso	17,22	13,83	22,08
Deficiencias viscerales	19,72	17,77	22,5
Otras deficiencias	5,09	6,27	3,39

La arquitectura telemática para e-salud, objeto de esta investigación, ha de facilitar la provisión de un servicio que permita al PAP identificar precozmente posibles trastornos del lenguaje en rutina clínica. Gracias a dicho sistema, el PAP podrá decidir de forma más eficiente si conviene adelantar la siguiente visita del niño, o bien, proceder a su derivación al especialista que corresponda, ya sea un neuropediatra, rehabilitador, logopeda o equipo de atención temprana.

Actualmente, los sistemas telemáticos existentes en los servicios de e-salud se centran exclusivamente en el almacenamiento y acceso a información de la historia clínica electrónica, pero no en el apoyo a la toma de decisiones clínicas, objeto del trabajo de investigación presentado. Asimismo, dichos sistemas apenas han empezado a permitir compartir información sobre procesos de derivación y posible diagnóstico. El sistema descrito incorpora, en resumen, tres características diferenciales: (1) Apoyo a la toma de decisiones en procesos compartidos entre profesionales, en este caso pediatra y especialista (neuropediatra, rehabilitador, logopeda o equipo de atención temprana); (2) Construcción de la base de conocimiento no sólo basada en tests o protocolos de desarrollo sino también en el histórico revisado por expertos de más de 40 casos recogidos a lo largo de más de 10 años de ejercicio; (3) Desarrollo abierto, usando tecnologías telemáticas que facilitan su integración e interacción con otros sistemas de e-salud, públicos o privados.

II. METODOLOGÍAS EMPLEADAS

La obtención del conocimiento necesario para la creación de la ontología es un aspecto crítico en esta investigación, puesto que condiciona su utilización efectiva en AP.

El proceso de Adquisición de Conocimiento (AC) es fundamental para la creación de la arquitectura telemática descrita puesto que determina las bases para la provisión de un servicio efectivo. La metodología empleada para la AC requiere contemplar tanto la definición de los conocimientos a sistematizar como la conceptualización y formalización de la información recopilada de las fuentes humanas y materiales. Por este motivo, se han analizado en primer lugar las metodologías de mayor interés para extraer el conocimiento necesario, comparando GROVER, CommonKADS (CK), Methontology e IDEAL. Tras este estudio se decidió emplear una combinación de CK y Methontology por su mayor potencial de aplicación en ciertas fases del proceso de construcción de un Sistema Experto (SE) como el requerido para el desarrollo de la presente investigación. Se detalla a continuación la justificación de dicha elección:

(a) CommonKADS es una metodología de Ingeniería de Conocimiento (IC) que tiene como fines el diseño y desarrollo de un SE a partir del conocimiento extraído de expertos humanos en un área determinada, y la codificación de dicho conocimiento de manera que pueda ser procesada por un sistema [13].

(b) Methontology es una metodología orientada a la implementación de una ontología en la actividad de conceptualización [14]. Methontology define un conjunto de tareas que permiten pasar de la especificación informal del dominio de aplicación de la ontología a la especificación semi-formal del dominio a través de representaciones intermedias a modo de tablas donde se define cada uno de los conceptos del sistema.

El equipo de expertos, del ámbito sanitario, que ha participado en la construcción de la ontología, está compuesto por:

- Dos PAP.
- Un neonatólogo experto en trastornos del desarrollo y discapacidad infantil, exjefe del servicio de neonatología del Hospital Clínico San Carlos de Madrid.
- Una neuropediatra que trabaja actualmente en el hospital Quirón de Madrid.
- Dos expertas en Trastornos Específicos del Lenguaje (TEL) terapeutas del Centro de Intervención del Lenguaje (CIL) de Universidad de La Salle (Madrid).

En el proceso de validación de la ontología están participando también las terapeutas en las etapas 0-3 y 4-6 del colegio Legamar de Leganés (Madrid).

Los procesos de adquisición y formalización se han desarrollado a partir de la información recogida en reuniones abiertas y estructuradas con el equipo de expertos.

El proceso de educción del conocimiento experto se apoyó en el uso de técnicas complementarias tales como formularios, encuestas y entrevistas diseñadas en función de los objetivos que se desea cubrir con el sistema inteligente para el apoyo al PAP en el contexto del sistema de salud público.

El presente artículo presenta la interconexión de la ontología desarrollada y presentada en IEEE 12th International Conference on BioInformatics and BioEngineering [15] con el servicio web telemático proporcionado por el sistema de e-salud construido y que actualmente está siendo validado por las terapeutas del colegio Legamar, se tiene previsto que el sistema sea validado por PAP en entornos reales a finales de este año.

III. ANÁLISIS FUNCIONAL

El análisis del sistema resultante se ha elaborado utilizando UML (Unified Modelling Language) por lo cual se presenta en la Fig. 1 el diagrama de casos de uso referente al proceso de *Evaluación del Lenguaje del niño*. El actor que interactúa con el sistema en este caso de uso es el PAP, responsable del seguimiento del desarrollo normal del niño. Las tareas asociadas al caso de uso "Evaluación del Lenguaje" comienzan por la selección del paciente con el que trabajar a partir de lo que se ha denominado "datos generales". Estos datos permitirán identificar al niño y al mismo tiempo asegurar la privacidad en el acceso a sus datos generando un código único para cada niño a partir de dicha información.

Los datos generales que se solicita a los padres para la realización de las evaluaciones son: sexo del niño, iniciales del nombre del niño, fecha de nacimiento y semanas de gestación.

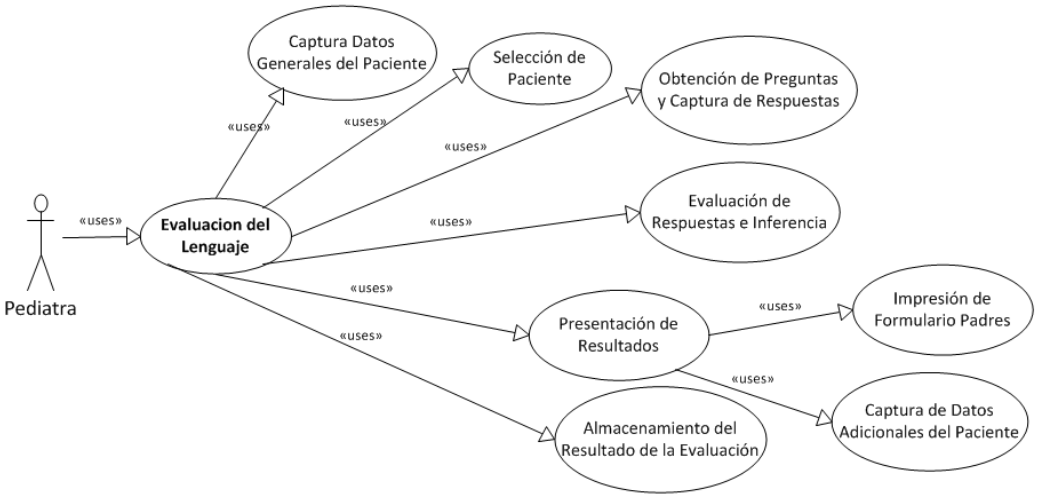


Fig. 1. Diagrama de casos de uso del proceso de Evaluación del Lenguaje.

El conocimiento por parte del sistema de la fecha de nacimiento del niño y de sus semanas de gestación permite calcular su edad en meses que servirá para obtener las preguntas necesarias para la posible detección precoz de trastornos del lenguaje considerando la etapa actual de desarrollo esperado del niño. El sistema valorará, a partir de las respuestas introducidas y su base de conocimiento, si el desarrollo del niño es normal o, por el contrario, inferirá qué acciones debe recomendar el pediatra para el adecuado tratamiento de un posible trastorno.

Las acciones que el sistema puede sugerir al pediatra para la toma de decisión pueden ser: fijar una próxima visita en 1-3 meses con objeto de volver a realizar el proceso de evaluación del lenguaje, o bien, proponer la derivación al especialista correspondiente.

La Fig. 2 muestra el diagrama de casos de uso que describe las funciones de *consultar las evaluaciones del lenguaje realizadas* y *valorar las decisiones propuestas por el sistema*. En dicha figura puede observarse que los actores son el PAP y un especialista que puede ser un neuropediatra, logopedas o profesional de la Atención Temprana. Esto significa que cualquier usuario autorizado del sistema podrá consultar y valorar las evaluaciones realizadas por los pediatras.

Las actividades de la consulta de resultados comienzan de forma análoga a la evaluación del lenguaje: se solicitan los datos necesarios para localizar al paciente en cuestión.

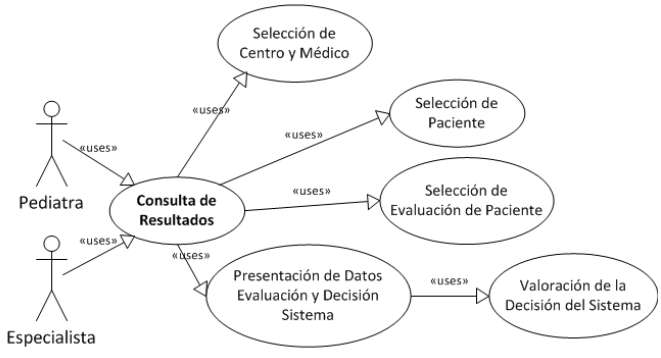


Fig. 2. Diagrama de casos de uso del proceso de Consulta de Resultados.

Posteriormente se obtiene su evaluación o evaluaciones para presentar los datos de las mismas.

Finalmente, el sistema permite que cada usuario que consulta una evaluación pueda valorar la decisión propuesta por el sistema. Esta valoración tiene el propósito de que en un futuro el propio sistema aprenda de lo acertado o no de sus decisiones.

IV. Diseño del Sistema

La arquitectura del sistema resultante ha de facilitar la interacción dinámica entre los actores implicados, las plataformas distribuidas de gestión fiable de la información, los modelos de razonamiento y los procesos de actuación acordes con el modelo sanitario en el que se ubica.

La Fig. 3 resume esta interacción que se explica con mayor detalle a continuación:

Paso 1. El niño acude al pediatra de familia acompañado de un miembro de su familia.

Paso 2. El pediatra de AP decide utilizar el sistema desarrollado para evaluar si existe algún trastorno del lenguaje en el niño, en cuyo caso se realizará la derivación precoz al especialista correspondiente o bien se adelantará la próxima visita del niño con objeto de realizar una nueva evaluación. El pediatra interactúa con el sistema realizando la introducción de información correspondiente.

Paso 3. El sistema devuelve el resultado al pediatra.

Existen dos posibilidades:

- El resultado es que todo es normal en cuyo caso el

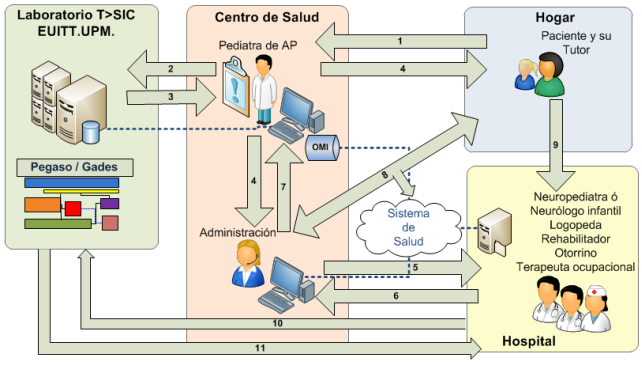


Fig. 3. Arquitectura del sistema.

niño vuelve a su casa sin modificar el curso normal de visitas al pediatra.

- El resultado modifica el calendario de visitas del niño al pediatra, o bien hay que derivar al especialista pertinente del hospital correspondiente.

Paso 4 y 5. Se realiza la petición de cita con el especialista correspondiente del hospital.
Paso 6. Se recibe respuesta a la petición de cita con el hospital.
Paso 7. Los datos de la cita con el especialista los recibe el pediatra.
Paso 8. Los datos de la cita llegan al niño y a su familia.
Paso 9. El niño acude al especialista correspondiente.
Paso 10 y 11. El especialista quiere consultar la respuesta que el sistema produjo para el caso de estudio correspondiente.

V. Aprendizaje Supervisado en Atención Primaria

El sistema de detección implementado facilita la detección precoz de trastornos del desarrollo a partir de patrones de razonamiento generados incrementalmente en función del conocimiento existente, formulado científicamente mediante protocolos de desarrollo y organizado experimentalmente en la información clínica recogida por una base de casos suficientemente significativa para el espacio muestral de trastornos del lenguaje conocidos. La metodología de aprendizaje utilizada actualmente se basa en la verificación sistemática del correcto funcionamiento del sistema por parte de pares de expertos atendiendo a la diversidad de casos validados. Para ello, se ha desarrollado un módulo de validación que permite el aprendizaje supervisado acerca de los casos resueltos satisfactoriamente o no, ofreciendo así realimentación sobre la efectividad del mismo en su apoyo al PAP. El módulo desarrollado se complementa con un módulo futuro, actualmente en fase de diseño, que facilitará la toma de decisiones para un aprendizaje semiautomático y supervisado que permita a los profesionales, que utilizan el sistema, realizar propuestas de adaptación de la base de conocimiento o al propio sistema ante la detección de falsos positivos y verdaderos negativos.

VI. Desarrollo de la Plataforma

La construcción de la ontología, según Methontology, requirió categorizar las preguntas que el pediatra debe comprobar según los meses de edad del niño en el momento de la evaluación.

En la tarea de formalización de la ontología se ha empleado Protégé como herramienta para crear la ontología y el motor de inferencias necesario para el apoyo a la toma de decisiones.

La construcción de la ontología en Protégé se ha realizado creando una jerarquía de clases para los 6 primeros años la cual incluye una subjerarquía de clases por cada mes al que correspondan las preguntas que el pediatra debe comprobar.

La jerarquía de clases contenida en AvanceSL, dentro de cada mes, incluye como clases las preguntas correspondientes a ese mes, según muestra la Fig. 4 para los meses 2 y 3 del primer año.

Las preguntas a realizar para cada mes son clases que tienen como clase padre el mes al que corresponden las preguntas.

La definición de relaciones binarias establecidas entre clases de la ontología resultante sustentará el proceso de razonamiento del sistema mediante axiomas del tipo: Si el niño tiene 2 meses y existe una respuesta negativa a la pregunta "Emite OOOAAH" o "Chilla para interaccionar", el sistema debe proponer: "Fijar una próxima visita en 3 meses".

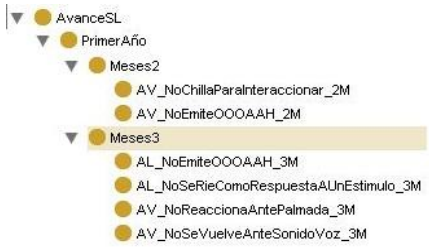


Fig. 4. Clases en Protégé para los meses 2 y 3.

La Fig. 5 muestra el código OWL correspondiente para las clases del mes dos.

```
<owl:Class rdf:ID="ProximaVisitaEn3Meses">
  <rdfs:subClassOf rdf:resource="#Año_1"/>
    <owl:equivalentClass>
      <owl:Restriction>
        <owl:someValuesFrom>
          <owl:Class>
           <owl:unionOf rdf:parseType="Collection">
            <owl:Class rdf:ID="AV_NoEmiteOOOAAH_2M"/>
            <owl:Class rdf:ID="AV_NoChillaParaInteraccionar_2M"/>
           </owl:unionOf>
          </owl:Class>
        </owl:someValuesFrom>
      <owl:onProperty>
        <owl:ObjectProperty rdf:about="#hayRespuestaNegativaEn"/>
      </owl:onProperty>
      </owl:Restriction>
    </owl:equivalentClass>
  </owl:Class>
```

Fig. 5. Código en OWL para las preguntas del mes 2.

La jerarquía de clases ha sido creada para realizar las inferencias a través de la clase DecisionSistema, recogiéndose dentro de esta clase las decisiones del motor según el año y tipo de hito al que pertenece la decisión.

La Fig. 6 muestra la formulación lógica de la correspondencia de estos axiomas con inferencias en Protégé a través del ejemplo de cómo una respuesta negativa, a los dos meses de edad, a la pregunta "Emite OOOAAH" o "Chilla para interaccionar" generaría la decisión "Fijar una próxima visita en 3 meses".

Fig. 6. Inferencia en Protégé para preguntas de 2 meses de edad.

La Fig. 7 muestra la estructura de la arquitectura básica del sistema desarrollado.

Puede observarse como el cliente es un cliente web típico formado por un conjunto de páginas web definidas en los lenguajes asociados al entorno web.

En el lado del servidor web tendremos dentro del contenedor Tomcat diferentes tipos de componentes de software Java:

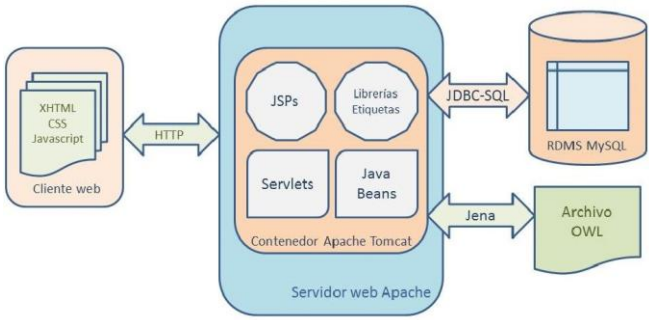


Fig. 7. Arquitectura del sistema.

(a) Las **páginas JSP** que se encargarán de generar todo el código de la parte cliente de forma dinámica desde el servidor.
(b) Las **librerías** de etiquetas personalizadas que se requiere implementar para poder ser utilizadas dentro de las páginas JSP.
(c) Los **Servlets**, como componentes especializados en la gestión de peticiones y respuestas HTTP, cuya función es dar soporte a la gestión de la interfaz de usuario web y además actuar como intermediaros con la capa de lógica.
(d) Los **objetos Java Bean**. Se han clasificado en dos tipos diferentes: *Java Beans de lógica de negocio*, en los que se implementará la lógica de la aplicación.
En uno de estos controladores de lógica tiene lugar el acceso a los datos de la ontología contenidos en el archivo OWL (Ontology Web Language) y se realiza mediante clases del API Apache Jena y *Java Beans de acceso a datos*, que contendrán el código de acceso a datos.
La implementación del motor de acceso a datos se realiza a través del API Java DataBase Connectivity (JDBC) que permite el acceso a los datos mediante el uso de sentencias del Structured Query Language (SQL) embebido dentro del código Java.

Con el fin de poder evaluar la aplicación resultante, y tras mantener sucesivas reuniones con los distintos tipos de usuarios, se decidió construir dos aplicaciones web encargadas de validar la misma ontología, pero que proporcionan un resultado de validación distinto por estar dirigidas a diferentes tipos de expertos. La aplicación **Gades** que será validada por las terapeutas del lenguaje que participaron en la construcción de la ontología, introduciendo casos de niños que han recibido terapia en el CIL y también con casos reales de niños del colegio Legamar de Leganés (Madrid), y la aplicación **Pegaso** que es la plataforma construida para facilitar a los PAP la detección precoz de trastornos del lenguaje.

Se decide utilizar dos plataformas distintas, para separar los resultados obtenidos en dos bases de datos y para conseguir adaptar la interfaz según las necesidades de cada tipo de usuario.

A continuación se va a presentar la interfaz que proporciona Pegaso para el proceso de evaluación del lenguaje, que será realizado por el PAP (Fig. 8 y 9).

Fig. 8. Recogida de datos generales.

La Fig. 8 muestra la solicitud de datos generales del niño, estos datos permitirán autenticar al niño en Pegaso.

La Fig. 9 muestra las preguntas que se presentan en el proceso de evaluación de lenguaje para un niño de 40 meses.

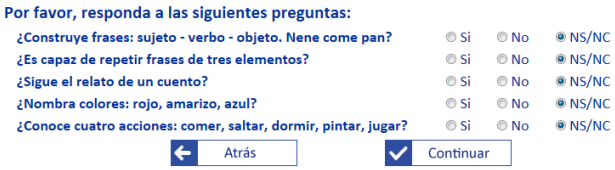


Fig. 9. Preguntas proceso evaluación niño de 40 meses.

Tras responder a las preguntas como se muestra en la Fig. 9, el resultado proporcionado por el sistema será el que se presenta en la Fig. 10. El pediatra debe indicar si va a realizar lo propuesto por el sistema, de forma que se recoja la opinión del pediatra en el proceso de evaluación del lenguaje.

Fig. 10. Resultado del proceso de evaluación del lenguaje.

Los siguientes apartados recogen los resultados de verificación y validación de las plataformas construidas.

VII. VERIFICACIÓN Y VALIDACIÓN

El proceso de verificación de la ontología es el resultado fundamental que debe proporcionarse para indicar la bondad del servicio telemático de e-salud.

La verificación se realizará en varias etapas, interviniendo en cada una de ellas los expertos que participaron en el proceso de adquisición de conocimientos que tuvo como resultado el desarrollo de la ontología.

Durante la construcción de la ontología se fue realizando la implementación de los distintas interfaces que el sistema debe proporcionar a los usuarios. Estas interfaces fueron diseñadas a partir de los requisitos que los PAP, como futuros usuarios de la herramienta, iban manifestando. Es importante señalar que se ha conseguido una interfaz usable y que permite al PAP recoger toda la información necesaria, de forma que el proceso de evaluación del lenguaje pueda llevarse a cabo en el menor tiempo de consulta posible. Uno de los requisitos en los que todos los PAPs han coincidido es que el proceso de evaluación del lenguaje les debe quitar pocos minutos en su consulta. Por eso, desde el primer momento, y con la colaboración de las terapeutas del lenguaje, se decidió limitar el número de preguntas del proceso de evaluación a un máximo de seis, según la edad del niño. La Fig. 11 muestra la interfaz de acceso de la aplicación **Pegaso**.

A. *Verificación de la plataforma Gades*

La ontología pasó por una primera verificación por parte de las terapeutas del CIL que realizaron pruebas en la aplicación Gades con los casos de 21 niños que recibieron terapia en el CIL. Sobre los resultados obtenidos en esta verificación indicar que se cumple que este tipo de patologías se den con más frecuencia en niños que en niñas, el 24% de los casos del CIL eran de niñas y el 76% eran de niños.

Fig. 11. Interfaz de acceso al sistema.

Se decide utilizar para la verificación casos de niños con desarrollo normativo para comprobar que el sistema funciona correctamente en el proceso de evaluación de estos casos. Obteniéndose un 100% de acierto en la evaluación del lenguaje para los sujetos con desarrollo normativo. El 14% de los 21 casos son sujetos con desarrollo normativo que fueron tratados en el CIL pero el resultado del proceso de evaluación fue positivo, no diagnosticándose en estos casos ninguna patología del lenguaje.

El 86% de los 21 casos son de niños que fueron diagnosticados con un retraso lingüístico.

A continuación se compara el tipo de resultado obtenido según el sexo del sujeto: En el 100% de los sujetos femeninos el resultado obtenido ha sido una alerta, que implica derivar al especialista correspondiente. Mientras que para los niños se obtiene: en un 69 % de los casos un proceso de derivación al especialista correspondiente, en el 12 % de los casos se procede a fijar una próxima visita y en el 19 % de los niños el resultado del proceso de evaluación del lenguaje ha sido normal.

Existe bajo número de casos para los que el resultado obtenido es fijar una próxima visita (solo el 12% de los niños), esto es normal con la población estudiada puesto que todos sujetos objetos de estudio estaban siendo tratados en el CIL, lo que hace que lo normal en esos casos es que el sistema produzca una alerta. Habrá que comparar este resultado con los que obtendrá la terapeuta del colegio Legamar, evaluando a los niños de la escuela infantil en los dos ciclos (etapa evolutiva 0-3 años y etapa evolutiva 3-6 años).

Con respecto a los casos por etapa evolutiva existen muy pocos sujetos de estudio en la etapa de 0-3 años, únicamente un 19% de los sujetos se encontraban en esa etapa, esto es así porque los sujetos de estudio pertenecen a una población que está recibiendo terapia por patologías en el lenguaje. Lo que hace en los 21 niños que se han utilizado en el proceso de verificación el 81% se encuentre en la etapa evolutiva de 3-6 años.

B. Verificación de la plataforma Pegaso

En el mes de abril comenzó el proceso de verificación de usabilidad de la plataforma Pegaso por parte de 5 pediatras de Atención Primaria de dos centros de salud de la Comunidad de Madrid, y una pediatra y neuropediatra del hospital Quiron de Madrid. El proceso de verificación está todavía sin completar, se ha estimado una duración de 6 meses para poder evaluar los resultados.

C. Validación funcional del sistema

El proceso de validación contempla distintos escenarios según la plataforma y en la actualidad ya se han completado las primeras fases planificadas.

En el caso de la **plataforma Gades**, se está contando con la valiosa colaboración del colegio Legamar (Leganes-Madrid), y se ha puesto en marcha la validación de esta plataforma utilizando la herramienta con un 100% de los niños de infantil en la etapa 0-3 años, y con un 40 % de los niños de la etapa 4-6 años (ver Fig. 12). Se tiene previsto finalizar el proceso de validación en este escenario en septiembre de 2013.

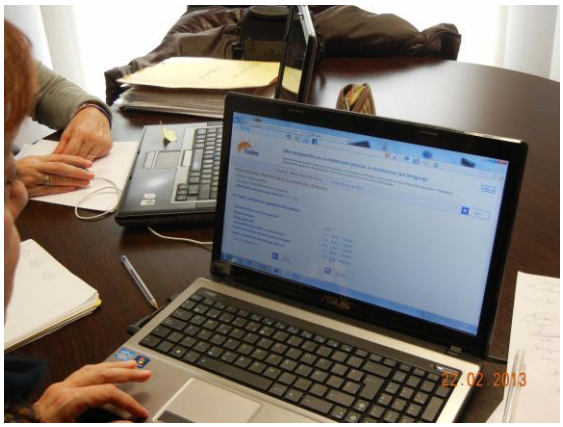


Fig. 12. Terapeuta del colegio Legamar realizando la validación de Gades.

La plataforma Gades va a ser validada con los 95 niños de la etapa 0-3 puesto que dicha etapa es clave para lograr la detección precoz de posibles patologías en la adquisición del lenguaje en la etapa pragmática y expresiva. En esta etapa el niño comienza con las primeras manifestaciones de la adquisición del lenguaje (jerga, interacción con el adulto, comprensión de órdenes sencillas, respuesta al juego simbólico, etc.). El comienzo en la emisión de las primeras

palabras depende de muchos de un niño a otro y son innumerables los factores que intervienen en la correcta adquisición del mismo. En las primeras pruebas de la plataforma Gades con niños de la etapa 0-3, se proporcionó a las cuidadoras la batería de preguntas que debían responder para cada niño, según la edad del niño en meses, y tras un proceso de observación de 10 días, la cuidadora respondía a las preguntas que posteriormente la terapeuta del colegio introducía en la plataforma Gades. Hasta el momento se ha observado que en algunos casos las educadoras no sabían responder a alguna de las preguntas, puesto que en ocasiones el comportamiento del niño en la casa y la escuela es distinto por esto, la educadora contó con la colaboración de las familias para responder correctamente a alguna de las preguntas.

En el momento presente, resulta esencial el poder conocer la validez de la ontología desarrollada para la **detección precoz** de trastornos del lenguaje. Se ha constatado que la plataforma Gades permite suplir la falta de conocimiento de las educadoras sobre los mecanismos que determinan la correcta adquisición del lenguaje de sus alumnos. La terapeuta señala, hasta el momento, que las preguntas de la ontología son de enorme utilidad en la actuación de la educadora en clase, ya que le permite una observación de cada niño que antes le era imposible realizar. Así mismo, las pruebas realizadas están permitiendo detectar un posible retraso en la adquisición del lenguaje en niños que no habían alarmado hasta el momento, en estos casos la terapeuta decide que se les va a realizar a una evaluación logopédica completa, que va a permitir comprobar la validez de la respuesta del sistema en estos casos.

En la etapa 4-6 el lenguaje es mucho más rico y la herramienta pretende alarmar de posibles patologías del lenguaje una vez instaurado, etapa expresiva del lenguaje. La detección en este caso se va a realizar sobre 60 niños siguiendo el mismo procedimiento explicado en la otra etapa. Estas pruebas todavía no han comenzado.

Para la **plataforma Pegaso** se prevé que la validación tendrá lugar a partir de septiembre de 2013 contando con la participación de 5 pediatras que trabajan en dos centros de salud de la Comunidad de Madrid, y se contempla que en el proceso de validación intervengan pacientes reales atendidos en rutina clínica. Se tiene previsto iniciar el proceso de validación a partir de las mejoras que se decidan introducir en la ontología una vez concluido el proceso de verificación realizado para la plataforma Gades.

Con el fin de minimizar en lo posible el número de 'falsos positivos' se prevé incorporar un segundo ajuste fino en la base de conocimiento, modulado por los expertos, solamente utilizable en los casos en los hayan existido dichos sucesos. Así mismo, el sistema informará al PAP sobre decisiones homólogas que hayan sido 'falsos positivos' para que valore con mayor detalle la posible respuesta correcta o incorrecta del sistema. La respuesta verdadera de si es o no es 'falso positivo' sólo puede ser mejorada por el sistema cuando recibe la segunda opinión del experto y el proceso de diagnóstico ha sido completado con más información adicional a la que puede recoger el sistema y que conoce el PAP.

Para reducir los 'verdaderos negativos' se propone actualizar, de forma recurrente e iterativa, el registro de todas las evaluaciones realizadas. Cuando un sujeto al que se le realizó la evaluación del lenguaje sea diagnosticado con un retraso en el lenguaje, se rescatará la evaluación realizada y analizará con los expertos las preguntas que se formularon justificándose la necesidad o no de modificar o añadir preguntas para la edad de ese niño en el momento de la evaluación. Se contempla, aunque requiere ser validado, el facilitar a los padres o tutores una batería de indicadores de hitos en la adquisición del lenguaje del niño. Esta aproximación puede adolecer de una subjetividad en la respuesta que siempre debe ser contrastada por el PAP.

VIII. Conclusiones y Futuros Trabajos

La detección de trastornos del lenguaje en niños, puede facilitar el diagnóstico precoz de diversas patologías neurológicas. El desarrollo de una arquitectura telemática para e-salud como la presentada en esta investigación puede facilitar al PAP la detección precoz de este tipo de trastornos en la población infantil.

La implicación de los expertos y su trabajo en las distintas etapas, ha sido clave para dar como solución un sistema que cumple con un alto número de requisitos y ha permitido también un correcto refinamiento de la ontología.

El proceso de AC llevo implícito el estudio de un amplio número de metodologías, facilitando la elección de una combinación de dos metodologías ampliamente utilizadas en la construcción de un SE. Se considera muy favorable la utilización de Protégé como un entorno abierto y usable para el diseño, modelado, implementación, manipulación y visualización de ontologías.

La verificación y validación de las plataformas construidas permitirá obtener un amplio y contrastado número de conclusiones que serán analizadas con objeto de mejorar la ontología y las plataformas desarrolladas.

Hasta el momento la terapeuta del colegio Legamar que está participando en la validación de la plataforma Gades, considera de enorme utilidad para sus educadoras la información que la herramienta proporciona para conocer el grado de adquisición del lenguaje de sus alumnos.

El lenguaje del niño es un hito clave del desarrollo neurológico y así debe ser tratado por parte de los padres, pediatras y educadores, el sistema construido pretende facilitar su observación a estos tres colectivos.

La continuidad de la línea de investigación presente tiene por objeto el modelado de un sistema que permita refinar la efectividad de la ontología creada a través de un proceso de consulta-supervisada y colaborativa con los usuarios del sistema. Dicha mejora podría facilitar la provisión de un servicio con capacidad de auto-aprendizaje supervisado por los expertos, siempre que exista una muestra de información y experiencia de uso suficientemente significativa.

Agradecimientos

Dr. José Arizcun neonatólogo experto en trastornos del desarrollo y discapacidad infantil. Dra. Beatriz Chiclana y Dr. Erwin Kirchschlager pediatras del Centro de Salud Jazmín (Madrid). Dña. Paloma Tejeda del Centro de Intervención del Lenguaje (CIL) La Salle Campus Madrid, Universidad Autónoma de Madrid. Dña. María Teresa Ferrando Lucas, neuropediatra en el hospital Quiron de Madrid.

Este artículo es parte de la investigación realizada en el proyecto Talisec+ (TIN2010-20510-C04-01), financiado por el Ministerio de Educación y Ciencia de España a través del Plan Nacional de I+D+I (investigación, desarrollo e innovación).

REFERENCIAS

[1] E.H. Shortlife, "Computer –based medical consultations: MYCIN". American Elsevier. 1976.

[2] Council on Children With Disabilities, Section on Developmental Behavioral Pediatrics, Bright Futures Steering Committee and Medical Home Initiatives for Children With Special Needs Project Advisory Committee, "Identifying infants and young children with developmental disorders in the medical home". Pediatrics. 2006.

[3] M.C. Arrabal Terán, J. Arizcun Pineda, "Alteraciones del desarrollo y discapacidad". Grado de pediatría en España. Genysi. 2007.

[4] R. Castro-Rebolledo, M. Giraldo-Prieto, L. Hincapié-Henao, F. Lopera, D.A. Pineda, "Trastorno específico del desarrollo del lenguaje: una aproximación teórica a su diagnóstico, etiología y manifestaciones clínicas". Revista de neurología. 2004.

[5] R. Paul, "Language disorders from infancy through adolescence: Assessment and intervention", 3rd ed. Mosby-Elsevier. 2007.

[6] R. Paul, "Language disorders from infancy through adolescence: Listening, speaking, reading, writing, and communicating". 4th ed. Elsevier. 2011.

[7] World Health Organization & Unicef. "Early childhood development and disability: discussion paper". 2012.

[8] N. Fejerman, E. Fernández Álvarez, "Neurología pediátrica". Cap. 51 y 54. 2007.

[9] R. Parrilla Muñoz, C. Sierra Córcoles, "Trastornos del lenguaje". Unidad de Gestión Clínica de Pediatría Sociedad de Pediatría de Andalucía Oriental. 2010.

[10] R. Mossabeb, K.C. Wade, K. Finnegan, E. Sivieri, S. Abbasi, "Language development survey provides a useful screening tool for language delay in preterm infants". Clinical Pediatrics, vol. 51, n. 7, pp. 638-644, 2012.

[11] H.D. Nelson, P. Nygren, M. Walker, R. Panoscha, "Screening for speech and language delay in preschool children: Systematic evidence review for the US preventive services task force". Pediatrics, vol. 117, pp. 298-319, 2006

[12] J. Narbona, C. Chevrie-Muller, "El lenguaje del niño. Desarrollo normal, evaluación y trastornos". 2ª Edición. Masson. 2003.

[13] A. Alonso Betanzos, B. Guijarro Berdiñas, A. Lozano Tello, J.T. Palma Méndez, M.J. Taboada Iglesias, "Ingeniería del conocimiento. Aspectos metodológicos". 2004.

[14] O. Corcho, M. Fernández-López, A. Gómez-Pérez, A. López-Cima, "Building legal ontologies with METHONTOLOGY and WebODE". vol. 3369, pp 142-157, 2005.

[15] M.L. Martín-Ruiz, M.A. Valero Duboy, I. Pau de la Cruz, "Development of a Knowledge Base for smart screening of language disorders in primary care". 12th International Conference on Bioinformatics & Bioengineering (BIBE). IEEE, pp. 121-126, 2012.

Servicio Ubicuo de Estimulación Cognitiva Orientado a Personas con Enfermedad de Parkinson

Carolina García Vázquez[1], Esther Moreno Martínez[1], Miguel A. Valero Duboy[1],
María Teresa Martínez Juez[2] y Mari Satur Torre Calero[3]
[1] Grupo de Investigación de Sistemas Telemáticos para la Sociedad de la Información y el Conocimiento
Universidad Politécnica de Madrid. EUIT de Telecomunicación
Ctra. de Valencia, Km. 7. 28031 Madrid. {carogar, emoreno, mavalero}@diatel.upm.es
[2] Asociación Parkinson Madrid. C/ Andrés Torrejón, 18. 28014 Madrid. teresamartinez@parkinsonmadrid.org
[3] Fundación Vodafone España. Parque Empresarial La Moraleja
Avda. de Europa, 1. 28108 Alcobendas (Madrid). mari-satur.torre@vodafone.com

***Resumen*- Este trabajo de investigación detalla el diseño y evaluación de un servicio de e-salud cuyo objetivo es mejorar la estimulación y seguimiento de personas con un trastorno cognitivo. Con este fin, se ha desarrollado un protocolo de transferencia de mensajes que facilita la provisión de un servicio telemático para personas afectadas de Parkinson, pudiendo así realizar estimulación cognitiva personalizada, de forma ubicua, mediante un dispositivo fácil de usar como un tablet Android. Asimismo, este servicio permite a los terapeutas adaptar y monitorizar de forma segura la terapia, vía web, beneficiándose así de una mejor calidad en el seguimiento efectivo de cada paciente. El sistema ha sido evaluado satisfactoriamente durante tres meses con 10 pacientes entre 59 y 77 años. La solución resultante es fácilmente integrable con otras terapias complementarias y puede ser adaptada para otros deterioros cognitivos, como el debido a la enfermedad de Alzheimer o el deterioro cognitivo leve.**

***Palabras Clave*- Estimulación cognitiva, ubicuidad, rehabilitación, Android, enfermedad de Parkinson**

I. INTRODUCCIÓN

Hoy en día, las nuevas tendencias en el telecuidado y las necesidades de la sociedad así como los avances tecnológicos justifican la inclusión de tecnología en el desarrollo de nuevos servicios de salud [1]. La computación ubicua provee de soluciones óptimas para el desarrollo de estos servicios gracias al respaldo de nuevas posibilidades tanto para el diagnóstico como para la realización de terapias de forma remota [2]. Los servicios para este tipo de cuidado son desarrollados de forma que permitan garantizar un tratamiento médico adaptado y personalizado para cada paciente, resolviendo con elementos tecnológicos los problemas que surgían tradicionalmente por la distancia y la disponibilidad de los servicios entre pacientes y médicos.

En el presente artículo se detalla la descripción, diseño, verificación y validación de un servicio completo de realización de terapias de estimulación cognitiva ubicua orientadas a pacientes con enfermedad de Parkinson, donde los usuarios pueden utilizarlo en cualquier lugar y en cualquier momento.

En primer lugar, se analizan los trabajos relacionados para justificar este estudio. A continuación, se presenta una breve descripción del sistema desarrollado y su plan de evaluación, así como los resultados obtenidos tras su implantación en un escenario real. Finalmente, se recogen las conclusiones obtenidas tras la realización del estudio, así como los trabajos futuros.

II. TRABAJOS RELACIONADOS

Actualmente, los sistemas conocidos como "brain games" están siendo muy populares y existen múltiples plataformas tecnológicas destinadas a personas con deterioro cognitivo, principalmente sobre PC. Esta es la situación de *SmartBrain*, un sistema interactivo multimedia para estimulación cognitiva y que ha sido diseñado para el deterioro que sufren las personas con enfermedad de Alzheimer [3]. Este sistema consiste en una serie de ejercicios de memoria, lenguaje, cálculo o atención. Otra aplicación de este tipo es *GRADIOR*, un programa específicamente diseñado para la rehabilitación y evaluación de la estructura neuropsicológica [4]. En él, el terapeuta define los parámetros de la sesión de estimulación del paciente y permanece con él/ella durante la realización de la terapia.

Por otro lado, existen en el mercado sistemas basados en tablet y centrados en el tratamiento de información médica. En este segmento el más popular es *Parkinson's toolkit*, que ha sido diseñado pensando en personal médico que necesita conocer más información sobre los síntomas y el tratamiento de la enfermedad de Parkinson [5]. Esta herramienta se encuentra disponible tanto para iOS como para Android. También existen aplicaciones orientadas al paciente como *Parkinson Home Exercises* sobre iPad [6]. Esta aplicación se centra principalmente en ejercicios de rehabilitación física que el paciente puede realizar en su domicilio.

La tecnología móvil ha permitido proyectos orientados al bloqueo en la marcha que sufren los pacientes con enfermedad de Parkinson. El proyecto *CuPiD* [7] utiliza un smartphone Nexus One para el preprocesamiento de los datos de aceleración de los pasos del paciente para detectar y prevenir estos bloqueos, siendo útil a su vez para la prevención de caídas. Dentro de este ámbito, se encuentra también *iTrem*, una aplicación para smartphones que se encarga de comprobar el grado de temblor que sufre un paciente [8]. Por otro lado, para las personas con deterioro cognitivo, existen proyectos orientados a prevenir su aislamiento. Este es el caso del proyecto *IntouchFun* [9], que provee de un marco colaborativo para integrar a familiares y cuidadores informales en una red social familiar, de forma que sus miembros puedan participar en las actividades de estimulación cognitiva de la persona y permitiendo que las actividades realizadas por el paciente puedan estar mediadas por interfaces multimodales adecuadas para cada miembro de la red.

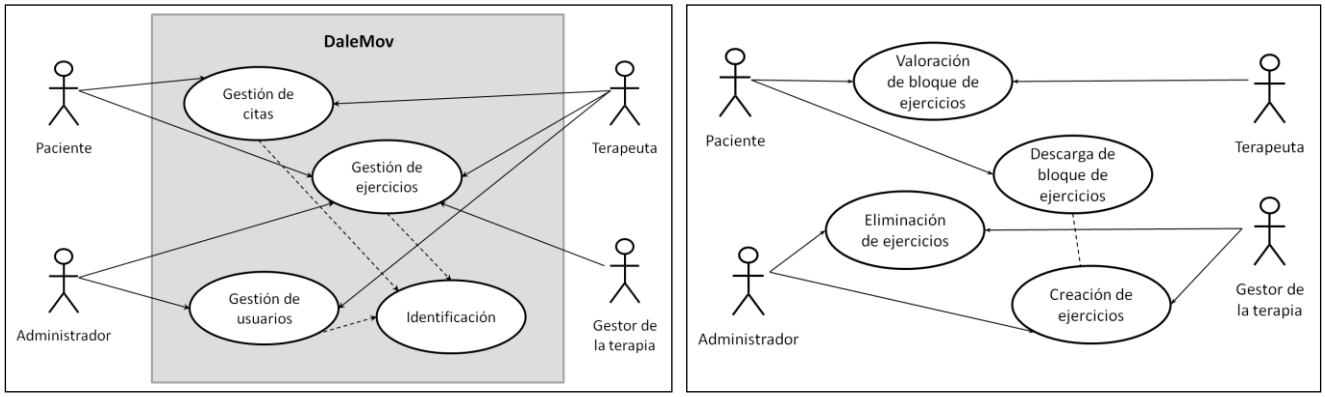


Fig. 1. Diagramas de casos de uso: general y de gestión de ejercicios respectivamente

Por la parte de las terapias orientadas a pacientes con enfermedad de Parkinson, para iOS existe *iParkinson App*, una aplicación preparada para el diagnóstico y tratamiento de los problemas del lenguaje que presentan estos pacientes [10]. Esta aplicación funciona de forma local, permitiendo al paciente realizar ejercicios de logopedia. Además, tiene una sección orientada al diagnóstico.

El trabajo que se presenta en este artículo es continuación de la plataforma EsCoTDT, que permite a personas con deterioro cognitivo debido a la enfermedad de Parkinson el llevar a cabo terapias de estimulación cognitiva a través de un sistema interactivo de Televisión Digital Terrestre [11]. Este sistema consiste en una aplicación de televisión interactiva para los pacientes basada en tecnología MHP (Multimedia Home Platform) y un servidor con tecnologías web que permiten al terapeuta el seguimiento de los ejercicios que ha desarrollado el paciente en cada sesión.

Sin embargo, en la bibliografía no se han encontrado trabajos que permitan a los pacientes con este tipo de deterioro la realización de las terapias de estimulación cognitiva con el seguimiento de su terapeuta de forma ubicua. Esta es la razón principal por la que surge DaleMov.

III. Descripción del sistema: DaleMov

DaleMov es una plataforma móvil, ubicua y distribuida que permite a personas con deterioro cognitivo debido a la enfermedad de Parkinson llevar a cabo sus terapias de estimulación cognitiva en cualquier lugar y en cualquier momento. Su principal ventaja es que el terapeuta puede gestionar, monitorizar y personalizar la terapia de cada paciente.

A. Análisis del sistema

En la Fig. 1 se presentan dos diagramas de casos de uso: el primero de ellos relativo a la funcionalidad general del sistema y el segundo, al desglose del caso de uso general *Gestión de ejercicios*. Los actores que interactúan con el sistema son los siguientes:

- Paciente: realiza su terapia de estimulación cognitiva a través de una tablet Android. Puede descargar bloques de ejercicios, consultar la valoración introducida por el terapeuta a la vista de los resultados o consultar la fecha de la próxima cita presencial con su terapeuta.
- Terapeuta: se encarga de valorar los resultados de los bloques de ejercicios realizados por el paciente en su tablet, así como de la personalización de la terapia decidiendo cuál es el siguiente bloque que éste se descargará en su tablet y de la introducción de citas para consulta presencial. Accede a través de web.
- Gestor de la terapia: su labor es la de la actualización de los ejercicios almacenados en el servidor a través de web. Se encarga de la introducción de nuevos ejercicios y de la eliminación de los ya existentes.
- Administrador: lleva a cabo las tareas de gestión de usuarios (darlos de alta o de baja y modificación de los datos personales), así como de la actualización de los ejercicios almacenados. Accede a través de web.

Con respecto a la funcionalidad del sistema, se recogen varios casos de uso dentro escenario principal (Fig. 1). Estos son:

- Gestión de citas: el terapeuta puede introducir una cita para consulta presencial que será consultada por el paciente a través de su tablet.
- Gestión de ejercicios: abarca las tareas de realización de la terapia de estimulación cognitiva (explicado más adelante).
- Gestión de usuarios: contiene las acciones necesarias para la gestión de usuarios, como es darlos de alta o baja o modificar sus datos personales.
- Identificación: para realizar cualquiera de las tareas anteriores, los usuarios deben identificarse para acceder al sistemas.

El caso de uso *Gestión de ejercicios* se presenta desglosado en la Fig. 1. La funcionalidad que contiene es la siguiente:

- Descarga de bloques de ejercicios: el paciente se descarga un bloque de ejercicios de estimulación cognitiva a través de su tablet. El bloque a descargar ha sido previamente definido por el terapeuta según las necesidades del paciente.
- Valoración de bloques de ejercicios: el terapeuta, a la vista de los resultados que ha obtenido el paciente en la realización de un bloque de ejercicios, decide cuál es el siguiente bloque que el paciente debe realizar e introduce una valoración subjetiva para que, posteriormente en su tablet, pueda ser consultada por el paciente.
- Creación de ejercicios: el gestor de la terapia y el administrador pueden introducir nuevos ejercicios de estimulación en la base de datos.
- Eliminación de ejercicios: cuando un ejercicio queda obsoleto, puede eliminarse de la base de datos. Los usuarios que tienen permiso para realizar esta acción son el gestor de la terapia y el administrador.

B. Especificación de la terapia de estimulación cognitiva

Con respecto a la terapia de estimulación cognitiva, ha sido necesaria la adaptación de los ejercicios de estimulación que se realizaban en las asociaciones de Parkinson de forma tradicional. La Asociación Parkinson Madrid realiza este tipo de terapias semanalmente con grupos de pacientes, dentro de las sesiones de psicología o de logopedia. Para llevarla a cabo se utiliza un cuaderno de ejercicios específicamente diseñado con este fin [12]. A continuación, se presentan las áreas de estimulación que abarcan los ejercicios recogidos en este cuaderno:

- Ejercicios de atención: se presentan cadenas de letras o números donde hay que marcar los que cumplen una determinada condición. Según se avanza por los ejercicios, el nivel de dificultad va aumentando. Este tipo de ejercicio es para ayudar a mantener la atención en la tarea para, posteriormente, realizar otro tipo de ejercicios.
- Ejercicios de funciones ejecutivas: a través de ellos se intenta que sea el paciente el que tome la iniciativa, ya que no existe sólo una respuesta correcta. De esta forma se consigue, además de captar la atención del paciente, que busque elementos de su vida cotidiana. Este tipo de ejercicios tiene 4 bloques bien diferenciados, según la capacidad del individuo en la que se centren:
  - Iniciativa: el paciente debe rellenar una lista con los elementos solicitados.
  - Categorización: consisten en la clasificación de objetos en grupos de características similares.
  - Seriación: se presenta una secuencia de acciones y el paciente debe ordenarlas en el orden lógico de realización. Se pretende que la secuencia de acción a ordenar se corresponda con una tarea cotidiana.
  - Planificación: existen dos tipos de ejercicios de planificación. En el primero se pretende que el paciente describa las acciones necesarias para llegar a un fin, definiendo también su orden lógico. En el segundo, se presenta una cuadrícula, y el paciente debe unir con líneas los objetos que son iguales sin que las líneas se crucen.
- Ejercicios de memoria: en estos ejercicios hay tipos muy diversos, entre los que se encuentran la lectura de una noticia y el escribir dos resúmenes sobre ella (uno el día de la lectura y otro el siguiente), el presentar una lista de personajes y realizar preguntas sobre ellos o el mostrar una lista de objetos y posteriormente recordar cuáles eran.

Una vez analizados los ejercicios, se procedió a su adaptación a la interfaz de la tablet, donde se decidió utilizar cinco modelos de interfaz para mostrarlos. Estos modelos, los cuales se muestran con un ejemplo de la interfaz gráfica implementada en la Fig. 2, tienen la siguiente estructura:

- Modelo 1: se presenta un enunciado y tres respuestas en formato texto, de las que el paciente debe elegir una.
- Modelo 2: se presenta un enunciado y tres respuestas en formato imagen, de las que el paciente debe elegir una.
- Modelo 3: se presenta una imagen en una pantalla durante unos segundos y, posteriormente, se muestra un enunciado sobre la imagen anterior y tres respuestas en formato texto, de las que el paciente debe elegir una.
- Modelo 4: se presenta un enunciado y el paciente debe escribir la respuesta.
- Modelo 5: se presentan un enunciado y una imagen, y el paciente debe escribir la respuesta que crea correcta.

Como se puede observar, estos modelos están diseñados en modo pregunta-respuesta para que para los pacientes que tengan problemas motóricos más severos puedan utilizar la plataforma sin que esto suponga una barrera. Por ello, para la adaptación de los ejercicios se ha intentado buscar una solución que esté centrada en esa área de estimulación aunque la interfaz no se corresponda exactamente con los ejercicios recogidos en el cuaderno, siempre bajo el asesoramiento de la neuropsicóloga y los terapeutas de la Asociación Parkinson Madrid. Por ejemplo, un ejercicio de atención podría recogerse en el modelo 5, para la iniciativa se suele utilizar el modelo 4 y para la planificación se pueden emplear tanto el modelo 1 (indicando una secuencia de

Fig. 2. Aplicación Android: ejemplos de ejercicios (modelos 1, 2, 3, 4 y 5 respectivamente. En el caso del modelo 3, sólo se presenta la primera pantalla, ya que la segunda coincide con la interfaz del modelo 1)

acciones y que seleccione la que es correcta) o el modelo 2 (teniendo que elegir la primera, segunda o tercera acción para una tarea concreta).

C. Diseño del sistema

Según la experiencia de la Asociación Parkinson Madrid el grado de satisfacción en el uso del ordenador y dispositivos tipo videoconsola no son satisfactorios en pacientes de Parkinson, el primero por la dificultad que les supone a este colectivo el uso del ratón y los segundos para evitar que los pacientes lo consideren algo lúdico en contraposición con la seriedad con la que valoran a sus terapias. Dado el creciente éxito que estaban empezando a tener las tablets Android en 2011 realizamos una primera prueba de validación tecnológica con una pequeña aplicación de prueba con 5 pacientes de Parkinson (con un estadío motor entre el 1 y el 3,5 y con edades comprendidas entre los 65 y los 79 años) que manejaron la tablet fácilmente y mostraron un grado de aceptación elevado. Además, destacaron su uso intuitivo e incidieron en que un dispositivo de estas características les permite la realización de la terapia en cualquier momento y lugar, lo que nos hizo tomar la decisión de decantarnos por esta tecnología.

La aplicación cliente ha sido desarrollada en todas las versiones Android para tablet (3.x, 4.0, 4.x). Esta aplicación permite al paciente la gestión de su terapia de estimulación (realización de bloques de ejercicios de estimulación y consulta de las valoraciones introducidas por el terapeuta) así como la consulta de la próxima cita con su terapeuta. Por otro lado, el terapeuta accede a través de web a la plataforma, donde puede visualizar los resultados obtenidos por los pacientes, asignarles un nuevo bloque de ejercicios de estimulación e introducir un mensaje que luego el paciente podrá visualizar a través de la tablet. Para ambas interfaces se han seguido criterios de accesibilidad y usabilidad. De esta forma, la tecnología es más atractiva debido a su facilidad de uso.

La Fig. 3 presenta la arquitectura del sistema, donde se pueden apreciar distintos elementos:

- Tablet Android: es el dispositivo del paciente, necesario para llevar a cabo la terapia de estimulación cognitiva tanto en la asociación como en casa. Los requisitos que debe cumplir son disponer de conexión a internet, ya sea mediante WiFi o mediante una tarjeta 3G, y sistema operativo Android.
- Navegador web: utilizado por el terapeuta para gestionar y realizar el seguimiento de la terapia de cada paciente. También lo utilizan el gestor de la terapia y el administrador para gestión de ejercicios y/o de usuarios.
- Servidor y base de datos: usados para el almacenamiento de los datos personales de los pacientes y la información relativa a la terapia.

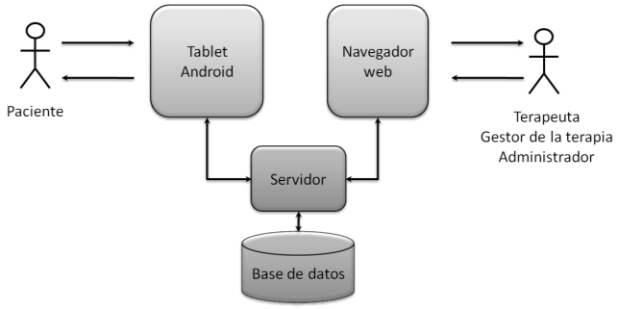


Fig. 3. Arquitectura del sistema

D. Implementación

1. Interfaces y modelo de interacción

Todas las interfaces se han diseñado siguiendo los criterios de accesibilidad de la Iniciativa de Accesibilidad Web del World Wide Web Consortium.

El diseño del modelo de interacción se ha elaborado conjuntamente con los pacientes mediante pruebas realizadas durante todas las fases del desarrollo del proyecto, añadiendo las mejoras que ellos han ido proponiendo. De esta manera, el diagrama de navegación es muy intuitivo y los menús sólo tienen dos niveles de profundidad. La interfaz de usuario de la aplicación Android ha sido diseñada teniendo en cuenta siempre las necesidades del colectivo implicado (fuente con color y tamaño apropiados, texto sencillo, uso intuitivo). En la Fig. 2 se presenta un ejemplo de esta interfaz, donde se puede observar que se han diseñado teclados adaptados para estos pacientes, con las letras colocadas en orden alfabético y teclas grandes que presenten alto contraste con el fondo. En cuanto a la pulsación en la pantalla, la aplicación evita pulsaciones indeseadas debido a movimientos incontrolados.

Al realizar un diseño accesible e intuitivo de la interfaz web, tanto terapeutas como gestores de la terapia han destacado la comodidad a la hora de realizar el seguimiento de los pacientes y para la introducción de nuevos ejercicios, para lo que no hace falta un programador.

2. Protocolo

Se ha diseñado un protocolo *ad hoc* (Fig. 4) para la conexión entre la tablet Android y el servidor, el cual contribuye a minimizar el intercambio de datos para así

Tipo 1 byte	**Id** 8 bytes	**Respuestas**												
		%	Ejercicio 1			%	Ejercicio 2			%...%	Ejercicio n			
			Resp	%	t		Resp	%	t		Resp	%	t	

Tipo 1 byte	**Sexo** 1 byte	**Nombre y apellidos**

Tipo 1 byte	**Nº total** 1 byte	**Modelo** 1 byte	**Imagen asociada**	**Enunciado**	**R1**	**R2**	**R3**	**Correcta** 1 byte	**Tiempo**

Tipo 1 byte	**Nº bloque** 1 byte	**Fecha término** 10 bytes	**Fecha valoración** 10 bytes	**Terapeuta**	**Valoración**

Tipo 1 byte	**Fecha** 10 bytes	**Hora** 5 bytes	**Lugar**

Tipo 1 byte	**Código** 1byte

Fig. 4. Protocolo *ad hoc* diseñado

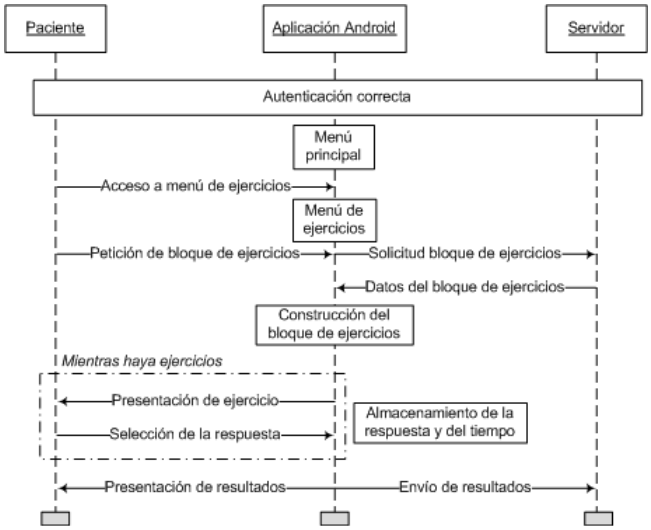


Fig. 5. Diagrama de secuencia de la descarga de un bloque de ejercicios

conseguir una mejora en los tiempos de respuesta del sistema. De las unidades de datos de la Fig. 4, la primera es la que se corresponde al sentido aplicación Android → servidor, y el resto en sentido contrario. La aplicación envía el tipo de petición y el identificador del paciente que la esté utilizando. Los tipos de peticiones posibles son:

- Petición de datos personales del usuario: de esta forma se personaliza la aplicación, para que el paciente perciba que esos ejercicios están diseñados específicamente para él/ella.
- Petición de un bloque de ejercicios: la aplicación solicita el bloque de ejercicios al servidor. Ese bloque de ejercicios ha sido definido por el terapeuta de forma específica para ese paciente. Únicamente se envían la información relacionada con cada ejercicio, que será construido dinámicamente por la aplicación Android. De esta forma, se consigue que el intercambio de datos sea mínimo y que no sea necesario un programador que cree los ejercicios, permitiendo su inserción en el servidor de forma sencilla e intuitiva, como se verá más adelante.
- Petición de valoración: el terapeuta realiza una valoración a la vista de los resultados obtenidos por el paciente, diseñando el nuevo bloque de ejercicios que se le enviará y añadiendo un mensaje, que será el que se envíe a la aplicación Android cuando el paciente seleccione esta opción.
- Petición de cita: el paciente consulta la fecha, hora y lugar de la próxima cita para consulta presencial que ha introducido previamente el terapeuta.
- Envío de los resultados: cuando el paciente termina un bloque de ejercicios, los resultados obtenidos y los tiempos de respuesta se envían automáticamente al servidor para su posterior consulta por el terapeuta.

3. Terapia de estimulación cognitiva

Los ejercicios se clasifican en bloques de 9, donde cada uno de un área de estimulación y cada bloque de un nivel de dificultad. En la Fig. 5 se muestra el diagrama de secuencia llevado a cabo entre cliente y servidor cuando el paciente solicita uno de estos bloques. Cuando el paciente selecciona la opción en el menú de la aplicación, se descarga los datos de los ejercicios y éstos son construidos dinámicamente por la aplicación Android. De esta forma, se consigue que el

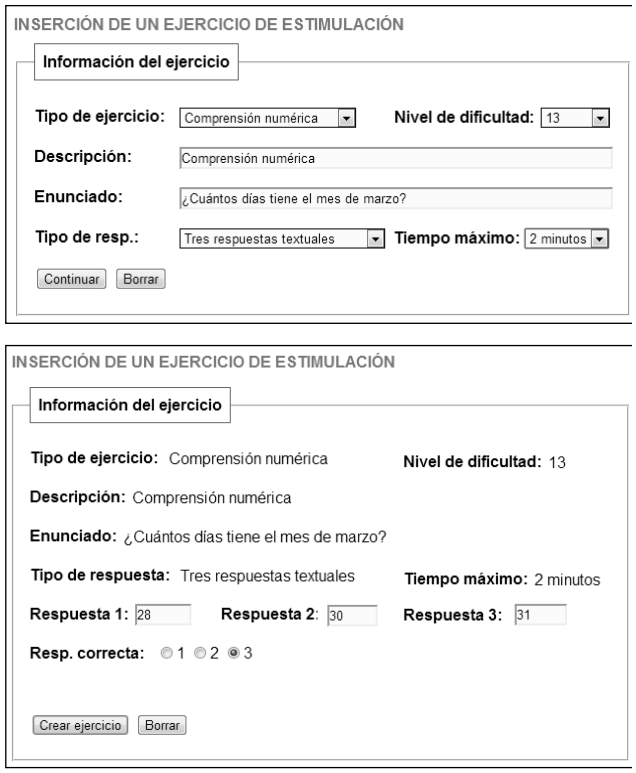


Fig. 6. Interfaz para la introducción de nuevos ejercicios

intercambio de información sea mínimo, mejorando la eficiencia. Una vez el paciente finaliza la realización del bloque de ejercicios, los resultados se envían al servidor para la posterior valoración por parte de su terapeuta.

En la Fig. 6 se muestra la forma de introducción de los ejercicios por parte del gestor de la terapia. Aparece la primera pantalla donde se deben introducir los datos comunes a todos los ejercicios, como son el área de estimulación, el nivel de dificultad, una breve descripción, el enunciado, el tiempo máximo del que dispone el paciente para su realización y el modelo de ejercicio. Según el modelo seleccionado, en la segunda pantalla se recogerán unos campos u otros, como son las respuestas posibles (ya sean textos o imágenes), la respuesta correcta o las imágenes asociadas al ejercicio.

IV. Plan de evaluación

El plan de evaluación ha sido diseñado por el equipo terapéutico de la Asociación Parkinson Madrid. Mediante los cuestionarios desarrollados, se ha pretendido evaluar el grado de satisfacción del colectivo implicado, como son pacientes y terapeutas.

A. Requisitos de usuario

El equipo de trabajo seleccionó un grupo de pacientes para llevar a cabo la terapia de estimulación cognitiva a través de esta plataforma de acuerdo a los siguientes requisitos:

- 10 personas con Parkinsonismo idiopático.
- Se tuvo en cuenta el género, buscando paridad entre hombres y mujeres.
- Uno de los datos recogidos fue si el paciente tenía experiencia en el uso de las Tecnologías de la Información y la Comunicación, aunque no era excluyente.

Tabla I
RESULTADOS DE LOS CUESTIONARIOS DE LOS PACIENTES

Pregunta	Sesión	TA	A	I	D	TD	Media por sesión	Media entre sesiones
1. Puedo realizar fácilmente los ejercicios de estimulación cognitiva utilizando la tablet	1	8	2	0	0	0	4,8	4,52
	2	4	4	1	1	0	4,1	
	3	7	1	1	0	0	4,67	
2. Me parece divertido hacer los ejercicios y la terapia de esta manera	1	6	3	1	0	0	4,5	4,59
	2	6	4	0	0	0	4,6	
	3	7	1	1	0	0	4,67	
3. He aprendido rápido a realizar la estimulación cognitiva con la tablet	1	5	4	1	0	0	4,4	4,24
	2	3	5	1	1	0	4	
	3	4	4	1	0	0	4,33	
4. No he tenido ningún problema para utilizar la aplicación yo solo/a	1	5	3	1	1	0	4,2	4,24
	2	4	4	2	0	0	4,2	
	3	4	4	1	0	0	4,33	
5. Me motiva el poder ver la valoración realizada por el terapeuta al corregir mis resultados	1	7	3	0	0	0	4,7	4,37
	2	2	8	0	0	0	4,2	
	3	3	5	1	0	0	4,22	
6. En general, me gusta realizar la estimulación cognitiva con la tablet	1	8	2	0	0	0	4,8	4,61
	2	7	3	0	0	0	4,7	
	3	4	4	1	0	0	4,33	
7. Si pudiera, realizaría la terapia en casa con este sistema	1	6	4	0	0	0	4,6	4,44
	2	5	5	0	0	0	4,5	
	3	5	2	1	1	0	4,22	

- Los pacientes que participaron en el estudio previo (EsCoTDT [11]) fueron excluidos para que esa experiencia no fuera un condicionante y poder validar y evaluar la facilidad de aprendizaje y la intuitividad de la plataforma.

B. *Muestra de usuarios*

Finalmente, la muestra de usuarios fue la siguiente:

- 10 pacientes, de los cuales 4 eran hombres y 6 mujeres.
- La media de edad era de 70 años, con el más joven de 59 y el mayor de 77.
- Los pacientes tenían experiencia muy baja o ninguna en el uso de las TIC.

Por parte del equipo terapéutico, participaron 3 logopedas que habitualmente llevan a cabo las terapias de estimulación cognitiva con los pacientes en la Asociación Parkinson Madrid de la forma tradicional.

C. *Diseño de la terapia*

Cada paciente realizó tres sesiones de estimulación cognitiva utilizando el sistema diseñado. En la primera sesión, el terapeuta explicó las operaciones que podía llevar a cabo con la aplicación Android y permaneció con el paciente por si necesitaba ayuda. En la segunda sesión, el paciente llevaba a cabo la terapia solo pero bajo la supervisión del terapeuta por si el paciente tenía algún problema para la utilización. Por último, en la tercera sesión, el paciente realizaba la terapia sin ninguna ayuda. La duración de estas sesiones fue de entre 20 y 30 minutos, donde los pacientes realizaron 3 bloques de ejercicios en cada una.

En cada sesión, tanto pacientes como terapeutas rellenaban un cuestionario donde se evaluaban aspectos como la accesibilidad, la usabilidad y el interés en utilizar este sistema como terapia complementaria en el domicilio. Mediante este piloto, se pretendió medir el grado de satisfacción de los usuarios con la plataforma desarrollada.

D. *Resultados*

La Tabla I presenta los resultados de los cuestionarios de los pacientes: totalmente de acuerdo (TA), de acuerdo (A) indiferente (I), en desacuerdo (D) o totalmente en desacuerdo (TD). Como se repartió a cada paciente un cuestionario en cada una de las 3 sesiones que se realizaron, la tabla muestra un total de 29 respuestas, ya que un paciente no pudo realizar la tercera sesión. Las dos últimas columnas presentan el grado de satisfacción de los pacientes. Para calcularlo, se han pasado las respuestas de cuestionario a puntuación numérica, dándole 5 puntos a TA, 4 puntos a A, 3 puntos a I, 2 puntos a D y 1 punto a TD y posteriormente se ha calculado la media aritmética según el número de pacientes que contestaron a los cuestionarios en cada sesión (10 en las sesiones 1 y 2, 9 en la sesión 3). La última columna presenta la media de las tres sesiones. Esto se puede ver de forma más clara a la vista de la Fig. 7, donde se contrasta en forma de gráfico la comparativa entre sesiones y entre la media de las tres.

En esta comparativa entre sesiones, se puede apreciar que, según va desapareciendo la supervisión del terapeuta, la media de cada pregunta desciende ligeramente, excepto en el caso de la pregunta 2 *Me parece divertido hacer los ejercicios y la terapia de esta manera* y de la pregunta 4 *No*

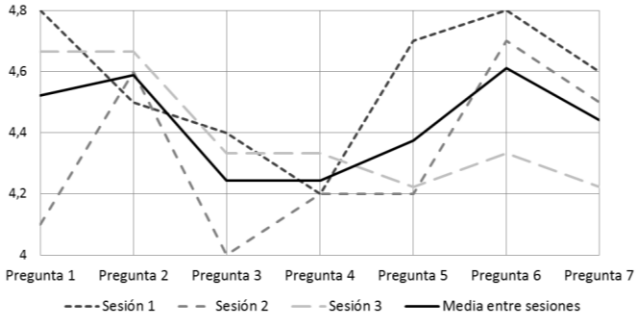


Fig. 7. Gráfico comparativo entre los resultados de cada sesión, mostrando también la media de las tres sesiones

he tenido ningún problema para utilizar la aplicación yo solo/a, donde la media mejora cuanto más independiente se siente el paciente. Estos dos puntos les parecen decisivos a los terapeutas en cuanto a la futura motivación para realizar terapia de forma independiente en el hogar. Pese a esa variación de la media podemos afirmar que tras los resultados obtenidos la experiencia ha sido muy positiva dado, que en un rango de satisfacción de 1 a 5 la media más baja ha sido de 4,24 (entre A y TA).

Los pacientes han apreciado los beneficios del sistema, destacando como ventajas de uso de esta plataforma tanto la interfaz intuitiva como el diseño de la terapia, enfatizando la utilidad percibida para su enfermedad. Además, están de acuerdo en realizar este tipo de terapias en casa. El diseño del sistema permite que, debido a que la tablet dispone de una SIM 3G o conexión WiFi, esta terapia puede estar disponible en cualquier lugar. Asimismo, la pregunta *No he tenido ningún problema para utilizar la aplicación yo solo/a* muestra la facilidad de uso, donde un 83% de los pacientes que han participado en el estudio están totalmente de acuerdo o de acuerdo.

La Fig. 8 presenta los resultados obtenidos tras esta experiencia en comparación con los de la experiencia previa sobre TDT interactiva. Se ha optado por utilizar grupos distintos de pacientes para cada una de las plataformas para que el conocimiento de la aplicación de TDT no condicionara los resultados de satisfacción de la aplicación Android. El grupo de prueba para la aplicación Android se ha seleccionado a partir de los parámetros que se tuvieron en cuenta para el piloto de la plataforma anterior (grado de deterioro cognitivo, rango de edad, paridad entre hombres y mujeres y experiencia en tecnología).

Las preguntas que se muestran en la Fig. 8 para realizar la comparativa entre plataformas son:

- Pregunta 1: Puedo realizar fácilmente los ejercicios de estimulación cognitiva utilizando la tablet / el mando a distancia y la televisión.
- Pregunta 2: Me parece divertido hacer los ejercicios y la terapia de esta manera.
- Pregunta 3: Me motiva el poder ver la valoración realizada por el terapeuta al corregir mis resultados.
- Pregunta 4: En general, me gusta realizar la estimulación cognitiva con la tablet / el mando a distancia.
- Pregunta 5: Si pudiera, realizaría la terapia en casa con este sistema.

Es importante destacar el incremento en el porcentaje de personas que están totalmente de acuerdo o de acuerdo en las dos últimas preguntas: *En general, me gusta realizar la estimulación cognitiva con la tablet / el mando a distancia* y *Si pudiera, realizaría la terapia en casa con este sistema*, que han cambiado de un 82% a un 97% y de un 76% a un 93% respectivamente. Este resultado indica que el cambio del dispositivo de acceso del paciente le hace sentir más seguro y cómodo cuando está realizando la terapia de forma remota.

Tabla II
RESULTADOS DE LOS CUESTIONARIOS DE LOS TERAPEUTAS

Pregunta	TA	A	I	D	TD
Creo que a los pacientes les gusta realizar la terapia a través de la tablet	23	2	0	0	0
Creo que el paciente puede usar la tablet él solo (Sesiones 2 y 3)	12	2	0	1	0
La aplicación web que uso para adaptar los ejercicios y valorar a los pacientes es sencilla de usar y completa en relación con las funciones que ofrece	20	5	0	0	0
Veo útil poder consultar la información de los ejercicios a través de la web	20	5	0	0	0
Creo que es sencillo añadir nuevos ejercicios a los bloques	17	5	3	0	0
Los ejercicios se adecúan a los requisitos de un paciente de Parkinson	22	3	0	0	0
Considero que la forma de consultar los resultados de los pacientes es apropiada	21	4	0	0	0
El realizar la terapia de esta forma no me quita más tiempo que de la forma tradicional	20	5	0	0	0
Creo que sería útil para los pacientes que también pudieran realizar la terapia desde sus casas utilizando este sistema	21	4	0	0	0

Por otro lado, en la Tabla II se presentan los cuestionarios orientados a comprobar el grado de satisfacción de los terapeutas implicados en el estudio, donde se puede observar cómo destacan la utilidad de un sistema como este para llevar a cabo el seguimiento de los pacientes de forma remota, apreciándose también la comodidad con la que ven a los pacientes cuando se enfrentan al sistema.

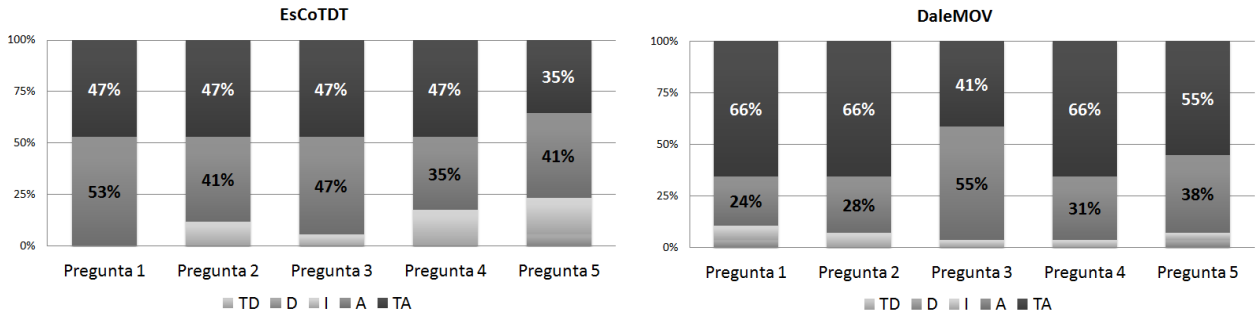


Fig. 8. Gráfico comparativo entre los resultados obtenidos de EsCoTDT y DaleMov. La leyenda es la siguiente: totalmente de acuerdo (TA), de acuerdo (A), indiferente (I), en desacuerdo (D) o totalmente en desacuerdo (TD). Las preguntas se presentan en el apartado *D. Resultados*

V. Conclusiones y trabajos futuros

La conclusión principal que se alcanza tras llevar a cabo este estudio es que la utilización de dispositivos móviles para la realización de terapias de estimulación cognitiva es factible. Este estudio refleja un alto grado de aceptación debido al diseño intuitivo de su interfaz y a la garantía dada en relación con los factores humanos como la privacidad y la confianza. Además, al implicar a los terapeutas en el estudio, el trabajo de investigación ha podido cubrir todas las necesidades de la plataforma de telecuidado ubicuo y la solución ha sido aceptada por todos los roles implicados en el sistema.

Los terapeutas que se han implicado en esta experiencia han hecho una evaluación positiva de la plataforma, la cual utilizan para el seguimiento de los pacientes y para ver el resultado de los ejercicios que han hecho. Además, destacan el valor de la personalización de la terapia según las necesidades y resultados de cada paciente. Al mismo tiempo, se realiza un mejor seguimiento del progreso del paciente. De esta manera, el cuidado que la persona recibe es mejor por la individualización de la terapia diseñada especialmente para él/ella.

La principal ventaja que el grupo de evaluación ha definido es la ubicuidad del sistema, porque ha dado la posibilidad de personalizar la terapia de estimulación cognitiva cuando los pacientes no pueden acudir a la asociación. Esto beneficia a personas que viven en zonas rurales que de otra manera no podrían acceder a este tipo de terapias.

Finalmente, este sistema con pequeños cambios, puede ser adaptado a otros colectivos con otro tipo de deterioro cognitivo, como es el asociado a la enfermedad de Alzheimer o el Deterioro Cognitivo Leve. Esto es debido a la facilidad de personalización de las terapias y la flexibilidad a la hora de crear nuevos ejercicios. Por ejemplo, para el caso de la enfermedad de Alzheimer, se podrían crear bloques de ejercicios que principalmente trataran la memoria a corto plazo (mucho más presente en esta enfermedad que en el Parkinson) y no se tendría en cuenta el tiempo que tardan los pacientes en realizar los ejercicios que en este caso es importante por las pérdidas de atención asociadas al Parkinson que no suelen estar presentes en Alzheimer.

Como trabajos futuros aparece la incorporación de técnicas de inteligencia artificial para la evaluación automática de los resultados de los pacientes. Esto puede ser útil cuando el número de pacientes que realizan la terapia utilizando esta plataforma es alto. Así, el equipo terapéutico no consume mucho tiempo en la evaluación. Además, otro trabajo futuro será tener en cuenta cómo aplicar diseño centrado en la actividad para la interacción persona-máquina para alcanzar ratios de aceptación más altos.

Agradecimientos

Este trabajo ha sido realizado gracias al apoyo del Ministerio de Economía y Competitividad en el marco del proyecto TALISEC+ (TIN2010-20510-C04-01).

Los autores quieren agradecer a la Asociación Parkinson Madrid y a la Federación Española de Parkinson su colaboración en las fases de análisis y validación de esta solución.

Referencias

[1] Tan, J.: E-Health Care Information Systems: An Introduction for Students and Professionals, Jossey-Bass (2005). Estados Unidos.

[2] Muras, J., Cahill, V., Stokes, E.: A taxonomy of pervasive healthcare systems, En Pervasive Health Conference and Workshops, pp. 1-10 (2006)

[3] Tárraga, L.; Boada, M.; Modinos, G. et al., A randomised pilot study to assess the efficacy of an interactive, multimedia tool of cognitive stimulation in Alzheimer's disease, En Journal of Neurology, Neurosurgery and Psychiatry with Practical Neurology, (04/07/2006), vol. 77, no. 10, pp. 1116-1121.

[4] Franco, M.; Jones, K.; Woods, B.; Gómez, P., GRADIOR: A personalized computer-based cognitive training program for early interaction in dementia, En Early Psychosocial Interventions in Dementia, (2009), Jessica Kingsley Publishers, pp. 93-105.

[5] National Parkinson Foundation, Parkinson's Toolkit: A Free Reference and Resource for Clinicians, En National Parkinson Foundation, (05/03/2013). [En línea] Disponible: http://www.parkinson.org/Professionals/Professional-Resources/Parkinson-s-Toolkit.aspx

[6] European Foundation for Health and Exercise, Parkinson Home Exercises, En iTunes, (05/03/2013). [En línea] Disponible: https://itunes.apple.com/es/app/parkinson-home-exercises/id473641730?mt=8

[7] Mazilu, S.; Hardegger, M.; Zhu, Z.; Roggen, D.; Troster, G.; Plotnik, M.; Hausdorff, J.M., Online detection of freezing of gait with smartphones and machine learning techniques, En Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2012 6th International Conference on (21-24/05/2012), San Diego, California, Estados Unidos, pp.123-130.

[8] B. Edwards; Using smartphones for objective diagnosis and monitoring of Parkinson's patients, En iMedicalApps, (26/07/2011). [En línea] Disponible: http://www.imedicalapps.com/2011/07/smartphone-diagnosis-monitoring-parkinsons-patients/

[9] Meza-Kubo, V.; Morán, A. L.; Rodríguez, M., IntouchFun, a Pervasive Collaborative System to Cope with Elder's Isolation and Cognitive Decline, En 12th ACM International Conference on Ubiquitous Computing (UbiComp 2010) (26-29/09/2010), Copenhague, Dinamarca.

[10] iParkinsons iOS app, (consultado en mayo de 2013). [En línea] Disponible: http://www.casafuturatech.com/iparkinsons/

[11] García Vázquez, C.; Moreno Martínez, E.; Valero Duboy, M.A.; Gómez Oliva, A., Distributed System for Cognitive Stimulation Over Interactive TV, En Information Technology in Biomedicine, IEEE Transactions on (noviembre de 2012), vol.16, no.6, pp.1115-1121.

[12] Asociación Parkinson Madrid; Cuaderno de ejercicios. Consejos sobre trastornos cognitivos para pacientes con enfermedad de Parkinson. Biblioteca Parkinson, 2007.

Líneas de investigación futuras continuación del proyecto europeo INTEGRIS

Josep M. Selga, Guiomar Corral, Agustín Zaballos
Departamento de Ingeniería,
Universitat Ramon Llull
C/ Quatre Camins, 2, 08022 - Barcelona
jmselga@salle.url.edu, guiomar@salle.url.edu, zaballos@salle.url.edu

***Resumen*- La necesaria introducción masiva de energías renovables en la red eléctrica con el objetivo de reducir las emisiones de gases de efecto invernadero y mejorar la sostenibilidad no se puede entender sin el despliegue de redes telemáticas y sistemas TIC de gran eficiencia sobre las redes de distribución de energía eléctrica. Tales redes telemáticas deben cumplir requerimientos que para algunos servicios son muy exigentes. Este documento presenta estos requerimientos, los resultados del proyecto europeo FP7 INTEGRIS y las líneas de investigación futura sugeridas a partir de los mismos y que constituyen líneas futuras de investigación en La Salle.**

Tales líneas incluyen un amplio espectro de tecnologías cuya eficiente integración es necesaria para la Smart Grid. Entre estas tecnologías están las de la gestión eficiente de redes malladas Ethernet, la QoS, la ciberseguridad, incluyendo la encriptación homomórfica, la virtualización de redes, los sistemas cognitivos y el almacenamiento y replicación de datos.

El objetivo es la obtención de un sistema capaz de dar servicio al conjunto de aplicaciones que se prevén para la Smart Grid de distribución de energía eléctrica.

***Palabras Clave*- telemática, smart grid, ciberseguridad, cognitive systems, TRILL.**

I. INTRODUCCIÓN

Las Smart Grids o redes eléctricas inteligentes son una red de redes que incluye múltiples tecnologías a veces poco relacionadas entre sí, pero que precisan ser integradas y coordinadas, habiendo sido comunes hasta el momento las soluciones parciales sin visión global, lo cual ha propiciado sistemas difíciles de integrar entre sí con los consiguientes sobrecostes.

Tal situación se ha tratado de superar en el recientemente finalizado proyecto europeo FP7 INTEGRIS: *INTelligent Electrical GRId Sensor communications* (http://fp7integris.eu), cuyo objetivo fue la consecución de un sistema capaz de albergar de forma eficiente todas las aplicaciones previstas para las redes de distribución eléctrica inteligentes. Aunque el mencionado proyecto alcanzó sus objetivos, en el mismo se identificaron una serie de problemas esenciales que las tecnologías actuales aun no resuelven y que son objeto del presente artículo.

El capítulo II describe el concepto de la Smart Grid y sus retos. El capítulo III introduce los requerimientos de la Smart Grid en cuanto a tecnologías TIC. El capítulo IV expone la arquitectura TIC definida en el proyecto INTEGRIS y muestra los resultados del mismo y el capítulo V comenta las líneas de investigación futuras identificadas en el proyecto. Finalmente, el capítulo VI contiene las conclusiones.

II. LA SMART GRID Y SUS RETOS

Las redes eléctricas han permanecido excepcionalmente estables durante mucho tiempo en gran contraste con la evolución de los sistemas TIC.

Sin embargo, en la actualidad, esta estabilidad debe cambiar por la necesidad existente de introducir energías renovables y distribuidas en la red, incluso en la red de distribución, para reemplazar las energías fósiles, con el fin de reducir costes, emisiones de gases y mejorar la fiabilidad de los sistemas eléctricos. También debe evolucionar por la necesidad asociada de facilitar la participación de los usuarios en los mercados de energía.

Tal introducción presenta numerosos problemas operacionales que no pueden ser resueltos por los sistemas y tecnologías actuales. Estas dificultades se deben básicamente a las razones siguientes: (1) el flujo de energía deja de ser unidireccional para pasar a ser bidireccional dependiendo de las necesidades del momento, lo cual hace necesario controlar la tensión en todos los puntos de consumo, (2) aumenta la potencia de cortocircuito en estos puntos, (3) se hace necesario introducir esquemas eléctricos de protección que hasta ahora solo se empleaban en las redes de alta tensión y (4) la introducción de energías renovables dificulta el necesario equilibrio entre consumo y producción haciendo aun más necesario actuar de forma flexible sobre la

Tabla I

REQUERIMIENTOS DE LA SMART GRID DE DISTRIBUCIÓN SEGÚN EL PROYECTO INTEGRIS (ENTREGABLES 2.2 Y 3.2)

Clase de Servicio	Descripción	Latencia	Fiabilidad
APF	Funciones activas de protección	<20 ms	Muy Alta (99,999%)
CMD	Mando y regulación	<2 s	Alta (99,99%)
MON	Monitorización y análisis	<2 s	Alta (99,99%)
AMS	Funciones de medición avanzada y de gestión del suministro	<5 m (Medidas de energía) <10 s(Alarmas)	Baja (99%)
IEM	Intercambio de datos de extremo a extremo y respuesta de la demanda	<5 m (Medidas de energía) <5 s (Otras señales)	Media (99,9%)

demanda.

Por fortuna, la evolución y madurez de los sistemas TIC permite ahora abordar los problemas mencionados; en especial para la red de distribución, donde en la actualidad los sistemas TIC se hallan poco desplegados.

En la práctica la Smart Grid será una íntima superposición de la red eléctrica y de una red de comunicaciones de altas prestaciones y sistemas de información asociados que deberá alcanzar todos los rincones a los cuales se extiende la red eléctrica y que permitirá ofrecer una plétora de nuevos servicios con distintos requerimientos, algunos muy exigentes.

Abundando en ello, la siguiente sección se centra en los requerimientos TIC de la Smart Grid.

III. Requerimientos TIC de la Smart Grid

Los distintos servicios a proveer por la Smart Grid presentan un amplio abanico de requerimientos TIC, algunos muy exigentes [1,2,3]; aunque estos requerimientos solo se han definido de forma exhaustiva para las redes de alta tensión, pero no para las redes de distribución.

Para cubrir este hueco, el proyecto europeo INTEGRIS, basándose en las mencionadas referencias, ha definido los requerimientos para las redes de distribución indicados en la Tabla I, que suponen un cierto relajamiento respecto a los de alta tensión. En la misma se puede ver que algunas funciones requieren al mismo tiempo latencias y fiabilidades muy altas mientras que, sin embargo, otras, son mucho más relajadas. De todas formas, algunas fuentes [3] sugieren también requerimientos de latencia para control de recursos energéticos distribuidos (DER) y gestión de la red de distribución muy bajos, del orden de 20 ms -100 ms.

Otros requerimientos cualitativos identificados son los siguientes:

- Servicios siempre conectados; sin previo establecimiento de conexión.
- Servicios difíciles de modelar como flujos.
- Servicios que requieren operar directamente sobre Ethernet (los mensajes “Goose” del protocolo IEC61850).
- Una gran exigencia en cuanto a integridad, en especial para los comandos, y en cuanto a confidencialidad, en especial para telelectura de contadores y datos personales.

Además, las redes de distribución presentan dificultades específicas para el despliegue de redes de telecomunicación debidas a su naturaleza heterogénea y parcialmente subterránea y también por la conveniencia de operar autónomamente en caso de desconexión temporal.

Por todo ello resulta evidente que la Smart Grid precisa de una red de comunicaciones muy robusta y flexible y que muchas tecnologías de comunicación actuales no cumplen con los mencionados requerimientos, ya que pocas tecnologías ofrecen latencias de pocos ms. A ello hay que añadir que normalmente la comunicación se halla compuesta de varios saltos, lo cual dificulta todavía más cumplir con la requerida latencia.

Asimismo, la baja latencia de algunos servicios debe mantenerse también en caso de fallos, por lo que el sistema de comunicaciones debe recuperarse también en 20 ms, lo cual es aun más complejo de alcanzar.

En cuanto a fiabilidad, los altos requerimientos pueden ser conseguidos con redundancia pero esto es también un reto en una red de distribución.

IV. Arquitectura y resultados del proyecto INTEGRIS

A. Ámbito y objetivos

El ámbito del proyecto INTEGRIS es la creación de sistemas TIC adecuados para las redes Smart Grid de distribución de energía eléctrica.

En este ámbito, sus objetivos científicos y tecnológicos son los siguientes:

- Consecución de un sistema TIC autónomo y autocicatrizante capaz de ofrecer garantías de calidad de servicio para la Smart Grid.
- Integración e interoperabilidad eficiente de sistemas de comunicación heterogéneos que incluyan el PLC y sistemas radio.
- Desarrollo de aplicaciones y tecnología IEC 61850 para la Smart Grid de distribución.
- Investigar en la aplicación de técnicas de sistemas distribuidos en la Smart Grid.
- Investigar en la aplicación de los sistemas cognitivos a la Smart Grid.
- Desarrollo de un sistema de ciberseguridad multinivel adecuado a los requerimientos de la Smart Grid.

B. Arquitectura

El proyecto INTEGRIS se concibió para interconectar de forma segura y eficiente los recursos de comunicaciones, almacenamiento y computación requeridos por la Smart Grid en un único tipo de dispositivo llamado “INTEGRIS Device” o I-Dev [4] que actúa como, (1) un bridge Ethernet con alta fiabilidad, (2) como concentrador de datos del entorno y (3) como host de aplicaciones de la Smart Grid distribuibles.

El bridge de alta fiabilidad I-Dev es capaz de integrar distintas tecnologías de comunicaciones ya sean cableadas (PLC, Fibra óptica) o radio, en una sola red que opera en capa MAC en base al protocolo TRILL [5]. También incluye mejoras para tratar la QoS y un sistema cognitivo que permite controlar el sistema con visión global. Todo ello con el objetivo de alcanzar los requerimientos TIC de la Tabla I.

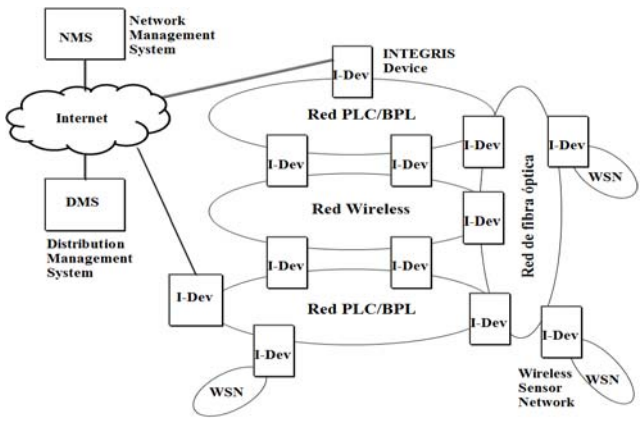


Fig. 1: Ejemplo de topología de un dominio INTEGRIS

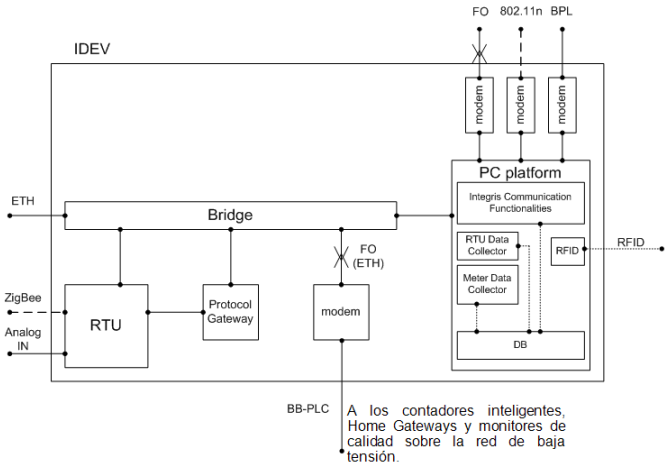


Fig. 2: Arquitectura interna de un INTEGRIS Device

La Fig.1 ejemplifica el tipo de redes que tal dispositivo permite formar. Un grupo de I-Devs interconectados a nivel 2, como muestra la Fig. 1, constituye un dominio INTEGRIS de forma que la Smart Grid en la visión de INTEGRIS puede ser vista como una colección de dominios INTEGRIS.

La adquisición de datos del entorno se realiza a través de sensores, contadores inteligentes o estaciones remotas de telecontrol (RTU) como se indica en la Fig.2, que muestra el detalle de la arquitectura interna del I-Dev.

El hosting de aplicaciones es posible por el hecho de que el I-Dev se halla dotado de recursos extra de almacenamiento y computación pero también por la potenciación de las mismas mediante un servicio de replicación de datos. Dichas características permiten mejorar tanto la fiabilidad como la latencia del acceso a los datos, la posibilidad de encriptar/desencriptar los datos almacenados e, incluso, la posibilidad de operar sobre datos encriptados mediante el método Pailler [6] de encriptación homomórfica.

Los I-Devs pueden localizarse en cualquier punto de la red eléctrica de distribución que se desee tales como centros de transformación, o concentraciones de contadores.

Un aspecto relevante de crear redes a nivel 2 sobre la red de distribución es que permite extender sin cambios los protocolos de la Smart Grid ya definidos para las subestaciones de alta tensión [7] a su zona circundante de distribución, obviando así la necesidad de ulteriores estándares para la red de distribución, algunos de los cuales aun no se han definido.

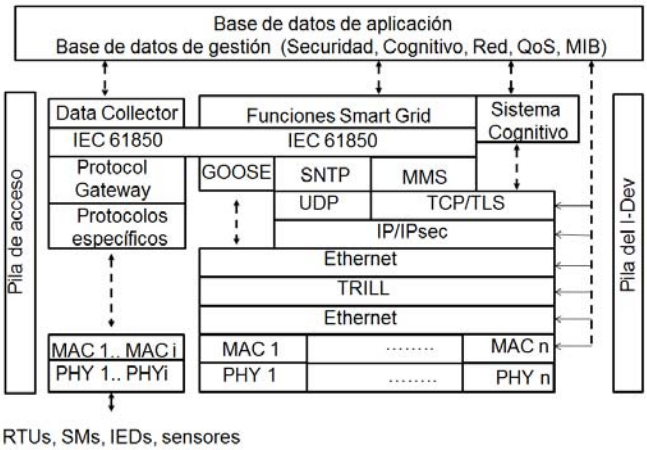


Fig. 3: Pila de protocolos de un INTEGRIS Device

La pila de protocolos del I-Dev se muestra en la Fig. 3, donde puede verse que las aplicaciones del sistema operan siempre sobre un único protocolo, el IEC61850 [7], que es el protocolo de referencia para la Smart Grid, traduciendo, siempre que sea necesario, desde otros protocolos antes de almacenar los datos. La comunicación con el centro de control se realiza también en IEC 61850. Como protocolo de este centro se ha empleado IEC 61850 en uno de los trials mientras que en el otro se ha traducido del mencionado protocolo a IEC61870-5-104, protocolo para el cual existe un mapeo claramente definido. De esta forma se ha obviado comunicar con centros de control que empleen el protocolo CIM (Common Information Model) (IEC 61970/61968) para el cual los temas de armonización y mapeo con IEC 61850 se hallan aun en estudio. De hecho, la cooperación con centros de control CIM se debería resolver en los propios centros de control mediante un mapeo de los objetos de cada protocolo.

También es importante destacar la posibilidad de usar mensajes directamente sobre Ethernet en la red de distribución lo cual permite los mensajes IEC61850 conocidos como “Goose”.

C. Resultados

El proyecto INTEGRIS alcanza sus objetivos en base a la creación de un nuevo sistema de información para la Smart Grid basado en un único tipo de dispositivo (el I-Dev) que integra todas las aportaciones del proyecto

Las aportaciones en cuanto a conectividad y formación de redes son las siguientes:

1-Consecución de una arquitectura de comunicaciones de alta fiabilidad y baja latencia a nivel 2 para las redes de distribución eléctrica que permite la integración de sistemas de comunicación heterogéneos y la gestión de redes malladas en base al protocolo TRILL, creando redes Ethernet malladas entre I-Devs. TRILL permite reducir latencias, complejidad de configuración y no impone restricciones a la topología física, ventajas muy convenientes para la Smart Grid de distribución.

2- Multiconectividad WAN para la conexión fiable con Centros de Control, sistema de gestión de red (NMS) u otros dominios INTEGRIS.

3- Capacidad multicamino dentro del dominio INTEGRIS.

4- Aplicación de las técnicas de QoS correctas según sea la Clase de Servicio (CoS) de cada paquete o aplicación y la salida del sistema cognitivo.

5- Sistema coordinado de ciberseguridad multinivel (MAC, IPsec, IEC62351 (TLS) [8]).

Las aportaciones en cuanto a distribución de aplicaciones y de almacenamiento de datos son:

1- Capacidad de hosting de aplicaciones distribuidas pudiéndolas localizar cerca de su lugar de uso.

2- Servicio de replicación de datos para optimizar la fiabilidad y latencia de acceso a los datos.

3- Servicio de encriptación de datos para el almacenamiento.

4- Servicio para trabajar sobre datos encriptados homomórficamente con el sistema Pailler que permite efectuar sumas con datos encriptados y multiplicaciones por constantes sin desencriptar los datos.

Y, finalmente, la coordinación de los anteriores mecanismos mediante un sistema cognitivo que dirige el sistema INTEGRIS.

El sistema cognitivo [4] adquiere datos sobre el desempeño del sistema (flujos, latencias, conectividad, ciberseguridad y otros) y, con la visión global obtenida, actúa sobre el sistema para corregir las deficiencias detectadas. La Fig. 5 representa el funcionamiento del sistema cognitivo en INTEGRIS. El sistema debe entrenarse inicialmente por un experto pero luego los módulos de Reinforcement Learning y de algoritmo genético van ajustando el sistema. Tal sistema cognitivo se ha aplicado en INTEGRIS al control de la red de datos pero no al control de los sistemas de gestión de las instalaciones eléctricas, posibilidad que resulta un tema de investigación futura de gran interés.

Todos estos mecanismos se han implementado y probado satisfactoriamente en campo en España (Barcelona) y en Italia (Brescia), así como también en los laboratorios de La Salle (Universitat Ramon Llull) en Barcelona y en la Universidad finlandesa de Tampere.

Tal combinación de elementos así como la aplicación de TRILL, de la replicación de datos y de los sistemas cognitivos a la Smart Grid son novedades que no han sido nunca realizadas con anterioridad.

V. Retos y Líneas futuras de investigación

Como se ha dicho, las realizaciones mencionadas en el capítulo anterior se han probado en campo y en laboratorio, lo cual ha arrojado cual es el nivel de cumplimiento de las expectativas iniciales y cuáles son los retos aun por superar.

A. *Protocolo TRILL*

Respecto al protocolo TRILL las pruebas efectuadas muestran su correcto funcionamiento general en cuanto al retardo introducido, que es menor a 1 ms en la implementación de INTEGRIS, pero también la lentitud de recuperación ante fallos. A este respecto, la Fig. 4 representa cuatro muestras de los resultados de las pruebas de recuperación del protocolo TRILL ante fallos para un escenario simple formado por dos I-Devs interconectados por dos enlaces según se representa en la propia Fig. 4. De los dos enlaces, uno lleva datos y el otro no. Tales pruebas miden el tiempo, en segundos, necesario para que TRILL detecte la pérdida de adyacencia del enlace en caso de desconexión de cada uno de los enlaces y de que la recupere una vez restablecido el enlace. En el caso de desconexión del enlace que lleva datos, se ha representado el tiempo durante el cual se pierden datos. En la misma se puede ver que el tiempo de recuperación mínimo de adyacencia nunca se sitúa por debajo de un segundo, cosa normal si se considera que el estándar TRILL prevé temporizadores ajustados con una precisión de segundos. De todas formas, las pruebas efectuadas con temporizadores ajustados a valores inferiores solo han permitido alcanzar un tiempo de recuperación de un segundo y ello a expensas de aumentar mucho el tráfico de control. Por tanto esta es una limitación esencial que hay que afrontar en el futuro.

Otra limitación proveniente del propio protocolo IS-IS es que solo considera caminos paralelos de igual longitud, lo cual limita las capacidades de multicamino y balanceo de carga.

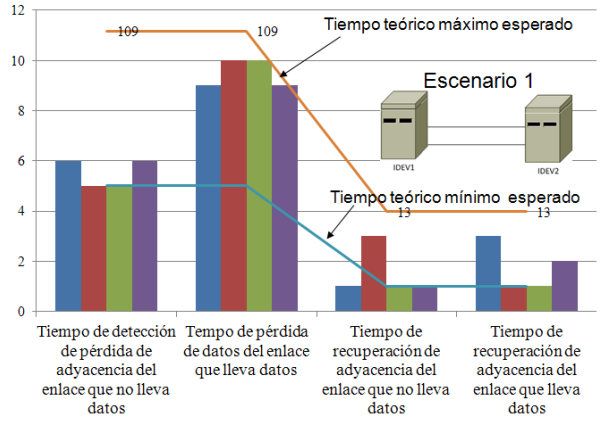


Fig. 4: Resultados de los tests de recuperación del protocolo TRILL

Una posible alternativa a TRILL puede ser el protocolo IEEE 802.1aq [9], pero en el momento de la implementación su estandarización no se hallaba suficientemente avanzada. Sin embargo, la impresión es que este protocolo, al basarse también en IS-IS [10] para la selección de caminos, presentará limitaciones parecidas.

Una posible solución al problema consiste en inspirarse en las soluciones existentes para las subestaciones de alta tensión para las cuales se han desarrollado los estándares Paralell Redundancy Protocol (PRP) y High Speed Redundancy Protocol (HSRP) [11] que pueden servir de inspiración para mejorar la solución de INTEGRIS como se sugiere en [12] por los autores.

B. *Sistema cognitivo*

El sistema cognitivo empleado en INTEGRIS [4], que es un componente no estándar en una red de datos, se ha diseñado como un sistema global que percibe el estado general de la red de datos y que decide sobre qué acciones realizar, ya sea directamente o a través de los otros subsistemas, con el objetivo de corregir deficiencias y maximizar el desempeño global. La técnica empleada en INTEGRIS ha sido la de eXtended learning Classifier Systems [13] (XCS) por su (1) aprendizaje incremental que permite al sistema aprender directamente de flujos de datos, (2) su robustez frente a datos ruidosos, (3) la transparencia y generalización del modelo producido y (4) que ha sido probado en entornos parecidos que prueban que XCS funciona adecuadamente en situaciones dinámicas.

Para mejorar la escalabilidad del sistema cognitivo y reducir el número de atributos del sistema de aprendizaje, cosa que aumenta su velocidad, se ha partido el sistema XCS en un sistema jerárquico de dos niveles: (1) los “PerceptionActionAgents” (PAA), y (2) los “Domain ManagementAgents” (DMA). Ello es posible porque la propia Smart Grid también se ha partido en dominios INTEGRIS que son zonas de la red de distribución eléctrica relativamente pequeñas y que se hallan malladas desde el punto de vista de su red de comunicaciones, lo cual permite al sistema aprender en paralelo.

Dentro de cada I-Dev hay una PAA. Los PAAs son la jerarquía más baja y tienen un nivel de percepción local y reportan al DMA, el cual a su vez redistribuye el conocimiento entre los distintos PAAs. El DMA es

responsable de decidir las acciones a aplicar a nivel de dominio.

De vez en cuando, las reglas se comparten entre dominios con el fin de encontrar el mejor modelo de control.

Se han efectuado pruebas de laboratorio [4] así como pruebas de campo y destacamos que el sistema funciona correctamente, pero que cabe mejorar en los siguientes aspectos:

- Conviene mover el sistema desde el sistema actual de aprendizaje supervisado, en el cual el mismo debe ser entrenado inicialmente por un experto (aunque luego los módulos de Reinforcement Learning y de algoritmo genético van ajustando el sistema) hacia un sistema no supervisado que permita aumentar su campo de aplicación práctico.
- Para mejorar el sistema es esencial dedicar más tiempo a aprender de la interacción entre la Smart Grid, el cognitivo y el experto para así ajustar las métricas, los actuadores y el propio sistema cognitivo.
- Hay que explorar la posibilidad de incorporar al sistema cognitivo inputs provenientes de las mismas aplicaciones Smart Grid.
- También cabe mejorar el tiempo de respuesta del mismo.

C. *Sistema de replicación de datos*

Respecto al sistema de replicación de datos [4] podemos decir que INTEGRIS ha probado el concepto y su correcto funcionamiento y que la mejora que cabe introducir en el futuro es la de suplementar el actual repositorio de datos con particiones automáticas.

La Fig. 6 expone la arquitectura del sistema de replicación de datos con una profundidad de replicación de valor 3.

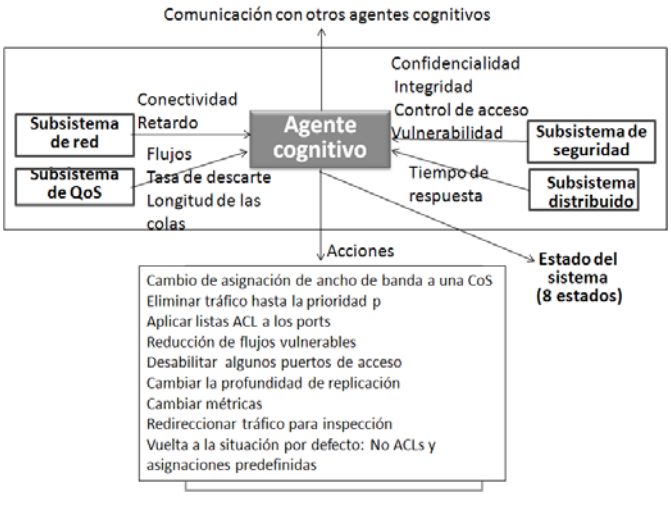


Fig. 5: Funcionamiento del sistema cognitivo como un broker en INTEGRIS

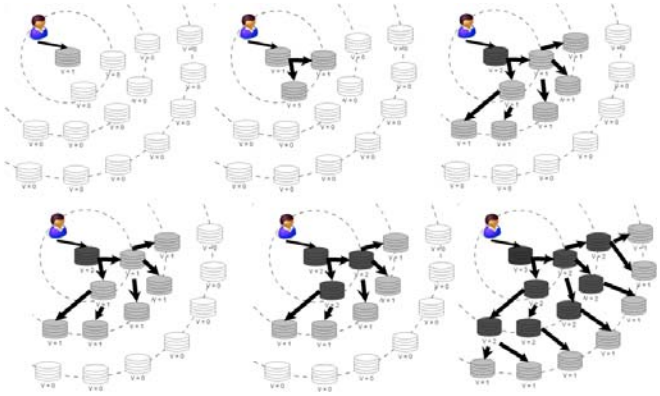


Fig. 6: Sistema de replicación de datos de INTEGRIS. Profundidad de replicación: 3.

El sistema de replicación de datos también contribuye a la consecución de una baja latencia para las aplicaciones, acercando los datos a las mismas, así como aquellas pueden también acercarse a los datos moviéndose desde el centro de control (funcionamiento tradicional) hacia los I-Devs distribuidos (funcionamiento INTEGRIS), tal y como se ha representado en la Fig. 7.

D. *Tecnologías de telecomunicaciones*

Respecto a las tecnologías de comunicaciones empleadas, los tests mostraron las limitaciones de PLC cuando los niveles de ruido en la red eléctrica aumentan en desmesura. Estas limitaciones afectan la garantía de latencia necesaria aunque, en general, no limitan la capacidad de transmisión requerida por la Smart Grid de distribución (unos 4Mbps en el peor de los casos) cuando se emplea PLC de banda ancha (capacidades nominales de centenares de Mbps). La solución puede pasar por mejorar la capa MAC orientándola más a los servicios de la Smart Grid. A este respecto cabe recordar que tanto el estándar IEEE P1901 [14] como el sistema PLC desarrollado en el proyecto europeo FP6 OPERA (Open PLC European research alliance for new generation PLC integrated network), que ha sido el empleado en INTEGRIS de la mano del partner Marvell Hispania, se diseñaron pensando en los mercados de acceso e in-home y, solo al final, tomaron en cuenta algunas características de los servicios Smart Grid.

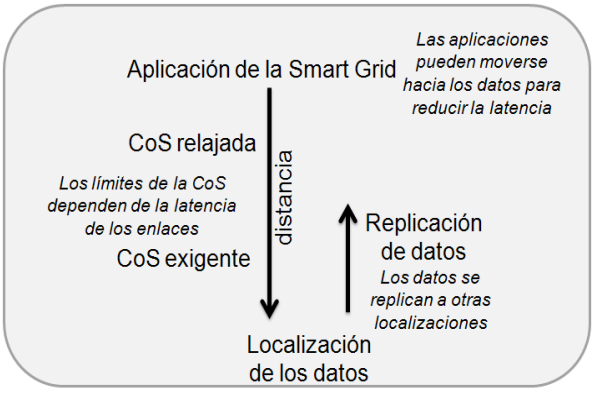


Fig. 7: Representación de cómo tanto las aplicaciones como los datos pueden moverse para cumplir con la Class of Service.

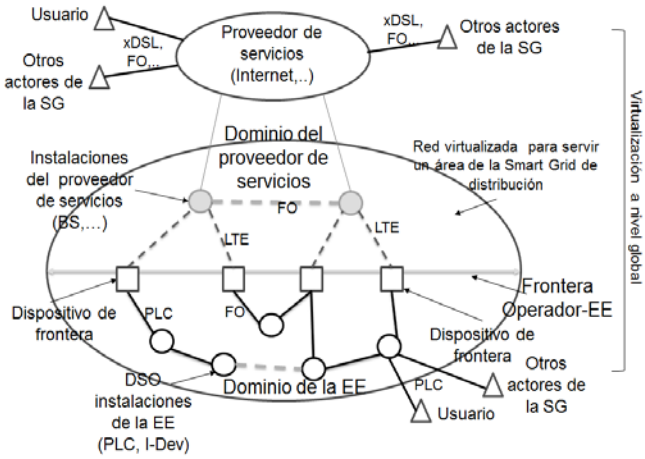


Fig. 8: Un posible esquema de integración de PLC y redes de la empresa eléctrica con las redes de operador de telecomunicaciones.

Al respecto de las tecnologías de comunicación, cabe destacar que PLC es necesario en la Smart Grid por su capacidad de acceder a las partes subterráneas de la red que son alrededor de un 50% de la misma aunque también por su conveniencia para la empresa eléctrica pero que, sin embargo, la alta fiabilidad requerida sugiere que tal red se complemente, no solo con sistemas radio y cableados como se ha hecho en INTEGRIS, sino también con tecnologías y servicios ofrecidos por los operadores de telecomunicación que podrían incrementar la fiabilidad del sistema comunicando sus partes aéreas e integrando los sistemas PLC y de fibra de la eléctrica con las tecnologías de operador en una sola red diseñada para la Smart Grid.

A este respecto la impresión es que tal interoperación o integración se podría ver facilitada por la virtualización de recursos y redes, cosa que constituye una nueva línea de investigación de La Salle surgida del proyecto INTEGRIS. Tal posibilidad se ha grafiado en la Fig. 8.

E. Sistema de ciberseguridad

El sistema multinivel implementado cuyo stack de protocolos se representa en la Fig. 9 resulta correcto para proteger la red y los datos. Sin embargo, en INTEGRIS, ha resultado evidente la falta de mecanismos de seguridad en

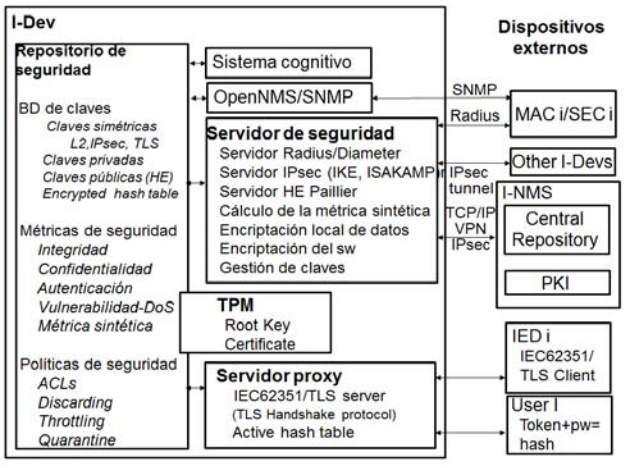


Fig. 9: Arquitectura de ciberseguridad de INTEGRIS

muchos de los dispositivos terminales empleados por las empresas eléctricas tales como Estaciones Remotas de Telecontrol (RTU), contadores inteligentes, sensores y otros.

Por otra parte las vulnerabilidades de la Smart Grid son muy amplias y ningún sistema actual se puede considerar suficiente. Por ello se proponen las siguientes mejoras:

- Profundizar en el sistema jerárquico de repositorios AAA desarrollado en INTEGRIS con el fin de reducir los incrementos de latencia introducidos por los sistemas de seguridad y permitir el funcionamiento incluso con desconexiones temporales.
- Incrementar la eficiencia del sistema de encriptación homomórfica implementado para acercarla a su uso práctico. Esta es una de las líneas de investigación actuales de La Salle (Universitat Ramon Llull).
- Crear un sistema de gestión de claves y certificados del conjunto.
- Proteger el sistema también a nivel de aplicación, algo que estaba fuera del objetivo de INTEGRIS.
- Incorporar sistemas de ciberseguridad a todos los terminales conectados a la red. En especial, emplear el protocolo IEC 62351 [8].

F. Aplicaciones Smart Grid distribuidas

Respecto a las aplicaciones de la Smart Grid cabe destacar que la distribución de las mismas es un reto en sí mismo y que al respecto INTEGRIS, a través de casos de uso implementados en campo, ha probado que [15]:

- El proceso de toma de decisiones distribuido es técnicamente posible para problemas simples como el control de congestión de la red de baja tensión, en especial cuando se requieren de forma esporádica pero con un tiempo de respuesta muy estricto.
- La arquitectura INTEGRIS es eficiente para manejar grandes volúmenes de datos en tiempo real ya sean de monitorización u otros.
- La monitorización distribuida de las redes de media y baja tensión es suficientemente precisa para las aplicaciones de planificación de red y para la operación.
- Es posible detectar de forma distribuida cualquier tipo de fallo de la red de distribución y distinguir entre fallos de media y de baja tensión.
- La estimación de estado en redes de baja tensión funciona en la práctica y reduce tanto los requerimientos de comunicación en tiempo real como los errores.

VI. Conclusiones

El proyecto INTEGRIS ha alcanzado sus hitos mediante la creación de un único tipo de dispositivo (I-Dev) modular y en base a estándares que da respuesta a los requerimientos de la Smart Grid de distribución de forma distribuida.

Las líneas maestras en que se basa INTEGRIS son:

1- Posibilidad de despliegue de aplicaciones Smart Grid distribuidas.

2- Centrado en el protocolo IEC61850.

3- Uso del protocolo IEC 61850 también en las redes de distribución.
4- Extensión de los protocolos de la subestación de alta tensión a su entorno inmediato.
5- Plataforma única integrando todas las aportaciones del proyecto de forma modular y siguiendo estándares.
6- Creación de redes a nivel Ethernet.
7- Sistema coordinado de ciberseguridad multinivel.
8- Gestión de QoS.
9- Sistema TIC dirigido por un sistema cognitivo.
10- Replicación automática y adaptativa de datos.

El proyecto INTEGRIS ha permitido implementar y probar la validez del concepto y la utilidad de las aplicaciones Smart Grid distribuidas.

En el proceso se han identificado retos esenciales que merecen ser investigados. Entre los mismos cabe destacar los siguientes:

- Dificultad de obtener redes redundantes malladas que se recuperen de los fallos en milisegundos o que dispongan de mecanismos alternativos para evitar que los fallos afecten a las aplicaciones.
- Dificultad en el uso flexible de los caminos redundantes.
- Necesidad de sistemas PLC con menos latencia y más estables y orientados a las aplicaciones Smart Grid.
- Creación de aplicaciones Smart Grid que sean fácilmente movibles, incluso automáticamente.
- Mejorar el conocimiento del sistema (comportamiento, métricas, acciones) a través de más experimentación con el sistema cognitivo.
- Inclusión de servicios de telecomunicación ofrecidos por los operadores de telecomunicación en el esquema INTEGRIS. Posible aplicación de técnicas de virtualización de recursos y redes para conseguir este objetivo.

AGRADECIMIENTOS

Los autores agradecen al proyecto INTEGRIS (no. 247938) del séptimo programa marco de la Unión Europea de la Call conjunta “ICT-Energy, 2009” y a La Salle (Universitat Ramon Llull) por su soporte.

REFERENCIAS

[1] IEEE Std 1646-2004, “IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation”.
[2] IEC 61850-5:2003, Communication networks and systems in substations – Part 5: Communication requirements for functions and device models.
[3] U.S. Department of Energy. “Communication requirements of smart grid technologies”. October, 2010
[4] J. Navarro; A. Zaballos; A. Sancho-Asensio; G Ravera; J.E. Armendáriz Iñigo, “The Information System of INTEGRIS: INTelligent Electrical GRId Sensor Communications”, IEEE Transactions on Industrial Informatics, November, 2012
[5] IETF RFC6325, Touch R. Perlman, D. Eastlake 3rd, D. Dutt, S. Gai, A. Ghanwani “Transparent Interconnection of Lots of Links (TRILL): Base Protocol Specification”. July 2011
[6] Paillier, P. (1999) “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes”. J. Stern, Ed., Advances in Cryptology – EUROCRYPT'99, vol. 1592 de Lecture Notes in Computer Science, p. 223-238, Springer-Verlag.
[7] IEC 61850 series of standards.
[8] ISO-IEC 62351, Part 6: Security for IEC 61850, October 2006
[9] IEEE 802.1aq-2012 - IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks--Amendment 20: Shortest Path Bridging
[10] IETF RFC 1142, “OSI IS-IS Intra-domain Routing Protocol“, February, 1990
[11] International Electrotechnical Commission, IEC 62439-3 Clauses 4 and 5- Parallel Redundancy Protocol and High-availability Seamless Redundancy
[12] Selga, J.M., Navarro, J and Zaballos, A., “Solutions to the Computer Networking Challenges of the Distribution Smart Grid“, IEEE Communication Letters, March, 2013
[13] O. Sigaud and S. Wilson, “Learning Classifier Systems: A survey”, Université Pierre et Marie Curie, Paris Cedex 05, France, Tech. Rep., September, 2007
[14] IEEE Std. P1901-2010, “Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications”, 2010
[15] Sami Repo, Shengye Lu, Timo Pöhö, Davide Della Giustina , Guillermo Ravera, Josep M. Selga, “Active Distribution Network Concept for Distributed Management of Low Voltage Network”, IEEE PES Innovative Smart Grid Technologies (ISGT) Europe Conference, ISGT, 2013.

Comunicaciones Oportunistas y Contextuales para Redes Multi-hop Celular con Retransmisores Móviles

Baldomero Coll-Perales [(1)], Javier Gozalvez [(1)] y Vasilis Friderikos [(2)]
[(1)] UWICORE, *Ubiquitous Wireless Communications Research Laboratory* http://www.uwicore.umh.es,
Universidad Miguel Hernández de Elche, Avda. de la Universidad s/n, 03202, Elche, España
[(2)] CTR, *Center for Telecommunications Research*, King's College London, London, U.K., WC2R 2LS
bcoll@umh.es, j.gozalvez@umh.es, vasilis.friderikos@kcl.ac.uk

***Resumen*- La creciente demanda de datos y las limitaciones de capacidad de los actuales sistemas celulares representan un verdadero reto para las operadoras de red. Las redes multi-hop celular con retransmisores móviles (*Multi-hop Cellular Networks with Mobile Relays*, MCN-MR) han emergido como una tecnología capaz de abordar estos problemas a través de la integración de las redes celulares y ad-hoc utilizando comunicaciones entre dispositivos (*Device to Device*, D2D). Este trabajo estudia la integración de técnicas oportunistas en redes MCN-MR para incrementar la eficiencia energética de las comunicaciones celulares. En primer lugar este trabajo identifica la configuración óptima de las comunicaciones oportunistas en un escenario MCN-MR de 2 saltos. A partir de estas configuraciones se desarrollan dos novedosas técnicas oportunistas para redes MCN-MR que explotan la comunicación D2D entre dispositivos móviles. Los resultados obtenidos demuestran los importantes beneficios energéticos de la integración de las técnicas oportunistas en redes MCN-MR.**

***Palabras Clave*- Eficiencia energética, comunicaciones oportunistas, comunicaciones contextuales, redes multi-hop celular con retransmisores móviles**

I. INTRODUCCIÓN

Las redes de telefonía móvil han experimentado un importante incremento en el tráfico de datos, lo cual representa un verdadero reto para las operadoras de red. Para hacer frente a este incremento en la demanda de tráfico se han desarrollado nuevas tecnologías de acceso radio y técnicas avanzadas de comunicación que han conseguido incrementar la eficiencia espectral. A pesar de los importantes avances logrados, las redes celulares tradicionales podrían no ser capaces de hacer frente a las altas demandas de tráfico de datos previstas. En este contexto, la integración de técnicas distribuidas basadas en retransmisores dentro de los sistemas celulares (a lo que se conoce como redes celulares multi-salto o MCN) ha despertado un gran interés en la comunidad investigadora debido a sus posibles beneficios en términos de capacidad, eficiencia energética, y balanceo de carga [1]. Los beneficios esperados por las redes MCN se basan en la sustitución de enlaces de comunicación de larga distancia entre los terminales móviles y la estación base, y que por lo general se establecen en condiciones de no visión directa (*Non-Line of Sight*, NLOS), por múltiples enlaces de menor distancia con mejores condiciones de comunicación. La introducción de las técnicas de retransmisión en los estándares celulares se ha centrado inicialmente en soluciones con retransmisores fijos (MCN-*Fixed Relay*, MCN-FR). Sin embargo, la consideración de nodos retransmisores móviles en redes MCN (MCN-MR) ofrece enormes posibilidades de comunicación al explotar los recursos de los dispositivos móviles desplegados de un modo colaborativo y oportunista [2]. Las redes MCN-MR pueden contribuir a la eficiencia energética de los futuros sistemas de comunicaciones móviles a través de la integración de soluciones oportunistas. Los mecanismos oportunistas basan su modo de operación en la movilidad de los nodos y explotan el paradigma 'almacena-transporta & retransmite' (*Store-Carry & Forward,* SCF) para establecer enlaces de comunicación entre dispositivos móviles. Sin embargo, las limitadas oportunidades de contacto entre los dispositivos móviles conllevan un posible incremento del retardo en la transmisión extremo a extremo [3]. La integración de las técnicas oportunista en las redes MCN-MR en las que los dispositivos móviles poseen continuamente conectividad celular representa una opción interesante para incrementar la calidad del servicio, balancear tráfico tolerante a retardos y mejorar la eficiencia energética.

En este contexto, el presente trabajo estudia la integración de técnicas oportunistas en redes multi-hop celular de 2 saltos para reducir el consumo energético de las comunicaciones celulares en el enlace ascendente. En particular, este artículo formula matemáticamente el problema de optimización de la comunicación oportunista MCN-MR de 2 saltos, con el objetivo de identificar la localización óptima del terminal móvil retransmisor y la localización a la que el retransmisor necesita iniciar el reenvío de la información a la estación base con el fin de minimizar el consumo energético. A partir de esta configuración óptima, este trabajo desarrolla también dos técnicas oportunistas que hacen uso de información contextual difundida por la estación base para seleccionar al nodo móvil retransmisor cuando no se pueda garantizar su localización en la ubicación óptima identificada.

El resto de este artículo está organizado del siguiente modo. La Sección II resume los estudios relacionados con la eficiencia energética en redes MCN-MR y en redes que integran técnicas oportunistas. La Sección III presenta el modelo de comunicación oportunista MCN-MR considerado en este trabajo y obtiene las configuraciones óptimas a partir de la formulación matemática del problema. La Sección IV muestra las dos técnicas oportunistas contextuales que se proponen en este trabajo para seleccionar al nodo móvil retransmisor. Finalmente, la Sección V concluye el trabajo resumiendo las principales aportaciones del estudio realizado y señalando los trabajos futuros.

II. Trabajos Relacionados

Diferentes estudios han investigado el impacto de la utilización de retransmisores móviles y de las comunicaciones oportunistas en el consumo energético dentro de un sistema celular. El trabajo presentado en [4] considera un escenario en el que una celda se divide en anillos concéntricos, y sólo los dispositivos móviles dentro del anillo más interno pueden enviar los datos a la estación base. Por otra parte, los dispositivos móviles situados en anillos más externos son los encargados de retransmitir la información a los dispositivos móviles situados en el anillo inmediatamente interior; hasta alcanzar al dispositivo móvil situado en el anillo más interno. El estudio realizado en [4] demuestra que con una adecuada selección del tamaño de los anillos es posible reducir el consumo de energía en comunicaciones MCN con retransmisores móviles si se compara con la transmisión tradicional directa entre el dispositivo móvil y la estación base.

En las redes oportunistas, las rutas multi-hop se establecen a partir de las oportunidades de conectividad y del tiempo de contacto (y entre contactos) de los nodos móviles [3]. Como resultado, los nodos móviles almacenan y transportan la información cuando no existen oportunidades de comunicación, y esperan a futuras oportunidades que pueden llegar por la continua movilidad de los nodos. Aunque este modo de operación puede aumentar los retardos en la transmisión extremo a extremo, ha demostrado una importante reducción del consumo de energía en redes de comunicación inalámbricas multi-hop.

Los beneficios de la integración de las técnicas oportunistas en las redes MCN se demuestran en [5], donde los autores presentan novedosas políticas de enrutamiento que hacen uso de información sobre la movilidad de los retransmisores móviles para reducir el consumo de energía, aumentar la capacidad espacial, reducir la interferencia co-canal, distribuir la carga de tráfico a través de distintas celdas, y desconectar estaciones base infrautilizadas. Los autores de [5] desarrollan políticas de enrutamiento oportunistas mediante la formulación de grafos espacio-temporales finitos de la red, donde los vértices representan la ubicación de los retransmisores móviles en el tiempo, y las aristas los enlaces de comunicación entre los dispositivos móviles. El grafo de la red resultante incluye todas las rutas posibles (incluyendo espacios en los que los terminales móviles almacenan y transportan la información) para la transmisión de la información a la estación base celular. En este estudio, los autores demuestran que cuanto mayor es el tiempo disponible para transmitir la información (i.e. cuanto mayor sea la tolerancia al retardo de las aplicaciones), mayores son los beneficios en términos de eficiencia energética de la integración de las comunicaciones celulares y oportunistas. Los autores de [5] extienden su estudio anterior a redes celulares cognitivas [6] en las que las oportunidades de comunicación con la estación base a través de técnicas oportunistas se limitan a los recursos que encuentran disponibles los 'usuarios secundarios' (*Secundary Users*, SU). En [6] se pone de manifiesto además la importancia de considerar el consumo de energía de las unidades de almacenamiento de los retransmisores móviles para el adecuado estudio integral de los mecanismos oportunistas.

III. Comunicaciones Oportunistas en Redes MCN-MR

Estudios anteriores han demostrado los beneficios energéticos resultantes de la integración de los mecanismos oportunistas en las redes celulares a expensas de los posibles retardos en la comunicación extremo a extremo. Por lo tanto, esta integración ofrece a los terminales móviles la posibilidad de retrasar el envío de la información a la estación base. En este contexto, un aspecto clave es cómo realizar la gestión del tiempo disponible para lograr el resultado deseado; en el caso de este estudio, reducir el consumo de energía.

Este trabajo se centra en un escenario MCN-MR de 2 saltos, en el que el nodo de origen (*Source Node*, SN) es estático y tiene información que transmitir a la estación base (*Base Station*, BS). Para ello, el SN puede explotar la cooperación de nodos retransmisores móviles (*Mobile Relay*, MR) capaces de almacenar, transportar y retransmitir la información (Fig. 1). En este contexto, el tiempo necesario para transmitir la información desde el SN a la BS se calcula en base a: 1) el tiempo necesario para la transmisión ad-hoc desde el SN al MR (*D2D tx*), 2) el tiempo que el MR almacena y transporta la información (*Store-Carry & Forward*, SCF), y 3) el tiempo necesario para que el MR transmita la información a la BS (*Celular tx*). Es importante señalar que el tiempo necesario para la transmisión *D2D tx* desde el SN al MR depende de la localización del MR (o dicho de otro modo, de la distancia entre el SN y el MR), al igual que el tiempo necesario para la transmisión *Celular tx* depende del lugar en el que el MR inicie la transmisión celular a la BS. En este contexto, este trabajo se centra inicialmente en la estimación de estos dos lugares, con el objetivo final de reducir el consumo total de energía de la comunicación MCN-MR oportunista de 2 saltos.

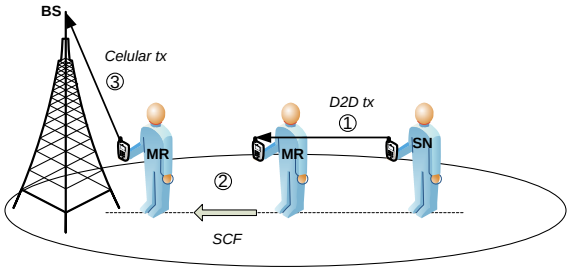


Fig. 1. Escenario de la comunicación MCN-MR oportunista de 2 saltos.

A. Formulación matemática del problema

Para determinar la configuración óptima que permite reducir al mínimo el consumo total de energía de la comunicación MCN-MR oportunista de 2 saltos se ha formulado un problema de optimización multi-objetivo con restricciones. Para ello, se ha definido la función objetivo que se muestra en (1) junto con dos restricciones (2) y (3). Una restricción intrínseca del problema es la necesidad de que la BS reciba la información dentro del tiempo máximo permitido T. Este tiempo límite se ha discretizado en (1) como $\{\tau_0, \tau_1, ..., \tau_T\}$. La definición de la función objetivo tiene en cuenta la energía consumida por la transmisión *D2D tx* ①, el proceso de almacenamiento, transporte y reenvío (SCF) ② y la transmisión celular *Celular tx* ③. E_{adhoc} es la energía consumida en la transmisión D2D, y es una función que depende de la distancia entre el SN y el MR y el tiempo necesario para la transmisión D2D. P_R, P_W y P_{IDLE} están relacionadas con la energía consumida en el proceso de

almacenar y transportar la información en los dispositivos móviles. E_{cell} representa la energía consumida en la transmisión celular, y es una función que depende de la distancia entre el MR y la BS y el tiempo necesario para la transmisión celular. La función objetivo incluye dos restricciones para asegurar que el mensaje (de tamaño F) sea completamente transmitido en la transmisión celular (3) y en la transmisión D2D (2). R_{adhoc} y R_{cell} representan las tasas de transmisión de los enlaces ad-hoc y celular, respectivamente. En este contexto, la identificación de la ubicación óptima del retransmisor móvil para que de inicio la transmisión D2D, y la ubicación en la que el MR tiene que empezar a transmitir la información a la red celular, es equivalente a encontrar τ_{b-1}, τ_{c-1} y τ_{c+m} en (1).

$$o.f: \min \left(\begin{array}{l} \underbrace{\sum_{\tau=\tau_0}^{\tau_{b-1}} \left(E_{adhoc}\left(d_{SN-MR},\tau\right) + \tau \cdot \left(P_R + P_W\right)\right)}_{①} + \\ \underbrace{\sum_{\tau=\tau_b}^{\tau_{c-1}} \tau \cdot P_{IDLE}}_{②} + \\ \underbrace{\sum_{\tau=\tau_c}^{\tau_{c+m}} \left(E_{cell}(d_{MR-BS},\tau) + \tau \cdot P_W \right)}_{③} \end{array} \right) \quad (1)$$

$$st:$$

$$\sum_{\tau=\tau_0}^{\tau_{b-1}} R_{adhoc}\left(d_{SN-MR}\right) \cdot \tau \geq F \quad (2)$$

$$\sum_{\tau=\tau_c}^{\tau_{c+m}} R_{cell}\left(d_{MR-BS}\right) \cdot \tau \geq F \quad (3)$$

A continuación se detallan los modelos utilizados en este trabajo en cada uno de los procesos involucrados en la comunicación MCN-MR oportunista de 2 saltos:

1) D2D tx. Las pérdidas de propagación entre el SN y el MR se han modelado utilizando el modelo determinista de 2 rayos. En este contexto, la energía consumida en las transmisiones ad-hoc entre dispositivos móviles puede expresarse como [5]:

$$E_{adhoc}\left(d\right) = \begin{cases} (e_r + e_t + e_{LOS} \cdot d^2) \cdot R_{adhoc} & si\ d < d_{brake} \\ (e_r + e_t + e_{MP} \cdot d^4) \cdot R_{adhoc} & si\ d \geq d_{brake} \end{cases} \quad (4)$$

donde e_t y e_r representan el consumo de energía por bit en el transmisor y la electrónica del receptor, respectivamente, y R_{adhoc} es la tasa de transmisión de datos en el enlace ad-hoc. La distancia entre el transmisor y el receptor es d, y $d_{brake} = 4\pi h_T h_R/\Lambda$ es la distancia crítica (h_T y h_R representan la altura de las antenas de los dispositivos móviles transmisor y receptor, y Λ es la longitud de onda de la frecuencia portadora, todos en m). Para $d < d_{brake}$, el parámetro e_{LOS} representa el consumo de energía por bit cuando las condiciones de propagación son de visión directa (LOS). e_{MP} representa el consumo de energía por bit cuando la señal llega al receptor a través de múltiples rutas (*MultiPath*, MP) para $d \geq d_{brake}$. Este modelo de energía considera que la potencia de transmisión (P_{LOS} y P_{MP}) empleada por el transmisor es la necesaria para garantizar que el nivel de señal en el receptor sea igual al umbral de potencia requerido (P_r) para que la comunicación pueda ser considerada exitosa. Por este motivo, P_{LOS} y P_{MP} pueden expresarse como se muestra a continuación [5]:

$$P_{LOS} = \frac{P_r \left(4\pi\right)^2}{\lambda^2} \quad ; \quad P_{MP} = \frac{P_r}{h_t^2 h_r^2} \quad (5)$$

y e_{LOS} y e_{MP} equivalen a P_{LOS}/R_{adhoc} and P_{MP}/R_{adhoc}, respectivamente.

La comunicación ad-hoc entre los terminales SN y MR se lleva a cabo utilizando la tecnología IEEE 802.11g a 2.4GHz (el estudio podría reproducirse para otras tecnologías de acceso radio). La tasa de transmisión de IEEE 802.11g puede modelarse como [7]:

$$R_{adhoc}\left(d\right) = DataRate(d) \cdot Eff \cdot \left(1 - PER\left(d\right)\right) \quad (6)$$

donde *DataRate* representa el modo de transmisión ad-hoc de IEEE 802.11g:

$$DataRate\left(d\right) = \begin{cases} 54 & d < 78.47m \\ \dfrac{54}{\dfrac{1}{78.47} - \dfrac{1}{270.85}} \cdot \left(\dfrac{1}{d} - \dfrac{1}{270.85}\right) & 78.47m \leq d < 270.85m \\ 0 & 270.85 \leq d \end{cases} \quad (7)$$

PER (*Packet Error Ratio*) es la tasa experimentada de paquetes IEEE 802.11g erróneos[1]:

$$PER\left(d\right) = \frac{0.75}{1 + e^{-0.019 \cdot \left(d - 115.15\right)}} \quad (8)$$

y *Eff* es la eficiencia del canal IEEE 802.11g que depende del tiempo de transmisión de los paquetes de datos (t_d) y paquetes ACK (t_{ack}), el periodo de contención (t_{cont}), y de los tiempos de guarda entre tramas (*DIFS* y *SIFS*) [7]:

$$Eff = \frac{t_d}{DIFS + t_{cont} + t_d + SIFS + t_{ack}} \quad (9)$$

2) Almacenamiento, transporte y reenvío (SCF). Como se sugiere en [6], este trabajo considera la energía consumida por el proceso de almacenamiento y transporte de la información. Los dispositivos móviles almacenan automáticamente los paquetes de datos recibidos por la interfaz inalámbrica en la unidad de almacenamiento principal del sistema DRAM. La información podría ser transferida a las unidades de almacenamiento internas tales como la memoria flash NAND si se considera apropiado, dado su menor consumo de energía (el tiempo que se almacena la información, y la velocidad de transferencia y el coste de energía son factores a evaluar). Sin embargo, la información debe ser transferida de nuevo a la memoria DRAM cuando el dispositivo inicia el proceso de reenvío. Este trabajo considera que la información siempre se transfiere de DRAM a NAND flash. En este contexto, P_R representa la potencia consumida por las unidades de almacenamiento DRAM y NAND flash durante la lectura (R) y escritura (W) de la información, así como la energía consumida por la transferencia de la información desde la DRAM a la memoria flash NAND (*Transf_DF*). P_{IDLE} incluye la energía consumida por la memoria flash NAND durante el almacenamiento de la información en estado inactivo o *idle*, y la potencia consumida por la DRAM que se encuentra en estado 'semi-activo' (*Idle_self-refresh*). Por último, P_W es la potencia consumida por las dos unidades de almacenamiento cuando transfieren la información de nuevo a la memoria DRAM para la transmisión.

3) Celular tx. Las pérdidas de propagación en la transmisión celular también se han modelado utilizando el

[1] Los modelos IEEE 802.11g *DataRate* y PER han sido obtenidos por los autores mediante una extensa campaña de medidas [8].

modelo de dos rayos descrito en *D2D tx*. El consumo de energía de la comunicación entre el MR y la BS se modela utilizando (4), pero sustituyendo R_{adhoc} por R_{cell}. Además, las alturas de las antenas y de longitud de onda se deben actualizar en (4). Este estudio considera HSPA a 2,1 GHz para la transmisión celular entre el MR y la BS (el estudio podría ser reproducido para otras tecnologías de acceso radio). Para el modelado de la tasa de transmisión de datos celular se ha supuesto que el sistema celular adapta su funcionamiento a las condiciones del canal radio utilizando modulación y codificación adaptativa (*Adaptive Modulation and Coding*, AMC) y mecanismos de retransmisión avanzados (*Automatic Repeat Request*, ARQ). De modo general, la tasa de transmisión de datos celular se puede modelar teniendo en cuenta anillos concéntricos [9] como:

$$R_{cell}(d) = k \cdot C \cdot log_2\left(M(d)\right) \cdot BW \quad (10)$$

donde *BW*, *M* y *C* representan el ancho de banda del sistema, el tamaño de la constelación de la modulación y la tasa de codificación, respectivamente. *M* y *C* se seleccionan de acuerdo a la distancia entre el dispositivo móvil y la BS (cuanto mayor sea la distancia, menor es la intensidad de la señal medida en el dispositivo móvil, y por lo tanto menor deberá ser el esquema de modulación/codificación). *k* representa un factor de atenuación que limita la tasa de transmisión de datos celular, e incluye, entre otros, el efecto de los fallos en la transmisión, retransmisiones e interferencias [9].

B. Investigación Numérica

La resolución numérica de la función objetivo que se muestra en (1) se ha realizado teniendo en cuenta los parámetros de configuración del escenario que se recogen en la Tabla I. El estudio considera una celda con un radio de 1000m. La celda está dividida en siete anillos equidistantes y concéntricos definidos por los esquemas AMC que se muestran en la Tabla I. La tasa de transmisión celular se considera que disminuye con el aumento de la distancia entre el MR y la BS. En el primer anillo (más cercano a la BS) posee una tasa de datos HSUPA máxima de 7Mbps en el enlace ascendente. Los valores de consumo de energía de las unidades de almacenamiento flash NAND y DRAM se han obtenido a partir de [10], y los valores de e_t, e_r y P_r de [5]. El mensaje que el nodo fuente estático tiene que transmitir a la BS tiene un tamaño nominal de 10 Mb, y el tiempo disponible para completar la transmisión se ha establecido en 40s. Ejemplo de este tipo de aplicación podría ser: actualizaciones en redes sociales, almacenamiento de ficheros en 'la nube' o envío de correos poco urgentes. En el escenario se considera que el MR está en línea con el nodo fuente, y avanza hacia la BS con una velocidad de 2m/s.

TABLA I.
PARÁMETROS DE CONFIGURACIÓN DEL ESCENARIO

Parámetro	Valor	Parámetro	Valor
F	10Mb	*T*	40s
R	1000m	*v*	2m/s
h_{SN}, h_{MR}, h_{BS}	1.5m, 1.5m, 10m	*Max UL Thr*	7Mbps
e_t, e_r	50 x 10^{-9}J/b	P_r	-52dBm
DRAM P_R, P_W, $P_{Idle\_self\text{-}refresh}$	252mW, 252mW, 1.35mW	*AMC*	BPSK (r=1/3) QPSK (r=1/3, 1/2, 2/3) 16QAM (r= 1/2, 2/3, 5/6)
NAND Eff_{Read}, Eff_{Write}, P_{Idle}	1.83nJ/b, 11.92nJ/b,	*Transf_DF*, *Transf_EF*	4.85 MiB/s, 927.1 KiB/s

La Fig. 2 muestra la localización óptima del MR en función de la distancia entre el SN y la BS. Dicha localización se ha representado como la distancia entre el SN y el MR. A modo de ejemplo, cuando el SN se encuentra a 400m de distancia de la BS, la función objetivo desarrollada en este trabajo determina que, con el fin de reducir al mínimo el consumo de energía, el MR debe estar idealmente situado a 120m de distancia del SN en la dirección de la BS. La Fig. 2 muestra que la distancia óptima desde el SN al MR que minimiza el consumo de energía aumenta con la distancia entre el SN y la BS. Esto es debido a que el incremento de la distancia entre el SN y el MR resulta en que el MR esté más cerca de la BS y por lo tanto se consigue disminuir el consumo energético de la transmisión celular. Por otro lado, la energía consumida en la transmisión D2D desde el SN al MR aumenta a medida que el MR está más cerca de la BS. En este contexto, la distancia óptima entre el SN y el MR sólo aumenta cuando el ahorro de energía del proceso de almacenar y transportar la información llevado a cabo por el MR compensa el aumento en el consumo de energía en la transmisión D2D. Los picos que se muestran en la Fig. 2 se corresponden con situaciones en las que el MR se desplaza hacia la BS y se aproxima a un anillo con una mayor tasa de transmisión celular; el uso de anillos con tasas de transmisión superiores reduce el consumo de energía.

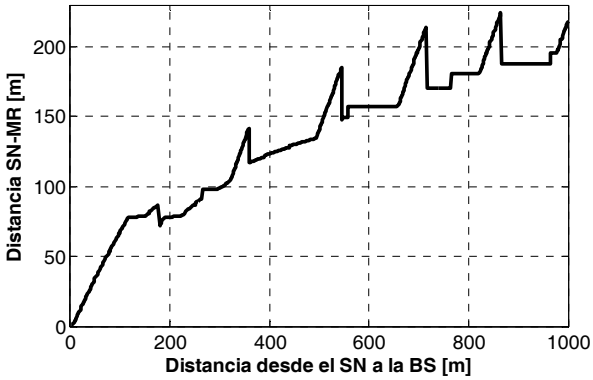


Fig. 2. *D2D tx*: localización óptima del MR.

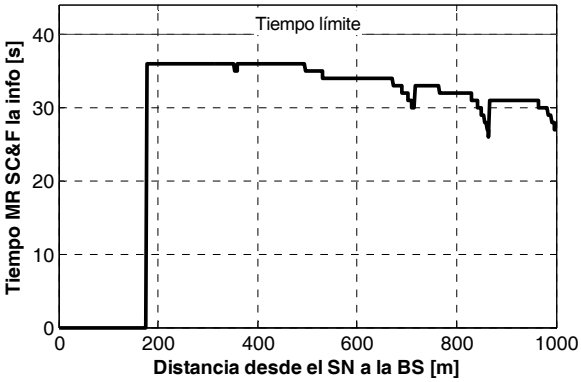


Fig. 3. *Store-carry & Forward (SC&F)*: tiempo que el MR almacena y transporta la información mientras se desplaza hacia la BS.

La Fig. 3 muestra el tiempo que el MR necesita almacenar y transportar (SC&F) la información en su desplazamiento hacia la BS desde la localización identificada en la Fig. 2. Siguiendo el ejemplo anterior, el MR óptimo situado a 125m de distancia del SN (cuando la distancia SN-

BS es de 400m) necesita almacenar y transportar la información durante 36s antes de enviar la información a la BS. Los resultados obtenidos indican que cuando el SN está cerca de la BS (en el anillo con mayor tasa de transmisión celular), el MR seleccionado no necesita almacenar y transportar la información. En este caso, el MR debe retransmitir la información a la BS tan pronto como la reciba del SN. Esto es debido a que la energía consumida en estos lugares por el proceso de almacenar y transportar la información no compensa el ahorro que podría conseguirse por transmitir más cerca de la BS. A medida que la distancia desde el SN a la BS se incrementa, el MR seleccionado debe almacenar y transportar la información para que se pueda llevar a cabo la comunicación celular con la BS desde un anillo con una tasa de transmisión superior a la que se encontraba inicialmente el MR. Cuando el SN se va acercando al borde de la celda, el tiempo que el MR debe almacenar y transportar la información disminuye debido al incremento en el tiempo necesario para completar la transmisión D2D (Fig. 2) y la transmisión celular (Fig. 4). La Fig. 4 muestra el tiempo que el MR seleccionado necesita para transmitir la información a la BS utilizando la interfaz radio celular ('2-saltos MCN (Opt localización MR)').

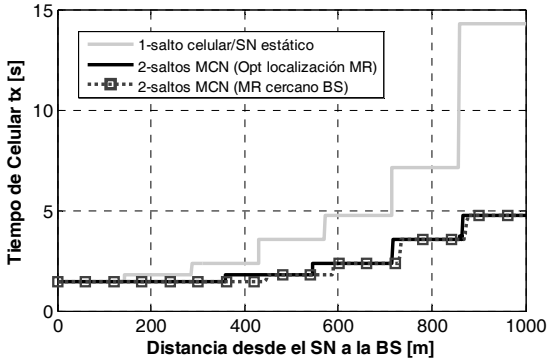


Fig. 4. *Celular tx*: tiempo que el MR necesita para transmitir la info a la BS.

Las configuraciones óptimas[2] ilustradas en las Figs. 2, 3 y 4 resultan en los niveles de consumo energético (en escala logarítmica) que se muestran en la Fig. 5 ('2-saltos MCN (Opt localización MR)'). La Fig. 5 también muestra los niveles de consumo energético medidos en el SN estático si éste comunicase directamente con la BS a través de la interfaz radio celular ('1-salto celular/ SN estático'). Los resultados obtenidos demuestran que la configuración óptima de la comunicación MCN-MR oportunista de 2 saltos resulta en significativos beneficios energéticos en comparación con las transmisiones directas celulares desde el SN a la BS. El ahorro energético aumenta con la distancia entre el SN y la BS: desde el 61% cuando el SN está a 200m de distancia de la BS al 80% cuando está situado al borde de la celda. La Fig. 5 deja patente también que cuando el SN está cerca de la BS no es energéticamente eficiente transmitir a través de un enlace MCN-MR de 2-saltos. Los resultados que se muestran en la Fig. 5 también consideran el caso en el que el SN es móvil y puede almacenar, transportar y transmitir la información a la BS sin utilizar un MR ('1-salto celular (Opt SCF)'). En este caso, la función objetivo presentada en este trabajo proporcionaría la ubicación óptima a la que el SN móvil debe comenzar la transmisión de la información a la BS. Los beneficios energéticos del proceso de almacenar y transportar la información en la comunicación de 1 salto se demuestran en la Fig. 5 si se comparan los resultados obtenidos con los de la comunicación directa desde el SN estático (en media la reducción del consumo energético es del 27%). Sin embargo, la comunicación MCN-MR oportunista de 2-saltos supera estos beneficios energéticos, excepto para distancias muy cortas entre el SN y la BS. Los resultados obtenidos demuestran claramente el potencial de las comunicaciones MCN-MR oportunistas de 2 saltos para reducir el consumo de energía en servicios/aplicaciones tolerantes a retrasos. Sin embargo, este potencial depende en gran medida de la correcta selección de la localización del MR y la localización desde la que el MR debe comenzar la transmisión de la información a la BS. Para demostrar esta dependencia, este trabajo ha evaluado también la energía consumida en el caso de una comunicación MCN-MR oportunista de 2 saltos en la que el MR seleccionado es aquel que se encuentra lo más cerca posible a la BS ('2-saltos MCN (MR cercano BS)'). Esta configuración minimiza el tiempo necesario para enviar la información a la BS (Fig. 4), pero a costa del incremento en los niveles de consumo energético total que se muestran en la Fig. 5.

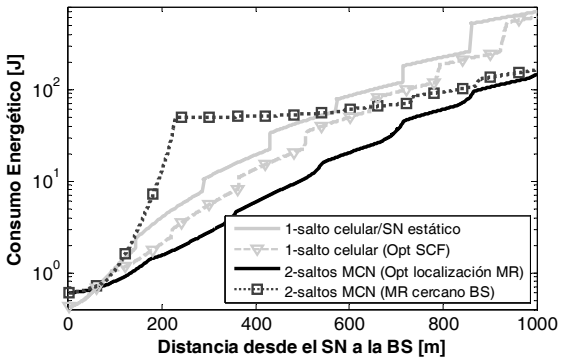


Fig. 5. Energía consumida total.

IV. Técnicas Contextuales para Seleccionar al MR

El estudio llevado a cabo en la sección anterior ha permitido obtener la configuración óptima de la comunicación MCN-MR oportunista de 2 saltos. En particular, el estudio ha permitido identificar la localización óptima del nodo móvil retransmisor MR y la localización a la que el MR debe iniciar la retransmisión de la información a la BS para minimizar el consumo energético global. Estas configuraciones óptimas han de considerarse como límites del rendimiento. Esto es así puesto que podría darse el caso de que en el momento de iniciar la comunicación el SN no fuese capaz de encontrar ningún MR en la localización óptima identificada. Por este motivo, estas localizaciones deberían considerarse como puntos de referencia desde los que buscar al nodo móvil retransmisor. En este contexto, esta sección presenta 2 técnicas oportunistas contextuales para la selección del nodo retransmisor. Estas técnicas se basan en las configuraciones óptimas obtenidas a partir del proceso de optimización presentado en la sección anterior, y además, hacen uso de información contextual proporcionada por la BS a través de sus mecanismos de señalización para identificar límites espacio-temporales en los que garantizar la presencia de un MR.

[2] La localización del MR y la localización en la cual el MR debe iniciar la transmisión de la información a la BS.

A. Incrementar área de comunicación D2D

La primera propuesta consiste en incrementar el área de búsqueda del MR alrededor de la localización óptima identificada. Un ejemplo de esta propuesta se muestra en la Fig. 6, en la que también se ha incluido la configuración óptima de la comunicación MCN-MR oportunista de 2 saltos. La configuración óptima indica que la comunicación D2D desde el nodo fuente SN_i ha de realizarse con un MR situado en X_i (esta comunicación se completaría en el instante temporal τ_{b-1}). El MR almacena y transporta la información hasta el instante temporal τ_{c-1} e inicia la transmisión celular con la BS cuando alcanza la localización Y_i. Puesto que SN_i podría no encontrar a ningún MR en X_i en el momento de iniciar la transmisión D2D, la estrategia que se propone consiste en seleccionar un nodo retransmisor MR que se encuentre en un punto cercano de la localización óptima. Para ello se define un radio de búsqueda alrededor de X_i de tal modo que garantiza con cierta probabilidad la presencia de un MR. El hecho de seleccionar al MR en una localización distinta a la óptima daría lugar a una modificación en el resto de la configuración de la comunicación. Por ejemplo, en la Fig. 6, el MR seleccionado está situado en X'_i (más alejado de SN_i que X_i). El MR seleccionado inicia la transmisión celular con la BS a una menor distancia de la BS (localización Y'_i) si se compara con la configuración óptima debido al mayor avance logrado en la comunicación D2D.

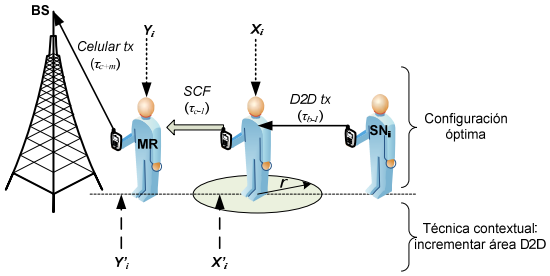


Fig. 6. Técnica contextual para selección de MR: incrementar área D2D.

El principal objetivo en el funcionamiento de esta técnica reside en la determinación del área en la que buscar al MR (o lo que es equivalente, el radio r desde la localización óptima). Este área debe garantizar con probabilidad δ la presencia de al menos un MR. El cálculo de r depende de la densidad y de la distribución de los MR en la celda. Este trabajo ha considerado que los nodos están distribuidos según una distribución homogénea de Poisson. En general, la distribución de Poisson puede expresarse como:

$$P\left(x;\lambda\cdot d\right)=\frac{\left(\lambda\cdot d\right)^{x}\cdot\exp\left(-\lambda\cdot d\right)}{x!},\quad x=0,1,2,... \tag{11}$$

donde x representa el número de 'éxitos' y λ el número medio de 'éxitos' por unidad de tiempo/distancia/área/etc. d representa la magnitud de interés. Para el escenario bajo estudio en este trabajo, y considerando que en media hay μ MRs en la celda de radio R, el número medio de MRs por unidad de distancia puede calcularse como $\lambda=\mu/R$. Por lo tanto, la probabilidad de encontrar al menos un MR alrededor de la localización óptima X_i, denotado por P_{Xi}, equivale a 1 menos la probabilidad de no encontrar a ningún MR (i.e. x=0):

$$P_{X_i}=P\left(x>0;\frac{\mu}{R}\cdot d\right)=1-P\left(x=0;\frac{\mu}{R}\cdot d\right)=$$
$$1-\frac{\left(\frac{\mu}{R}\cdot d\right)^{0}\cdot\exp\left(-\frac{\mu}{R}d\right)}{0!}=1-\exp\left(-\frac{\mu}{R}d\right),\ \forall X_i\in(1,...,R) \tag{12}$$

Es importante resaltar que la expresión obtenida en (12) es válida para cualquier localización de X_i dentro de la celda. Para identificar el radio alrededor de X_i, la expresión (12) puede modificarse usando el límite de la probabilidad en la que se quiere garantizar la presencia del MR (i.e. δ) del siguiente modo:

$$P_{X_i}=1-\exp\left(-\frac{\mu}{R}d\right)\geq\delta;\qquad r\geq\frac{R\cdot\ln\left(1-\delta\right)}{-2\cdot\mu} \tag{13}$$

donde se ha utilizado que $d=2r$.

Como se puede apreciar en (13), el radio r del área donde garantizar la presencia del MR es proporcional al radio de la celda R e inversamente proporcional al número medio de MRs en la celda μ. Además, r incrementa a medida que lo hace la probabilidad de garantizar la presencia de un MR (δ).

Una vez obtenido r y basándonos en la formulación matemática presentada en la Sección III.A es posible obtener la configuración que resulta de la comunicación MCN-MR oportunista de 2 saltos si el MR es seleccionado dentro del área de búsqueda. En este caso, la localización del MR (i.e. X'_i) está limitada dentro del área definida alrededor de la localización óptima (X_i) y radio r; la cual se expresa como $X'_i \in o(Xi, r)$. De este modo, la configuración que minimiza el problema formulado en la Sección III.A (ϑ) [3] puede calcularse como:

$$\left[\tau'_{b-1},\tau'_{c-1},\tau'_{c+m},X'_i,Y'_i\right]=$$
$$\underset{X'_i\in o(X_i,r)}{\arg\min}\left(\vartheta(F,T,R_{adhoc},R_{cell},E_{adhoc},E_{cell},P_R,P_W,P_{IDLE})\right) \tag{14}$$

Es importante notar que la resolución de (14) proporciona la solución óptima puesto que la nueva restricción $X'_i \in o(Xi, r)$ la incluye. En este contexto, el objetivo de este estudio es conocer el peor rendimiento (concepto de '*maximin*') de entre todas las posibles localizaciones del MR dentro de $o(Xi, r)$ (i.e. $\forall X'_i \in o(Xi, r)$). Esto puede expresarse como:

$$\left[\tau'_{b-1},\tau'_{c-1},\tau'_{c+m},X'_i,Y'_i\right]=\arg\max\left(\vartheta\left(\underset{\forall X'_i\in o(X_i,r)}{\arg\min}\ \vartheta(...)\right)\right) \tag{15}$$

B. Retrasar la transmisión D2D

La segunda propuesta consiste en retrasar la transmisión D2D el tiempo necesario que garantice que un MR pasa sobre la localización óptima identificada. La Fig. 7 ilustra un ejemplo de esta segunda propuesta junto con la configuración óptima de la comunicación MCN-MR oportunista de 2 saltos. La transmisión D2D se lleva a cabo con un MR situado en la localización óptima X_i. Sin embargo, para garantizar la presencia del MR en X_i la transmisión D2D se ha retrasado t unidades de tiempo y por este motivo la *D2D tx* se completa en $\tau_{b-1}+t$. La Fig. 7 también muestra como el tiempo añadido a la transmisión D2D resulta en una modificación en la localización en la que el MR inicia la transmisión celular si se compara con la configuración óptima. Por este motivo, Y'_i se ha situado más alejado de la BS.

[3] ϑ representa la función objetivo definida en (1) junto con las restricciones (2) y (3) que como se mostró dependen de los parámetros F, T, R_{adhoc}, *etc*.

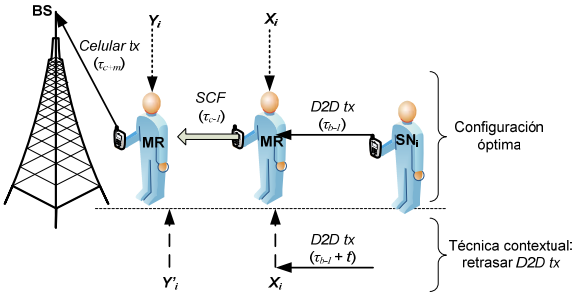


Fig. 7. Técnica contextual para selección de MR: retrasar *D2D tx*.

En esta segunda técnica, el objetivo clave es por lo tanto determinar el tiempo t que ha de retrasarse la transmisión D2D para garantizar con cierta probabilidad δ que al menos un MR alcanza la localización óptima identificada. El cálculo de t depende de la densidad de nodos en el escenario y de su distribución, y como se ha indicado en la sección anterior este trabajo considera que los nodos están distribuidos siguiendo una distribución homogénea de Poisson. La distribución de Poisson se definió en (11) – en este caso la magnitud de interés se ha definido como t. La tasa media de llegada de MRs al escenario puede calcularse como $\mu' = \mu v/R$, siendo μ el número medio de MR en la celda, v la velocidad de desplazamiento de los MRs y R el radio de la celda. Realizando un desarrollo similar al llevado a cabo para el cálculo de r en la técnica anterior, es posible calcular la probabilidad de que al menos un MR alcance la localización X_i antes de que transcurra el tiempo t como:

$$P_{X_i} = P(x>0;\mu' t) = 1 - P(x=0;\mu' t) = 1 - \frac{(\mu' t)^0 \cdot \exp(-\mu' t)}{0!} = 1 - \exp(-\mu' t),\ \forall X_i \in (1,\ldots,R) \quad (16)$$

Utilizando la expresión (16), el tiempo t que garantiza con probabilidad δ la presencia de un MR en la localización óptima X_i puede calcularse como:

$$P_{X_i} = 1 - \exp(-\mu' \cdot t) \geq \delta; \qquad t \geq \frac{R \cdot \ln(1-\delta)}{-\mu \cdot v} \quad (17)$$

Como se muestra en (17), el retraso en la transmisión D2D es independiente de la localización óptima del MR dentro de la celda. También se puede apreciar como t es directamente proporcional a R e inversamente proporcional al número medio de MRs en la celda y a la velocidad v de los MRs. Además, t se incrementa a medida que lo hace el parámetro δ.

La configuración óptima que resulta de la comunicación MCN-MR oportunista de 2 saltos en la que el MR se selecciona transcurridos t instantes de tiempo en la localización óptima puede calcularse como:

$$[\tau_{b-1} + t, \tau'_{c-1}, \tau'_{c+m}, X_i, Y'_i] = \underset{\tau'_{b-1}=\tau_b+t}{\arg\min} \left(\vartheta(F, T, R_{adhoc}, R_{cell}, E_{adhoc}, E_{cell}, P_R, P_W, P_{IDLE})\right) \quad (18)$$

donde al problema original ϑ se ha añadido la restricción del retardo t en la transmisión D2D inicial ($\tau'_{b-1} = \tau_{b-1} + t$). Esto podría resultar en una modificación del tiempo que el MR almacena y transporta la información (τ'_{c-1}), y el tiempo necesario para la transmisión celular o lugar en el que se inicia la transmisión celular con la BS (τ'_{c+m} ó Y'_i). La transmisión D2D se lleva a cabo con el MR situado en X_i.

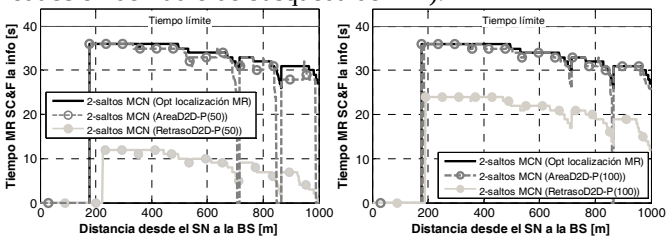
C. Evaluación numérica

El estudio de las técnicas contextuales para la selección del MR de la comunicación MCN-MR oportunista de 2 saltos propuestas se ha llevado a cabo en el mismo escenario en el que se evaluó la configuración óptima, y cuyos parámetros se resumen en la Tabla I. Además, se ha considerado que los MRs están distribuidos dentro del escenario según una distribución homogénea de Poisson con 50 y 100 MRs de media dentro de la celda. Por último, se ha fijado el valor de δ igual a 0.9.

Para este escenario, y para las distintas densidades de nodos, es posible calcular el radio alrededor de la localización óptima y el tiempo que ha de retrasarse la transmisión D2D para garantizar la presencia de un MR en la localización óptima a partir de las expresiones (13) y (17), respectivamente. El resultado es que cuando la densidad de MR distribuidos homogéneamente es igual a 50, el radio de búsqueda ha de incrementarse 24m. Cuando la densidad de MRs es de 100, el radio de búsqueda se reduce a 12m. Los resultados obtenidos a partir del proceso de optimización (15) demuestran que el peor rendimiento de la técnica se obtiene cuando el MR se encuentra en el límite del radio de búsqueda. Por lo tanto, el rendimiento de esta técnica mejoraría a medida que se seleccione al MR lo más próximo posible de la localización óptima. Para los parámetros utilizados en el escenario, el tiempo límite (17) que el nodo SN ha de esperar para que un MR alcance la localización óptima es de 12s y 24s cuando la densidad de nodos en el escenario es de 100 y 50 MR respectivamente.

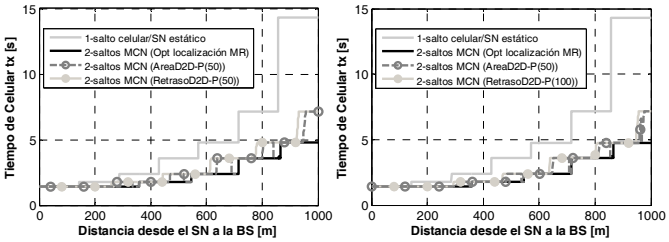
Como resultado del cambio de localización del MR en la técnica que incrementa el área de comunicación D2D o del retraso añadido a la comunicación D2D, el MR seleccionado tiene que ajustar los restantes mecanismos de comunicación y de red si se compara con la configuración óptima obtenida en la Sección III. La Fig. 8 muestra el tiempo que el MR seleccionado tiene que almacenar y transportar la información hacia la BS. Al igual que ocurría con la configuración óptima, el MR seleccionado con las técnicas contextuales no tiene que almacenar y transportar la información cuando el nodo fuente SN se encuentra próximo a la BS. En la figura también se muestra como la técnica que retrasa la transmisión D2D ha reducido considerablemente el tiempo que el MR tiene que almacenar y transportar la información hacia la BS debido al tiempo empleado en esperar a que el MR alcance la localización óptima. Por ejemplo, para el escenario en el que la densidad media de nodos es de 50 (‘2-saltos MCN (RetrasoD2D-P(50))’), el MR seleccionado por el SN situado a 400m tiene que almacenar y trasportar la información durante 12s comparado con los 36s en la configuración óptima (‘2-saltos MCN (Opt localización MR)’). Este hecho resulta en que el MR inicia la comunicación con la BS más alejado y por lo tanto la transmisión celular requiere mayor tiempo, tal y como se muestra en la Fig. 9.a. Cuando la densidad de MRs es de 100, el tiempo que el MR seleccionado almacena y transporta la información se incrementa a 24s (por el menor tiempo que hay que esperar a que el MR alcance la localización óptima) y por lo tanto se reduce *Celular tx* (Fig. 9.b). Por otro lado, en la técnica que basa su modo de operación en incrementar el área de comunicación D2D no se aprecian diferencias significativas en el tiempo que el MR almacena y transporta la información en comparación con la

configuración óptima. Esto es debido a que en este caso la transmisión D2D no se retrasa y las pequeñas diferencias de tiempo se deben a la variación de la localización del MR con respecto a la localización óptima (si se comparan las Fig. 8.a y 8.b se puede apreciar como las diferencias se reducen al incrementar la densidad de MRs en el escenario por la reducción del radio de búsqueda de MR).



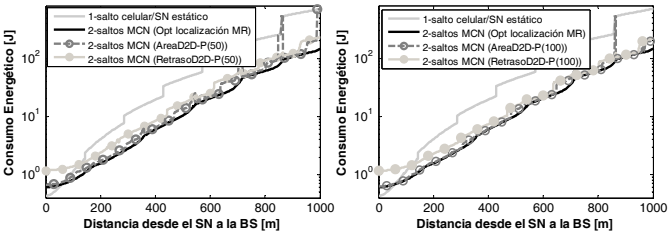
a) Densidad de MRs 50 b) Densidad de MRs 100

Fig. 8. SCF: tiempo que el MR almacena y transporta la información cuando los nodos están distribuidos según Poisson.



a) Densidad de MRs 50 b) Densidad de MRs 100

Fig. 9. Tx celular: tiempo que el MR necesita para transmitir la información a la BS cuando los nodos están distribuidos según Poisson.



a) Densidad de MRs 50 b) Densidad de MRs 100

Fig. 10. Engería consumida total. Nodos distribuidos según Poisson.

Las configuraciones resultantes de las técnicas contextuales para la selección del MR que se muestran en las Figs. 8 y 9 resultan en los niveles de consumo energético total que se muestran en la Fig. 10. La Fig.10 también muestra el consumo energético de la configuración óptima ('2-saltos MCN (Opt localización MR)') que como se puede apreciar sigue siendo la comunicación MCN-MR oportunista de 2-satos que minimiza el consumo energético. La técnica contextual que incrementa el área de comunicación D2D mejora el rendimiento de la técnica que retrasa la comunicación D2D cuando el nodo SN está cerca de la BS. Esto es debido a que es energéticamente ineficiente retrasar la comunicación con la BS cuando el SN está cerca de la BS, tal y como se demostró en la Sección III. Sin embargo, a medida que el SN se aleja de la BS las diferencias entre las dos técnicas se reducen. Como se puede apreciar, el rendimiento de ambas técnicas está próximo al logrado con la configuración óptima, reduciendo considerablemente el consumo energético medido si la transmisión se realiza directamente desde el SN estático a la BS. Por ejemplo, para una densidad de MRs igual a 100, el ahorro energético es en media del 60% y del 45% para las técnicas oportunistas que incrementan el área D2D y retrasan la transmisión D2D respectivamente.

V. Conclusiones

Este trabajo ha investigado el potencial de la integración de técnicas oportunistas en redes MCN-MR para mejorar la eficiencia energética de las comunicaciones celulares en tráfico tolerante a retardos. El estudio se ha centrado en un escenario MCN-MR de 2 saltos y ha formulado analíticamente el problema del consumo energético, lo cual ha permitido identificar la localización óptima del MR, y la localización a la que el MR necesita iniciar el reenvío de la información a la red celular. Los resultados obtenidos muestran que pueden conseguirse importantes beneficios energéticos (hasta un 85%) comparado con la transmisión celular tradicional. Este estudio también ha dado lugar a la propuesta de dos técnicas para la selección del MR, las cuales explotan además información contextual proporcionada por la BS celular. Las dos propuestas han demostrado un rendimiento esperanzador considerando el límite inferior de su rendimiento, llegando a reducir los niveles de consumo energético considerablemente con respecto a la transmisión celular tradicional.

Como trabajo futuro, los autores pretenden ampliar el estudio de las técnicas contextuales para seleccionar al MR a distribuciones de nodos no homogéneas y en escenarios bidimensionales. Es también un objetivo de los autores identificar en qué condiciones convendría emplear cada una de las técnicas contextuales de selección del MR.

Agradecimientos

Este trabajo ha sido financiado en parte por el Ministerio de Economía y Competitividad y los fondos FEDER (TEC2011-26109), y la Generalitat Valenciana (ACIF/2010/161 y BEFPI/2012/065).

Referencias

[1] L. Long and E. Hossain, "Multihop Cellular Networks: Potential Gains, Research Challenges, and a Resource Allocation Framework", *IEEE Commun. Mag., vol. 45, no. 9, pp. 66-73*, Sept. 2007.

[2] J. Gozalvez and B. Coll-Perales, "Experimental Evaluation of Multi-hop Cellular Networks using Mobile Relays", *IEEE Commun. Mag., vol. 51, no. 7, pp.122-129,* Jul. 2013.

[3] L. Pelusi, A. Passarella and M. Conti, "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad-hoc Networks", *IEEE Commun. Mag., vol. 44, pp. 134-141*, Nov. 2006.

[4] A. Radwan and H.S. Hassanein, "Does Multi-hop Communication Extend the Battery Life of Mobile Terminals?", *Proc. IEEE GLOBECOM, pp. 1-5,* San Francisco, Nov. 2006.

[5] P. Kolios, V. Friderikos and K. Papadaki, "Future Wireless Mobile Networks", *IEEE Veh. Technol. Mag., vol. 6, no. 1, pp. 24-30*, Mar. 2011.

[6] B. Zhao and V. Friderikos, "Optimal Stopping for Energy Efficiency with Delay Constraints in Cognitive Radio Networks", *Proc. IEEE PIMRC, pp. 820-825*, Sydney, Australia, Sept. 2012.

[7] A. Duda, "Understanding the Performance of 802.11 Networks", *Proc. IEEE PIMRC, pp. 1-6*, Cannes, France, Sept. 2008.

[8] B. Coll-Perales, J. Gozalvez and J. Sánchez-Soriano, "Empirical Performance Models for P2P and two hops Multi-Hop Cellular Networks with Mobile Relays", *Proc. ACM PM2HW2N*, Nov. 2013.

[9] R. Schoenen and B.H. Walke, "On PHY and MAC Performance of 3G-LTE in a Multi-Hop Cellular Environment", *Proc. IEEE WiCom, pp. 926-929*, Shangai, China, Sept. 2007.

[10] M. Greenberg, "How Much Power Will a Low-Power SDRAM Save you?", White Paper Denali Software, 2009.

Red de sensores *pervasiva* para el bienestar basada en RaspberryPi

Rubén Vilches, Toni Oller, Marc Bajet, Jesús Alcober.
Departamento de Ingeniería Telemática en colaboración con Alteraid, S.L,
Universitat Politècnica de Catalunya – Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels
Dirección Calle Esteve Terradas, 7, 08860 Castelldefels, Barcelona.
ruben.vilches@estudiant.upc.edu, antoni.oller@upc.edu, marc.bajet@aaaida.com, jesus.alcober@upc.edu.

***Resumen*- Las redes de sensores "pervasivas" permiten convivir con los usuarios ofreciendo servicios de manera transparente y sin la necesidad que los usuarios interactúen de manera directa. Este trabajo define una arquitectura que permite la creación de productos y servicios para ofrecer funcionalidades domóticas a un gran sector de la población. Se ha diseñado una plataforma, sobre un dispositivo de bajo coste y alta capacidad de computación, como base de una red de sensores transparente e indistinguible. La plataforma dispone de métodos de configuración muy simples y es capaz de albergar múltiples servicios; desde automatización de persianas, control de la iluminación, seguridad; hasta mecanismos para la monitorización de la salud de un paciente.**

La primera aplicación desarrollada es un servicio de recordatorio y aviso de medicación totalmente transparente al usuario. Este servicio reproducirá, en el momento configurado, un recordatorio a través de los altavoces. El usuario, simplemente realizando la acción (tomarse la píldora) finalizará el evento, gracias a la información transmitida por un dispositivo situado en el cajón de los medicamentos. Por otro lado, si se olvidara, se le iría recordando cada cierto tiempo.

***Palabras Clave*- RaspberryPi, domótica, sensores, Z-Wave**

I. INTRODUCCIÓN

El trabajo que se propone ha creado un entorno de computación y comunicación integrado e imperceptible a las personas. Para ello, se han introducido dispositivos en la vida cotidiana, para que se mezclen de manera transparente (indistinguible). De esta manera, las personas se centrarán en realizar las tareas que deben hacer y no en las herramientas que utilizan, ya que pasan desapercibidas y no interfieren en las actividades planificadas.

El punto de partida es un equipamiento de bajo coste y alta capacidad de computación que nos permite desplegar aplicaciones y servicios para mejorar el bienestar de las personas, en especial, las de edad avanzada. El equipamiento debe poderse utilizar en los hogares mediante una simple configuración que minimice la intervención humana. Se propone desarrollar una aplicación (móvil) que analice el entorno (por ejemplo conectividad) y dé soporte para configurar este equipamiento.

Al mismo tiempo, se ha integrado en el equipo una plataforma para interactuar con elementos domóticos del hogar, si los hubiera. Por ejemplo: luces, ventanas, puertas, el cajón de las medicinas, etcétera. La plataforma está preparada para añadir módulos que proporcionen nuevos servicios como: automatización de persianas, mecanismos de riego, seguridad, control de iluminación o energía, entre muchos otros. O bien interfaces para facilitar la comunicación hombre-máquina, mediante control por voz o detección de presencia.

Además, se ha implementado un primer servicio. Éste sirve para recordar la toma de los medicamentos mediante la configuración de alarmas. Cuando una alarma se dispara, se reproduce por los altavoces el texto introducido en la configuración, que podría ser el nombre del medicamento o una descripción más amena. El usuario escucha el mensaje y cuando interactúa con el cajón de las medicinas, el sistema reconoce la acción y finaliza la tarea. En caso de haberse olvidado tomar la pastilla, se irán reproduciendo mensajes cada cierto tiempo a modo de recordatorio.

En el próximo apartado se analiza el entorno actual donde se define el marco social y tecnológico en el que se va a trabajar. En el apartado III se plantea el problema y la solución escogida para solventarlo. El apartado IV detalla la estructura diseñada para el cumplimiento de los objetivos propuestos; se pretende ofrecer una solución de lo más sencilla y cómoda para el usuario. Más adelante se analizan los Costes y finalmente se presentan las CONCLUSIONES obtenidas.

II. ENTORNO ACTUAL

A continuación se explicará la situación social y tecnológica actual, es importante tenerlo presente, ya que la evolución en ambos campos es muy acelerada.

En primer lugar, se hablará de la sociedad tecnológica y de cómo se está redistribuyendo la pirámide generacional. Se continuará con el estado del arte, donde se detallarán las tecnologías disponibles en este momento y sus capacidades.

A. Situación social

Actualmente la tecnología es la protagonista en todos los aspectos y niveles de la sociedad. Internet, la red de redes, está presente en todos los hogares y éstos a su vez disponen de redes privadas ya sea para que múltiples dispositivos accedan a Internet o para poder tener servicios propios, como centros multimedia.

Además, los avances en procesado han permitido que todo el mundo tenga a su alcance ordenadores más potentes, pero lo más interesante es que ha reducido el tamaño y abaratado el coste de productos más simples.

Por otro lado, la sociedad se está adaptando rápidamente a nuevos entornos tecnológicos, promueve su desarrollo e incorpora las nuevas funcionalidades a su vida cotidiana. Actualmente la tecnología llega a todas las edades, desde

juegos infantiles a mejoras en la calidad de vida de gente mayor.

Desde siempre, la sociedad se estructura en forma piramidal; en la base se sitúa la gente joven y en la cima la gente mayor, pero esta distribución se está invirtiendo (como prevé el Instituto Nacional de Estadística [1]). Los avances en el bienestar y la disminución de la natalidad conducen a un envejecimiento general de la sociedad.

Los siguientes gráficos presentan la relación de la población (hombres y mujeres) de España y su edad. La Fig. 1 es un estudio realizado en 1970 donde se puede apreciar perfectamente la estructura piramidal. A medida que avanzamos en el tiempo esta estructura se deforma, como podemos apreciar en la Fig. 2, estudio del 2010; las estimaciones para los próximos años indican que la estructura piramidal se irá invirtiendo, Fig. 3.

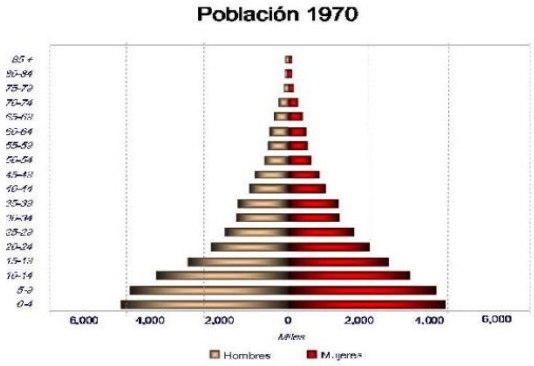


Fig. 1. Población española en 1970.

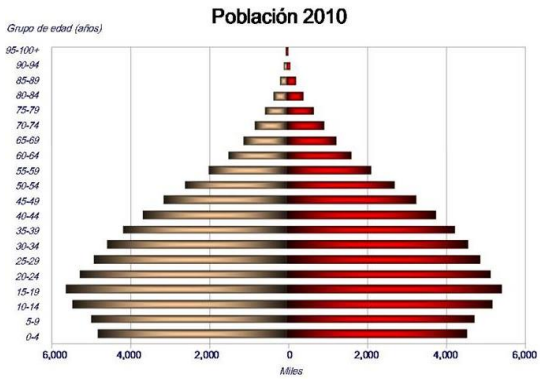


Fig. 2. Población española en 2010.

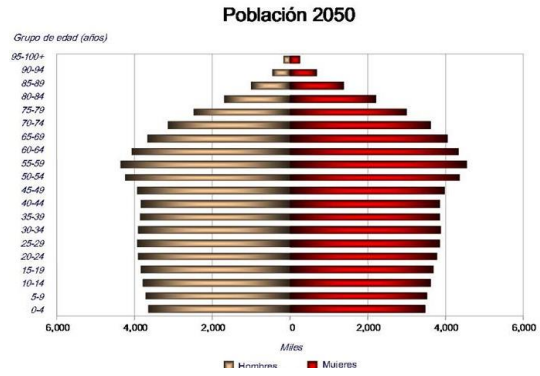


Fig. 3. Previsión de la población española para el 2050.

Esta situación no pasa desapercibida por el sector comercial, el cual ha redistribuido sus esfuerzos para desarrollar productos del interés de este nuevo gran consumidor. Especialmente en el campo de la salud, uno de los temas que más preocupa y necesita este sector de la población. El hecho de no disponer suficiente gente joven para solventar estas necesidades otorga a la tecnología la oportunidad de suplantar dichas funciones.

Otro gran protagonista en la sociedad de consumo actual es la eficiencia, en especial la energética. Cualquier optimización de recursos es bien recibida. En esta línea se encuentra la domótica, que proporciona a nivel del hogar una mejora de recursos, sumada a un conjunto de nuevos servicios y comodidades. Un ejemplo sencillo es la automatización de luces y persianas; en primer lugar, evita al usuario dicha tarea y, en segundo lugar, permite el ahorro en energía, dado que los sensores realizarán un ajuste perfecto entre la luz artificial y solar, permitiendo disminuir el consumo energético y el coste económico de la factura de la luz.

B. Estado del arte

Es de interés conocer las actuales tecnologías entre las que podemos escoger para crear un centro de domótica en el hogar.

Como se ha mencionado anteriormente, en la actualidad, se dispone de productos de reducido tamaño y bajo coste con potencia suficiente para el desempeño de tareas específicas. Algunos ejemplos son la RaspberryPi [2], Arduino, PICAXE o BASIC Stamp. Los dos primeros se han vuelto muy populares, están basados en una placa con un microcontrolador y un entorno de desarrollo de software y hardware libre. Esto permite que esté al alcance de cualquier interesado y pueda generar sinergias con los esfuerzos realizados por otros desarrolladores.

En concreto se ha seleccionado la RaspberryPi especialmente por su bajo coste, inferior a los 40$. En la Tabla I se encuentran las especificaciones técnicas.

Se dispone de aplicaciones como OpenRemote [3] o DomotiGa [4] para ofrecer los servicios necesarios en una red domótica para un hogar. Se ha escogido DomotiGa dada su mayor potencia y compatibilidad con múltiples tecnologías de sensores.

DomotiGa es un proyecto de software libre que está creciendo día a día. Tiene una estructura modular, de modo que se adapta muy bien a las necesidades de los usuarios. Algunos ejemplos de dichos módulos son: convergencia de dispositivos, gestor de eventos, comunicación con redes sociales, control climático, control de seguridad, mostrar los sensores y su información sobre el mapa de la casa, múltiples conectores de las actuales tecnologías de sensores, etc.

Por otro lado su gran inconveniente es la complejidad, este software está enfocado a personas expertas.

Por último, hay un mercado muy amplio de sensores, dispositivos capaces de traducir alguna magnitud física en digital y transmitir los resultados; así como actuadores que permiten, a partir de una orden lógica, ejecutar alguna acción física. Se han creado múltiples soluciones para la transmisión de información entre sensores, éstas pueden basarse en tecnologías como X10, Bluetooth, ZigBee, Ethernet, Wifi, Z-wave, entre muchos otros. Se diferencian dos grandes grupos: los que utilizan transmisiones radio y los que no. El primer caso proporciona gran movilidad a cambio de un canal con

mayores interferencias y menores velocidades. El segundo, lo contrario.

Tabla I
ESPECIFICACIONES DE RASPBERRYPI

	Modelo A	Modelo B
Precio	25$	35$
SoC	Broadcom BCM2835 (CPU + GPU + DSP + SDRAM + puerto USB)	
CPU	ARM1176JZF-S a 700 MHz (familia ARM11)	
GPU	Broadcom VideoCore IV, OpenGL ES 2.0, -2 y VC-1 (con licencia), 1080p30 H.264/MPEG-4 AVC	
Memoria (SDRAM)	256 MB (compartidos con la GPU)	512 MB (compartidos con la GPU) desde el 15 de octubre de 2012
Puertos USB 2.0	1	2 (vía hub USB integrado)
Entradas de video	Conector [MIPI] CSI	
Salidas de vídeo	Conector RCA (PAL y NTSC), HDMI (rev1.3 y 1.4), Interfaz DSI para panel LCD	
Salidas de audio	Conector de 3.5 mm, HDMI	
Almacenamiento integrado	SD / MMC / ranura para SDIO	
Conectividad de red	Ninguna	10/100 Ethernet (RJ-45) via hub USB
Consumo energético	500 mA, (2.5 W)	700 mA, (3.5 W)
Fuente de alimentación	5 V vía Micro USB o GPIO header	
Dimensiones	85.60mm × 53.98mm	
Sistemas operativos soportados	Debian, Fedora, Arch Linux,Slackware Linux, RISC OS	

Los sensores radio se ajustan más a las características deseadas y, de entre ellos, se ha elegido la tecnología Z-wave ya que, actualmente, es la que ofrece un amplio mercado al mejor precio. Los sensores crearán redes ubicuas o *pervasivas* [5][6] con el objetivo de formar parte del entorno del usuario.

III. PROBLEMA Y SOLUCIÓN

El futuro de la sociedad es una población de edad avanzada que necesita atenciones y cuidados especiales.

El problema que se va a abordar es crear una plataforma que incluirá aplicaciones relacionadas con sensores en el hogar; con el fin de mejorar el confort de los usuarios. Dicha plataforma incluirá una funcionalidad de recordatorio de medicamentos para ayudar a recordar a las personas mayores tomarse sus medicinas. Así se mejorará su calidad de vida ya que en primer lugar se elimina la tarea de recordar cuando y qué medicamento tomar, en segundo lugar, se mejorará la eficiencia de los tratamientos y en tercer lugar se podrá llegar a evitar problemas de salud que impliquen desplazamientos al hospital por culpa de haberse olvidado de tomar cierta pastilla.

La solución ofrecida consta de una serie de alarmas configurables para enviar emails o reproducir por los altavoces cualquier texto deseado. A partir de ahí el usuario recibe dicho mensaje y coge el medicamento de su cajón de medicinas, el cual está provisto de un sensor. Este sensor informará de su actividad se enviará al sistema para que sepa que se ha llevado a cabo la acción; si no se recibe dicha confirmación se irían reproduciendo mensajes de recordatorio.

A. *Objetivos*

1. Crear una plataforma modular. Admitiendo futuras ampliaciones y diferentes arquitecturas, como arquitectura basada en procesado en la nube.
2. Ofrecer un mecanismo para la configuración del producto en el hogar. Mediante una aplicación móvil o navegador web, permitir a los usuarios no técnicos, configurar de manera muy sencilla la conectividad del equipamiento.
3. Implementar un servicio para la administración del dispositivo.
4. Implementar un servicio para la creación de eventos.
5. Desarrollar un entorno visual muy simple e intuitivo para usuarios inexpertos.
6. Crear una aplicación para el recordatorio de medicamentos. Facilitar la interacción hombre-máquina, mediante mensajes reproducidos por los altavoces y recopilación de información a partir de sensores. La aplicación disparará una alarma y activará un servicio para recordar al usuario, múltiples veces, tomarse la medicación en caso de que se le haya olvidado.

IV. ARQUITECTURA

En este apartado se explicará la estructura configurada para llevar a cabo los objetivos planteados. Se han definido dos versiones:

La primera, se basa en situar toda la inteligencia sobre la RaspberryPi que actuará como controlador, la piedra angular del escenario. En los siguientes apartados se describirán los elementos del escenario y sus conexiones en todos los niveles.La segunda versión se detallará en el último punto, en ella se plantea una estructura basada en la nube, cloud computing [7]. Se separará la parte web de la RaspberryPi para situarla en un servidor exterior más potente.

A. *Estructura global*

A continuación se detalla la estructura planteada.

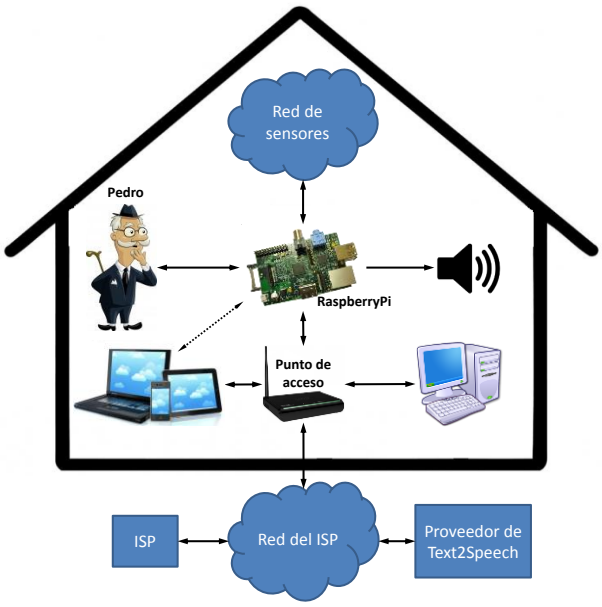


Fig. 4. Escenario global.

En el centro del esquema encontramos el núcleo, la inteligencia, que funciona sobre la RaspberryPi. Ésta se conecta a un altavoz y a una red de sensores, que puede contener distintas tecnologías ya que el software que se utiliza, DomotiGa, lo soporta.

En el escenario es necesario que exista un punto de acceso a Internet, de modo que necesitamos un ISP (Internet service provider = proveedor de conexión a Internet) que nos proporcione dicha conectividad. El punto de acceso permitirá a su vez que distintos dispositivos accedan a la RaspberryPi a través de la red privada.

La conexión a Internet es indispensable para poder disfrutar de las funcionalidades de envíos de correos electrónicos o de text2speech (traducción de texto a voz). Como proveedor de esta última función se ha escogido el servicio de Google por su calidad y disponibilidad.

B. *Configuración inicial*

El mecanismo ideado para simplificar a los usuarios la configuración y uso de la plataforma, se basa en la utilización de una aplicación que analizará el entorno (rastreando e identificando puntos de acceso) y realizará la configuración de la conexión de la plataforma, minimizando la intervención humana. Para que ello sea posible se deben seguir los siguientes pasos.

En primer lugar, una vez llega el producto al hogar, se debe configurar la conexión inalámbrica (Wifi) del dispositivo para que se conecte al punto de acceso. Para ello se debe poner la RaspberryPi en modo configuración para que permita realizar una conexión directa entre esta y un dispositivo móvil o PC mediante wifi.

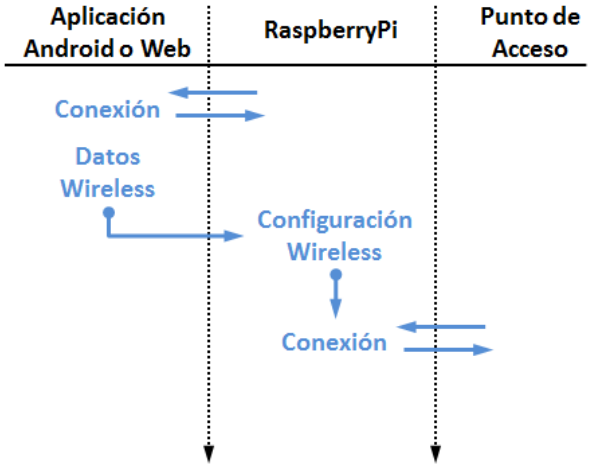


Fig. 5. Diagrama temporal. Comunicación inicial.

Una vez configurado el dispositivo, la conexión directa desaparece y a partir de entonces se puede acceder a la RaspberryPi a través del punto de acceso de la red privada del hogar.

Fig. 6. Cambio de escenario de modo configuración a estándar.

C. *Ejemplo de uso*

En la Fig. 7 queda demostrada la necesidad y utilidad de los elementos anteriormente descritos. El ejemplo que se detalla es para la funcionalidad incorporada por defecto que informa a Pedro (el usuario) que debe tomarse un medicamento. Este servicio gestiona unas alarmas que se han planificado previamente e interactúa con el usuario por medio de unas locuciones que se han personalizado. Al mismo tiempo el sistema interpreta que Pedro se ha tomado la píldora ya que un sensor en el cajón de las medicinas notifica esta acción de Pedro.

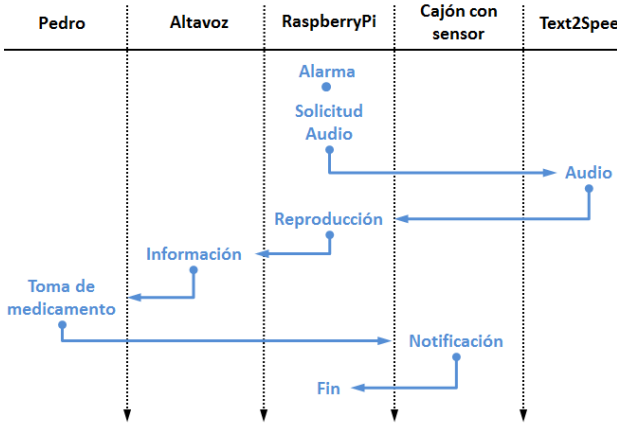


Fig. 7. Diagrama temporal. Proceso alarma de medicamento.

D. *Hardware de la RaspberryPi*

Para poder realizar las conexiones mencionadas es necesario disponer del siguiente hardware: RaspberryPi, adaptador Wireless 802.11a/b/g, adaptador Z-wave y un circuito propio que ha sido necesario diseñar y construir. Este equipamiento adicional basado en dos botones permitirá simplificar la configuración y uso de la plataforma (botón de configuración y botón de vinculación de dispositivos).

Fig. 8. Hardware necesario.

Los dos adaptadores se conectan vía USB y en el caso que sea necesario por tamaño o distribución física nos ayudaremos de un HUB USB.

La RaspberryPi proporciona una conexión mediante múltiples GPIO (General Purpose Input/Output), pines de entrada-salida, que permiten a un desarrollador añadir hardware directamente a la placa. Más adelante se detallará dicho mecanismo.

En la Fig. 9 se observa la funcionalidad, necesidad y conectividad de cada elemento añadido a la RaspberryPi. Las flechas indican la dirección en que se transmite información.

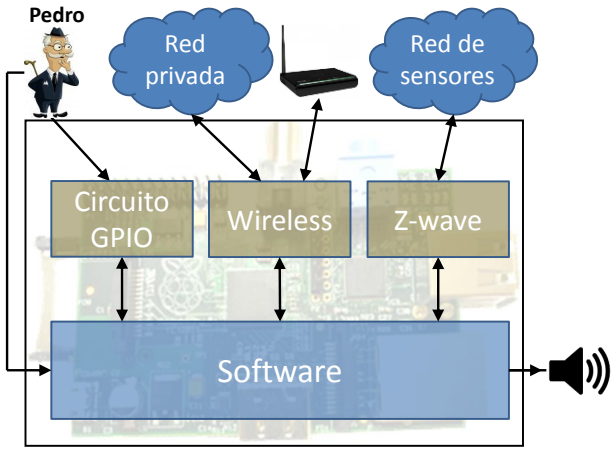


Fig. 9. Esquema del hardware conectado a la RaspberryPi.

E. *Circuito conectado a los GPIO de la RaspberryPi*

El producto final necesita permitir al usuario dar dos órdenes básicas y la mejor forma de hacerlo es mediante dos pulsadores directamente conectados a la placa. Para incorporar estos pulsadores se crearán dos circuitos como el de la Fig. 10.

La resistencia y el condensador ofrecen, respectivamente, seguridad y fiabilidad. La resistencia evita que se genere un cortocircuito y se sobrecargue el sistema. El condensador elimina las frecuencias altas, generadas al presionar y soltar el pulsador, puliendo la señal de salida.

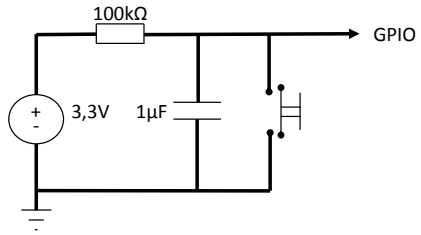


Fig. 10. Diseño del circuito eléctrico para un pulsador.

La apariencia del prototipo se puede observar en la Fig. 8, el dispositivo situado sobre la RaspberryPi.

El primer pulsador es el encargado de poner la RaspberryPi en modo configuración. Esto implica la creación de una red wireless privada para permitir la conexión del dispositivo (móvil o PC) que le subministrará los datos necesarios del punto de acceso al que se debe conectar.

El segundo pulsador es un atajo ofrecido al usuario para vincular un nuevo dispositivo (sensor Z-wave) de un modo rápido y sencillo.

F. *Software de la RaspberryPi*

A nivel lógico son necesarios dos programas: DomotiGa y la aplicación web desarrollada. DomotiGa es un software que ha desarrollado la comunidad de software libre que implementa múltiples protocolos y estándares en el campo de la domótica. Adicionalmente implementa una interfaz (muy poco amigable) de gestión y una API basada en XML-RPC (Extensible Markup Language - Remote Procedure Call) que permite que se puedan implementar otras aplicaciones.

En la Fig. 11 se observa la relación con el hardware y se puede apreciar que la comunicación interna entre la aplicación web y DomotiGa se realiza mediante el protocolo XML-RPC. Además DomotiGa proporciona información extra a la aplicación mediante transmisiones REST (Representational State Transfer).

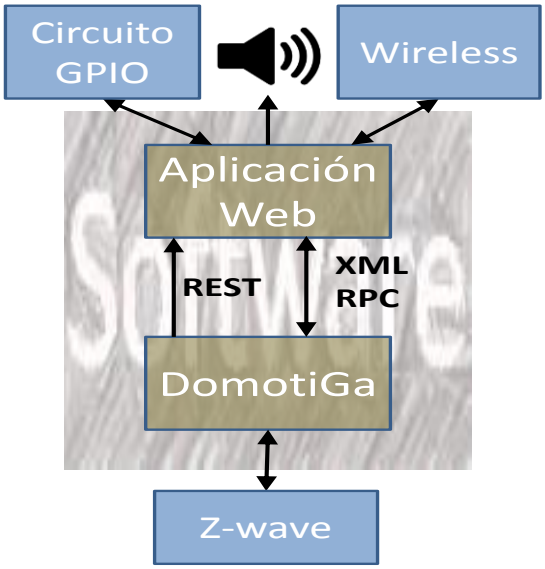


Fig. 11. Software implementado en la RaspberryPi y sus conexiones con el hardware.

G. *DomotiGa*

Los módulos necesarios de DomotiGa son:

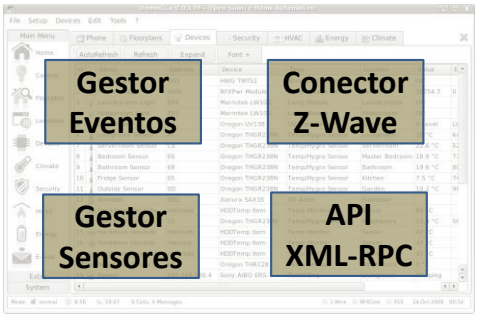


Fig. 12. Módulos necesarios de DomotiGa.

- Gestor de eventos: permite crear eventos nuevos, modificarlos, listarlos y accionar funciones en el momento especificado
- Gestor de sensores: permite añadir nuevos sensores, modificarlos, listarlos y enviar órdenes a actuadores.
- Conector Z-Wave: permite la comunicación entre sensores Z-Wave y DomotiGa.

- API XML-RPC: permite que aplicaciones externas puedan comunicase con DomotiGa y realizar las funciones que implementa, todo ello mediante el formato XML.

El modulo XML-RPC no incluye todas las funcionalidades concretas que son necesarias para realizar las comunicaciones deseadas. DomotiGa es de código libre, de modo que permite que los desarrolladores obtengan el código fuente del programa y puedan realizar las modificaciones oportunas. Además, estas modificaciones indispensables que se han llevado a cabo, han sido notificadas a DomotiGa a la espera de su aprobación e introducción en el código original.

Todas las nuevas funciones de DomotiGa se han añadido a la clase *CXMLRPC.class*:

- LocationsGetList: proporciona la lista de localizaciones espaciales por defecto que incluye DomotiGa.
- ModifyDevice: modifica la información de un sensor de la lista de dispositivos.
- ZWaveAddDevice: añade un nuevo sensor Z-wave; esta función prepara el conector Z-wave para una nueva conexión, una vez se indica al dispositivo que se conecte automáticamente se crea una nueva entrada en la lista de dispositivos.
- ZWaveDeleteDevice: elimina un sensor de la lista de dispositivos.
- TriggerGetList: devuelve la lista de disparadores.
- TriggerGet: devuelve la información completa de un disparador concreto.
- TriggerDelete: elimina un disparador.
- TriggerAdd: añade un disparador.
- ActionGetList: devuelve la lista de todas las acciones.
- ActionDelete: elimina una acción.
- ActionAdd: añade una nueva acción.
- EventGetList: devuelve la lista de todos los eventos.
- EventGetAction: devuelve la lista de acciones vinculadas a un evento en concreto.
- EventDelete: elimina un evento concreto.
- EventAdd: añade un evento.
- EventActionDelete: elimina el vínculo entre un evento y una acción, de modo que dicha acción deja de pertenecer al evento.
- EventActionAdd: añade un nuevo vínculo entre un evento y una acción.

H. Aplicación Web

La aplicación se ha diseñado para poder ofrecer al usuario una interfaz de control web mucho más simple que la que incorpora DomotiGa; además de ofrecer funcionalidades nuevas.

Se ha escogido la utilización de un servicio web para disponer de un entorno multiplataforma, además la página web está preparada para su correcta visualización en dispositivos como smartphones, PCs o tablets.

Desde la versión avanzada de la página web se puede visualizar los dispositivos (Fig. 13) y eventos disponibles, crear nuevos (Fig. 14), modificarlos o eliminarlos. También se puede configurar los datos de la wifi a la que se debe conectar y el email donde se desea recibir las notificaciones programadas.

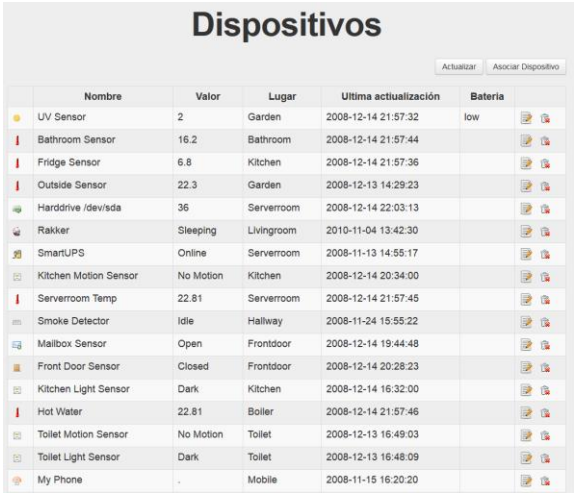


Fig. 13. Página web. La lista de sensores asociados.

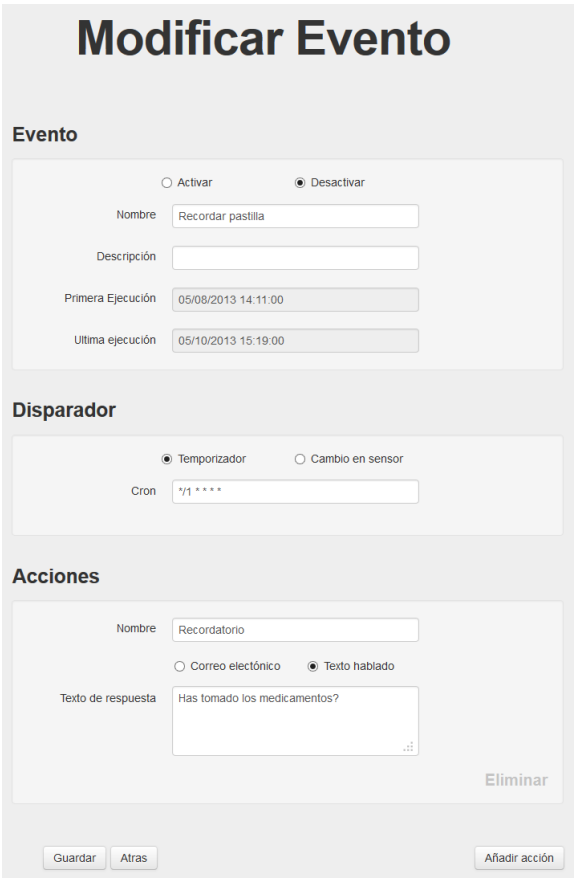


Fig. 14. Página web. Crear o modificar un evento desde el modo avanzado.

En la versión simple se ven los diferentes módulos que se hayan desarrollado (por defecto se incluye el modulo para recordar tomarse la medicación). Este módulo permite añadir qué medicamentos se deben tomar a ciertas horas del día de una manera muy simple e intuitiva (Fig. 16). Para cualquier especificación extra se puede acceder al evento desde el modo

avanzado, el cual permitirá configurar más parámetros libremente.

Fig. 15. Página web. Crear o modificar un evento tipo Medicamento.

I. *Estructura basada en la nube*

La RaspberryPi tiene un hardware muy limitado y no soportará añadir infinitos servicios. Gracias a la modularidad del diseño, se ha creado una segunda estructura donde se separa la aplicación web de la RaspberryPi y la sitúa en un ordenador con mayores recursos.

En la Fig. 16 se observa una nueva pieza en el escenario, el servidor de la aplicación web. Esto supone un requisito extra al usuario, un ordenador funcionando las 24h de los 7 días de la semana conectado a la red del hogar.

Este cambio permite liberar a la RaspberryPi de una gran cantidad de tareas. Ahora solo se usará como Gateway (puerta de enlace) de los sensores y gestor de eventos.

El nuevo servidor será el encargado de ofrecer la interfaz web que comunicará los datos con el usuario, pero a diferencia de antes, esta interfaz puede ser más potente y ofrecer más servicios. Además se podrán diseñar servicios que requieran gran cantidad de procesado, como por ejemplo, reconocimiento de imágenes.

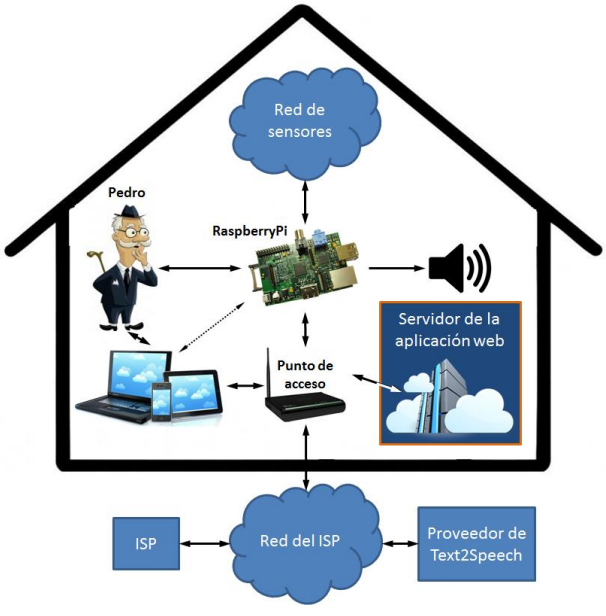


Fig. 16. Estructura global basada en la nube.

V. Costes

El producto final es de bajo coste, en la Tabla II se tiene desglosado el precio de los materiales necesarios.

Esto permite ofrecer un producto muy competitivo en el mercado, ya que por menos de 150€ se ofrece al consumidor una base con la que se puede comenzar a *domotizar* el hogar.

Tabla II
Coste del material del producto

Componente	Precio
RaspberryPi	26.8 €
Tarjeta SD 8Gb	7.75€
Receptor Wireless	15€
Receptor Z-wave	28.35€
Sensor Cajón Medicinas	35.58€
Material para el circuito	5€
Carcasa (caja para el producto)	10€
Total	**128.48€**

La modularidad permite aumentar la oferta de servicios, estos se podrán comprar conjuntamente con los sensores necesarios.

Disponer de un producto de bajo coste que ayude a optimizar funcionalidades del hogar, para reducir el importe de las facturas a final de mes, es sumamente interesante. En especial en el estado económico actual, plena crisis económica.

VI. Conclusiones

El producto está en línea con la situación económica, social y tecnológica actual. Mediante dispositivos lanzados recientemente al mercado, se ha conseguido diseñar e implementar un producto que puede ser desplegado en una red de sensores. El entorno ofrecido permite construir servicios para mejorar el bienestar de las personas, minimizando la acción de los usuarios en la gestión de los sistemas. Además, la evolución de la sociedad conduce a la necesidad, en un futuro próximo, de disponer de estos tipos de servicios para solventar problemas cotidianos.

Recordando los objetivos que se habían planteado, se ha conseguido crear una plataforma modular (objetivo 1), que ha admitido añadir el servicio de aviso de medicamentos (objetivo 6), sin necesidad de posteriores modificaciones. También se ha conseguido ofrecer un mecanismo para la configuración del producto en el hogar (objetivo 2); mediante un ordenador o Smartphone se pueden transmitir los datos de la red wireless a la que se debe conectar. Se ha implementado un servicio para la gestión de dispositivos (objetivo 3) y otro para el control de eventos (objetivo 4). Todo ello, en un entorno web muy simple e intuitivo, que ofrece grandes prestaciones a partir de mínimas configuraciones (objetivo 5).

VII. Agradecimientos

This research work was supported by the Spanish Ministry of Science and Innovation under the research grant TIN2010-20136-C03.

REFERENCIAS

[1] Proyección de la Población de España a Largo Plazo, 2009-2049, http://www.ine.es/prensa/np587.pdf.
[2] RaspberryPi, http://www.raspberrypi.org, 2013.
[3] OpenRemote, http://www.openremote.org/display/HOME/OpenRemote, 2013.
[4] DomotiGa, http://www.domotiga.nl, 2013.
[5] Dimitris Komnakos, Demosthenes Vouyioukas, Ilias Maglogiannis,Charalabos Skianis, "Cooperative Mobile High-Speed and Personal Area Networks for the Provision of Pervasive E-Health Services", School of Electrical and Computer Engineering, National Technical University of Athens, Zografou, Athens, Greece and Department of Information, Communication Systems Engineering, University of the Aegean, Karlovassi, Samos, Greece and Department of Biomedical Informatics, University of Central Greece, Papasiopoulou 2-4, Lamia, Greece.
[6] Yifeng He, Member, IEEE, Wenwu Zhu, Fellow, IEEE, and Ling Guan, Fellow, IEEE, "Optimal Resource Allocation for Pervasive Health Monitoring Systems with Body Sensor Networks".
[7] Cloud computing, http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

Estrategia de planificación de redes de sensores pro-activas

Sebastià Galmés
Dept. de Ciencias Matemáticas e Informática
Universidad de las Illes Balears
Cra. de Valldemossa, km. 7.5, 07122 Palma de Mallorca
sebastia.galmes@uib.es

***Resumen*- En las redes de sensores pro-activas o activadas por tiempo, cada nodo está programado para, de forma regular o periódica, tomar una muestra de su entorno, digitalizarla, empaquetarla, y enviarla mediante encaminamiento *multihop* a la estación base. En estas condiciones, es el módulo de comunicaciones del nodo el que más energía gasta en cada ciclo, sobretodo teniendo en cuenta que no sólo tiene que transmitir el propio paquete generado, sino que también tiene que reenviar los paquetes de sus nodos descendientes en el árbol de encaminamiento. En general, la literatura centrada en la optimización del consumo energético de estas redes, ha desarrollado soluciones a nivel de capa física, capa MAC y capa de red por separado, sin abordar su diseño conjunto. En este artículo se propone una estrategia de planificación combinada en la que el diseño del árbol de encaminamiento se realiza teniendo en cuenta las especificaciones de las capas MAC y física.**

***Palabras Clave*- red de sensores, TDMA, árbol de encaminamiento, capa física, capa MAC, capa de red.**

I. INTRODUCCIÓN

Una de las aplicaciones más llamativas de las redes de sensores es la monitorización regular del entorno, que consiste en el seguimiento de alguna variable ambiental (física, química o incluso biológica) con fines que pueden ser científicos o de control preventivo. En este contexto, resulta habitual que la red adopte un modelo de distribución de datos pro-activo o activado por tiempo (*time-driven model*), según el cual cada nodo toma una muestra de la variable bajo estudio, la digitaliza y empaqueta, y a continuación la envía hacia la estación base, todo ello siguiendo un patrón regular o periódico [1-3]. Algunos ejemplos interesantes de esta clase de redes de sensores se pueden encontrar en [1], [4-6].

Dada la regularidad con que los nodos sondean el entorno y transmiten, el tráfico generado por las redes de sensores activados por tiempo resulta bastante predecible, de ahí que los llamados protocolos planificados (*scheduled protocols*) resulten los más adecuados para regular el acceso de los nodos al canal inalámbrico (capa MAC – *Medium Access Control*). También es habitual que el despliegue de las redes pro-activas se lleve a cabo de forma estructurada [3-4], [6-7], bien ubicando los nodos en posiciones estratégicas que sean de especial interés para el observador, como es el caso del proyecto *Duke Island* [8], o bien de acuerdo con algún patrón de muestreo regular (en forma de malla, por ejemplo). Puesto que las posiciones estratégicas no tienen porqué estar próximas entre sí, o porque la magnitud monitorizada presenta una baja variabilidad espacial, como es el caso de la temperatura, la humedad y muchas otras, el campo sensorial resultante consiste en una serie de ubicaciones más o menos dispersas sobre una región relativamente grande. Estas hipótesis de trabajo contrastan con las que habitualmente se suelen adoptar, que consisten en suponer despliegues aleatorios y masivos de nodos en el campo sensorial. Es el caso de las llamadas redes reactivas o activadas por eventos (*event-driven sensor networks*) [9], y también de otras de carácter pro-activo [10-12].

En un escenario como el que se acaba de describir, resulta especialmente importante reducir el consumo energético de los nodos con el fin de garantizar un tiempo de vida de la red suficientemente elevado. Téngase en cuenta que los nodos se abastecen de sus baterías exclusivamente, y que el módulo de comunicaciones de cada uno consume una cantidad de energía muy significativa en cada ciclo. Ello se debe a una doble razón: por un lado, el transmisor-receptor es el componente que mayor potencia consume con respecto a los otros componentes que integran la arquitectura de un nodo (módulo sensorial y unidad de procesamiento); por otro, en cada ciclo, un nodo tiene que enviar su propio paquete y los paquetes de sus nodos descendientes en el árbol de encaminamiento. Estas consideraciones abarcan directa o indirectamente diversas capas de la arquitectura de redes, concretamente las capas física, MAC y de red. No obstante, la literatura centrada en la optimización de este tipo de redes ha propuesto soluciones a nivel de estas tres capas por separado, sin abordar su diseño conjunto. Por ello, en este artículo se propone una estrategia de planificación combinada en la que el diseño del árbol de encaminamiento se realiza sin restricciones excesivamente simplificadoras y teniendo en cuenta las especificaciones de las capas inferiores.

El artículo se organiza como sigue. En la Sección II, se describen las principales soluciones a nivel de capa física, MAC y de red para las redes de sensores activados por tiempo. En la Sección III, se propone una estrategia de planificación combinada, consistente en determinar el árbol de encaminamiento que optimiza el tiempo de vida de la red, teniendo en cuenta las especificaciones de la capa MAC y la capa física. En la Sección IV se presenta un ejemplo ilustrativo del procedimiento propuesto y, finalmente, en la Sección V se exponen las principales conclusiones.

II. SOLUCIONES ACTUALES POR CAPAS

En esta sección se describen las características principales de las soluciones propuestas para las capas física, MAC y de red de las redes de sensores pro-activas.

A. Capa física

A nivel de capa física, una técnica muy utilizada para aumentar el tiempo de vida de los nodos, aparte del uso de componentes o módulos más eficientes en términos de consumo energético, es el control de potencia (*power control*) [13]. Cuando esta característica está habilitada, el nodo puede regular la potencia transmitida en función del alcance deseado, a diferencia de los nodos que trabajan con potencia fija, en cuyo caso ésta se ajusta para obtener un alcance máximo. Además, la posibilidad de reducir la potencia transmitida cuando el nodo destinatario está más cerca, contribuye a reducir el nivel de interferencia en toda la red. Generalmente, esta funcionalidad se implementa de manera discreta, como es el caso de los nodos MICA2 o MICAz [14], de forma que el nodo puede elegir dentro de un conjunto discreto de niveles de potencia transmitida. No obstante, con el objeto de simplificar el tratamiento analítico, en la práctica suele utilizarse un modelo de radio continuo para caracterizar la relación entre potencia transmitida y distancia. El más utilizado es el siguiente [15-16]:

$$E_R = E_{elec} \cdot m \tag{1a}$$

$$E_T = E_{elec} \cdot m + E_w \cdot m \cdot d^f \tag{1b}$$

En la Ec. 1a, E_R representa la energía consumida por el circuito transmisor-receptor (*transceiver*) para recibir un paquete de m bits, siendo E_{elec} la que corresponde a recibir un solo bit. En la Ec. 1b, la energía gastada para transmitir un paquete de m bits, E_T, comprende además una componente de energía radiada, que es proporcional a la potencia f de la distancia entre el nodo transmisor y el nodo receptor, es decir, d. Concretamente, el término E_w es la energía radiada para transmitir un solo bit a la distancia de 1m, y f es el exponente de pérdida por propagación. A su vez, tanto E_w como f dependen del valor de la distancia comparado con una distancia de referencia, d_0, del siguiente modo:

$$d \le d_0 \Rightarrow E_w = E_{fs} \ , \ f = 2 \tag{2a}$$

$$d > d_0 \Rightarrow E_w = E_{mp} \ , \ f > 2 \tag{2b}$$

B. Capa MAC

Los protocolos MAC más extendidos para redes de sensores son de contención, ya que aprovechan la experiencia adquirida y el grado de implantación de los protocolos de contención para redes inalámbricas convencionales de los cuales derivan. Por tanto, puede afirmarse que los protocolos de contención para redes de sensores se inspiran en la técnica CSMA (*Carrier Sense Multiple Access*), que se utiliza en redes tan conocidas como las IEEE 802.11. El inconveniente de este tipo de protocolos es que no eliminan completamente las deficiencias del canal de transmisión inalámbrico en términos de colisiones, escucha ociosa (*idle listening*) y sobre-escucha (*overhearing*), las cuales provocan un consumo extra de energía. Por ello, la investigación encaminada a adaptar estos protocolos a redes de sensores se ha centrado en paliar estas deficiencias. En concreto, la técnica LPL (*Low Power Listening* [17]), en sus diferentes modalidades, se ha desarrollado para reducir la duración de los períodos largos de escucha ociosa en que un nodo tiene que ser capaz de detectar y recibir un paquete dirigido a él. Con esa reducción, el ciclo de trabajo (*duty-cycle*) de los nodos en los protocolos de contención en que se ha introducido dicha técnica (*LPL MAC protocols*), también se ve notablemente reducido. Entre los protocolos de contención más relevantes para redes de sensores, podemos citar S-MAC [18], BoX-MAC [19] y el propio ZigBee (IEEE 802.15.4 [20]), cuando trabaja sin supertrama.

No obstante, incluso con la introducción de la técnica LPL, el consumo energético extra provocado por las deficiencias antes señaladas, sugiere que los protocolos de contención no son los más adecuados para las redes de sensores activadas por tiempo, en las que los nodos tienen que recibir y transmitir regularmente. Téngase en cuenta que el flujo de datos generado por estas redes es bastante predecible, ya que básicamente consiste en el envío de tantos paquetes como nodos en cada ciclo de muestreo. Por ello, a la hora de controlar el acceso de los nodos al medio de transmisión compartido, resultan más apropiados los llamados protocolos MAC planificados (*scheduled protocols*), que permiten organizar y regular las transmisiones de forma que no se produzcan conflictos (colisiones). No debe extrañar, pues, que los protocolos planificados para redes de sensores pro-activas se inspiren en el mecanismo TDMA (*Time Division Multiple Access*), que además conlleva la ventaja adicional de posibilitar una mayor reducción del ciclo de trabajo de los nodos que en el caso de los protocolos de contención. Esto es debido a que, en TDMA, el intervalo de tiempo en que cada nodo tiene que transmitir está predeterminado, lo cual permite a su vez predeterminar los intervalos completos de actividad de cada uno de ellos, entre recepción y transmisión de paquetes. Así pues, cualquier nodo puede conmutar al modo de bajo consumo (*sleep mode*) durante el resto de tiempo. Algunos ejemplos representativos de protocolos basados en TDMA para redes de sensores son SMACS [21], ReSync [22] y TRAMA [23]. No obstante, el inconveniente principal de los protocolos planificados es que requieren que los nodos estén sincronizados (local o globalmente), lo cual es precisamente difícil de conseguir con bajo coste energético en redes teóricamente constituidas por nodos baratos y de prestaciones limitadas. Otra desventaja de estos protocolos es su escasa flexibilidad a las variaciones del patrón de tráfico.

Por todos estos motivos, recientemente se ha desarrollado un nuevo protocolo, RDG (*Randomized Data Gathering*) [24], que intenta evitar el requisito de sincronización de los protocolos planificados, y al mismo tiempo alcanzar los reducidos ciclos de trabajo que ofrecen estos. Este protocolo se fundamenta en dos elementos: (a) la aleatorización de los instantes de muestreo y transmisión, y (b) la inserción en el campo de control de cada paquete del margen de tiempo hasta el siguiente envío. Este último mecanismo tiene la desventaja de que, en caso de pérdida o recepción errónea del paquete, el nodo destinatario del mismo pierde la referencia de tiempo, y por tanto no puede conmutar al modo de bajo consumo hasta recibir un nuevo paquete correcto del nodo emisor. Así, el nodo receptor inicia un período de escucha ociosa, cuyo coste energético sólo puede paliarse aplicando la técnica LPL. Por ello podemos afirmar que RDG es un protocolo híbrido entre las dos categorías antes expuestas. Debido a los períodos de escucha ociosa, aunque su efecto

sea mitigado con LPL, RDG no alcanza el tiempo de vida de los protocolos basados en TDMA, pero evita los requisitos fuertes de sincronización de estos últimos. En la Tabla I se muestra una comparativa desde diversos puntos de vista de los protocolos planificados más importantes y RDG. Como puede observarse, RDG ofrece también una mayor flexibilidad frente a variaciones de tráfico (causadas, por ejemplo, por cambios en el patrón de muestreo de algunos nodos). Por todas las ventajas expuestas, RDG se utilizará como base del ejemplo descrito en la Sección IV.

Tabla I
COMPARATIVA ENTRE PROTOCOLOS PLANIFICADOS Y RDG

Protocolo	Ciclo de trabajo	Requisitos de sincronización	Adaptabilidad al tráfico
TDMA (puro)	Mínimo	Fuerte, global	Baja
SMACS	Mínimo	Fuerte, local	Baja
ReSync	Bajo	Fuerte, local	Alta
TRAMA	Bajo	Fuerte, global	Alta
RDG	Bajo	Débil, local	Muy alta

C. Capa de red

La función principal de la capa de red es determinar la topología de encaminamiento de los datos. En el caso de una red de sensores pro-activa, esta topología toma la forma de un árbol de encaminamiento estático, en el que el camino entre cada nodo y la estación base queda predeterminado a través de una serie de nodos intermedios (encaminamiento *multi-hop*), por lo general. Así pues, la capa de red ejecuta de forma centralizada o distribuida un algoritmo de encaminamiento, que permite fijar el destinatario inmediato de cada nodo en el camino de los paquetes hacia la estación base. Generalmente, los algoritmos de encaminamiento se basan en asignar un coste a cada enlace, y en ejecutar una serie de instrucciones a fin de satisfacer un criterio de optimización, que puede ser MHC (*Minimum Hop Count*), MST (*Minimum Spanning Tree*) o SPR (*Shortest Path Routing*), entre los más habituales. No obstante, ninguno de estos algoritmos resulta útil para determinar el árbol de encaminamiento óptimo de una red de sensores pro-activa cuando el criterio de optimización es maximizar el tiempo de vida de la misma. La razón es que el consumo energético de un nodo en este tipo de redes depende de dos factores topológicos, como son la distancia entre el nodo y su destinatario inmediato (asumiendo que el control de potencia está habilitado), y el número de paquetes que tiene que reenviar de todos sus descendientes en cada ciclo de trabajo (intensidad de tráfico reenviado). Desafortunadamente, este último factor no puede formularse como un coste asociado a un enlace, puesto que depende del número de descendientes del nodo y, en definitiva, del subárbol enraizado en el mismo; por lo tanto, los algoritmos señalados arriba, muy eficientes desde el punto de vista computacional, no resultan aplicables. Analizando el problema más detalladamente, consideremos una red de N nodos y una estación base, y sea $\mathbf{T}(j)$, $j = 1\ldots M$, un árbol cualquiera del conjunto total $\mathbf{T}$, cuyo cardinal es M, de todos los árboles que permiten conectar los N nodos con la estación base, y $d(i, j)$ y $w(i, j)$, $i = 1\ldots N$, $j = 1\ldots M$, respectivamente la distancia a la que el nodo i tiene que transmitir y el número de paquetes que dicho nodo tiene que reenviar cuando el árbol de encaminamiento es $\mathbf{T}(j)$. En base a estas variables, la Fig. 1 muestra las relaciones causa-efecto que justifican la importancia de una selección adecuada del árbol de encaminamiento a la hora de maximizar el tiempo de vida de la red. Concretamente, en dicha figura, $E(i, j)$, $i = 1\ldots N$, $j = 1\ldots M$, representa la energía consumida durante un ciclo por el nodo i cuando el árbol de encaminamiento es $\mathbf{T}(j)$, L(j) es el tiempo de vida de la red cuando el árbol de encaminamiento es $\mathbf{T}(j)$, y B es la batería disponible inicialmente en cada nodo. Nótese que para el tiempo de vida de la red se ha adoptado la definición más habitual, que es el tiempo que transcurre hasta que un primer nodo consume toda su batería.

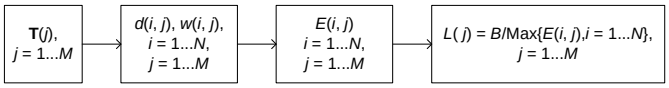


Fig. 1. Influencia del árbol de encaminamiento en el tiempo de vida de la red.

En consecuencia, la selección del árbol de encaminamiento queda formulada como el siguiente problema de optimización:

$$\text{Seleccionar } \mathbf{T}(j_{opt}) : L(j_{opt}) = L = \text{Max}\{L(j),\ j = 1\ldots M\} \quad (3)$$

Desafortunadamente, este problema es NP-complejo, como se demuestra en [25]. Concretamente, su dimensión viene dada por el número total de árboles de encaminamiento distintos, que es $M = (N+1)^{N-1}$ (fórmula de Cayley's [26]). Salvo en los casos en que N sea muy pequeño, este problema requiere la aplicación de algún algoritmo heurístico, que permita obtener una solución suficientemente buena en un tiempo razonable. Cualquiera que sea la técnica que pueda utilizarse en el desarrollo de este algoritmo, su complejidad computacional va a ser muy superior a la de los algoritmos básicos de la teoría de grafos señalados anteriormente. Quizás por ello los algoritmos básicos se han seguido utilizando, directa o indirectamente, en redes de sensores, dando como resultado tiempos de vida muy por debajo de los valores óptimos. Un claro ejemplo es el protocolo CTP (*Collection Tree Protocol* [27]), desarrollado específicamente para redes de sensores activadas por tiempo. En este protocolo, se ejecuta una versión del algoritmo SPR (*Shortest Path Routing*), en el que la métrica utilizada para asignar un coste a cada enlace es ETX (*Expected Number of Transmissions*), que cuantifica la calidad del enlace por medio del número medio de transmisiones requeridas de un mismo paquete. Por lo tanto, la aplicación de este algoritmo contribuye a mejorar el tiempo de vida en la medida que obtiene rutas que minimizan el número de retransmisiones, pero no aborda los factores topológicos esenciales, es decir, la distancia a transmitir y la intensidad del tráfico de reenvío. Con los protocolos de encaminamiento encaminados a minimizar el número de saltos (MHC), ocurre algo similar: contribuyen métricas de comportamiento tales como el retardo promedio de las rutas o la probabilidad de pérdida/error de los paquetes, pero no inciden de manera directa en el tiempo de vida de la red. Una mejora la representan los algoritmos de encaminamiento basados en MST, ya que en este caso se contempla uno de los factores topológicos esenciales, como es la distancia a transmitir, pero ignorando la carga de trabajo de los nodos representada por la intensidad del tráfico de reenvío. El algoritmo propuesto en [25], que denotamos como MLAA (*Maximum Lifetime*

Approximation Algorithm), constituye el primer intento de abordar la carga de trabajo de los nodos en la evaluación del tiempo de vida de la red. No obstante, este algoritmo se basa en dos simplificaciones muy restrictivas: (a) uso de un fuerte esquema de agregación de paquetes, en el que se supone que los paquetes de los nodos descendientes son agregados conjuntamente con el propio paquete, de forma que, en cada ciclo, cada nodo envía un solo paquete independientemente del subárbol que dependa de él, y (b) el control de potencia está deshabilitado, de forma que se elimina la dependencia con la distancia a transmitir. La Tabla II muestra la adecuación de los algoritmos/protocolos de encaminamiento comentados a diversos objetivos de diseño, como son PER (*Packet Error Rate* - tasa de paquetes que se reciben con error en un enlace), PLR (*Packet Loss Rate* – tasa de paquetes emitidos que no alcanzan la estación base), el retardo promedio que transcurre entre la transmisión de un paquete y su recepción en la estación base, el *throughput*, que es el número de paquetes que la red de sensores puede transmitir a la estación base por unidad de tiempo, y, por supuesto, el tiempo de vida. Con respecto a este último objetivo, se puede observar que ninguno de los algoritmos señalados en la tabla aborda la problemática de la optimización del tiempo de vida en toda su extensión. Precisamente, la estrategia de planificación que se propone a continuación trata de subsanar esta deficiencia al contemplar la utilización de algoritmos heurísticos combinados con modelos más completos a nivel de capa MAC y capa física en la obtención del árbol de encaminamiento con máximo tiempo de vida.

Tabla II
ADECUACIÓN DE ALGUNOS ALGORITMOS/PROTOCOLOS DE ENCAMINAMIENTO A DIVERSOS OBJETIVOS DE DISEÑO

Objetivos de diseño	MHC	MST	CTP (SPR-ETX)	MLAA
PER, PLR	Moderada	-	Alta	-
Retardo	Alta	Baja	-	-
Throughput	-	-	Alta	-
Tiempo de vida	-	Moderada	Baja	Moderada

III. ESTRATEGIA DE PLANIFICACIÓN

Como se sugiere en la sección anterior, el problema de optimización representado por la Ec. 3, sólo puede abordarse en toda su extensión, es decir, teniendo en cuenta los dos factores topológicos señalados, mediante un algoritmo heurístico o de optimización estocástica. Este tipo de algoritmos son los más indicados para tratar problemas de optimización combinatoria como el que se está tratando aquí, a diferencia de los métodos deterministas. Entre los algoritmos de optimización estocástica podemos citar los métodos tradicionales de Monte Carlo, los métodos de búsqueda local (*Tabu search*, *simulated annealing*), los algoritmos evolutivos (algoritmos genéticos, evolución diferencial), los llamados algoritmos de inteligencia colectiva o enjambres inteligentes (*swarm optimization*: *ant colony optimization*, *particle swarm optimization*) y las redes neuronales. En general, se trata de algoritmos basados en imitar comportamientos que ya se dan en la Naturaleza; configurados correctamente, pueden ofrecer soluciones de compromiso muy satisfactorias en términos de bondad o ajuste del resultado y complejidad computacional. En el caso que nos ocupa, la consecución de dicho compromiso no es tarea sencilla. La razón se explica en la Fig. 2, que muestra la estructura de buena parte de estos algoritmos (la parte sombreada es específica del problema de optimización que se trata en el presente artículo). Como puede observarse, suelen contener dos niveles de iteraciones, uno encapsulado dentro del otro. Por ejemplo, en el caso de *simulated annealing*, el primer nivel de iteración lo constituye la temperatura o parámetro de control, mientras que el segundo nivel está formado por un conjunto de iteraciones que se ejecutan para cada valor de temperatura. En el caso de los algoritmos genéticos, el primer nivel son las generaciones de individuos (árboles de encaminamiento en el caso que nos ocupa), y el segundo nivel lo constituyen los individuos de cada población, y por tanto viene dado por el tamaño de la población (se supone que todas las generaciones tienen el mismo tamaño de población). En general, la dimensión de los dos bucles es grande, aunque depende del problema tratado y de la magnitud del mismo. En el caso de la optimización del árbol de encaminamiento de una red de nodos, la experiencia adquirida nos indica que la magnitud del primer nivel de iteraciones es de un mínimo de 50 para redes de hasta 100 nodos [28], en el caso de *simulated annealing*, y del orden de 20 para redes de sólo hasta 10 nodos (resultados preliminares [29]), cuando se aplica un algoritmo genético. La magnitud del segundo nivel es de unas 1000 iteraciones en el caso de *simulated annealing*, y de unos 200 individuos (tamaño de la población) en el caso del algoritmo genético, en las mismas condiciones señaladas al especificar la complejidad del primer nivel.

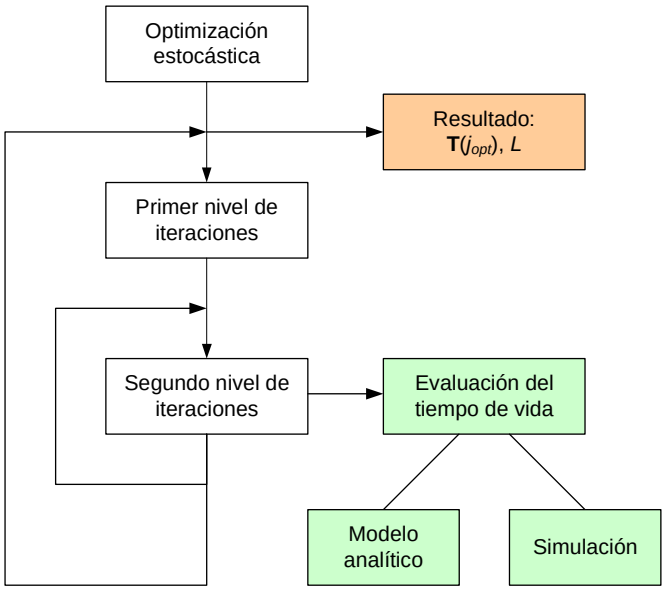


Fig. 2. Estructura habitual de algunos algoritmos heurísticos para problemas de optimización estocástica (la parte sombreada es específica del problema de la red de sensores).

En cualquier caso, el producto de las magnitudes de los dos niveles de iteraciones suele ser muy elevado. En el caso que nos ocupa, se requiere que en cada iteración del segundo nivel se calcule el tiempo de vida de la red para el despliegue de nodos dado, lo que supone una dificultad adicional en términos de coste computacional. Para evaluar ese tiempo de

vida, es necesario encapsular el modelo de radio dado por las Ecs. 1a-1b y 2a-2b, en un modelo de consumo energético más completo que contemple la especificación de la capa MAC (protocolo de acceso utilizado – véase la Tabla I a modo de referencia), y los factores topológicos que dependen del árbol de encaminamiento (capa de red). En el mejor de los casos, el modelo de consumo energético desarrollado es resoluble analíticamente, lo que contribuye a preservar el coste computacional global del proceso descrito en la Fig. 2. Desafortunadamente, esto no sucede para la mayor parte de protocolos de acceso (capa MAC), cuya complejidad sólo puede capturarse mediante modelos de simulación. Como es sabido, la simulación es una técnica costosa en cuanto a consumo de recursos (tiempo de CPU sobretodo), lo cual, unido a la propia complejidad del algoritmo heurístico, daría lugar a tiempos de ejecución inaceptables. Por ello, la estrategia que se propone aquí es una aproximación al problema basada en suponer un protocolo MAC lo suficientemente sencillo (y al mismo tiempo representativo), como para que dé lugar a un modelo analítico fácilmente tratable. En este sentido, la mejor opción es el protocolo TDMA, ya que, como se vio en la Sección II.B, no provoca consumos energéticos extra más allá de los debidos a la transmisión y recepción de paquetes en cada ciclo de muestreo, lo cual conlleva dos ventajas: (a) constituye la referencia óptima para el resto de protocolos MAC en términos de consumo energético (en ausencia de agregación de paquetes), y (b) resulta fácilmente representable mediante el siguiente modelo analítico:

$$E(i,j) = g(i,j)\cdot E_T(i,j) + w(i,j)\cdot\left(E_R + E_T(i,j)\right), \quad i = 1\ldots N,\ j = 1\ldots M \tag{4}$$

En esta ecuación se ha introducido el término $g(i, j)$, que denota el número de paquetes generados por el nodo i durante un ciclo (intensidad del nodo i), cuando el árbol de encaminamiento es $\mathbf{T}(j)$. Esta variable cuantifica la carga de trabajo generada por un nodo sobre la red, si bien por lo general es igual a 1 (cada nodo genera y envía un solo paquete en cada ciclo de muestreo).

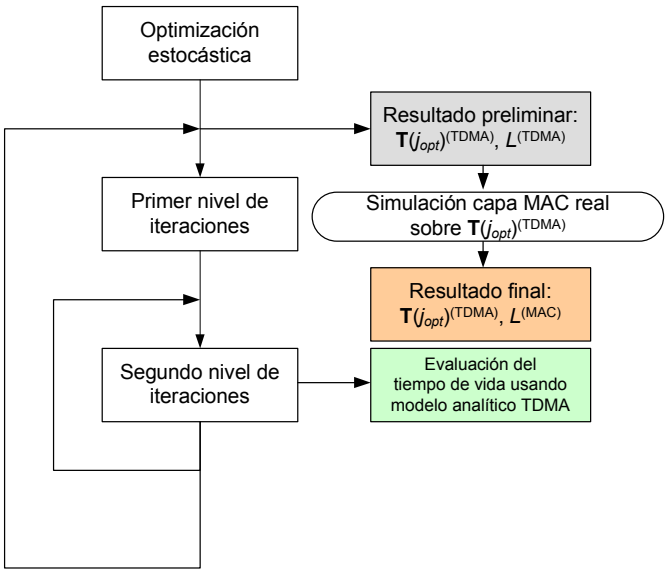


Fig. 3. Aproximación al problema de optimización estocástica consistente en determinar el árbol de encaminamiento óptimo de una red de sensores activa por tiempo utilizando cualquier protocolo MAC.

En la Fig. 3. se muestra la estrategia propuesta. Como puede observarse, es una variación de la mostrada en la Fig. 2 orientada a reducir la complejidad computacional de esta última. Nótese que en el algoritmo heurístico se utiliza el modelo analítico de TDMA en cada iteración del segundo nivel, con lo cual el cálculo del tiempo de vida de la red resulta muy simple desde el punto de vista computacional (nótese también que, a los efectos del procedimiento que se está describiendo, el coste energético que conlleva la sincronización en TDMA se puede ignorar, sobretodo teniendo en cuenta que este coste no existe en el caso de algoritmos y protocolos en los que se evita precisamente la sincronización). Al final, sobre el árbol de encaminamiento obtenido con TDMA, $\mathbf{T}(j_{opt})^{(\mathrm{TDMA})}$, cuyo tiempo de vida es $L^{(\mathrm{TDMA})}$, se simula el protocolo MAC considerado, y se obtiene el tiempo de vida definitivo $L^{(\mathrm{MAC})}$. Si aceptamos que el tiempo de vida $L^{(\mathrm{TDMA})}$ es el máximo o suficientemente próximo al máximo, porque el algoritmo heurístico busca el árbol de encaminamiento óptimo y porque TDMA es, como ya se ha dicho, el protocolo MAC más eficiente en cuanto a consumo energético, la solución que se habría obtenido aplicando el procedimiento de la Fig. 2 quedaría en un margen muy reducido entre $L^{(\mathrm{TDMA})}$ y $L^{(\mathrm{MAC})}$, suponiendo que efectivamente el protocolo MAC utilizado alcance ciclos de trabajo suficientemente reducidos. En tal caso, la aplicación del procedimiento de la Fig. 2 no vendría compensada por una mejora sustancial de los resultados.

Obviamente, esta metodología resulta aceptable siempre y cuando el protocolo MAC realmente considerado permita alcanzar valores del ciclo de trabajo lo suficientemente buenos (bajos), es decir, próximos al óptimo garantizado por TDMA para las condiciones dadas. Precisamente la reducción del ciclo de trabajo es el objetivo principal de diseño de todos los protocolos MAC para redes de sensores, y por lo tanto buena parte de ellos satisfacen esta condición. El propio resultado final confirma la bondad de la aproximación, como se verá en el apartado siguiente.

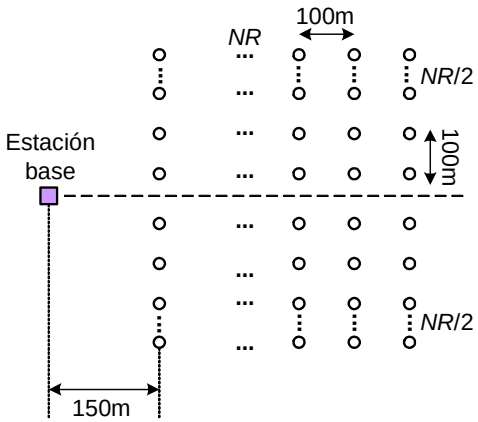


Fig. 4. Despliegue de prueba.

IV. Ejemplo

En esta sección se propone un ejemplo numérico que ilustra la idoneidad de la estrategia de planificación propuesta. El despliegue de prueba es el que se muestra en la Fig. 4, que ya fue utilizado en [24]. Se trata de una malla de nodos con separación de 100m entre nodos adyacentes, tanto en sentido vertical como en horizontal, y una estación base

situada a 150m de la primera columna de nodos. En dicha figura, *NR* representa el número de filas o columnas, de forma que el número total de nodos es $N = NR^2$. El protocolo MAC considerado es RDG, cuya capacidad para alcanzar ciclos de trabajo reducidos quedó refrendada en [24], y el algoritmo heurístico utilizado es *simulated annealing*, con un criterio de parada de 50 temperaturas y un número de iteraciones por temperatura de valor 1000. Los parámetros del modelo de radio y del protocolo RDG se muestran en la Tabla III.

En la obtención de resultados, se ha considerado una intensidad de tráfico por nodo de valor 1, y valores de *NR* iguales a 2, 4, 6 y 8 (por tanto, redes de 4, 16, 36 y 64 nodos respectivamente). Para cada número de nodos se simula el protocolo RDG mediante QNAP2 [30] sobre el árbol resultante de aplicar el algoritmo heurístico (implementado en *Mathematica*), y se obtiene el tiempo de vida definitivo. En cada simulación, se ejecutan 100 réplicas, alcanzándose para cada tiempo de vida un intervalo de confianza inferior al 1% para un nivel de confianza del 95%.

Tabla III
PARÁMETROS DEL MODELO DE RADIO Y EL PROTOCOLO RDG

Parámetro	Valor
Energía disipada por el transmisor/receptor de cada nodo (E_R)	50nJ/bit
Energía radiada por el transmisor de cada nodo en condiciones de espacio libre (E_{fs})	10pJ/bit/m^2
Energía radiada por el transmisor de cada nodo en propagación multicamino (E_{mp})	0.0013pJ/bit/ m^4
Exponente de pérdida por propagación multicamino (f)	4
Distancia de referencia (d_0)	75m
Alcance (máximo) de los nodos	250m
Batería	15kJ
Tamaño de los paquetes (m)	50B
Duración de los ciclos de muestreo (RDG)	75000 *slots* 1 *slot* = duración 1 paquete
LPL (RDG)	10%

Los resultados se muestran en la Fig. 5, donde SA hace referencia al algoritmo basado en *simulated annealing*. Como puede comprobarse, efectivamente la franja resultante entre los tiempos de vida obtenidos al aplicar el algoritmo SA en base a TDMA (SA-TDMA) y al simular RDG sobre la misma red obtenida con SA-TDMA (SA-RDG), es muy estrecha. Aproximadamente $L^{(RDG)} \cong 0.9 \cdot L^{(TDMA)}$ en todos los casos. En la gráfica también se muestra, a modo de referencia, la curva de tiempo de vida obtenida al aplicar el algoritmo MST. Como puede observarse, esta curva está bastante por debajo de las anteriores, y ello se debe a que el algoritmo MST sólo optimiza uno de los factores topológicos que influyen en el tiempo de vida (distancia de transmisión).

Para terminar, las Figs. 6-9 muestran el árbol de encaminamiento resultante de la aplicación del algoritmo *simulated annealing* (utilizando el modelo analítico de TDMA) para cada uno de los tamaños de red considerados en la Fig. 5 (los nodos están numerados por orden creciente de su distancia a la estación base). Las soluciones $L^{(RDG)}$ y $L^{(TDMA)}$ mostradas en la Fig. 5 corresponden a estos árboles de encaminamiento. Como puede observarse, el hecho de que, en la evaluación de la energía consumida por cada nodo, se haya considerado el efecto de la carga de tráfico (número de paquetes a reenviar) además de la distancia de transmisión, juntamente con la propia aleatoriedad del algoritmo, da como resultado topologías con apariencia desordenada. Por ejemplo, en el grafo de la Fig. 7, el nodo 10 envía sus paquetes al nodo 5 en lugar del 6 que está más próximo, precisamente para no sobrecargar este último. También se pueden observar conexiones algo sorprendentes, como las conexiones cruzadas que se observan en la Fig. 6, o, también en la Fig. 7, la conexión directa del nodo 14 al 15 en lugar del 13. Estas arbitrariedades se producen como resultado de la aleatoriedad del algoritmo, en la medida en que no afectan al resultado final.

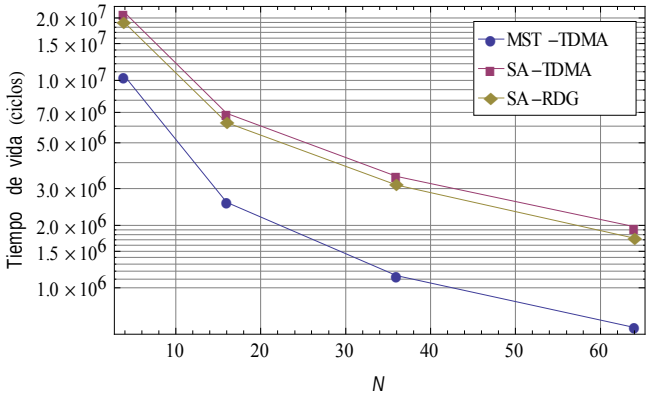


Fig. 5. Comparativa de tiempos de vida obtenidos con los algoritmos MST y SA basados en TDMA, y el algoritmo SA basado en RDG según la metodología aproximada propuesta.

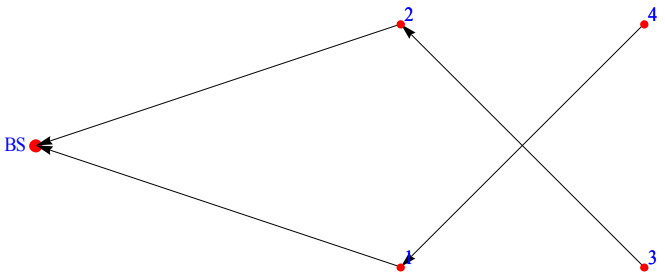


Fig. 6. Árbol optimizado para el caso de 4 nodos.

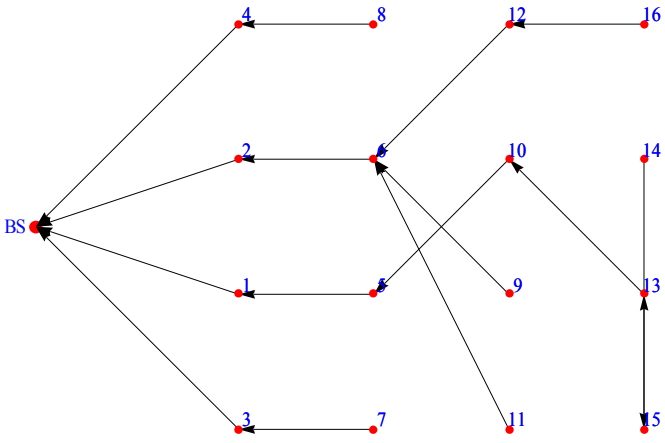


Fig. 7. Árbol optimizado para el caso de 16 nodos.

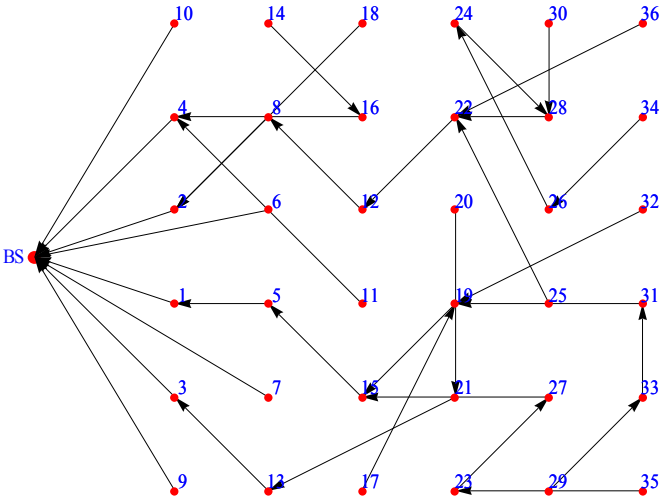


Fig. 8. Árbol optimizado para el caso de 36 nodos.

V. CONCLUSIONES

En este artículo se ha propuesto una estrategia o metodología de planificación de redes sensoriales pro-activas que consiste en determinar el árbol de encaminamiento óptimo para unas especificaciones concretas de la capa física y la capa MAC. En esta estrategia se contemplan todos los factores topológicos que determinan el tiempo de vida de la red, y se propone una aproximación al problema basada en la utilización del modelo analítico de consumo de energía correspondiente al protocolo MAC TDMA, para obtener posteriormente el tiempo de vida de cualquier otro protocolo MAC utilizado. Con ello se consiguen resultados satisfactorios en términos de bondad de la solución y coste de ejecución, bajo la hipótesis de que el protocolo MAC considerado alcanza ciclos de trabajo reducidos. Como línea de trabajo futuro, se trataría de realizar una evaluación más detallada de la complejidad computacional de la estrategia propuesta, en comparación con la que resultaría de aplicar el procedimiento riguroso.

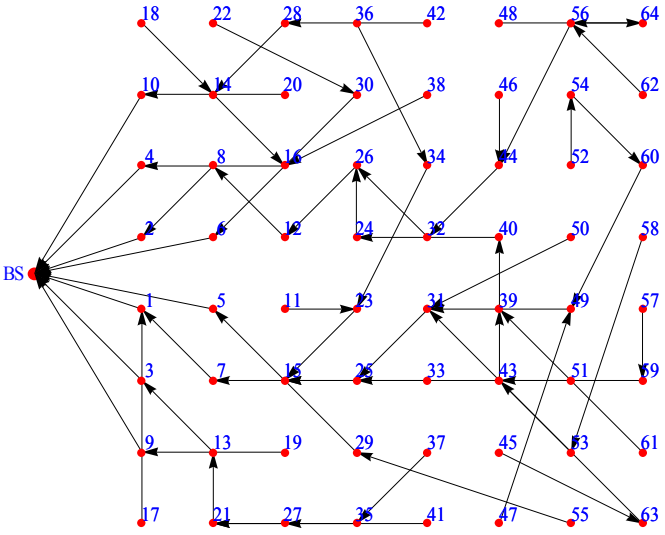


Fig. 9. Árbol optimizado para el caso de 64 nodos.

AGRADECIMIENTOS

Este trabajo ha sido financiado por el Ministerio de Ciencia e Innovación a través del proyecto TIN2010-16345.

REFERENCIAS

[1] C. de M. Cordeiro and D. P. Agrawal, *Ad Hoc and Sensor Networks: Theory and Applications*, World Scientific Publishing, 2006.

[2] S. Tilak, N. Abu-Ghazaleh and W. Heinzelman, "A taxonomy of wireless micro-sensor network models", *ACM Mobile Computing and Communications Review (MC2R)*, Vol. 6, No. 2, April 2002.

[3] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks", *Ad Hoc Networks*, Vol. 3, pp. 325-349, 2005.

[4] B. Krishnamachari, *Networking Wireless Sensors*, Cambridge University Press, 2005.

[5] R. Szewczyk, E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring and D. Estrin, "Habitat monitoring with sensor networks", *Communications of the ACM*, Vol. 47, No. 6, June 2004.

[6] I. Stojmenovic, *Handbook of Sensor Networks: Algorithms and Architectures*, Wiley, 2005.

[7] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*, Wiley, 2005.

[8] F. Zhao and L. Guibas, *Wireless Sensor Networks*, Elsevier, 2004.

[9] S. Taruna, M. R. Tiwari, and S. Shringi, "Event-driven routing protocols for wireless sensor network – a survey", *International Journal on Computational Sciences and Applications*, vol. 3, no. 2, April 2013.

[10] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", *IEEE Trans. on Wireless Communications*, vol. 1, no. 4, pp. 660-670, October 2002.

[11] O. Younis and S. Fahmy, Distributed clustering in ad-hoc sensor networks: a hybrid, energy-efficient approach, *Proc. of IEEE Infocom*, 2004.

[12] S. Lindsey and K. M. Sivalingam, "Data gathering algorithms in sensor networks using energy metrics", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 13, No. 9, pp. 924-934, 2002.

[13] N. A. Pantazis and D. D. Vergados, "A survey on power control issues in wireless sensor networks", *IEEE Communication Surveys*, vol. 9, n. 4, pp. 86-106.

[14] Crossbow: http://www.crossbow.com.

[15] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

[16] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice-Hall, 2002.

[17] C. J. Merlin and W. B. Heinzelman, "Duty cycle control for low-power-listening MAC protocols", *IEEE Trans. on Mobile Computing*, vol. 9, n. 1, pp. 1508-1521.

[18] W. Ye, J. Heidemann and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks", *IEEE/ACM Transactions on Networking*, Vol. 12, No. 3, pp. 493-506.

[19] D. Moss and P. Levis, "BoX-MACs: Exploiting physical and link layer boundaries in low-power networking", TR SING-08-00. Stanford University, 2008.

[20] ZigBee Alliance: http://www.zigbee.org.

[21] K. Sohrabi, J. Gao, V. Ailawadhi, G. J. Pottie, "Protocols for self-organization of a wireless sensor network". *IEEE Personal Communications*, vol. 7, no. 5.

[22] W. S. Conner, J. Chhabra, M. Yarvis, L. Krishnamurthy, Experimental evaluation of synchronization and topology control for in-building sensor network applications. *Proc. of ACM WSNA*, Sep. 2003.

[23] V. Rajendran, K. Obraczka, J. J. Garcia-Luna-Aceves, Energy-efficient, collision-free medium access control for wireless sensor networks. *Proc. of ACM Sensys*, Nov. 2003.

[24] S. Galmés and R. Puigjaner, "Randomized data-gathering protocol for time-driven sensor networks", *Computer Networks*, vol. 55 (2011), pp. 3863-3885.

[25] Y. Wu, S. Fahmy, and N. B. Shroff, "On the construction of a maximum-lifetime data gathering tree in sensor networks: NP-completeness and approximation algorithm", Proc. of IEEE Infocom 2008 (Phoenix, AZ, USA, April 13-18, 2008).

[26] M. Aigner and G. M. Ziegler, Proofs from THE BOOK. Springer-Verlag, 1998, pp. 141-146.

[27] R. Fonseca, et al., "The Collection Tree Protocol (CTP)". http://www.tinyos.net/tinyos-2.x/doc/html/tep123.html.
[28] M. L. Santamaría, S. Galmés, and R. Puigjaner, "Simulated annealing approach to optimizing the lifetime of sparse time-driven sensor networks", Proc. of 2009 IEEE International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS 2009), pp. 193-202.
[29] J. Pou and S. Galmés, "A genetic algorithm for spanning tree optimization in sensor networks", Proc. of IEEE LCN 2013, Sydney, Australia, October 21-24, 2013.
[30] QNAP2 (Queueing Network Analysis Package, v.2) User's Guide. SIMULOG, 1992.

Competencia Entre Operador Primario y Secundario con Alquiler de Espectro y Suscripción Óptima de Espectro por Parte de los Usuarios

Julián Romero y Luis Guijarro
Departamento Comunicaciones,
Universitat Politècnica de València (UPV)
Camino de Vera s/n, 46022 Valencia, España
jurocha@upvnet.upv.es y lguijar@dcom.upv.es

***Resumen*—Se platea un escenario donde un operador dueño de una licencia se enfrenta al ingreso de un nuevo operador que quiere alquilar parte de su espectro para competir en el mercado de telefonía móvil. Éste escenario se desarrolla utilizando la Teoría de Juegos planteando un juego de dos etapas. En la primera etapa ambos operadores juegan un juego simultáneo de un solo disparo para determinar los precios que anuncian y debe cumplir el equilibrio de Nash. En la segunda etapa los usuarios determinan la cantidad de espectro que deben suscribir utilizando el equilibrio de Wardrop, el juego de dos etapas se resolvió por inducción hacia atrás.**

Los resultados muestran las condiciones bajo las cuales existe un perfecto equilibrio, y dos escenarios se identifican en función de la cantidad de espectro que está disponible. Los resultados se evaluaron desde el punto de vista de los beneficios de los operadores, desde el bienestar del usuario y del bienestar total. Con base en esta evaluación, se justifica la intervención de una autoridad reguladora para imponer la entrada de un operador.

***Palabras Clave*—equilibrio de Nash, equilibrio de Wardrop, espectro alquilado, radio cognitiva, teoría del juegos.**

I. Introducción

En la mayoría de los países, la utilización del espectro es gestionada y supervisada en el marco internacional establecido por los Estados Miembros en la Unión Internacional de Telecomunicaciones (UIT), utilizando el sistema tradicional de gestión, llamado de comando y control [1], pero esta gestión implica una rigidez que no facilita el uso eficiente del espectro, por lo que se han planteado tecnologías que permitan usar de manera más eficiente este espectro.

La FCC (Federal Communications Commission) [2] demostró que gran parte del espectro asignado está infrautilizado y propuso replantear las actuales arquitecturas de redes inalámbricas utilizando la Radio Cognitiva (RC) [3]. Un dispositivo de RC es un sistema de radiofrecuencia capaz de variar sus parámetros de transmisión basándose en su interacción con el entorno en el que opera, en este trabajo se estudiara un entorno que implementa la compartición del espectro radioeléctrico.

Nos centramos Operador Principal (PO) que compra una licencia dándole el derecho exclusivo de utilizar el espectro para atender los usuarios de telefonía móvil, y un operador móvil virtual o Operador Secundario (SO) que alquila una fracción de espectro del PO. El SO ingresa después en el mercado y suponemos que ha desplegado una nueva tecnología que permite un uso más eficiente del espectro que el utilizado por el PO. Los usuarios pueden suscribir con el operador que deseen y la cantidad de espectro que más les convenga.

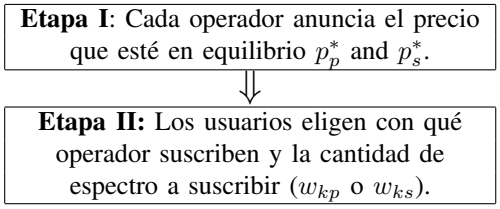


Fig. 1. Juego de Dos Etapas

Utilizando la teoría de juegos [4] se diseña un juego de dos etapas mostrado en la Fig. 1. El juego en cada una de las etapas se resuelve por inducción hacia atrás, lo que significa que en la segunda etapa los jugadores actúan estratégicamente anticipando la solución del juego de la primera etapa.

El principal aporte de este trabajo es el planteamiento de un nuevo modelo donde los usuarios son capaces de escoger el espectro a suscribir y con qué operador suscribe, y obtenemos como resultados: la elección de precio de los operadores que compiten entre sí, los beneficios de los operadores, la asignación de recursos equitativa y previsible para los usuarios, los casos donde es posible el ingreso de un nuevo operadores, las mejoras que tienen los usuarios y los operadores con el ingreso de un nuevo operador y se obtiene siempre que el bienestar social mejora cuando un nuevo operador ingresa en el mercado, dado el escenario que plantearemos.

A. Trabajos Relacionados

Existe varios trabajos que estudian la interacciones entre los operadores de redes cognitivas y los usuarios (por ejemplo [5], [6], [7], [8], [9]), en [5], [6] y [7] se estudia un escenario donde un nuevo operador alquila parte de espectro a un operador propietario de una licencia, pero solo se estudia la elección de los usuarios y no la cantidad de espectro que suscriben, en este trabajo utilizamos el modelo económico para saber cuál es la cantidad de espectro que demandan todos los usuarios y poder tener una expectativa de lo que debe alquilar el SO. En [8] se plantea el juego entre los usuarios y se determina la cantidad de espectro a suscribir y el operador a suscribir un servicio, pero es un escenario donde dos operadores alquilan espectro a un operador con licencia y compiten entre sí con la misma tecnología solo variando los presupuestos, este escenario no es realista porque no se plantea la competencia del operador ya existente, en nuestro escenario es PO, en [9] es un escenario similar a [8] pero se considera los costos de alquiler simétricos.

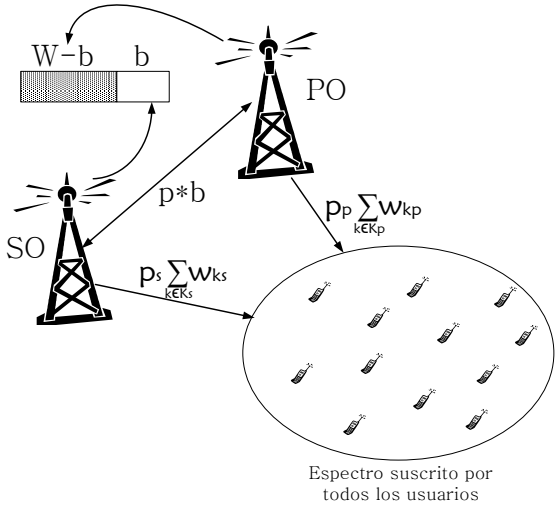


Fig. 2. Escenario

La principal diferencia entre nuestro trabajo y trabajos previos es que se presenta estudio analítico completo que tiene en cuenta el legado del PO y un modelo de compartición del espectro concreto para los usuarios finales.

II. Descripción del Modelo

Se plantea el modelo mostrado en la Fig. 2, donde dos operadores comparten el espectro, el PO dueño de una licencia de espectro W KHz presta un servicio de telefonía móvil, y SO que no tiene espectro de frecuencia se plantea alquilar parte del espectro de PO para competir en el mercado. El SO alquila una cantidad de espectro b KHz al PO y tendrá que pagar un precio por este alquiler p u.m. (unidades monetarias) por KHz. El PO se queda con el resto de espectro para competir por los usuarios es decir $W - b$ KHz. Asumiremos que b ya ha sido determinada y se conoce.

Los usuarios deben realizar un pago por suscribir a un servicio, está dado como el precio por unidad de espectro que anuncia el operador (p_p o p_s) multiplicado por la cantidad de espectro que el usuario suscribe (w_{kp} o w_{ks}).

Para desarrollar este escenario se utiliza el modelo de competencia de *Bertrand* [4], en el que las empresas fijan el precio y dejan que el mercado determine la cantidad que se vende, utilizando un juego simultáneo de un solo disparo para determinar los precios que anuncian se resolverá la elección de precio cumpliendo el equilibrio de *Nash* [4] que dice: *Existe un equilibrio, si la elección de un operador es óptima dada la elección del otro operador, por tanto ningún operador puede mejorar sus condiciones mediante un cambio en su elección*.

Cuando todos los usuarios (K) conocen los precios (p_p y p_s) determinan la cantidad de espectro que desean suscribir (w_{kp} y w_{ks}), esta elección debe cumplir el principio de *Wardrop* [10] que dice: *Existe un equilibrio, si ningún usuario puede reducir unilateralmente sus tiempos (costos) de viaje, mediante un cambio de ruta (camino).*

El escenario se desarrolla en un juego de dos etapas mostrado en la Fig.1 y se resuelve por inducción hacia atrás puesto que se utiliza el modelo de competencia de Bertrand y los operadores necesitan conocer las decisiones de los usuarios para poder determinar los precios que deben anunciar. En la segunda etapa asumimos que p_p y p_s se conocen y con los resultados obtenidos se resuelve la primera etapa.

A. Segunda Etapa

En esta etapa cada usuario determina:

- El operador con el que suscribe un servicio.
- La cantidad de espectro que suscribe (w_{kp} o w_{ks}).

La decisión de los usuarios se resuelve con la función de utilidad [5] que permite asignar un número a todas las posibles elecciones de un usuario de tal forma que la elección del usuario tiene el número mayor, en este modelo está dada como la relación entre la velocidad de datos que recibe un usuario al suscribir un servicio (r_k) y el pago del usuario por el servicio.

Los usuarios comparten espectro de frecuencia, asumiendo los mecanismos basados en la compartición del espectro para los usuarios FDM o OFDM para evitar interferencias mutuas. Con estos mecanismos de compartición de espectro cada usuario k recibe un espectro w_k donde $\sum_k w_k = W$, por tanto, la velocidad de datos que alcanza un usuario es [11]:

$$r_k(w_{kp}) = w_{kp} \cdot \ln\left(1 + \frac{P_{kp}^{max} h_{kp}}{n_o w_{kp}}\right) \tag{1}$$

$$r_k(w_{ks}) = w_{ks} \cdot \ln\left(1 + \frac{P_{ks}^{max} h_{ks}}{n_o w_{ks}}\right) \tag{2}$$

Donde $P_{k(p,s)}^{max}$ es la potencia de trasmisión máxima de un usuario (k) con el operador que suscribe, $h_{k(p,s)}$ es la ganancia del canal de un usuario (k) con el operador que suscribe y n_o es la potencia de ruido por unidad de espectro. Por simplicidad se crea una relación de la tecnología de un operador con un usuario (g_k) es el margen que hay entre la potencia de la señal que se transmite y la potencia del ruido que la corrompe de un usuario, se asume que $g_{ks} > g_{kp}$ porque SO es un operador nuevo y su tecnología será mejor: $g_{kp} = P_k^{max} \frac{h_{kp}}{n_o}$ y $g_{ks} = P_k^{max} \frac{h_{ks}}{n_o}$.

Dado g_k decimos que la relación señal a ruido con respecto a un usuario que suscribe con un operador está dada como: $\text{SNR}_p = g_{kp}/w_{kp}$ y $\text{SNR}_s = g_{ks}/w_{ks}$, $\text{SNR} \gg 1$ en el equilibrio como se demostrará más adelante. Se desprecia el 1 de las Ec. 1 y 2 con lo cual se obtiene una expresión simplificada de r_k con la que se trabajará:

$$r_k(w_{kp}) = w_{kp} \cdot \ln\left(g_{kp}/w_{kp}\right) \tag{3}$$

$$r_k(w_{ks}) = w_{ks} \cdot \ln\left(g_{ks}/w_{ks}\right) \tag{4}$$

Conociendo las Ec. 3 y 4 se obtiene la función de utilidad que percibe un usuario (u_k) con un operador:

$$u_k(p_p, w_{kp}) = w_{kp} \cdot \ln\left(g_{kp}/w_{kp}\right) - p_p \cdot w_{kp} \tag{5}$$

$$u_k(p_s, w_{ks}) = w_{ks} \cdot \ln\left(g_{ks}/w_{ks}\right) - p_s \cdot w_{ks} \tag{6}$$

Aplicamos el principio de *Wardrop* a este escenario como: Existe un equilibrio de usuario, si ningún usuario puede aumentar su función de utilidad variando la cantidad de espectro a suscribir o mediante un cambio de operador, por tanto los usuarios suscriben el espectro que maximice la función de utilidad y con el operador que les genere una mayor función de utilidad.

El espectro que suscribe un usuario es el que maximice la ecuación 5 y 6, obteniendo:

$$w_{kp}^*(p_p) = \arg\max_{w_{kp} \geq 0} u_k(p_p, w_{kp}) = g_{kp} e^{-(1+p_p)} \tag{7}$$

$$w_{ks}^*(p_s) = \arg\max_{w_{ks}\geq 0} u_k(p_s, w_{ks}) = g_{ks}e^{-(1+p_s)} \quad (8)$$

La elección óptima del espectro que debe suscribir un usuario con un operador determinado es $w_{kp}^*(p_p)$ y $w_{ks}^*(p_s)$, asumiendo que los usuarios tienen el presupuesto para suscribir dicha cantidad de espectro. Obtenemos que $\text{SNR}_p = e^{(1+p_p)}$ y $\text{SNR}_s = e^{(1+p_s)}$.

Reemplazando las Ec. 7 y 8 en las Ec. 5 y 6 se obtiene:

$$u_k(p_p, w_{kp}^*) = u_{kp} = g_{kp}e^{-(1+p_p)} \quad (9)$$

$$u_k(p_s, w_{ks}^*) = u_{ks} = g_{ks}e^{-(1+p_s)} \quad (10)$$

Como se dijo los usuarios suscriben con el operador que perciban una mayor función de utilidad, entonces si $u_{kp} > u_{ks}$ los usuarios prefieren suscribir con el PO, si $u_{kp} = u_{ks}$ los usuarios les es indiferente con qué operador suscriban ya que ambos operadores les ofrecen la misma función de utilidad, asumimos que los usuarios se dividen en partes iguales y si $u_{kp} < u_{ks}$ los usuarios suscriben con el SO.

1) Oferta y Demanda de los Operadores [4]:

La demanda de un operador (D) es el espectro que todos los usuarios quieren suscribir con él, en este modelo están dadas como:

$$D_p = \sum_{k\in K_p} w_{kp}^* = \begin{cases} Kw_{kp}^* & si\ u_{kp} > u_{ks} \\ \frac{K}{2}w_{kp}^* & si\ u_{kp} = u_{ks} \\ 0 & si\ u_{kp} < u_{ks} \end{cases} \quad (11)$$

$$D_s = \sum_{k\in K_s} w_{ks}^* = \begin{cases} 0 & si\ u_{kp} > u_{ks} \\ \frac{K}{2}w_{ks}^* & si\ u_{kp} = u_{ks} \\ Kw_{ks}^* & si\ u_{kp} < u_{ks} \end{cases} \quad (12)$$

Donde K_p y K_s son el conjunto de usuarios que desean suscribir con PO y SO respectivamente.

Se asume que todos los usuarios que suscriben con un operador tienen las mismas características tecnológicas, entonces $g_{kp} = g_p$ y $g_{ks} = g_s$, por tanto, $w_{kp}^* = w_p^*$, $w_{ks}^* = w_s^*$, $u_{kp} = u_p$ y $u_{ks} = u_s$.

La oferta de un operador es la cantidad de espectro que el operador está dispuesto a alquilar a los usuarios, en nuestro modelo la oferta del PO es $W - b$ y la del SO es b.

Si la oferta de un operador es menor que la demanda que tiene el operador entonces no va a poder atender a todos los usuarios que desean suscribir con él, por esto utilizamos el concepto de demanda realizada (Q) que es el total de la demanda generada por el conjunto de usuarios que logran suscribir el servicio (K_p^R y K_p^R), es decir:

$$Q_p = \min(W - b, D_p) = \sum_{k\in K_p^R} w_p^* \quad (13)$$

$$Q_s = \min(b, D_s) = \sum_{k\in K_s^R} w_s^* \quad (14)$$

La demanda realizada depende de la decisión de los usuarios y de la oferta que tiene cada operador, tenemos:

1) Si $u_p > u_s$, todos los usuarios prefieren suscribir con el PO, de las Ec. 11, 12, 13 y 14, tenemos que:
   - Si $W - b \geq D_p$, el PO tiene la oferta para cubrir D_p, y el SO no tendrá demanda que atender, tenemos:
     $$Q_p = \min(W - b, D_p) = D_p \qquad Q_s = 0$$
   - Si $W - b < D_p$, el PO no tiene la oferta para cubrir D_p, y el SO podrá atender aquellos usuarios que el PO no alcanzo a cubrir, tenemos:
     $$Q_p = \min(W - b, D_p) = W - b$$
     Tenemos que saber cuántos usuarios atendió el PO para saber cuántos usuarios puede atender el SO, esto se obtiene despejando K_p^R de $Q_p = K_p^R g_p e^{-(1+p_p)} = W - b$, y luego se obtiene K_s dado que $K_s = K - K_p$. Obtenemos la D_s después de que el PO atendiera a los K_p^R usuarios:
     $$D_s' = \left(K - \frac{W-b}{g_p}e^{(1+p_p)}\right) g_s e^{-(1+p_s)}$$
     $$Q_s = \min(b, D_s') = \begin{cases} b & si \quad W < D_p \\ D_s' & si \quad W \geq D_p \end{cases}$$
     Podemos observar que la demanda realiza del SO (Q_s) depende de los recursos del PO ($W - b$).
2) Si $u_p = u_s$, los usuarios que desean suscribirse les es indiferente con que operador lo hagan, de las Ec. 11, 12, 13 y 14, tenemos que:
   $$Q_p = \begin{cases} W - b & si \quad W < 2D_p \\ 2D_p - b & si \quad b < D_p,\ W \geq 2D_p \\ D_p & si \quad b \geq D_p,\ W \geq 2D_p \end{cases}$$
   $$Q_s = \begin{cases} b & si\ W < 2D_p \\ 2D_p - (W - b) & si\ W - b < D_p,\ W \geq 2D_p \\ D_p & si\ W - b \geq D_p,\ W \geq 2D_p \end{cases}$$
   Se observa que la demanda realizada de un operador depende de la oferta de él y también de la oferta del otro operador.
3) Si $u_p < u_s$, obtenemos la demanda realizada de los operadores de igual forma que en $u_p > u_s$:
   - Si $b \geq D_s$, tenemos:
     $$Q_s = \min(b, D_s) = D_s \qquad Q_p = 0$$
   - Si $b < D_s$, tenemos:
     $$Q_s = \min(b, D_s) = b$$
     $$D_p' = \left(K - \frac{b}{g_s}e^{(1+p_s)}\right) g_p e^{-(1+p_p)}$$
     $$Q_p = \min(W - b, D_p') = \begin{cases} W - b & si\ W < D_s \\ D_p' & si\ W \geq D_s \end{cases}$$
     Podemos observar que la demanda realiza del PO (Q_p) depende de los recursos del SO (b).

Conociendo las decisiones de los usuarios, la demanda y oferta de los operadores se procede a resolver la primera etapa.

B. Primera Etapa

En esta etapa se determinan los precios que deben anunciar los operadores. Cada operador anunciará un precio óptimo que esté en *equilibrio de Nash* [4], el cual dice que los precios de los operadores están en equilibrio si la elección de un operador es óptima dada la del otro operador. Ninguno de los dos operadores sabe que hará el otro cuando tenga que elegir su propio precio, pero sí puede tener una expectativa sobre lo que elegirá el otro operador, se maneja la expectativa que los

operadores eligen el precio que maximiza sus beneficios (π). Definimos los beneficios π como:

$$\pi = Ingresos - Costes$$

El ingreso [4] es el precio de un bien multiplicado por la cantidad vendida de dicho bien, en nuestro modelo el ingreso de un operador por parte de los usuarios es el precio por suscribir un servicio (p_p o p_s) multiplicado por la cantidad vendida de dicho servicio (Q_p o (Q_s). El PO obtiene ingresos por la cantidad de espectro alquilada al SO, están dados como $p \cdot b$, estos ingresos los asumimos constantes.

Los costes [4] es el valor monetario de todos los factores que intervienen en la producción del servicio, en nuestro modelo se expresan como C_p y C_s y los asumimos constantes. Pero el SO tiene un coste adicional por el alquiler de b.

Conociendo los ingresos y los costes de los operadores se obtienen las funciones de beneficio:

$$\pi_p = I_p + pb - C_p = p_p Q_p + pb - C_p \quad (15)$$

$$\pi_s = I_s - (pb + C_s) = p_s Q_s - (pb + C_s) \quad (16)$$

Se plantea un juego de precios para resolver la competencia entre operadores.

1) Juego De Precios:

La competencia entre los dos operadores, define el siguiente juego:

- Jugadores: PO y SO
- Estrategia: Los operadores pueden escoger el precio que deseen $p_p = [0, \infty)$ y $p_s = [0, \infty)$.
- Objetivo: Los jugadores anunciarán los precios que maximice sus beneficios y estén en equilibrio (p_p^* o p_s^*).

Como se mencionó anteriormente los operadores tienen la expectativa que su competidor anunciará el precio que maximice sus beneficios. Para determinar cuál es éste precio se estudia a continuación la estrategia de precios óptima para un Operador Monopolista (MO) y estos precios se definirá como la expectativa que tiene un operador de como actuará su competidor.

* ***Estrategia de precios óptima para un*** MO***:***

Si los operadores anuncian un par de precios que generan $u_p \neq u_s$ todos los usuarios suscriben con el operador que les genere una mayor utilidad, entonces el mercado está dominado por un único operador y elegirá un precio que maximice sus beneficios.

En la Fig. 3 se muestra el comportamiento de los ingresos por parte de los usuarios (I_m) de un MO, se observa como varían los I_m cada vez que el precio del MO (p_m) varía. Sabemos que $D_m = G_m e^{-(1+p_m)}$, dado $G_m = Kg_m$.

El MO tiene una cantidad fija de espectro (B_m) y los I_m están dados por: $I_m = p_m \cdot \min(B_m, G_m e^{-(1+p_m)})$. La estrategia de precios óptima para un MO es:

- Si $B_m < G_m e^{-2}$, el MO esta en régimen de baja oferta dado que si anuncia un $p_m = 1$ la oferta es menor que la demanda ($B_m < D_m(p_m = 1)$), en la Fig. 3 es $B_m^{'}$, es óptimo para MO elegir el precio tal que la oferta sea igual a la demanda:

$$p_m(B_m) = \ln\left(\frac{G_m}{B_m}\right) - 1$$

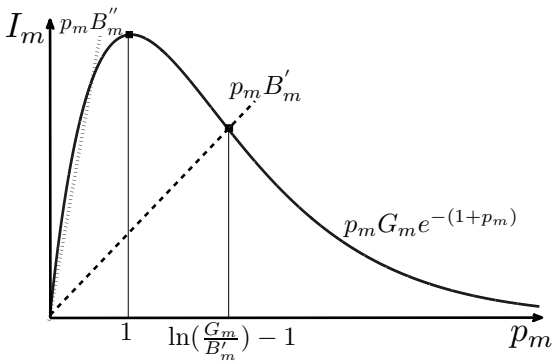


Fig. 3. Ingresos de un operador Monopolista

- si $B_m \geq G_m e^{-2}$, el MO esta en régimen de alta oferta dado que si anuncia un $p_m = 1$ la oferta es mayor que la demanda ($B_m \geq D_m(p_m = 1)$), en la Fig. 3 es $B_m^{''}$, entonces $I_m = p_m G_m e^{-(1+p_m)}$ y el MO nunca anunciaría un $p_m < 1$. Es óptimo elegir:

$$p_m(B_m) = 1$$

Definimos el p_m como la expectativa que tiene un operador con respecto al otro. Conociendo p_m se estudiará cuáles son los precios en equilibrio que deben anunciar los operadores que compiten entre sí.

** ***La estrategia de precios para la competencia entre operadores:***

Se estudiará cuál es el precio de equilibrio que deben anunciar los operadores cuando compiten en un mercado. En el siguiente análisis se estudiarán todos los posibles equilibrios de precios que existan cuando: $u_p < u_s$, $u_p = u_s$ o $u_p > u_s$ en cada una de las posibles regiones.

- *Estrategia de precios cuando $u_p < u_s$:*

Los precios que cumplen esta condición son: $p_p > p_s + \ln\left(\frac{g_p}{g_s}\right)$, el SO actúa como un MO. Los π_p dependen directamente de si el SO tiene o no el espectro suficiente para cubrir D_s, pero los π_s no depende de los recursos de PO, entonces de la Fig. 4 solo se utilizan los siguientes intervalos: $b > G_s e^{-2}$, $b \leq G_s e^{-2}$ y $W - b \geq 0$.

En II-A1 se dijo que: $D_p = 0$, $D_s = G_s e^{-(1+p_s)}$, $Q_p = \min(W - b, D_p^*)$ y $Q_s = \min(b, D_s)$. Se estudian los casos para determinar si existe equilibrio en estos intervalos:

(A) $b \geq G_s e^{-2}$, el SO esta en régimen de alta oferta entonces es óptimo anunciar $p_s = 1$ cubriendo toda la demanda preferida. Se obtiene: $I_s = D_s$ y $I_p = 0$. El PO debe disminuir su precio para lograr aumentar la u_p pero el SO siempre puede tener un precio menor que el PO. Ambos operadores disminuirán su precio hasta que el PO se salga de esta condición o $p_p^* = 0$ y como el SO aun puede disminuir más su precio se obtiene:

* Si $\ln(g_s/g_p) < 1$, entonces el SO anunciaría: $p_s = \ln(g_s/g_p) - \varepsilon$, donde ε es un numero pequeño mayor que cero, no existe ningún equilibrio en estos precios porque siempre existe un valor ε' que cumpla que: $0 < \varepsilon' < \varepsilon$, por tanto los operadores no encuentran un precio exacto que puedan anunciar.

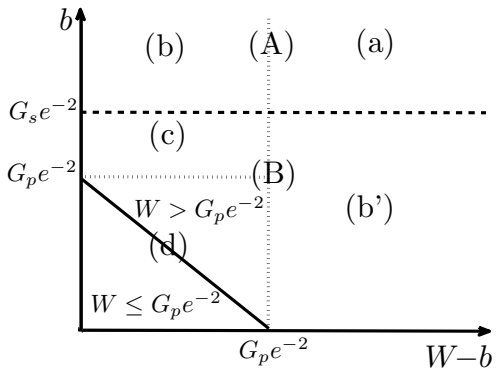


Fig. 4. Diferentes Regiones

- Si $\ln(g_s/g_p) > 1$, entonces el SO anunciaría: $p_s^* = 1$, **existe un equilibrio en estos precios** porque ningún operador puede variar su precio y aumentar sus ingresos de forma unilateral.

(B) $b \leq G_s e^{-2}$, el SO esta en régimen de baja oferta entonces es óptimo anunciar un precio tal que la oferta total sea igual a la demanda total, es decir, $b = D_s$ y se obtiene $p_s = \ln(G_s/b) - 1$, pero este precio vuelve a dejar al PO sin demanda, entonces el PO debe disminuir su precio para lograr aumentar la u_p, como el SO siempre puede tener un precio menor que el PO, ambos operadores disminuirán su precio hasta que PO se salga de esta condición o $p_p^* = 0$, como p_s aun puede disminuir más su precio, se obtiene:

- Si $\ln\left(\frac{g_s}{g_p}\right) < \ln\left(\frac{G_s}{b}\right) - 1$, entonces el SO anunciaría: $p_s = \ln\left(\frac{g_s}{g_p}\right) - \varepsilon$, no existe ningún equilibrio en estos precios porque siempre existe un valor $0 < \varepsilon' < \varepsilon$.
- Si $\ln\left(\frac{g_s}{g_p}\right) > \ln\left(\frac{G_s}{b}\right) - 1$, o lo que es lo mismo que $b > G_p e^{-1}$, entonces el SO anunciaría: $p_s^* = \ln\left(\frac{G_s}{b}\right) - 1$, **existe un equilibrio en estos precios** porque ningún operador puede variar su precio y aumentar sus ingresos de forma unilateral.

- *Estrategia de precios cuando $u_p > u_s$:*
  Aplicando los mismo argumentos que en la competencia cuando la $u_p < u_s$ para cada uno de los casos se llegan a unas conclusiones simétricas, la principal diferencia radica que $p_p < p_s + \ln(g_p/g_s)$, entonces SO disminuirá su precio para aumentar la u_s hasta salirse de esta condición ya que $p_s > p_p$.
  Nunca existe un equilibrio de precios con $u_p > u_s$, porque el SO tiene una mejor tecnología, lo cual permite que el SO varié el precio y logre que los usuarios perciben una función de utilidad mayor.
- *Estrategia de precios cuando $u_p = u_s$:*
  Los precios que cumplen esta condición son: $p_p = p_s + \ln(g_p/g_s)$, en II-A1 se dijo que: $D_p = D_s$, $Q_p = \min(W - b, D_p + \max(D_s - b, 0))$ y $Q_s = \min(b, D_s + \max(D_p - (W - b), 0))$.
  En este caso los recursos de ambos operadores influyen en los ingresos del otro, por esta razón es necesario los intervalos de ambos operadores, además se necesitará el caso donde ambos precios son mayores a 1 para esto se utiliza el intervalo del menor que es el del PO, obteniendo la Fig. 4.

(a) $W - b \geq G_p e^{-2}$ y $b \geq G_s e^{-2}$, en este caso ambos operadores están en régimen de alta oferta, por tanto si anuncian un precio igual a la unidad cada operador tiene los recursos suficientes para cubrir todo el espectro demandado por los usuarios. Ambos operadores quieren disminuir un poco el precio para quedarse con la demanda total. El p_p disminuirá hasta $p_p = 0$ y p_s aun puede disminuir más su precio sin ser inferior a cero, entonces anunciarían $p_p = 0$ y $p_s = \ln(g_s/g_p)$.
No existe ningún equilibrio de precios ya que el SO obtiene mayores ingresos disminuyendo su precio, porque si $p_s' = p_s - \varepsilon$ logra que la $u_p < u_s$ y por tanto quedarse con $D_s = G_s e^{-(1+p_s)}$ aumentado sus ingresos de forma unilateral.

(b) $W - b < G_p e^{-2}$ y $b \geq G_s e^{-2}$, el SO esta en régimen de alta oferta y el PO esta en régimen de baja oferta. Se puede utilizar los mismos argumentos que se aplicaron en la región (a) y se llegará a que no existe equilibrio de precios.

(b') $W - b \geq G_p e^{-2}$ y $b < G_s e^{-2}$, el PO esta en régimen de alta oferta y el SO esta en régimen de baja oferta , el PO tiene el incentivo de disminuir su precio para quedarse con toda la demanda, ambos operadores bajaran su precio hasta que el $p_p = 0$ y $p_s = \ln(g_s/g_p)$. No existe ningún equilibrio de precios ya que el PO obtiene mayores ingresos aumentando su precio y quedándose con la demanda que el SO no alcanza a cubrir, variarán siempre su precio sin encontrar equilibrio.

(c) $W - b < G_p e^{-2}$ y $G_p e^{-2} \leq b < G_s e^{-2}$, ambos operadores están en régimen de alta oferta, en este caso el precio óptimo es aquel que haga a la oferta igual a la demanda total, por tanto los operadores anunciarán $p_p = \ln(\frac{G_p}{W-b}) - 1$ y $p_s = \ln(\frac{G_s}{b}) - 1$, entonces $b = G_s e^{-(1+p_s)}$ y $W - b = G_p e^{-(1+p_p)}$, es decir ambos operadores tienen los recursos para cubrir toda la demanda y sucede lo mismo de la región (a), variarán sus precios sin encontrar ningún equilibrio.

Se demuestra que existe un equilibrio de precio cuando la oferta total sea igual a la demanda total, para esto es necesario que ambos operadores tengan que anunciar precios superiores a 1, porque si esto no sucede el operador con un precio inferior a 1 va aumentar sus ingresos anunciando un precio igual a 1. Se trabajará con los intervalos mostrados a continuación:

(d) $W - b \leq G_p e^{-2}$ y $b \leq G_p e^{-2}$, existen las siguientes opciones:

- Si $W > G_p e^{-2}$ el valor máximo de la demanda total en este caso es $\max(D_p + D_s) = G_p e^{-2}$ porque $p_p \geq 1$, entonces $W > D_p + D_s$. Los recursos totales son mayores a la demanda total, no existe un equilibrio de precios porque el operador que tenga mayores recursos va a querer disminuir su precio y de esta forma poder tener una demanda realizada mayor y no encuentran equilibrio de precios.

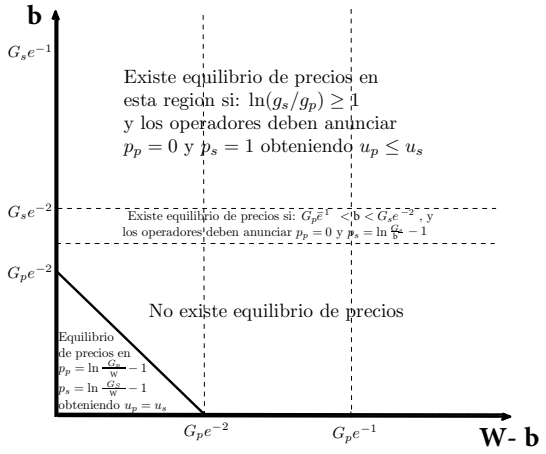


Fig. 5. Equilibrio de precios en cada región

– Si $W \leq G_p e^{-2}$ entonces $W < D_p + D_s$, los operadores no tienen los recursos suficientes para cubrir la demanda total, ambos operadores tienen un incentivo de aumentar su precio ya que ambos operadores no son capaces de cubrir la demanda total, se aplica el *principio de equilibrio [4]* que dice: "los precios se ajustan hasta que la cantidad que demandan los individuos de una cosa es igual a la que se ofrece", en nuestro modelo es la demanda total igual a la oferta total, es decir que $W = D_p + D_s$ y entonces no podrán aumentar su precio sin que disminuya la demanda realizada.
Se concluye que existe un equilibrio cuando aumentan su precio y logran que se cumpla que $W = D_p + D_s$, puesto que ningún operador puede variar su precio para aumentar sus beneficios de forma unilateral. $W = D_s + D_p = G_s e^{-(1+p_s)} = G_p e^{-(1+p_p)}$, obtenemos los precios que deben anunciar los operadores: $p_p^* = \ln(G_p/W) - 1$ y $p_s^* = \ln(G_s/W) - 1$

En la Fig. 5 se muestra donde existe los equilibrios de precios dependiendo de los recursos que tiene cada operador.

En la Tabla I se muestran los resultados del juego de dos etapas y conociendo esto se procede a evaluar el escenario.

Tabla I
SOLUCIÓN AL JUEGO DE DOS ETAPAS

Recursos de los Operadores	Precios Anunciados por los Operadores	Elección de suscripción de un usuario	Espectro óptimo que suscribe un usuario
$\ln(g_s/g_p) \geq 1$ $b > G_p e^{-1}$ $b \geq G_s e^{-2}$	$p_p^* = 0$ $p_s^* = 1$	$u_p < u_s$ Suscriben con el SO	$w_p^* = g_p e^{-1}$ $w_s^* = g_s e^{-2}$
$b > G_p e^{-1}$ $b < G_s e^{-2}$	$p_p^* = 0$ $p_s^* = \ln \frac{G_s}{b} - 1$	$u_p < u_s$ Suscriben con el SO	$w_p^* = g_p e^{-1}$ $w_s^* = \frac{b}{K}$
$W \leq G_p e^{-2}$	$p_p^* = \ln \frac{G_p}{W} - 1$ $p_s^* = \ln \frac{G_s}{W} - 1$	$u_p = u_s$ Suscriben con PO o SO	$w_p^* = \frac{W}{K}$ $w_s^* = \frac{W}{K}$

III. RESULTADOS

Se evalúa como se benefician los usuarios con la entrada de SO en el mercado y una forma de medirlo es con la función de bienestar de los usuarios (UW) [4], la cual permite conocer las preferencias sociales a partir de las preferencias de los individuos, en este modelo consiste en sumar las utilidades de los diferentes consumidores:

$$UW = \sum_{k \in K_p^R} u_p + \sum_{k \in K_s^R} u_s \tag{17}$$

Otra expresión para medir el bienestar es el PoA (Price of Anarchy) se relaciona con el concepto de función de bienestar social [4] (SW). La SW se calcula como la suma de las utilidades de todos los agentes del sistema, es decir usuarios y operadores, obteniendo:

$$SW = \sum_{k \in K_p^R} u_p + \sum_{k \in K_s^R} u_s + \pi_p + \pi_s \tag{18}$$

El PoA se define como el cociente entre el valor máximo de SW y SW en el equilibrio de Nash, $PoA = \max(SW)/SW$, si la SW es máxima entonces el $PoA = 1$.

A partir de las expresiones de la Tabla I y las Ec. 15, 16, 17 y 18, vamos a modelar la competencia entre los operadores teniendo en cuenta los parámetros K, g_p, g_s, W, C_p, C_s y p, se manejan valores utilizados en Long Term Evolution (LTE) y de esta forma ver cuáles son los resultados en escenarios posibles. LTE [12] soporta hasta 200 $usuarios$ activos por celda con $5MHz$ de espectro.

Se plantearon dos escenarios, en cada uno existe un equilibrio de precios que cumple las expresiones de la Tabla I.

A. Escenario 1

Los valores para modelar este escenario son:
$K = 150 usuarios$, $W = 2500KHz$, $g_p = 140$, $g_s = 400$, $C_p = 500u.m.$, $C_s = 300u.m.$, $p = 0.8u.m./KHz$. Trabajando sobre las expresiones de la Tabla I estamos en la región donde $W \leq G_p e^{-2}$, se evalúa el comportamiento del escenario variando el espectro alquilado por el SO (b) y se muestra en la Fig. 6. Se observa que:

- Los precios de los operadores dependen de W, G_p y G_s, estos parámetros son constantes del sistema, por tanto p_p^*, p_s^*, w_p^*, w_s^* y UW son constante sin importar el espectro que alquile el SO.
- Las utilidades se representan en $u_p = u_s = 1.67$, esto lo podemos realizara porque la función de utilidad permite poner un orden en la elección, y nos interesa saber cuál utilidad percibida por el usuario es mayor y no en qué cantidad lo es.
- Los beneficios de los operadores dependen directamente de b, como se muestra en las Ec.15 y 16, obteniendo que:

$$\frac{\partial \pi_p}{\partial b} = p - p_p^* \qquad si \begin{cases} p > p_p^* & \pi_p \ \ es\ creciente \\ p < p_p^* & \pi_p \ \ es\ decreciente \end{cases}$$

$$\frac{\partial \pi_s}{\partial b} = p_s^* - p \qquad si \begin{cases} p > p_s^* & \pi_s \ \ es\ decreciente \\ p < p_s^* & \pi_s \ \ es\ creciente \end{cases}$$

Los π_p son decreciente entonces el PO no tiene ningún incentivo para alquilar, este hecho sugiere que el PO debe ser obligado a alquilar una cantidad mínima de espectro con el fin de mejorar el bienestar social.

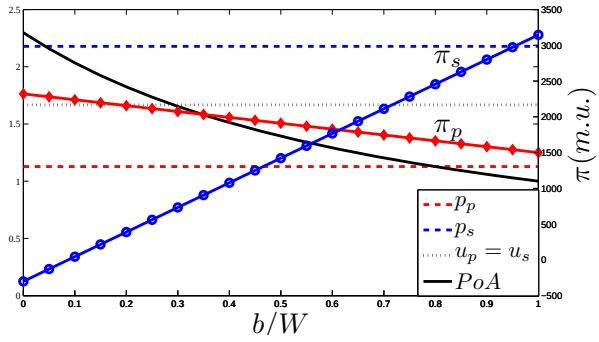


Fig. 6. Equilibrio del escenario 1 variando b/W

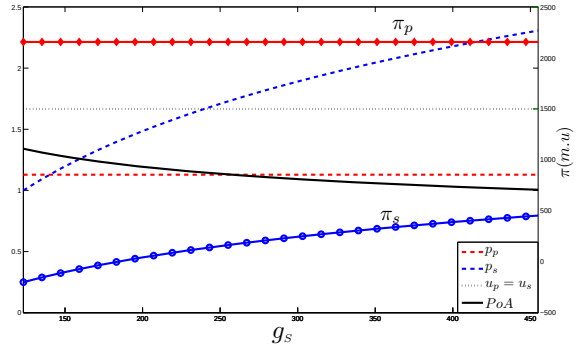


Fig. 7. Escenario 1 con b/Wconstante y variando g_s

El SO desea que b sea lo más grande posible ya que π_s es creciente.

- La SW tiene el máximo $(PoA = 1)$ en $b/W = 1$ ya que π_s crece en una mayor proporción que decrece π_p y por tanto $\pi_p + \pi_s$ aumenta entre mayor es b.
- $\text{SNR}_p = 8.4$ y $\text{SNR}_s = 24$, cumpliendo con $\text{SNR} \gg 1$.
- El valor mínimo de usuarios que deben suscribir para que exista un equilibrio de precios es: $K \geq e^2 W/g_p = 131.9\ Usuarios$.

Se concluye que está justificada una intervención reguladora que establezca un valor mínimo de espectro alquilado para acercarse al máximo de bienestar social y que exista una libre competencia entre los operadores.

1) Comportamiento del escenario variando g_k: El valor mínimo que utilizaremos de g_s es el que permite estar en la zona de equilibrio: $g_s \geq e^2 W/K = 123.15$. Se variara desde $123.15 < g_s < 455$, para esto se tomara un valor de $b/W = 0.2$ y lo representamos en la Fig. 7, obteniendo que:

- El p_s^* y π_s aumenta de manera logarítmica porque depende de la características tecnológicas del SO (g_s), el valor mínimo de p_s es $p_s^* = 1$.
- El p_p^* y π_p son constantes porque no depende de g_s.
- El $PoA = 1$ se encuentra en el máximo valor de g_s.

Se concluye que entre mejor sean g_s mayor van a ser sus π_s dado que los usuarios desean suscribir un mayor espectro.

B. Escenario 2

En este escenario se aumentaran los recursos que tienen los operadores para que tengan una oferta mayor a la demanda y cumplan las condiciones de la regiones donde $b > G_p e^{-1}$ mostradas en la Tabla I, el resto de valores se mantendrán iguales: $W = 20000 KHz$.

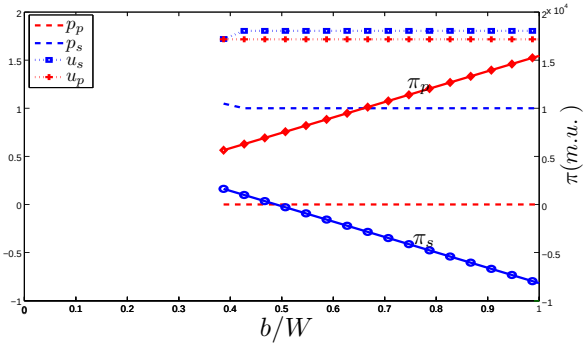


Fig. 8. Equilibrio del escenario 2 variando b/W

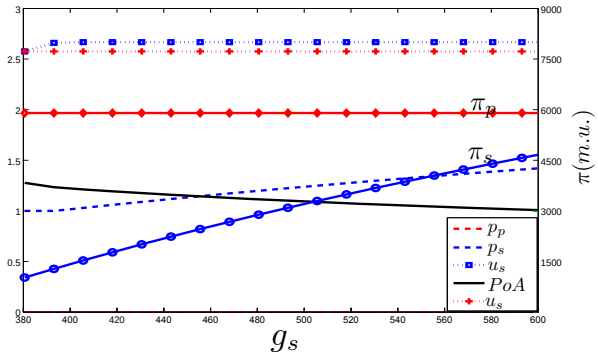


Fig. 9. Escenario 2 con b/Wconstante y variando g_s

Dado estos parámetros se evalúa el comportamiento de este escenario variando b, mostrado en la Fig.8, se observa que:

- Los precios de los operadores en este escenario depende de b, g_p y g_s, puesto que tiene que cumplirse las condición mostrada anteriormente.
- Cuando $b/W < 0.386$ no existe equilibrio de precios, excepto cuando $b/W = 0$ si esto sucede el PO actúa como MO y debe anunciar $p_p^* = 1$, obteniendo $u_p = 18.947$ y $\pi_p = 2342\ u.m.$, esto es un caso puntual ya que si $b/W > 0$ los operadores empiezan a competir y buscan el equilibrio de precios. Cuando $0.386 < b/W < 0.406$ el equilibrio se encuentra en $G_p e^{-1} < b < G_s e^{-2}$ y el operador disminuirá su precio entre mayores recursos tenga hasta llegar a $p_s^* = 1 m.u/KHz$ y ya estará en el equilibrio de precios cuando $b > G_s e^{-2}$, se ve que el PO siempre tiene un $p_p^* = 0$ y que no puede hacer nada para obtener una mayor utilidad, esto sucede porque $g_s > g_p$.
- El $PoA = 1$ se alcanza en $b/W \geq 0.406$, si la autoridad regulatoria quiere un máximo de bienestar social debe permitir que se alquile como mínimo esta cantidad de espectro.
- Los usuarios perciben una menor función de utilidad con el PO y por tanto no le demanda espectro entonces solo tiene ingresos por el alquiler de espectro al SO, por tanto π_p aumenta cada vez que alquila mayor espectro. π_s decrece entre mayor es el espectro alquilado, porque el SO alquila más de lo que le demandan y se convierte en un espectro que no le genera ingreso. Es óptimo para el SO alquilar el mínimo de espectro en el que exista un equilibrio de precios. Para el PO es óptimo alquilar la mayor parte de espectro.

Se concluye que está justificada una intervención reguladora, donde se debe establecer un valor mínimo y máximo de espectro alquilado para acercarse al máximo de bienestar social y que exista una libre competencia entre los operadores.

1) Comportamiento del escenario variando g_k: El valor mínimo de g_s es el que permita estar en la zona de equilibrio: $g_s \geq g_p e^1 = 380.56$, se varía desde $380.56 < g_s < 600$, para esto se tomara un valor de $b/W = 0.4$ en el que existe un equilibrio, se representa en la Fig. 9, obteniendo que:

- El PO siempre es constante porque no depende de g_s, mientras que SO mejora cada vez que aumenta g_s.
- En este equilibrio sucede que $u_p < u_s$ y el PO no puede cambiarlo porque $g_p < g_s$, obteniendo $I_p = 0$.
- El $PoA = 1$ se encuentra en el máximo de g_s.

Se concluye que entre mejor sean g_s mayor van a ser sus π_s dado que los usuarios demanda un mayor espectro.

IV. CONCLUSIONES

La interacción entre los operadores que compiten entre sí por los usuarios de telefonía móvil se analiza y se desarrolla en un juego de dos etapas. Teniendo en cuenta el análisis de los resultados realizados en un mercado donde la oferta de los operadores es limitada, se puede concluir que:

1) Con la entrada de un nuevo operador en el mercado los usuarios no aumentan la función de bienestar de los usuarios pero pueden realizar una elección: si pagar un mayor precio por mayor por obtener una mayor velocidad de datos, es decir suscribir con el nuevo operador o suscribir con el operador primario que cobra menos por alquilar el mismo espectro pero se obtiene una menor velocidad de datos, esta elección la realizaría según sus limitaciones presupuestarias.
2) La función de bienestar social mejora entre mayor es el espectro alquilado por el nuevo operador, pero los beneficios del operador primario disminuye cada vez que aumenta el espectro alquilado por el operador entrante ya que el precio que cobra al nuevo operador por el alquiler de espectro es menor que el precio que anuncia a los usuarios para que suscriban el servicio.
   Está justificada la intervención de una autoridad reguladora, para que establezca un valor mínimo de espectro alquilado y de esta forma mejorar la función de bienestar social y que exista una libre competencia entre los operadores.
3) La mejora de tecnología por parte de un operador le permite cobrar un mayor precio por un servicio y obtendrá mayores beneficios, por ende una mayor función de bienestar social y los usuarios perciben una mayor velocidad de datos.

Si los recursos que tienen los operadores son altos de tal forma que se encuentran en régimen de alta oferta se puede concluir que:

1) Existe un equilibrio de precios solo si la cantidad de espectro alquilada por el operador entrante cubre todo el espectro demandado por los usuarios y si mejora las características tecnológicas de tal forma que cumpla con que: $\ln(g_s/g_p) > 1$, en este caso todos los agentes del sistema (operadores y usuarios) obtienen una mejora con el ingreso, es decir aumenta la función de bienestar social y la función de bienestar de los usuarios lo que hace que este modelo sea viable y que tanto a los operadores como los usuarios les convenga el ingreso de un nuevo operador.
2) Los ingresos de operador primario solo son por el alquiler de espectro al operador entrante, aumentan sus beneficios porque al operador entrante los usuarios le demanda una cantidad mayor de espectro debido a la mejora de las características tecnológica. Al operador entrante le interesa alquilar la cantidad de espectro que sea igual al espectro que demanda los usuarios y de esta forma obtener mayores beneficios.
   Está justificada la intervención de una autoridad reguladora, para que establezca un valor mínimo y máximo de espectro que pueda alquilar y de esta forma mejorar la función de bienestar social, la función de bienestar de los usuarios y que exista una libre competencia entre los operadores. .
3) La entrada de un nuevo operador sólo es posible si se mejora las características tecnológicas utilizada por el operador primario, si esto no sucede no es posible encontrar un equilibrio en este mercado.

En próximos trabajos tenemos la intención de ampliar el análisis a un juego de tres etapas, en la nueva etapa se resolverá la negociación entre los operadores y de esta forma determinar la cantidad de espectro alquilado por el nuevo operador.

AGRADECIMIENTOS

Quiero agradecer el trabajo al continuo apoyo que me ha dado mi director Luis Guijarro, también agradecerle al grupo GIRBA y al programa de Formación del Personal de Investigador por la gran oportunidad que me están dando para realizar mi investigación.

REFERENCIAS

[1] ITU, "The regulatory environment for future mobile multimedia servicesa", pp. 6, june, 2006.
[2] FCC, "Spectrum Policy Task Force Report", ET Docket, n. 02 155, pp. 6, nov, 2002.
[3] FCC, "Notice of Proposed Rulemaking (NPRM 03 322): Facilitating Opportunities for Flexible, Efficient and Reliable Spectrum agile Radio Technologie", ET Docket, n. 03 108, dec, 2003.
[4] Hal R. Varian, "Microeconomía Intermedia, un enofoque actua", Antoni Bosch, ed. 8, pp. 543–555, 533–534, 544–548, 7–13, 290–291, 390, 660–664, 2, 2010.
[5] L. Guijarro, V. Pla, B. Tuffin, P. Maille and J. R. Vidal, "Competition and bargaining in wireless networks with spectrum leasing", IEEE Globecom, Houston (2011).
[6] L. Guijarro, V. Pla and J. R. Vidal , "Competition in cognitive radio networks: spectrum leasing and innovation", IEEE Consumer Communications and Networking Conference (CCNC), jan, Las Vegas (2011).
[7] J. Bae, E. Beigman, R. Berry, M. Honig, Fellow, and R. Vohra "Sequential bandwidth and power auctions for distributed spectrum sharing",IEEE Journal On Selected Areas In Communications, Vol. 26, No. 7, Sep 2008
[8] Duan, L, Huang, J and Shou, "Competition with dynamic spectrum leasing.", Proc. of Dyspan, Singapore (2010).
[9] J. Jia and Q. Zhang, "Competitions and dynamics of duopoly wireless service providers in dynamic spectrum market.", ACM MobiHoc, 2008.
[10] J. Wardrop, "Some theoretical aspects of road traffic research", Proc. of the Institute of Civil Engineers 1, pp. 325–378, 1952.
[11] J. Baei, E. Beigmang, R. A. Berry and M. L. Honig, "Sequential bandwidth and power auctions for distributed spectrum sharing", IEEE Journal on Selected Areas in Communications, vol. 26, n. 7, 2008.
[12] Motorola Inc, "Long Term Evolution (LTE): A Technical Overview", Motorola Inc, july, 2007.

Uso de canales solapados en una red de área de campus inalámbrica con IEEE 802.11

Ester Mengual, Eduard Garcia-Villegas, Rafael Vidal.
Departament d'Enginyeria Telemàtica
Universitat Politècnica de Catalunya·BarcelonaTech
Esteve Terradas, 7 - 08860 Castelldefels
ester.mengual@gmail.com, eduardg@entel.upc.edu, rvidal@entel.upc.edu.

***Resumen*- Las redes de área local inalámbricas (WLAN) basadas en la familia de estándares IEEE 802.11 utilizan mayoritariamente la banda industrial científica y médica (ISM) de 2,4GHz en la que compiten con un número cada vez mayor de dispositivos. En aquellos escenarios con una mayor densidad de puntos de acceso, esta situación puede derivar en un rendimiento de las celdas WLAN por debajo sus expectativas en condiciones ideales. En este artículo se estudia un escenario real de este tipo: un campus universitario con cerca 200 puntos de acceso y bajo condiciones de tráfico real. En primer lugar, se seleccionan y determinan una serie de parámetros radio con el fin de caracterizar el escenario en términos de carga e interferencias. Este objetivo se consigue a partir de la interacción con las herramientas de gestión de la propia red. A continuación, se implementa una solución de asignación de canales dinámica que interacciona con las mencionadas herramientas de gestión. La gestión de canales implementada se basa en un algoritmo resultado de investigaciones anteriores que, como aspecto novedoso, tiene en cuenta los canales solapados parcialmente. Para terminar, se presentan una serie de pruebas obtenidas del escenario real que permiten demostrar cómo esta aproximación mejora el rendimiento de la tradicional asignación con tres canales ortogonales (i.e. 1, 6 y 11).**

***Palabras Clave*- asignación de canales, estándares IEEE 802.11, gestión de espectro radio, Wireless LAN**

I. INTRODUCCIÓN

Las redes sin hilos de área local (WLANs) IEEE802.11 [1] utilizan las bandas sin licencia de uso médico, científico e industrial (ISM) de 2,4 GHz y 5GHz para los dispositivos que siguen el estándar IEEE 802.11bgn e IEEE 802.11an, respectivamente. En la banda de 2,4GHz se definen, dependiendo de la regulación de la zona, entre 11 y 13 canales WLAN 802.11. Las frecuencias centrales de estos canales están separadas por 5MHz pese a tener un ancho de banda cercano a los 20MHz (22MHz en el caso del 802.11b). En consecuencia, sólo tres de estos canales no se solapan, de manera que el número de comunicaciones cercanas que pueden tener lugar simultáneamente sin sufrir interferencias significativas está limitado a tres. Esta situación se traduce en una selección de canales típica por parte de los administradores de red: los canales ortogonales, llamados así por no estar solapados, 1, 6 y 11 (ver Fig. 1).

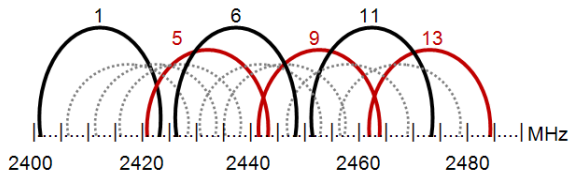


Fig. 1.División de la banda ISM de 2,4GHz en 13 canales.

En caso de poder utilizar 13 canales (e.g. dominio ETSI), los administradores pueden optar también por los canales 1, 5, 9 y 13 que, si bien están parcialmente solapados, sufren de una interferencia que puede considerarse tolerable frente al beneficio de ganar un canal adicional.

La disponibilidad de 3 ó 4 canales en entornos densos es claramente insuficiente. Tómese como ejemplo el despliegue de puntos de acceso Wi-Fi (APs) existente en el escenario objeto de estudio en este artículo, un campus universitario con más de 200 APs; tal y como se describe en la sección II, se trata de una red gestionada con una solución de la empresa Cisco Systems en la que se asignan los canales ortogonales 1, 6 y 11 para todos los APs gestionados y en la que cada AP tiene, de promedio, 14 vecinos aunque se necesitarían un mínimo de 16 canales ortogonales para evitar las interferencias entre ellos.

Este escenario, típico por otro lado, da lugar a la aparición de interferencias co-canal que pueden comportar el retardo en las transmisiones para evitar colisiones, de acuerdo al mecanismo de acceso al medio utilizado (CSMA/CA) en 802.11 [1]. Una posible solución a este problema sería el uso de la banda ISM de 5GHz. Esta banda dispone de una porción de espectro mayor que la de 2,4GHz, lo que se traduce en un mayor número de canales ortogonales y, por tanto, en la posibilidad de un mayor número de transmisiones concurrentes sin sufrir los mencionados problemas de interferencia y contención. Como contrapartida, al tratarse de frecuencias más elevadas, sufre de mayores pérdidas de propagación, lo que deriva en menores áreas de cobertura. Por si fuera poco, en Europa los dispositivos 802.11an deben evitar interferir con radares meteorológicos y con radioenlaces satelitales, "usuarios" preferentes de esta banda.

Estas circunstancias hacen que la banda de 2,4GHz sea todavía la más utilizada para desplegar WLANs y que las estrategias de gestión/asignación de los canales sean consideradas un aspecto clave en su despliegue y objeto de estudio frecuente [2], destacando inicialmente aquellos trabajos que utilizan algoritmos y heurísticas basados en la mencionada asignación de canales ortogonales y que en escenarios densos inevitablemente van a suponer una reducción de las prestaciones de las celdas 802.11.

Para cambiar esta situación es necesario cambiar la premisa inicial, es decir, utilizar toda la banda disponible, incluyendo los canales parcialmente solapados. Esta nueva premisa deriva en la aparición de interferencias por canal adyacente (ACI). Estas interferencias, que dependen de la intensidad de la señal y de la distancia entre canales,

degradan la relación señal a ruido e interferencias (SNIR) aumentando el número de errores en recepción. Este tipo de interferencia puede ser menos o más dañina que la interferencia co-canal dependiendo de diferentes factores que deben tenerse en cuenta si se quiere realizar una gestión eficiente de los recursos radio.

En [3] y [4] se estudia la ACI en WLANs IEEE 802.11abg. Más concretamente, en [3] se propone un modelo para cuantificar la degradación de las comunicaciones 802.11 bajo el impacto de la interferencia, teniendo en cuenta la utilización de la fuente interferente y su energía en la porción solapada del canal. El objetivo del modelo era evaluar los efectos de las interferencias sobre la capacidad de los enlaces 802.11.

Tanto [3] como [4] concluyen que los canales parcialmente solapados son un recurso útil cuando el número de canales no solapados disponible es pequeño y la densidad de celdas WLAN 802.11 es alta. A partir de estos artículos, otros trabajos han considerado también el uso de canales parcialmente solapados (como [5] y [6]); sin embargo ninguno de ellos presenta resultados en un escenario real. Por otro lado, se debe tener en cuenta que el uso de canales parcialmente solapados puede empeorar el rendimiento de la red si no se realiza siguiendo una gestión inteligente de los canales, tal y como se detalla en [7].

En [8], los APs intercambian una colección de estadísticas bien con un controlador centralizado, o bien de manera distribuida. Estas estadísticas son la base para construir un "grafo de interferencias ponderado" que es coloreado utilizando un conjunto de canales disponibles (incluyendo aquellos parcialmente solapados).

La contribución del presente artículo es doble. En primer lugar se realiza una implementación de la solución propuesta en [8] siguiendo una aproximación centralizada. En segundo lugar, se evalúa esta aproximación mediante medidas en un escenario real: una WLAN de campus con cerca de 200 APs compitiendo en la banda de 2,4GHz. Una evaluación que demuestra que, si las interferencias por canal adyacente y co-canal se consideran de manera adecuada, el empleo de una estrategia inteligente de gestión de los canales minimiza las colisiones así como los errores de transmisión, mejorando la capacidad de la red y la experiencia del usuario. Enfatizar que se trata de la primera implementación de la que tienen noticia los autores de un algoritmo de este tipo y de su evaluación en una red en explotación de estas características.

Como paso previo para conseguir estos objetivos se realiza un estudio pormenorizado de la solución de gestión existente en el escenario analizado. Este estudio permite tanto identificar los parámetros que permiten caracterizar el escenario, como obtener sus valores y presentar una implementación de la solución propuesta compatible con el sistema de gestión existente.

El resto del artículo se estructura de la siguiente manera. En la sección II se describe y caracteriza el entorno de pruebas y la solución de gestión que utiliza; en la sección III se describe la implementación del mecanismo alternativo de asignación de canales; en la sección IV se describen las pruebas realizadas y se comentan los resultados, y para terminar, las conclusiones (sección V) cierran el artículo.

II. DESCRIPCIÓN DEL ESCENARIO

El estudio que este artículo presenta se ha realizado en el Campus del Baix Llobregat (CBL) de la Universitat Politècnica de Catalunya (UPC-BarcelonaTech). Este campus aloja escuelas de ingeniería, varios centros de investigación, edificios de servicios (biblioteca, restaurante, etc.) así como alojamientos para estudiantes. A pesar de poder considerarse un campus pequeño (~30 hectáreas), es un escenario perfecto para llevar a cabo este estudio ya que consta de una red Wi-Fi de más de cien APs que compiten con una gran cantidad de APs ajenos (*rogue*[1]), lo que la convierte en una red lo suficientemente densa y compleja como para realizar experimentos interesantes en un entorno real.

En la Fig. 2 se muestra el grafo de interferencias que describe la red. Cada punto del grafo representa uno de los APs gestionados por nuestro sistema (nótese que los APs *rogue* se han omitido para mejorar la visibilidad del grafo); y cada enlace entre dos nodos indica que un nodo está dentro del área de cobertura del otro y viceversa. Como se puede observar, el mapa creado a partir de las interferencias entre los APs de la red describe un escenario caótico que sin duda requiere una gestión de recursos automática.

De acuerdo con la información recopilada en el grafo que muestra la Fig. 2 (véase la sección III para más detalles), cada AP tiene una media de 14 APs vecinos, de los cuales 6 son APs *rogue*. El mayor número de vecinos visto por un AP es de 26. El diagrama de la Fig. 3 sirve para ampliar estos datos estadísticos al mostrar la probabilidad con la que un AP recibe interferencias de un determinado número de vecinos. Se observa que ambos tipos de fuentes interferentes (APs vecinos y APs *rogue*) siguen una distribución diferente, aunque en ambos casos el grado de dispersión es alto; la probabilidad de sufrir interferencias de dos o menos APs *rogue* es alta, mientras que el número de APs vecinos es más probable que sea superior a seis (85%). Esta diferencia se puede explicar por el hecho que los APs *rogue* se concentran

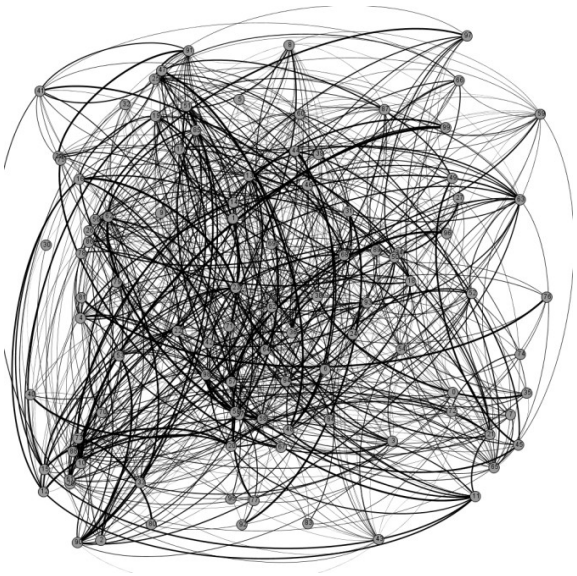


Fig. 2.Grafo de interferencias de la red Wi-Fi del campus.

[1] AP *rogue* hace referencia a cualquier AP instalado sin el consentimiento del propietario de la red; y por tanto, no queda bajo la gestión del administrador de dicha red.

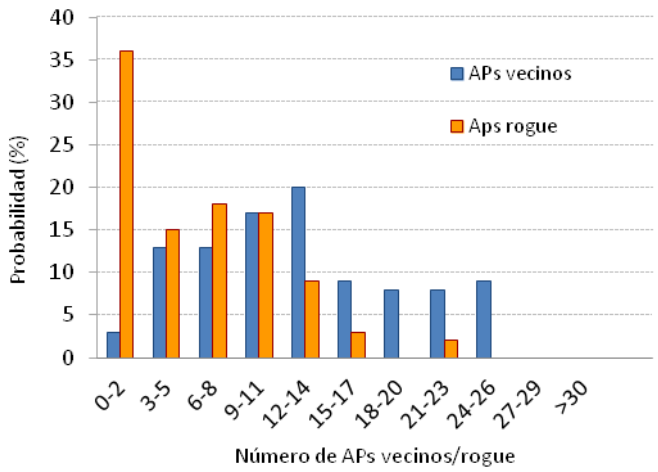


Fig. 3. Distribución de APs vecinos/rogue interferentes

en determinadas zonas, mientras que los APs de la red propia se distribuyen más homogéneamente para proporcionar cobertura a todo el campus.

El número y el tamaño de los cliques[1] también ayudan en la descripción de un escenario representado por un grafo. En este caso, el número clique del grafo de interferencias es 16; en otras palabras, serían necesarios un mínimo de 16 canales ortogonales para evitar por completo las interferencias en este escenario. Por otra parte, el tamaño de clique más frecuente es de 5 ó 6 APs.

A. *Estudio del tráfico en la red*

Además de analizar la red del campus en base a los dispositivos instalados, es necesario también estudiar su utilización en términos de tráfico. El objetivo principal del estudio es detectar los periodos de máxima actividad, puesto que son los momentos en que más necesaria es la presencia de una gestión inteligente de los recursos radio. Para hacerlo, se ha dedicado una etapa a su análisis, y esto ha permitido definir un perfil de tráfico que revelase las características más destacadas, incluyendo los momentos de máxima actividad.
La Fig. 4 y la Fig. 5 pertenecen a la interfaz de administración de la propia controladora LAN inalámbrica (WLC). La Fig. 4 muestra la evolución del tráfico cursado en el enlace de subida (azul) y en el enlace de bajada (naranja) durante una semana. Se observa que el comportamiento es similar día tras día. Más concretamente, se pueden apreciar dos picos de tráfico diarios ligeramente variables: uno por la mañana y otro por la tarde. Además, en la Fig. 4 se puede observar, en que la red soporta una carga significativa solo en los días de actividad en el campus (días laborables). La Fig. 5 muestra la evolución del uso de la red durante las horas de un día laborable. En este gráfico se aprecia que los picos de tráfico se dan alrededor de las 13:00 y las 19:00, aproximadamente. En ambas figuras también es visible el hecho de que el tráfico de bajada (*downlink*) es notablemente superior al de subida (*uplink*). La relación es aproximadamente de uno a tres.
Partiendo de la información recopilada, se ha definido un patrón que se repite a diario, que revela los momentos con mayor número de usuarios simultáneos y tráfico ofrecido. Por eso, será alrededor de cada pico cuando se ponga a prueba la gestión eficiente de recursos radio, ya que bajo estas circunstancias los beneficios serán más apreciables.

B. *Arquitectura WLAN*

La WLAN del Campus está basada en dispositivos Cisco Systems y sigue una arquitectura conocida como Cisco Unified Wireless Network Architecture [9]. Esta arquitectura centralizada se basa en la conexión de APs ligeros (LAPs) a un dispositivo central (controladora LAN inalámbrica o WLC) que establecen comunicación a través de protocolos como LWAPP o CAPWAP [10].
Los modelos de los APs y la controladora instalados en el escenario bajo estudio son 1142N y 1131G; y WLC 4404, respectivamente. Los LAPs están conectados físicamente a la controladora a través de una VLAN de tipo Fast Ethernet conmutada. Al estar gestionados por un dispositivo central, utilizan direcciones IP privadas, de manera que no son accesibles desde fuera de la VLAN, a diferencia de la WLC, que también cuenta con una IP de dominio público.

Arquitectura centralizada Split-MAC

El protocolo LWAPP (IETF RFC 5412) nació con el fin de facilitar la gestión centralizada de LAPs y su configuración automática, pero ha evolucionado con el tiempo hacia CAPWAP (IETF RFC 5415). Además de facilitar la comunicación entre WLCs y LAPs, a través de este protocolo también se gestiona la configuración, firmware, transacciones de control y transacciones de datos de todos los LAPs gestionados de forma centralizada. Para ello, se utiliza un

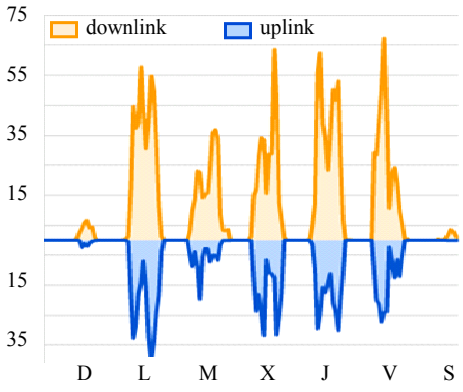


Fig. 4. Tráfico semanal en el campus (en Mbps)

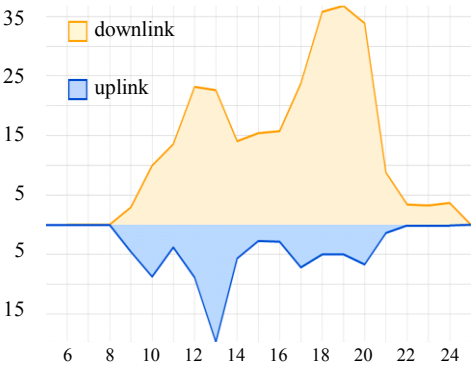


Fig. 5. Tráfico diario en el campus (en Mbps)

[1] En teoría de grafos, se llama clique al subconjunto de un grafo en el que todos los vértices están conectados entre sí. El número clique de un grafo es el tamaño del mayor clique dentro de ese grafo.

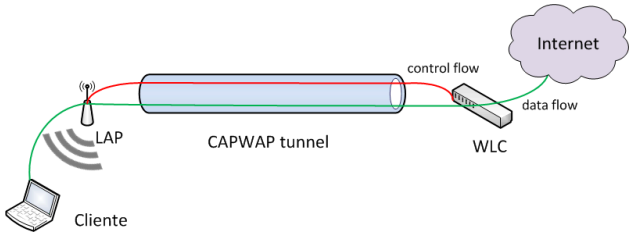


Fig. 6. Arquitectura centralizada Split MAC

canal de "control" para la gestión de los LAPs y su configuración; y un canal de "datos" para la transmisión de tráfico de usuario entre las dos entidades.

CAPWAP también define un protocolo de descubrimiento que permite a los LAPs asociarse automáticamente a una WLC. En este proceso, el LAP envía una petición y espera a recibir una respuesta de la WLC. Desde ese momento, la WLC se hace responsable de la gestión del LAP en cuestión, e incluso puede redirigirlo a otra WLC.

Una de las claves principales de este tipo de arquitectura es el concepto *Split MAC* (ver Fig. 6). Esta funcionalidad se basa en que la WLC administra parte del funcionamiento del protocolo 802.11 (funciones de distribución e integración), mientras que otras partes son administradas por el propio LAP (funcionalidades MAC). En concreto, es responsabilidad de la WLC: la gestión de seguridad, de la configuración y funciones sin requisitos temporales estrictos (asociación, des-asociación, gestión de claves de encriptación, etc.); y es responsabilidad de cada LAP: la encapsulación y des-encapsulación de datos vía CAPWAP, la fragmentación y re-ensamblado de tramas y las funciones con requisitos temporales estrictos (generación de *beacon*, mensajes de control, etc.) [11]. Entre las operaciones llevadas a cabo por la WLC se incluye la selección de canales dinámica (DCA).

Todas estas funciones requieren constantemente un intercambio de mensajes entre la WLC y los LAPs. Tanto la información de control como de datos se envían a través de mensajes UDP mediante sesiones seguras DTLS.

Gestión de canales

La gestión de canales realizada por la WLC parte de la obtención de estadísticas desde los LAPs gestionados. Básicamente, la WLC tiene en cuenta el número de LAPs de la propia red que interfieren con cada LAP gestionado y la intensidad de la señal recibida de cada uno. El DCA también tiene en cuenta información sobre la carga de cada LAP para minimizar los cambios de canal de los LAPs más utilizados. Es decir, la WLC cambiará con menos frecuencia el canal de un LAP muy cargado que el de un LAP poco utilizado. En su configuración por defecto, la WLC solo asigna los canales 1, 6 y 11 (2412, 2437 y 2462MHz, respectivamente).

La WLC calcula una nueva asignación cada 10 minutos, pero solo será aplicada si se prevé mejorar 15dB la relación señal/ruido (SNR) del peor AP.

III. SOLUCIÓN IMPLEMENTADA

El esquema que se muestra en la Fig. 7 describe la arquitectura general del sistema. El mecanismo que se propone, incluye un módulo de comunicaciones para interactuar con la WLC y un módulo que incluye el algoritmo encargado de la asignación de canales, como se muestra a continuación:

A. *Módulo de comunicaciones*

El esquema de gestión centralizada de canales que este artículo presenta consiste en un sistema basado en Linux que establece periódicamente comunicación SNMP con la controladora. La comunicación SNMP tiene como finalidad recoger estadísticas y proporcionar la asignación de canales más apropiada según el algoritmo propuesto en [8]. El proceso se divide en varias etapas.

En primer lugar, se ha dedicado una etapa al estudio de la utilización de la red con el propósito de localizar los momentos de máxima actividad y decidir cuándo poner a prueba la gestión eficiente de recursos radio (véase la sección II.A.). Las estadísticas SNMP se han recogido cuatro veces al día en momentos que permitan evaluar la información relativa a cada pico de tráfico. De esta manera, se logrará optimizar el funcionamiento de la red en las horas punta a través de las nuevas asignaciones de canales sugeridas por el algoritmo.

La controladora central permite acceso SNMP a un conjunto de parámetros útiles para el propósito que se sigue. Esos parámetros son objetos de la MIB Airespace-Wireless-MIB[1], un módulo MIB destinado a controladoras WLAN de Cisco que proporciona información sobre el estado y la configuración de los LAPs administrados por esa WLC. Las estadísticas que se recogen incluyen los siguientes datos para cada LAP:

- Contadores MAC: las estadísticas de la capa 2 como pueden ser el número de tramas enviadas / recibidas, el número de retransmisiones, errores CRC, etc. (véase la sección IV para más detalles).
- Vecinos: se construye una lista de APs potencialmente interferentes y la intensidad de señal que se recibe de ellos (RSSI). Incluye la información correspondiente a los objetos *bsnAPIfRxNeighborsTable, bsnRogueAPTable* y *bsnRogueAPAirespaceAPTable*.
- Carga: se guarda información sobre el porcentaje de tiempo que un AP está ocupado debido a la recepción o transmisión de paquetes. Esta información es accesible en el subconjunto *bsnAPIfLoadParametersTable*.

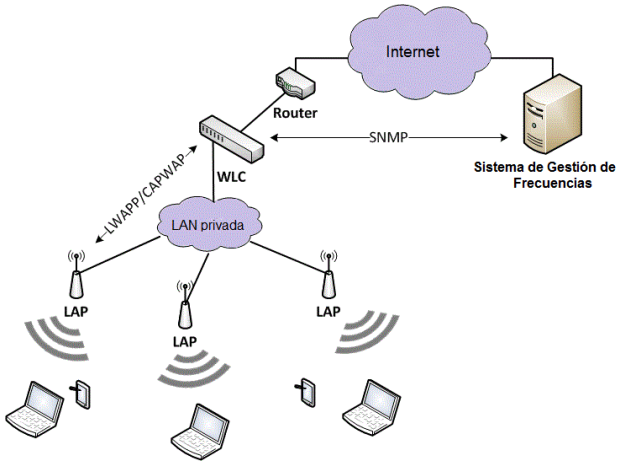


Fig. 7. Arquitectura del sistema propuesto

[1] http://www.oidview.com/mibs/14179/AIRESPACE-WIRELESS-MIB.html

B. Algoritmo

La nueva asignación de canales se lleva a cabo diariamente por la noche, coincidiendo con el momento del día de menor actividad en la red. Esta asignación es decidida en base a un algoritmo existente [8].

En primer lugar, se extrae una lista de vecinos a través de la controladora. Este listado se usa para construir un grafo de interferencias como el de la Fig. 2 que, a su vez, incluye información sobre carga y niveles de RSSI con los que se proporcionan diferentes pesos a los enlaces del grafo. Es importante señalar que, a pesar de que los APs *rogue* están fuera del control del sistema de gestión centralizado y no se les puede asignar un canal diferente, estos APs están presentes en el grafo de interferencias ya que su existencia sí es detectada y se conocen datos como el canal de trabajo y la intensidad de señal con la que un LAP los recibe.

Una vez construido el grafo de interferencias ponderado, la información contenida en él se usa como entrada para el algoritmo, que resuelve el problema de asignación frecuencial asignando canales a los LAPs gestionados, de manera que se maximiza una determinada métrica, dando prioridad a los LAPs con más carga y con más vecinos (i.e. se empieza asignando un canal libre al LAP más utilizado). La métrica que el algoritmo tiene como objetivo modela la capacidad potencial de cada uno de los LAPs que se gestionan en la red teniendo en cuenta tanto la interferencia co-canal como la de canal adyacente causada por los APs vecinos. El modelo tiene en cuenta que el nivel de interferencia sufrida depende del nivel de utilización (o carga) de los APs vecinos y no solo de la intensidad de señal recibida. Así pues, el algoritmo sólo sugerirá el uso de canales parcialmente solapados cuando el coste asociado a la interferencia co-canal sea mayor a la de canal adyacente, según los modelos mencionados (cf. [8]).

La nueva asignación de canales se transmite desde el módulo de comunicaciones a la WLC a través de comandos SNMP. A su vez, la WLC envía la nueva configuración a cada uno de los LAPs a través del protocolo CAPWAP.

IV. Evaluación

Nuestro sistema estuvo en funcionamiento durante un período de tres semanas en el escenario descrito en II. Durante ese tiempo se analizaron las estadísticas pertinentes para obtener una medida cuantificable de su rendimiento. Como referencia se había medido previamente, también durante tres semanas, el rendimiento de la gestión automática de canales que por defecto proporciona el WLC de Cisco (Cisco DCA). Dado que los beneficios de una buena estrategia de gestión de los recursos radio en una WLAN son visibles sobretodo en condiciones de carga elevada, sólo medimos el rendimiento durante las horas punta de los días laborables (véase la sección II.A.) de los veinte "peores" APs.

En la evaluación de las mejoras proporcionadas por nuestro mecanismo asumimos que, tanto la distribución de usuarios a lo largo y ancho del escenario, como sus requerimientos de recursos radio (i.e. su perfil de tráfico) se mantuvieron estadísticamente similares antes y después de aplicar el mecanismo que proponemos. Como consecuencia, asumimos también que las diferencias en los parámetros de rendimiento observados serán debidas a los cambios en el mecanismo de gestión de frecuencia y no a otros cambios en el escenario, ya que ningún otro aspecto clave de la configuración de la red fue modificado.

A. Distribución de canales

Dado que uno de los puntos claves del sistema propuesto se basa en proporcionar una asignación de canales que incluya canales parcialmente solapados, es interesante examinar cómo se han distribuido los canales de frecuencia durante el período de pruebas, en comparación con el DCA de Cisco.

La Fig. 8 muestra, de color azul claro, la distribución de los canales cuando las tareas de gestión de frecuencias están a cargo de la WLC (recordar que la asignación está restringida a los tradicionales 1, 6 y 11). Sorprendentemente, casi la mitad de los puntos de acceso habían sido configurados en el canal 1. Esto probablemente se debe al hecho de que cuando los LAPs se inician por primera vez, utilizan el primer canal no solapado de la/s banda/s que soportan (canal 1 para 11bg y canal 36 para 11a).

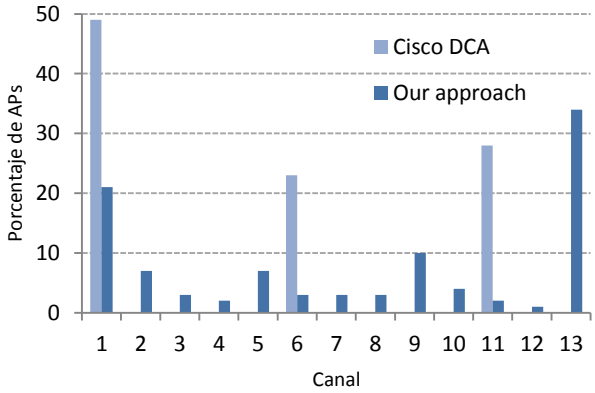


Fig. 8. Número de LAPs en cada canal

Además, la Fig. 8 también muestra cómo la distribución de canales ha cambiado después de ejecutar el sistema durante un tiempo prolongado. Ahora podemos observar que los LAPs utilizan toda la banda disponible (canales 1 a 13). Sin embargo, es interesante observar que la mitad de ellos están trabajando, o bien en el canal 1, o bien en el 13; es decir, los canales situados en los extremos de la banda, donde existe menos interferencia por canal adyacente. En menor medida, también se observan picos en los canales 5 y 9. Este resultado apoya la práctica recomendada de utilizar el conjunto de canales (casi) ortogonales 1, 5, 9 y 13 en zonas donde estén permitidos [3].

Como se ha explicado, la Fig. 8 muestra la distribución inicial y final de canales en el escenario. Sin embargo, también resulta interesante observar cómo ha ido evolucionando dicha distribución durante los días en que el sistema que proponemos ha estado en funcionamiento. La Fig. 9 muestra el número de LAPs en cada canal en diferentes días.

El cambio de estrategia al permitir el uso de canales solapados en el conjunto de LAPs gestionados mediante nuestro sistema tiene también influencia sobre la selección de canales en el conjunto de APs *rogue*. Al principio, la mayoría de APs *rogue* usaban alguno de los tres canales ortogonales, hecho que provocaba que en los primeros días nuestro sistema asignara estos mismos canales (1,6 y 11) a muchos LAPs. Paulatinamente, los APs *rogue* se iban adaptando al cambio de escenario mostrando una mayor distribución sobre todos los canales permitidos y eso, a su vez, provocaba cambios en la asignación proporcionada por nuestro sistema.

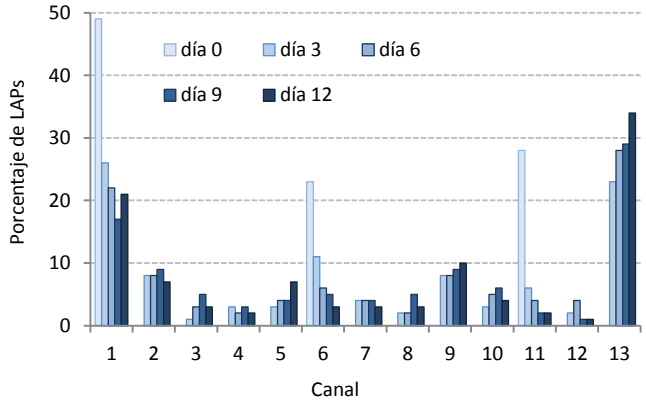


Fig. 9. Evolución de la distribución de canales

B. Medidas de rendimiento

Las mejoras en la gestión de los recursos radio se traducen en una mayor capacidad de la red, que podría ser medida en términos de *goodput* o ancho de banda disponible. Normalmente estas medidas requieren la generación de tráfico de datos suficiente para saturar los recursos disponibles. Este tipo de medidas es posible en entornos de laboratorio mediante el uso de una pequeña maqueta o demostrador y donde la mayoría de variables que pueden tener un impacto sobre la medida están controladas. Sin embargo, en un escenario real con centenares de APs y centenares de usuarios cuyo comportamiento es impredecible, estas medidas de capacidad no son viables, más cuando se nos exige no realizar acciones que puedan afectar al servicio ofrecido por la red. En su lugar monitorizamos pasivamente una serie de estadísticas relacionadas con la tasa de error de paquete (PER).

En un canal radio, un paquete puede no ser recibido correctamente por dos razones: o bien porque éste llegó al receptor sin la energía suficiente para ser decodificado (debido a la distancia emisor/receptor y otros efectos de la propagación), o bien por culpa de interferencias (otras transmisiones simultáneas en frecuencias muy cercanas). Asumiendo que el comportamiento de los usuarios no varía significativamente (su distribución por el escenario y su movilidad), las mejoras en la PER serán debidas a una disminución de la interferencia, que es el objetivo principal de nuestro sistema de gestión de frecuencias.

De entre la gran variedad de estadísticas accesibles vía SNMP, el análisis de tres contadores de la capa MAC proporcionados por la *dot11CountersTable*[1] nos permitirá evaluar las mejoras de nuestro sistema tanto en transmisión, como en recepción para cada LAP. La elección de las estadísticas usadas en la evaluación del sistema ha estado también limitada por la presencia de un *bug*[2] en el firmware de la WLC que provoca que ciertos contadores no se actualicen correctamente.

Mejoras en recepción

Los beneficios medidos en enlaces ascendentes (de estaciones cliente hacia AP) se han analizado a través del contador *FCSErrorCount*, cuyo valor se incrementa por cada trama recibida con errores, según la secuencia de verificación de trama (FCS). Las estaciones transmisoras cuyos paquetes *unicast* son contabilizados por *FCSErrorCount* en el LAP, deberán retransmitir la trama errónea hasta que sea recibida correctamente o hasta agotar el número máximo de retransmisiones (generalmente limitado a 5). La Fig. 10 muestra la variación de esta métrica a lo largo de los días, en comparación con el valor medio medido cuando el sistema DCA de Cisco estaba en funcionamiento. En promedio, al final del período de medición, los veinte "peores" LAPs habían reducido el número de errores FCS a la mitad con respecto a la configuración con DCA.

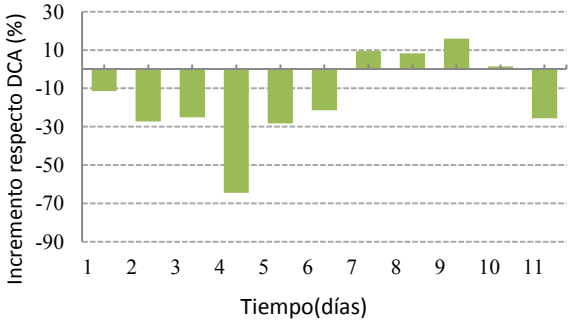


Fig. 10. Evolución diaria del contador *FCSErrorCount*

Mejoras en transmisión

A través de *FailedCount* (Fig. 11) y *MultipleRetryCount* (Fig. 12) hemos sido capaces de medir las mejoras relacionadas con la transmisión en el enlace descendente (desde el AP hacia el usuario Wi-Fi). De entre las estadísticas disponibles relacionadas con la PER, *FailedCount* se podría considerar como el parámetro más crítico, puesto que un aumento de su valor significa un fallo en la transmisión de un paquete a pesar de varios intentos (hasta un máximo de 5, como se menciona anteriormente). En este caso, los cambios aplicados en la asignación de canales hacen que este parámetro experimente una mejora media del 75% (teniendo en cuenta a los veinte peores puntos de acceso).

En cambio, la Fig. 11 muestra cómo *MultipleRetryCount* ha aumentado de manera significativa con respecto al esquema de gestión proporcionado por el DCA (26% de aumento, en promedio). Este contador se incrementa cada vez que una trama es transmitida con éxito desde el LAP tras varias retransmisiones. Aunque estos resultados pueden parecer contradictorios, en realidad son consistentes con una mejora en la PER. La probabilidad de que una trama sea transmitida con éxito tras múltiples intentos (i.e., la probabilidad de que la transmisión de un paquete incremente el contador *MultipleRetryCount*) es:

(1)

la cual, a diferencia de *FCSErrorCount* y *FailedCount*, no disminuye monótonamente con PER. En otras palabras, una mejora en la PER puede verse reflejada igualmente tanto por un aumento, como por una disminución del contador *MultipleRetryCount*, dependiendo de la gama de valores que toma PER. Teniendo en cuenta la mejora en los anteriores

[1] *dot11CountersTable* (OID: 1.2.840.10036.2.2) forma parte del estándar IEEE 802.11 y está, por tanto, soportada por la mayoría de APs comerciales

[2] http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn52xgmr1.html

contadores, podemos concluir que el incremento en *MultipleRetryCount* refleja una mejora de la PER.

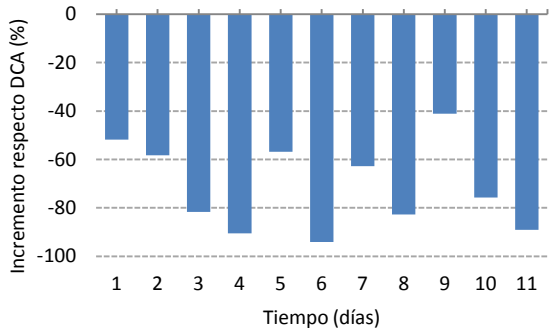


Fig. 11. Evolución diaria del contador *FailedCount*

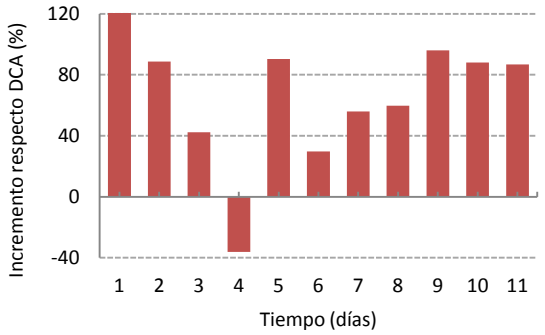


Fig. 12. Evolucion diaria del contador *MultipleRetryCount*

C. *Consideraciones adicionales*

Además de las mejoras evidentes en el rendimiento de la red, otros aspectos deben ser tenidos en cuenta. En primer lugar es importante señalar que el sistema propuesto supone un *overhead* por señalización poco significativo, pese a requerir una gran cantidad de datos vía SNMP. Como se relata en II, nuestro sistema gestor de frecuencias recoge estadísticas sobre los LAPs cuatro veces al día (justo antes y justo después de los dos picos de carga diarios). Cada una de las cuatro consultas supone que la WLC y nuestro gestor de frecuencias intercambian alrededor de 4,5MB de datos (en unos 45.000 paquetes SNMP) durante unos 20s. La asignación de canales se realiza una vez al día, en horario nocturno, coincidiendo con el mínimo de actividad. La cantidad de datos intercambiados durante esta tarea depende del número de LAPs cuyo canal necesita ser modificado. En el peor de los casos, en el que todos los LAPs son modificados, WLC y gestor de frecuencias intercambian alrededor de 40KB; en general, solo el 20% de los LAPs (en promedio) son modificados diariamente.

mal comportamiento del sistema. Esta medida de carácter protector reduce, por otro lado, los beneficios de la asignación dinámica de canales, ya que estas asignaciones no pueden realizarse de manera inmediata como respuesta a los frecuentes cambios de condiciones en la red. En estas condiciones, el plan de frecuencias adoptado para un día se decidía a partir de las características de la red medidas durante el día anterior. Además, el hecho que el número de

Aunque, como se explica en II.A. , el algoritmo DCA recalcula el plan de frecuencias cada 10 minutos, los LAPs cambian su canal, de media, cada 8 días. En nuestro sistema, los LAPs cambian de canal aproximadamente cada cinco días. Idealmente, la frecuencia con la que un AP Wi-Fi modifica su canal de trabajo depende de lo dinámico que sea su entorno, pero cambios de canal muy frecuentes pueden resultar perjudiciales ya que puede suponer la pérdida de conectividad de las estaciones. Ante un cambio de canal, las estaciones asociadas a un AP realizarán un barrido de los canales disponibles hasta dar de nuevo con su AP o hasta encontrar otro AP de la misma red. Esta situación puede implicar la repetición de los procesos de autenticación y asociación [1]. La duración del periodo de desconexión que hemos medido varía entre 0,8 y 4,7s, siendo el peor caso cuando el proceso de autenticación se realiza mediante 802.1X (WPA2 Enterprise). Sin embargo, el uso de la extensión IEEE 802.11h podría reducir aún más el tiempo de desconexión [12], ya que incorpora mecanismos mediante los cuales el AP puede anunciar en próximo cambio de canal con suficiente antelación para que las estaciones asociadas cambien de forma sincronizada el canal de trabajo.

V. Conclusiones y trabajo futuro

En este artículo se ha presentado un sistema de asignación de canales que tiene por objetivo minimizar las interferencias permitiendo el uso de canales parcialmente solapados. El sistema se integra en una arquitectura centralizada de Cisco, con APs ligeros gestionados por una controladora WLAN. En esta arquitectura, nuestro sistema asume una de las tareas del WLC: la gestión de frecuencias. Dejando a un lado este aspecto, la red opera de acuerdo a su configuración por defecto.

A diferencia de la literatura existente, donde la evaluación se basa en simulaciones o en medidas en pequeños demostradores, nuestra propuesta ha sido probada durante varias semanas en un WLAN de campus bajo condiciones de tráfico reales.

La evaluación del rendimiento de la red nos permite concluir que una asignación de canales que tenga en consideración canales parcialmente solapados proporciona mejoras significativas que son más evidentes en los momentos en que la red soporta una mayor carga. El análisis de métricas específicas relacionadas con el nivel contención e interferencia ha proporcionado resultados satisfactorios, tanto en el enlace ascendente, como descendente.

Como el principal objetivo era la implementación de nuestra aproximación en una red real y operativa, hemos tenido que cumplir con diferentes restricciones de acuerdo con los administradores de la red. Cabe destacar que se pudieron recoger estadísticas sin restricciones, pero las nuevas asignaciones de canales sólo podían realizarse una vez al día, en un horario en el que la utilización de la red es mínima. Con ello se pretendía reducir el potencial impacto de un posible

APs afectados por la reconfiguración diaria de los canales es pequeño (<20%), y que las reconfiguraciones sean casi completamente inocuas para los usuarios, nos hacen pensar que nuestro sistema ofrecería un mejor servicio si las asignaciones de canales se realizasen más frecuentemente de manera que fuesen optimas de acuerdo a las necesidades de la red en cada momento.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el Ministerio de Economía y Competitividad del gobierno de España a través del proyecto TEC2012-32531, por el Ministerio de Ciencia e Innovación a través del proyecto TEC2009-11453 y FEDER.

Los autores quieren también hacer explícito su agradecimiento a UPCnet, al delegado del rector de la UPC-BarcelonaTech en el Campus del Baix Llobregat, a los servicios técnicos de este Campus y al director de la Escuela de Ingeniería de Telecomunicación y Aeroespacial de Castelldefels.

REFERENCIAS

[1] IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2012 revision). IEEE-SA. 5 April 2012.

[2] S. Chieochan, E. Hossain and J. Diamond, "Channel assignment schemes for infrastructure-based 802.11 WLANs: A survey," in *Communications Surveys & Tutorials, IEEE , vol.12, no.1*, 2010, pp. 124,136.

[3] E. Garcia, E. López-Aguilera, R. Vidal and J. Paradells, "Effect of adjacent-channel interference in IEEE 802.11 WLANs," in *2nd. Int. Conference of Cognitive Radio Oriented Wireless Networks and Communications, CrownCom'07*, 2007.

[4] A. Mishra, V. Shrivastava, S. Banerjee and W. Arbaugh, "Partially overlapped channels not considered harmful," in *SIGMETRICS Perform. Eval. Rev. 34*, June 2006.

[5] Y. Cui, W. Li and X. Cheng, "Partially Overlapping Channel Assignment Based on "Node Orthogonality" for 802.11 Wireless Networks," in *IEEE INFOCOM 2011*, 2011.

[6] K. Zhou, L. Xie, Y. Chang and X. Tang, "Channel Assignment for WLAN by Considering Overlapping Channels in SINR Interference Model," in *IEEE International Conference on Computing Networking and Communications*, 2012.

[7] V. Angelakis, S. Papadakis, V. A. Siris and A. Traganitis, "Adjacent Channel Interference in 802.11a is Harmful: Testbed Validation of a Simple Quantification Model," *IEEE Communications Magazine,* pp. 160-166, March 2011.

[8] E. Garcia Villegas, R. Vidal Ferré y J. Paradells, «Frequency assignments in IEEE 802.11 WLANs with efficient spectrum sharing,» *Wireless Communications and Mobile Computing,* pp. 1125-1140, 2009.

[9] Cisco Systems, "Cisco Unified Wireless Network Architecure-Base Security Features," in *Wireless and Network Security Integration Design Guide*, p. Chapter 4.

[10] P. Calhoun, M. Montemurro and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification," in *Network Working Group - RFC 5415*, March 2009.

[11] P. Calhoun, M. Montemurro and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11," in *Network Working Group - RFC 5416*, March 2009.

[12] IEEE 802.11k-2003—Amendment 3: Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe. IEEE-SA. October 2003.

Formulación del problema de selección de acceso en entornos heterogéneos y multi-servicio como un problema de programación lineal binaria

Luis Francisco Diez, Johnny Choque, Ramón Agüero, Luis Muñoz
Departamento de Ingeniería de Comunicaciones,
Universidad de Cantabria
Avda Castros s/n, - 39005 Santander, España
{ldiez, jchoque, ramon, luis}@tlmat.unican.es

***Resumen*—En este artículo se modela la selección de acceso en entornos de redes heterogéneas como un problema de programación lineal. El modelo está basado en una función de utilidad flexible que permite la incorporación de varias figuras de mérito. En concreto, se estudia una estrategia basada en el precio, la preferencia de tecnologías en base a servicios concretos y la combinación de ambas; además, también se trata de minimizar el número de traspasos a fin de estudiar su impacto. Uno de los principales valores añadidos de este trabajo es que considera la disposición de los usuarios a tener conectividad en momentos concretos (de acuerdo a patrones de movilidad y tráfico), así como el histórico de sus conexiones (el estado previo de la conexión). Los resultados muestran que la selección apropiada de la función de utilidad es de extrema importancia para entender el rendimiento obtenido. A fin de evaluar la viabilidad del método propuesto se ha desplegado una topología de red ilustrativa que abarca diferentes tecnologías de acceso y tipos de servicios, ambos con diferentes requerimientos y características**

***Palabras Clave*—selección de acceso, redes heterogéneas, programación lineal**

I. INTRODUCCIÓN

Hoy por hoy se pueden encontrar estudios [1] que estiman que el tráfico debido a terminales móviles crecerá en torno a 15 veces para finales de 2017; a su vez se estima que en torno a un 85% de la población mundial tendrá la posibilidad de usar conexiones WCDMA/HSPA. Por otro lado, cabe destacar el notable incremento del número de terminales móviles considerados avanzados (*smartphones* y *tablets*), que permiten conectarse a redes celulares. Estos terminales típicamente implementan, además, otras tecnologías radio, por lo que la relevancia de las llamadas *Heterogeneus Networks (HetNets)* crecerá en el futuro.

Teniendo en cuenta lo anterior (aún sin considerar el impacto que puedan llegar a tener las comunicaciones *Machine-to-Machine* y el *Internet-of-Things*), la gestión óptima de los recursos en las redes de acceso inalámbricas es, si cabe, más importante y ha vuelto a atraer la atención de la comunidad científica. A pesar de los considerables esfuerzos llevados a cabo durante la última década, especialmente tras la aparición del paradigma *Always Best Connected* [2], todavía existen nuevos retos y aspectos que deben ser estudiados.

En este sentido, se puede encontrar un elevado número de trabajos que analizan diferentes técnicas, algoritmos y protocolos relacionados con la gestión de recursos radio mediante el estudio de las nuevas posibilidades que brindan los elementos avanzados que han ido apareciendo con el tiempo. Algunos de estos trabajos basan sus conclusiones en la comparación entre diferentes alternativas. Sin embargo, en ciertos casos, también resultaría interesante cuantificar la diferencia de estos estudios con respecto a la solución teóricamente óptima.

En este sentido, este trabajo trata de dar respuesta a la siguiente cuestión: ¿cuál es el mejor rendimiento que se podría esperar en una red heterogénea de acceso inalámbrico? A fin de proporcionar una respuesta razonable se plantea un problema de optimización que se modela como un problema de programación lineal. Para ello se define una función de utilidad genérica que es capaz de integrar diferentes figuras de mérito, que tienen en cuenta tanto a los operadores de red (como puede ser la carga) como a los usuarios finales (por ejemplo, el precio).

Uno de los aspectos más novedosos de este trabajo es que en el planteamiento del problema se tiene en cuenta tanto la disposición de un usuario a tener una conexión activa (no todos los usuarios quieren estar siempre conectados) como el resultado de las instancias previas del problema.

El artículo se estructura como se describe a continuación. En primer lugar, la Sección II presenta trabajos que comparten las mismas bases que el que aquí se presenta. Seguidamente, en la Sección III, se discute el modelado del problema como uno de programación lineal binaria, ilustrando cómo se tiene en consideración la evolución temporal de los servicios. La Sección IV describe brevemente algunos de los aspectos más relevantes de la implementación que se ha llevado a cabo. La Sección V presenta la función de utilidad que se usa en este trabajo, mientras que en la Sección VI se evalúa la viabilidad de dicha función y del procedimiento en general, mediante el estudio de algunos resultados obtenidos en el marco desarrollado para un escenario particular, sobre el cual se estudia un esquema de balanceo de carga basado en precios. Finalmente, la Sección VII concluye el artículo, mencionando algunos puntos a considerar en trabajo futuro, e indica las posibilidades potenciales que brinda el marco desarrollado.

II. ESTADO DEL ARTE

El lema *Always Best Connected* fue propuesto originalmente por Gustafsson y Johnson en 2003 en [2]. Como se ha mencionado anteriormente, esta línea de investigación ha arraigado en la última década, dando lugar a numerosas propuestas que buscan la gestión óptima de los recursos en redes de acceso inalámbricas, proporcionando la mejor calidad de servicio (*QoS*) a los usuarios finales. Algunos de los

trabajos realizados durante este período se mencionan en [3] y en sus referencias.

Con el paso del tiempo, se han propuesto nuevas posibilidades, sustentadas por nuevas técnicas que han aparecido. Un ejemplo claro es la capacidad de virtualizar recursos [4] como medio para ofrecer calidad de experiencia (*QoE*) a medida a los usuarios finales. Otra técnica que puede tener un impacto notable en el rendimiento de las redes de acceso inalámbrico es el *multi-path* (la posibilidad de dividir los flujos de tráfico por varios caminos con el fin de mejorar sus prestaciones) que permiten los dispositivos *multi-homed* [5]. Por otro lado, también se ha evidenciado que existen nuevos requerimientos a tener en cuenta, como es el caso del consumo energético [6]. La consideración de estos aspectos y el análisis de su influencia en el rendimiento y comportamiento de las *HetNets* as aún un aspecto que no se ha abordado.

A pesar de que las propuestas que aparecieron alrededor de hace 5 años se han concebido para proporcionar un cierto grado de flexibilidad, pueden no ser capaces de solventar los nuevos retos y requerimientos que están apareciendo continuamente. Recientemente, se ha propuesto un marco de referencia abierto para servicios de conectividad [7], que plantea un nuevo paradigma para la gestión de la conectividad en los escenarios de comunicaciones venideros.

Un aspecto común de la mayoría de los trabajos que buscan una mejor operación de las redes heterogéneas es que comparan el rendimiento logrado con otras alternativas (o con las técnicas actuales), sin embargo no se evalúa lo cerca o lejos que estos resultados están del comportamiento óptimo [8], [9], [5]. El principal objetivo de este trabajo es proponer una metodología para obtener la solución óptima, considerando diversas figuras de mérito sobre redes altamente heterogéneas, en las cuales los usuarios finales cursan diferentes tipos de servicios.

Este trabajo es una evolución del marco que originariamente se presentó en [10]. Al trabajo previo se le ha añadido la capacidad de modelar de manera apropiada y diferenciada servicios de diferente naturaleza (como contraposición al lema *Always Best Connected*), lo que ha tenido una clara influencia en cómo el problema ha de ser planteado y que ha llevado a la integración de un módulo que mantenga el histórico de las conexiones previas.

Como se ha mencionado, se propone el uso de programación lineal binaria para obtener la solución óptima. Cabe destacar que no existen muchos trabajos que busquen este tipo de soluciones, aunque se han empleado otras técnicas matemáticas recientemente como pueden ser la teoría de juegos [11], [12] o la toma de decisiones multi-atributo [13] [1].

III. FORMULACIÓN DEL PROBLEMA

El problema de la selección de acceso trata de establecer la asociación óptima entre los flujos activos (servicios) de los usuarios con las alternativas de acceso disponibles. El problema se ha definido sobre un escenario genérico que consta de N redes de tecnologías diferentes, por lo tanto, dotadas de diferentes características en términos de cobertura y capacidad. También se asume que existen U usuarios finales, capaces de iniciar S servicios diferentes de forma simultánea; además se asume que los usuarios poseen terminales capaces de establecer conexiones con todas las tecnologías presentes en el escenario.

El problema se formula como uno de optimización entera binaria en el cual aparecen $U \times N \times S$ variables básicas (x_{ijk}) que se definen como sigue:

$$x_{ijk} = \begin{cases} 1 \text{ si el usuario } i \text{ usa la red } j \text{ para el servicio } k \\ 0 \text{ en caso contrario} \end{cases} \tag{1}$$

Además, se incorpora una función de utilidad genérica (u_{ijk}), a fin de cuantificar el beneficio de una conexión en particular, que puede modularse de acuerdo a diferentes figuras de mérito. Es importante indicar que esta utilidad, a pesar de que pueda depender de condiciones particulares (por ejemplo conectividad física), se mantiene constante para cada instancia del problema, garantizando de esta manera la linealidad del modelo (lo que quiere decir que u_{ijk} no depende de x_{ijk}). Asimismo, se definen tres restricciones al problema: 2b asegura que las variables básicas son binarias; 2c fuerza a que cada flujo esté asociado a un único acceso; finalmente, 2d limita el número de conexiones que se pueden realizar sobre un acceso determinado (con capacidad C_j) de acuerdo a las capacidades requeridas por cada uno de los servicios (c_k).

$$\textbf{Max.} \quad \sum_{i,j,k} u_{ijk} \cdot x_{ijk} \tag{2a}$$

$$\textbf{s.t.} \quad \forall i,j,k \quad x_{ijk} \in \{0,1\} \tag{2b}$$

$$\forall i,k \quad \sum_{j} x_{ijk} \leq 1 \tag{2c}$$

$$\forall j \quad \sum_{i,k} x_{ijk} c_k \leq C_j \tag{2d}$$

Merece la pena aclarar que no todas las variables indicadas formarán parte del problema ya que, por ejemplo, aquellas que carezcan de conectividad física entre el usuario **i** y la estación base **j** se descartarán ($x_{\mathbf{ijk}} = 0 \quad \forall k$). De igual manera, cuando un determinado servicio **k** se encuentra inactivo para un usuario **i** también se descartará, añadiendo las restricciones adicionales correspondientes: $x_{i\mathbf{j}k} = 0 \quad \forall j$.

La formulación presentada es una evolución de la propuesta en [10] a la cual se ha añadido la dimensión de servicio. A fin de reflejar una situación realista, cuando un servicio es rechazado o interrumpido (*dropped*) no se considera en las instancias sucesivas del problema (hasta que es iniciado de nuevo). En este trabajo se propone usar los resultados de la instancia previa del problema para identificar los pares usuario-servicio que vayan a formar parte de la siguiente instancia según una máquina de estados. Se pueden distinguir cuatro situaciones diferentes que se explican a continuación:

- **Reposo.** El usuario **i** no tiene el servicio **k** activo y, por lo tanto, no requiere una conexión para ese servicio.
- **Activo.** El usuario **i** mantiene una conexión activa para el servicio **k**, que ha sido aceptada por alguno de los accesos disponibles.
- **Rechazado.** El usuario **i** inició un flujo asociado al servicio **k** pero éste no fue aceptado por la red.
- **Interrumpido.** El usuario **i** mantenía el servicio activo **k**, que fue inicialmente aceptado pero se ha interrumpido antes de finalizar debido a la movilidad del usuario u otros eventos.

[1] En este caso, normalmente no se obtiene la solución óptima.

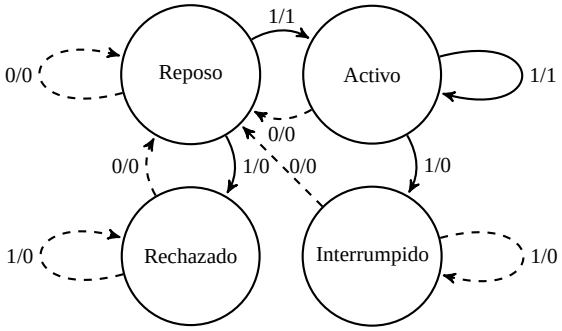
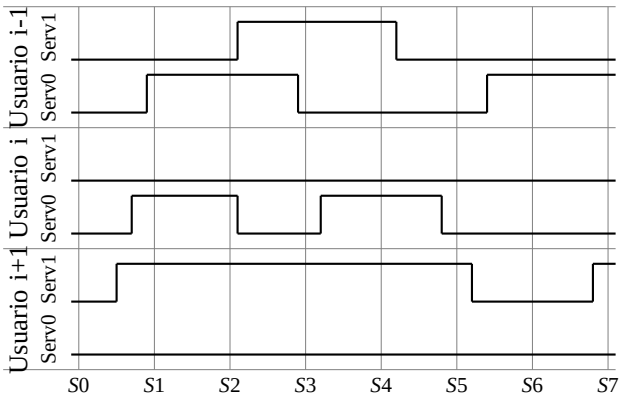


Fig. 1. Máquina de estados para un par usuario-servicio

Con los estados mencionados y considerando que la optimización para un escenario consiste en la resolución de sucesivas "fotografías" del estado de la red (topología y estados de los servicios), se puede representar la evolución de un par usuario-servicio concreto de acuerdo a la Figura 1. Las flechas representan la transición entre estados, que dependen de dos aspectos: la intención del usuario para ese servicio y el resultado de la instancia anterior del problema. Estos valores se representan con la pareja de números sobre las flechas (*intención/resultado*). Resulta sencillo ver que, dependiendo del estado previo y de la intención actual, existen situaciones para las cuales la variable correspondiente no entrará a formar parte del problema; estas situaciones se representan con líneas discontinuas. Independientemente del estado en el que se encuentre, cuando un usuario **i** no tiene intención de tener el servicio **k** activo, la variable básica correspondiente no se incluye en el problema de optimización ($x_{\mathbf{ij}k} = 0 \quad \forall j$) y, por lo tanto, pasa al estado *Reposo*. Por otro lado, en el momento en que un servicio sea rechazado o interrumpido la variable asociada al par usuario-servicio se descarta para la instancia del problema sin tener en cuenta la intención del usuario. Se asume que las conexiones que se han perdido no se pueden recuperar, por lo que permanecen en el mismo estado (*Rechazado* o *Interrumpido*) hasta que vuelven al estado *Reposo*.

IV. IMPLEMENTACIÓN

La solución de una instancia del problema se refiere a la conectividad óptima de una situación particular, que viene dada por la posición de los usuarios finales, su intención de mantener servicios activos, el resultado de la instancia anterior y el estado de la red (capacidad restante de los elementos de acceso). Estas situaciones se pueden entender como "fotografías" del escenario en el que los usuarios se mueven y generan flujos asociados a servicios durante un periodo de tiempo determinado. Estos patrones (tráfico y movimiento) se suministran por medio de trazas que se procesan por la herramienta que se ha desarrollado, que posee dos módulos bien definidos. El primero resuelve el problema de optimización obtenido a partir de las trazas que describen el movimiento y tráfico y usando la librería *GLPK* [14]; se genera un proceso para cada instancia del problema y, por lo tanto, no existe una relación entre el problema actual y la solución previa. Como se ha mencionado, para plantear el problema de manera apropiada resulta imprescindible dotar a la herramienta de la capacidad de tener en cuenta los resultados previos del problema (servicios rechazados o interrumpidos, carga de los elementos de acceso...); para ello se ha añadido a la herramienta otro módulo, el monitor, que no se consideró en el diseño anterior [10]. Esta segunda entidad analiza el resultado del problema y lo registra para que sea usado en la siguiente instancia; además, está a cargo de mantener y actualizar las estadísticas del escenario.



$\Omega^0_{i-1} = [0,1,1,0,0,0,1,1]$ $\quad \Omega^1_{i-1} = [0,0,0,1,1,0,0,0]$

$\Omega^0_{i} = [0,1,1,0,1,0,0,0]$ $\quad \Omega^1_{i} = [0,0,0,0,0,0,0,0]$

$\Omega^0_{i+1} = [0,0,0,0,0,0,0,0]$ $\quad \Omega^1_{i+1} = [0,1,1,1,1,1,0,1]$

Fig. 2. Ejemplo de fotografías de servicios

Como se ha mencionado, a la herramienta se le suministran trazas que deben reflejar: (1) la posición de los usuarios finales de acuerdo a un patrón de movilidad y (2) la intención de todos los usuarios de tener activos cada uno de sus servicios. La Figura 2 muestra un ejemplo ilustrativo de cómo los servicios correspondientes a tres usuarios se mapean en fotografías consecutivas. Cabe mencionar que el tiempo que un servicio se mantiene tanto en estado *Reposo* como *Activo* debe ser siempre mayor que el tiempo que dura una fotografía, con el fin de indicar de forma correcta la presencia de nuevos flujos (como es el caso del servicio 1 para el usuario *i* en la Figura 2). Para cada par usuario-servicio (*ik*) se define el vector $\mathbf{\Omega}^k_i = [\omega_0, \omega_1, \ldots, \omega_N]$, en el que el parámetro ω_n representa el estado del servicio en la $n_{ésima}$ fotografía. Como

Procedimiento 1 Optimización por fotografía

Configuración global
- Despliegue del escenario
  - Parámetros de configuración: desde fichero
  - Usuarios finales: desde fichero
  - Elementos de acceso: desde fichero

Procesado inicial
- Variables de optimización
  - Establecimiento de conectividad
  - Intención de servicio y estado previo
- Funciones de utilidad
  - Elemento de acceso previo
  - Carga actual
  - Precio actual

Optimización
- Resolución del problema: GLPK
  - Resultado del problema: actualizar estado
  - Actualizar estadísticas

se puede observar, el formato de las trazas procesadas por la herramienta es muy genérico, por lo que puede ser fácilmente extendida para acometer otros estudios.

El procedimiento que se ha seguido para cada una de las fotografías del escenario se muestra en el Procedimiento 1 y se divide en tres fases. (1) Se establece el escenario de acuerdo a parámetros de configuración generales, posición y características de los elementos de acceso, y posición y servicios de los usuarios finales, a partir de ficheros externos. (2) Una vez que el escenario ha sido desplegado, se verifica la conectividad física entre los usuarios finales y las diferentes estaciones base, así como el estado de los servicios. También se construye la función de utilidad considerando parámetros como el elemento de acceso previo (si el par usuario/servicio mantenía un flujo activo), la carga actual de los elementos de acceso o el precio que se fijará para un determinado servicio. (3) Finalmente se resuelve el problema por medio de la librería GLPK y el resultado se procesa, permitiendo actualizar el estado de cada par usuario-servicio y de las estadísticas.

V. FUNCIONES DE UTILIDAD

Tras presentar la herramienta queda por explicar el diseño de los parámetros que conforman la función de utilidad y que modulan el beneficio de cada conexión. Aunque existe un gran abanico de posibilidades, en el ámbito de este artículo nos centraremos en dos aspectos concretos: precio y RAT (*Radio Access Technology*) *affinity* (éste se ha definido como la preferencia de asociar un servicio determinado a una tecnología de acceso concreta) y la combinación de ambos. Además, también se estudiará la interacción de estos parámetros con el coste de realizar traspasos, entendiendo que es preferible evitar cambiar de elementos de acceso cuando el servicio se encuentra activo. Se podrá observar cómo las diferentes combinaciones de estos parámetros dan lugar a diferentes rendimientos, poniendo de relieve la importancia de una adecuada configuración.

Valga aclarar que en este trabajo se asume que tanto los servicios como los elementos de acceso usan una unidad de capacidad genérica y discreta denotada por TU (*Traffic Unit*) que representará recursos de la tecnología utilizada (*slots* en TDMA, códigos en CDMA, sub-portadoras en OFDMA...).

A. Parámetros comunes

1) Conectividad: Como parámetro común para las diferentes estrategias, se dará una cierta utilidad a la conectividad *per se*, priorizando, además, los servicios en curso sobre las nuevos al asumirse que siempre es preferible (desde el punto de vista de la QoE) rechazar un nuevo servicio a interrumpir uno ya iniciado. Este parámetro (α_{ijk}) se define como:

$$\forall j \quad \alpha_{ijk} = \begin{cases} 1 \cdot \frac{c_k}{\max_{\forall k} c_k} & \text{si el par usuario-servicio } ik \\ & \text{estaba conectado} \\ \lambda \cdot \frac{c_k}{\max_{\forall k} c_k} & \text{de otro modo} \end{cases} \quad (3)$$

en donde c_k representa la capacidad requerida por el servicio k y λ (parámetro de diseño) se elige a fin de asegurar que a un servicio en curso se le da siempre mayor prioridad que a nuevas llamadas sin importar la capacidad requerida por estas: $\lambda < \frac{\min_{\forall k} c_k}{\max_{\forall k} c_k}$.

Como se puede observar, esta función considera la capacidad requerida por cada servicio; de otro modo, a aquellos que necesitaran mayor capacidad se les daría (de manera indirecta) una prioridad más alta[2].

2) Traspaso-Handover (HO): También se considera la influencia que el realizar un traspaso tendría sobre el rendimiento. En este sentido, se modela la preferencia por mantener el acceso actual con el objetivo de incluir el coste del cambio. A este fin se define el parámetro β_{ijk} como:

$$\beta_{ijk} = \begin{cases} 1 & \text{si el par usuario-servicio } i/k \\ & \text{estaba conectado a la BS } j \\ 1-\mu & \text{de otro modo} \end{cases} \quad (4)$$

en donde $\mu < 1$ es un parámetro de diseño que se selecciona dependiendo de la configuración, como se explicará más adelante.

B. Parámetro de utilidad de precio

En este caso el objetivo es representar la inclinación de los usuarios finales por las alternativas más económicas. Para ello la utilidad de este parámetro debe crecer a medida que el elemento de acceso ofrece precios más bajos, por lo que se busca una función decreciente. A fin de permitir la comparación relativa entre los precios ofrecidos se propone el uso de una función logarítmica (véase Fig. 3(a)) que se define como:

$$\forall k \quad \gamma_{ijk} = \begin{cases} -\log(p_j) & p_j \in [p_i^{\min}, p_i^{\max}] \\ 1 & \text{de otro modo} \end{cases} \quad (5)$$

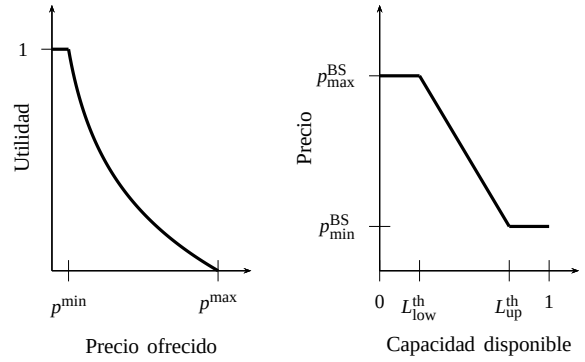
donde $p_i^{\max}$ es el precio máximo que un usuario i está dispuesto a pagar y $p_i^{\min}$ se corresponde con el menor precio por debajo del cual no se incrementaría la utilidad. También se asume que aquellas estaciones base que ofrezcan un precio por encima del máximo admisible serían descartadas por el usuario. Se han utilizado unidades de precio relativas al máximo precio ofrecido por los elementos de acceso que también se corresponderá con p_i^{max}; estas unidades también son relativas a 1 TU y fotografía.

Por otro lado, se ha considerado que los elementos de acceso usan el precio ofrecido a los usuarios como medio para incentivar o retraer a éstos de realizar una conexión; esto se refleja en la Figura 3(b), que representa la tarifa ofrecida por una estación base en función de su carga relativa (de la proporción de carga libre). Como se puede observar, cuando la estación base es encuentra muy cargada (carga libre por debajo de $L_{\text{low}}^{\text{th}}$), el precio ofrecido alcanza el máximo permitido. Por otro lado, si la estación base se encuentra poco cargada, el precio cae hasta el valor mínimo configurado. En este caso se ha optado por una función que decae linealmente entre los valores máximo y mínimo.

C. Parámetro RAT Affinity

El propósito de este parámetro es el de favorecer que los servicios se asocien a las tecnologías más apropiadas a sus características. Por ejemplo, se podría considerar la tecnología

[2]Una conexión de un servicio que requiriera 2 TUs tendría la misma utilidad que otra de 1 TU, mientras que consumiría el doble de recursos. Por ello la optimización siempre se decantaría por dos conexiones de 1 TU en detrimento de una de 2 TUs.



(a) Utilidad del precio (b) Precio de estación base en función de la carga

Fig. 3. Funciones de utilidad relativas al precio

WLAN como la más apropiada para servicios de datos, sin restricciones de retardo, al ofrecer un mayor ancho de banda. El parámetro correspondiente a esta utilidad (δ_{ijk}) se define como:

$$\forall i \quad \delta_{ijk} = \begin{cases} 1 & \text{si el servicio } k \\ & \text{tiene afinidad por la tecnología de la BS } j \\ \nu & \text{de otro modo} \end{cases} \tag{6}$$

en donde $\nu < 1$ es un parámetro de diseño que modula el peso que se le da a este aspecto en particular.

D. Combinaciones de parámetros

Mediante la combinación lineal de los parámetros descritos se puede definir la función de utilidad en forma general.

$$u_{ijk} = A \cdot \alpha_{ijk} + B \cdot \beta_{ijk} + C \cdot \gamma_{ijk} + D \cdot \delta_{ijk} \tag{7}$$

Existen dos maneras de favorecer cada uno de los parámetros: (1) modificando el factor correspondiente (A,B,C,D); o (2) usando una versión binaria de ellos (activado o no) y modulando su peso relativo mediante los parámetros de diseño (λ,μ,ν); en este trabajo se ha optado por la segunda alternativa. En concreto, se ha fijado $\lambda = \nu = 0.8$, mientras que el valor del parámetro μ se discute a continuación.

Si se desactiva el parámetro asociado al RAT *affinity* ($D = 0$), es posible comparar las utilidades de los accesos de las dos alternativas para un servicio en curso (notar que el parámetro α_{ijk} es igual en ambos casos): el acceso que está siendo utilizado (1) y otro diferente (2) que ofrece un precio ($p2$) menor que el del primero ($p1$). En concreto se asume que $p2$ es $100 \cdot \xi\%$ más bajo que $p1$ ($p_2 = (1-\xi)\,p_1$, con $\xi < 1$). Por lo que se deduce:

$$\begin{aligned} u^{(1)} = u^{(2)} \quad &\rightarrow \quad \mu - \log(p_1) = -\log(p_1(1-\xi)) \\ &\rightarrow \quad \mu = -\log(1-\xi) \end{aligned} \tag{8}$$

Si se establece el 20% como la variación del precio para la que un usuario estaría dispuesto a cambiar de estación base, el valor del parámetro μ es de ≈ 0.1.

Teniendo en cuenta todo lo expuesto en esta sección, existen seis funciones de utilidad que se utilizan en los análisis que se han llevado a cabo y que se indican en la Tabla I.

Tabla I
FUNCIONES DE UTILIDAD

	Precio		RAT affinity		Combinación	
	HO	No HO	HO	No HO	HO	No HO
Conectividad (A)	✓	✓	✓	✓	✓	✓
Traspasos (B)	✓		✓		✓	
Precio (C)	✓	✓			✓	✓
RAT Affinity (D)			✓	✓	✓	✓

Tabla II
PARÁMETROS DEL ANÁLISIS

Estaciones base	
Celular	
Cobertura (m)	150
Capacidad (TU)	16
Política de tarificación	$P \in [0.1, 1.0]$, Umbrales $= \{0.2, 0.8\}$
WiFi	
Cobertura (m)	50
Capacidad (TU)	8
Política de tarificación	$P \in [0.1, 1.0]$, Umbrales $= \{0.2, 0.8\}$
Modelo de movilidad	
Random Waypoint	
Velocidad (m/s)	$\mathbf{U}(1,3)$
Periodo de movimiento (s)	$\mathbf{U}(800,1000)$
Periodo de reposo (s)	$\mathbf{U}(80,100)$
Modelo de servicio	
Servicio 0: Voz	
Modelo	On-Off
Tiempo entre llegadas (s)	120
Tiempo del servicio (s)	180
Capacidad (TU)	1
RAT *Affinity*	Celular
Servicio 1: Transferencia de datos	
Modelo	On-Off
Tiempo entre llegadas (s)	60
Tiempo del servicio (s)	120
Capacidad (TU)	2
RAT *Affinity*	WiFi
Parámetros generales	
Tiempo de simulación (s)	3600
# de fotografías	360
# of ejecuciones	10

VI. RESULTADOS

Esta sección muestra algunos de los resultados que se han obtenido aplicando el método descrito sobre un escenario concreto con un doble objetivo: estudiar su viavilidad y discutir el impacto de una selección apropiada de la función de utilidad.

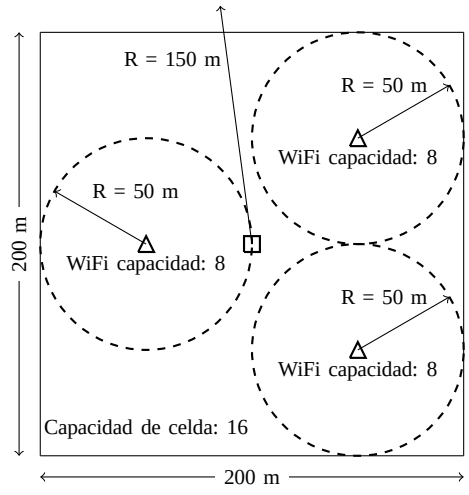


Fig. 4. Despliegue de red

El escenario que se considera tiene un área cuadrada de $200 \times 200\ m^2$ en la que se han desplegado dos tipos de estaciones base diferentes (ver Figura 4). El primer tipo corresponde a una tecnología celular tradicional con un radio de cobertura de 150 *m*, que cubre el escenario por completo, y una capacidad de 16 TUs; por su parte, el segundo tipo emula puntos de acceso *WiFi*, con una cobertura de 50 *m* y una capacidad de 8 TUs. Sobre este escenario se ha desplegado un número de usuarios que se ha incrementado de 20 a 200; éstos se mueven de acuerdo al modelo *Random Waypoint* [15], según los parámetros que se describen en la Tabla II. Cada uno de los usuarios genera flujos de dos tipos de servicios, de acuerdo a un modelo *ON-OFF* y mantienen una afinidad hacia una de las tecnologías. Todas las estaciones base hacen uso de la política de tarificación que se ha descrito anteriormente (Figura 3(b)), de modo que aumentan el precio a medida que se encuentran más cargadas. Se han realizado 10 ejecuciones independientes del escenario (cada una de ellas conlleva 360 problemas de optimización) y se han obtenido los valores medios de los resultados. Se han considerado las seis funciones de utilidad descritas en la Tabla I y, para ambos tipos de servicio (0 y 1), se han analizado las siguientes figuras de mérito:

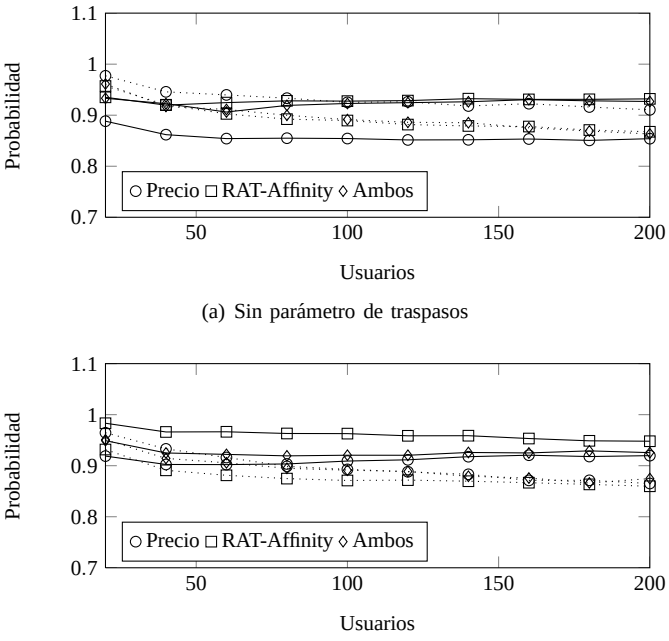
- **Tasa de éxito-Success Rate (SR).** Probabilidad de que un servicio finalice con éxito, es decir, que no sea rechazado ni interrumpido.
- **Traspasos (HO).** Número medio de traspasos que se llevan a cabo durante la duración de un servicio.
- **Precio por Servicio (PS).** Precio medio pagado por tiempo y unidad de tráfico.
- **RAT *affinity* (RA).** Este parámetro indica el porcentaje del tiempo que un servicio ha usado la tecnología hacia la que tiene afinidad.

En primer lugar, la Figura 5 muestra la probabilidad de finalizar un servicio con éxito. Como se puede observar, la definición de la función de utilidad (especialmente del parámetro α) hace que se obtengan resultados similares para ambos servicios [3]. Además, estos resultados muestran que no existe un impacto notable de las funciones de utilidad, ni del uso del parámetro asociado a los traspasos.

Sin embargo, el impacto del parámetro asociado a los traspasos queda patente en la Figura 6. Se puede observar una notable reducción del número de traspasos (particularmente para el servicio 0) cuando este parámetro (β) se considera en la función de utilidad. El impacto es menos relevante para el servicio 1, especialmente con un número elevado de usuarios, ya que la red se encuentra fuertemente cargada (esto es más evidente para la estación base celular) y no existen muchas alternativas de conexión. Por otro lado, cuando no se considera este parámetro ($B = 0$) también se observa que la función que considera el RAT *affinity* reduce el número de traspasos para el servicio 1, no siendo así para el servicio 0. Esto es parcialmente debido al efecto *ping-pong* que puede afectar a los flujos del servicio 0, ya que un doble cambio de acceso no tendrá ningún efecto en la utilidad global.

En lo que se refiere al precio, la Figura 7 arroja un resultado interesante. Para el servicio 0 se observa el comportamiento

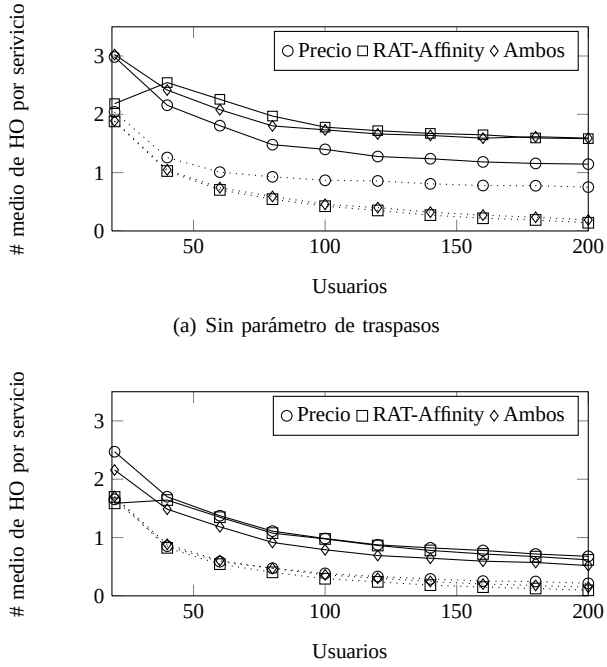
[3]De no haberse considerado la capacidad en la definición del citado parámetro la tasa de éxito del servicio 1 hubiera sido mucho menor.



(a) Sin parámetro de traspasos

(b) Con parámetro de traspasos

Fig. 5. Tasa media de finalización de servicios con éxito Vs. número de usuarios. Las líneas continuas se corresponden con el servicio 0 y las discontinuas con el servicio 1

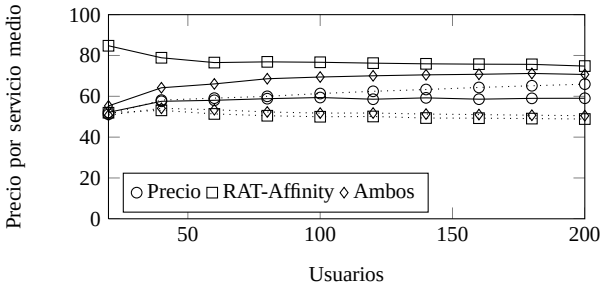


(a) Sin parámetro de traspasos

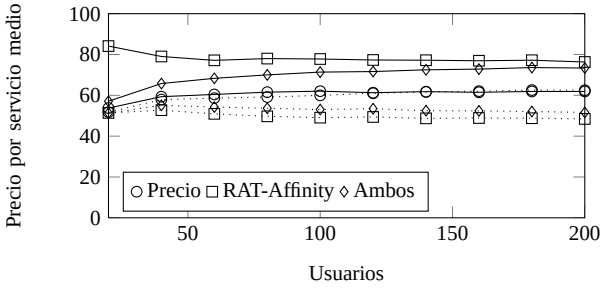
(b) Con parámetro de traspasos

Fig. 6. Número medio de traspasos por servicio Vs. número de usuarios. Las líneas continuas se corresponden con el servicio 0 y las discontinuas con el servicio 1

esperado, la función de utilidad que tiene en cuenta el precio abarata el servicio, comparado con la que tiene en cuenta el RAT *affinity*. Sin embargo, para el servicio 1 se observa que es precisamente la que tiene en cuenta el RAT *affinity* la que conlleva los precios más bajos, incluso por debajo de los ofrecidos por la basada en precio (recordar que la optimización es global, por lo que abarata el conjunto de los servicios en el escenario y no cada uno de ellos). La razón

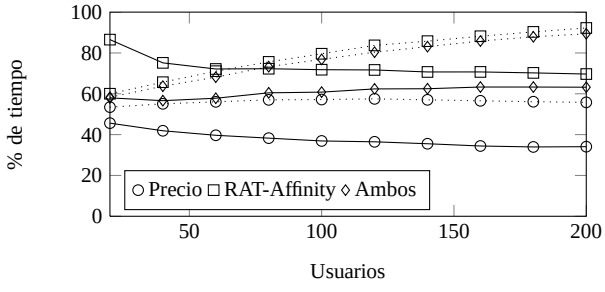


(a) Sin parámetro de traspasos

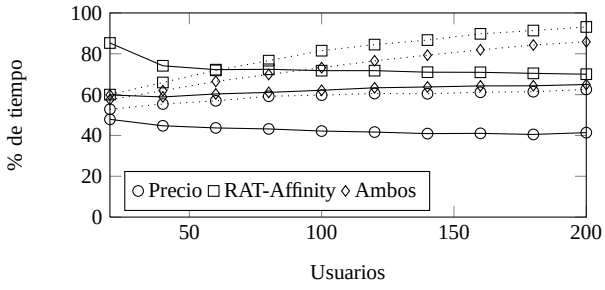


(b) Con parámetro de traspasos

Fig. 7. Precio medio por servicio y TU Vs. número de usuarios. Las líneas continuas se corresponden con el servicio 0 y las discontinuas con el servicio 1



(a) Sin parámetro de traspasos



(b) Con parámetro de traspasos

Fig. 8. RAT *affinity* medio por servicio Vs. número de usuarios. Las líneas continuas se corresponden con el servicio 0 y las discontinuas con el servicio 1

es que los punto de acceso *WiFi* (debido a su cobertura) se encuentran menos cargados que la estación celular y, por lo tanto, el precio que ofrecen es menor. Como los servicios de tipo 0 se mantienen en las estación base celular (sin importar la tarifa que ofrece) de acuerdo a su RAT *affinity*, los precios ofrecidos por los puntos de acceso *WiFi* se mantienen bajos, reduciendo por tanto el precio por servicio de tipo 1. Por otro lado, los resultados también reflejan que la función basada en precio no distingue entre los dos tipos de servicio, por lo que ambos tienden a pagar lo mismo. Por último, cabe destacar que no se observa una clara dependencia del parámetro de traspasos en lo relativo al precio.

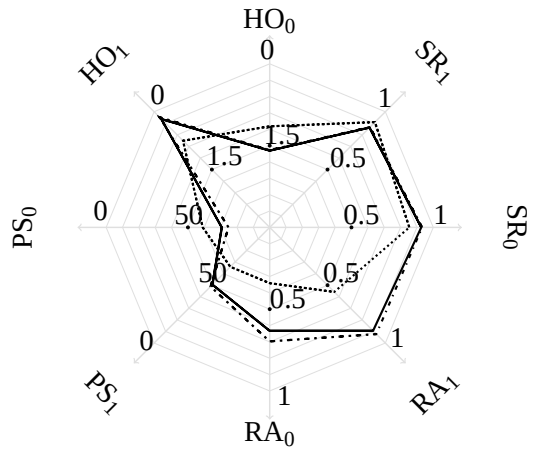
La Figura 8 muestra la proporción de tiempo que un servicio se encuentra asociado a una tecnología con la que tiene afinidad. Se puede afirmar que el uso de una función de utilidad apropiada tiene una gran influencia en este aspecto, ya que los resultados obtenidos para la utilidad basada en RAT *affinity* son mucho más elevados que aquellos que presenta la estrategia basada en precio. También se observa una cierta influencia del parámetro de traspasos, ya que aumenta ligeramente el tiempo que los servicios están conectados a su tecnología afín en las configuraciones tanto el la configuración que tiene en cuenta el precio como en la que tiene en cuenta precio y RAT *affinity*. Por último se puede ver que el servicio 1, para todas las estrategias estudiadas, presenta un mejor comportamiento en lo que al RAT *affinity* se refiere.

A fin de obtener una visión más global del comportamiento de las diferentes estrategias de acuerdo a las funciones de utilidad definidas, la Figura 9 hace uso de diagramas *cobweb* en los que se representa las cuatro figuras de mérito para ambos tipos de servicio. Los bordes de los ejes representan el mejor resultado que se puede obtener, mientras que el centro establece el peor caso (los límites del número de traspasos se han establecido empíricamente por observación). Los resultados se han obtenido para el escenario con 200 usuarios. Como se comentó anteriormente, se puede ver una mejora en los casos en que se hace uso del parámetro relacionado con los traspasos, ya que éste no afecta de forma relevante al resto, y mejora de manera notable el número medio de traspasos por servicio. En el caso de la estrategia ligada al RAT *affinity* se puede ver que el uso del parámetro de los traspasos incluso proporciona una leve mejoría de la probabilidad de completar un servicio con éxito para el servicio 0.

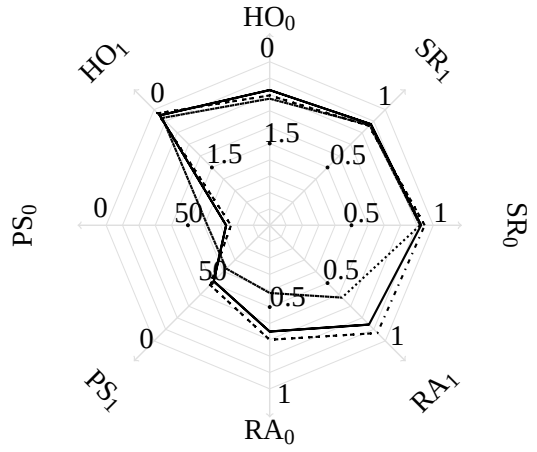
En general, todos los resultados indican que la estrategia que tiene en cuenta tanto el precio como el RAT *affinity* tiene un rendimiento similar al obtenido mediante la que únicamente tiene el cuenta el RAT *affinity*, sin producir un perjuicio notable en el precio; por su parte, la función basada sólo en precio tiene un rendimiento pobre en lo que a RAT *affinity* se refiere.

VII. CONCLUSIONES

En este artículo se ha propuesto el uso de técnicas de programación lineal con el objetivo de estudiar el mejor rendimiento en entornos de acceso altamente heterogéneos. El marco que se ha desarrollado, que considera la evolución temporal de los servicios, es lo suficientemente genérico como para extender su uso a diversos escenarios y casos de uso. Se ha estudiado la viabilidad del marco por medio de un escenario concreto y mediante funciones de utilidad basadas en precio, RAT *affinity* y coste de realizar traspasos. Los resultados muestran que elecciones diferentes de los parámetros de configuración llevan a rendimientos diversos, por lo que debe ser estudiada cuidadosamente al evaluar el rendimiento que se espere de una red. En concreto, los resultados revelan que la integración del coste de realizar traspasos en la función de utilidad tiene considerables beneficios, ya que lleva a una mejora notable en términos de número medio de traspasos por



(a) Sin parámetro de traspasos ($B = 0$)



(b) Con parámetro de traspasos ($B = 1$)

Fig. 9. Rendimiento de las diferentes funciones de utilidad. La línea con puntos representa la función ligada al precio; la línea discontinua para función ligada al RAT *affinity*; la línea continua representa la combinación de las anteriores

servicio sin provocar perjuicio en el resto de figuras de mérito estudiadas; de hecho en algunos casos las mejora.

Respecto a la líneas de trabajo futuro, el principal objetivo sería explotar el potencial del marco desarrollado con el fin de evaluar (mediante comparación con el óptimo) el rendimiento de diferentes algoritmos distribuidos y procedimientos de selección en entornos *HetNets*, incluyendo el uso de recursos virtualizados y técnicas de gestión de flujos. Como se ha podido observar, el diseño de la herramienta es bastante genérico y no se limita a optimización; se puede usar para emular cualquier escenario que se pueda representar en el formato de trazas usado. En este sentido, también se analizará el impacto que puedan tener diferentes modelos de tráfico, por ejemplo tráfico elástico, que daría lugar a problemas de optimización no lineales.

AGRADECIMIENTOS

Los autores expresan su gratitud al gobierno español por la financiación de los siguientes proyectos: “COnnectivity as a Service: Access for the Internet of the Future”, COSAIF (TEC2012-38574-C02-02) y “Cognitive, Cooperative Communications and autonomous SErvice Management”, C3SEM (TEC2009-14598-C02-01) respectivamente.

REFERENCIAS

[1] Ericsson Consumer Lab, “Traffic and market report - on the pulse of the networked society,” 2012.

[2] E. Gustafsson y A. Jonsson, “Always best connected,” *Wireless Communications, IEEE*, vol. 10, no. 1, pp. 49 – 55, feb. 2003.

[3] K. Pentikousis, R. Agüero, J. Gebert, J. A. Galache, O. Blume, y P. Pääkkönen, “The Ambient Networks heterogeneous access selection architecture,” in *Proceedings of the 1st Ambient Networks Workshop on Mobility, M2NM*, Octobre 2007.

[4] Y. Zaki, L. Zhao, C. Goerg, y A. Timm-Giel, “LTE mobile network virtualization,” *Mob. Netw. Appl.*, vol. 16, no. 4, pp. 424 – 432, Aug. 2011.

[5] U. Toseef, Y. Zaki, A. Timm-Giel, y C. Görg, “Uplink QoS Aware Multi-homing in Integrated 3GPP and non-3GPP Future Networks ,” in *Proceedings of the 4thd ICST International Conference on Mobile Networks & Management, MONAMI’12*, September 2012.

[6] L. Correia, D. Zeller, O. Blume, D. Ferling, Y. Jading, I. Goanddor, G. Auer, y L. Van Der Perre, “Challenges and enabling technologies for energy aware mobile radio networks,” *Communications Magazine, IEEE*, vol. 48, no. 11, pp. 66 – 72, november 2010.

[7] R. Agüero, L. Caerio, L. Correia, L. Ferreira, M. García-Arranz, L. Suciu, y A. Timm-Giel, “OConS: towards open connectivity services in the Future Internet,” in *Proc. of the 3rd ICST International Conference on Mobile Networks & Management, MONAMI’11*, Sept. 2011.

[8] L. Badia y M. Zorzi, “Dynamic utility and price based radio resource management for rate adaptive traffic,” *Wirel. Netw.*, vol. 14, no. 6, pp. 803 – 814, Dec. 2008.

[9] O. E. Falowo, S. Zeadally, y H. A. Chan, “Dynamic pricing for load-balancing in user-centric joint call admission control of next-generation wireless networks,” *International Journal of Communication Systems*, vol. 23, no. 3, pp. 335 – 368, 2010.

[10] J. Choque, R. Aguero, y L. Munoz, “Optimum selection of access networks within heterogeneous wireless environments based on linear programming techniques,” *ACM Springer Mobile Networks and Applications*, Aug 2011.

[11] D. Niyato y E. Hossain, “A game theoretic analysis of service competition and pricing in heterogeneous wireless access networks,” *Wireless Communications, IEEE Transactions on*, vol. 7, no. 12, pp. 5150 – 5155, december 2008.

[12] D. Niyato, P. Wang, E. Hossain, W. Saad, y Z. Han, “Game theoretic modeling of cooperation among service providers in mobile cloud computing environments,” in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, april 2012, pp. 3128 – 3133.

[13] C. Gu, Y. Zhang, W. Ma, N. Liu, y Y. Man, “Universal modeling and optimization for multi-radio access selection,” in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom ’09. 5th International Conference on*, sept. 2009, pp. 1 – 4.

[14] “The GNU linear programming kit (GLPK),” www.gnu.org/software/glpk, 2008.

[15] C. Bettstetter, G. Resta, y P. Santi, “The node distribution of the random waypoint mobility model for wireless ad hoc networks,” *Mobile Computing, IEEE Transactions on*, vol. 2, no. 3, pp. 257 – 269, sep 2003.

Esquema de Selección de Modo para Redes MCN-MR basado en Información de Contexto

M.Carmen Lucas-Estañ, Javier Gozalvez
Uwicore, *Ubiquitous Wireless Communications Research Laboratory* http://www.uwicore.umh.es
Universidad Miguel Hernández de Elche. Avda. de la Universidad, s/n, 03202, Elche España.
m.lucas@umh.es, j.gozalvez@umh.es.

***Resumen*- Las redes *multi-hop* celular con retransmisores móviles (MCN-MR) ofrecen una solución para superar ciertas limitaciones de los sistemas celulares basados en infraestructura mediante la integración de las tecnologías ad-hoc y celular. Un aspecto importante para un despliegue efectivo de las redes MCN-MR es el diseño de esquemas que sean capaces de seleccionar el modo de conexión más adecuado (el enlace celular tradicional o el enlace *multi-hop*) para cada transmisión. Este trabajo propone un esquema de selección de modo que decide el modo de conexión óptimo y el número de recursos radio que deberían ser utilizados en el modo seleccionado basando su decisión en información sobre el contexto actual del usuario. Este estudio demuestra que el esquema propuesto ayuda a alcanzar los beneficios esperados de las redes MCN-MR en términos de capacidad y rendimiento ofrecido a los usuarios, adaptando su decisión según la probabilidad de encontrar retransmisores adecuados para las transmisiones *multi-hop*.**

***Palabras Clave*- Selección de modo, redes celulares *multi-hop*, retransmisores móviles, gestión de recursos radio.**

I. INTRODUCCIÓN

Los sistemas celulares basados en infraestructura no son capaces de proporcionar niveles de calidad de servicio (*Quality of Service*, QoS) homogéneos en todo el área de cobertura debido al efecto de la distancia y de los obstáculos que atenúan e interfieren la señal entre la estación base (*Base Station*, BS) y los usuarios móviles. Las redes celulares multi-salto o *Multi-hop Cellular Networks* (MCNs), en las que la comunicación entre la BS y el usuario puede realizarse a través de otros nodos que actúan como retransmisores, han surgido como posible solución a este problema. Diferentes trabajos demuestran los beneficios que ofrecen las redes MCN en términos de capacidad, extensión del radio de cobertura y eficiencia energética [1]. Estos beneficios se obtienen por la sustitución del enlace celular directo de larga distancia entre la BS y el usuario, generalmente sin visión directa, por varias transmisiones *multi-hop* de menor distancia y mejores condiciones de comunicación. Los estándares celulares se han centrado inicialmente en el uso de retransmisores fijos [2]. Sin embargo, pruebas de campo han mostrado recientemente los importantes beneficios que se pueden obtener con el uso de retransmisores móviles (MCN-*Mobile Relays*, MCN-MR) [3]. En redes MCN-MR, la conexión entre el usuario y la BS se realiza a través de comunicaciones ad-hoc o dispositivo a dispositivo (*Device-to-Device*, D2D) entre el usuario y nodos retransmisores (*relay nodes*, RN), y un último enlace celular entre la BS y el RN más cercano a ésta. Los estándares comienzan a considerar los sistemas MCN-MR para aplicaciones de *public safety* y *proximity-services* (3GPP TR 22.803).

A pesar de que los beneficios que ofrecen las redes MCN-MR han sido demostrados en varios estudios, es importante resaltar que estos beneficios solamente son alcanzables en escenarios en los que sea posible establecer una conexión *multi-hop* (MH) entre el nodo fuente y el nodo destino de la comunicación que garantice mejores prestaciones que el enlace celular directo de un único salto o s*ingle-hop* (SH). Por tanto, la ganancia potencial de los sistemas MCN-MR está condicionada por la presencia de nodos retransmisores adecuados que ofrezcan buenas capacidades de comunicación para establecer el enlace MH. En este contexto, un aspecto clave para un despliegue eficaz de redes MCN-MR es el diseño de esquemas que sean capaces de seleccionar el modo de conexión (SH o MH) más adecuado bajo distintas condiciones de despliegue y operación del sistema [4].

Varios trabajos han analizado recientemente el problema de selección de modo. Los autores de [5] analizan un esquema de selección de modo que decide si dos usuarios de una tecnología celular situados en la misma celda deben comunicar entre ellos utilizando enlaces celulares tradicionales (es decir, realizando la comunicación a través de la BS) o utilizando comunicaciones D2D. Sin embargo, este escenario difiere del que tiene lugar en redes MCN-MR en el que la decisión que se debe tomar es si la conexión de un usuario con la BS debe realizarse a través del enlace celular SH o a través de un enlace MH utilizando otros nodos retransmisores móviles. Una propuesta interesante para redes MCN-MR es realizada en [6], donde se propone un esquema que selecciona el modo de conexión (SH o MH), y en el caso de MH, identifica de manera simultánea el RN a utilizar en la conexión MH. Para abordar ambos dilemas de manera conjunta, el mecanismo propuesto en [6] requiere que tanto el nodo destino de la comunicación (*Destination Node*, DN) como los posibles RN envíen información a la BS sobre el nivel de SINR (*Signal to Interference plus Noise Ratio*) experimentado y la distancia entre ellos. Extraer esta información y su envío a la BS tiene un coste que puede no ser despreciable en escenarios con alta densidad de nodos en el sistema. En este contexto, los autores de este artículo proponen en [7] un esquema de selección de modo para redes MCN-MR que basa su decisión en información disponible en la BS, en particular, en la distancia entre la BS y el DN y en la densidad media de nodos en la celda. Con esta información, el esquema de selección de modo evalúa el posible beneficio y riesgo de establecer una conexión MH en lugar de un enlace celular SH tradicional, y decide el modo de conexión más conveniente en base a las condiciones de operación y de despliegue actuales. Además, el rendimiento de las conexiones MCN-MR también está condicionado por el número de recursos radio celulares disponibles para la conexión entre la BS y el RN más cercano a la BS. En este

contexto, un aspecto novedoso del esquema de selección de modo propuesto es que de manera simultánea a la decisión sobre el modo de conexión más conveniente (SH o MH), decide el número de recursos radio celulares que deberían ser utilizados en función del modo seleccionado.

Tal y como muestran [4] y [6], el uso de información de contexto es muy importante para realizar una gestión adecuada de los sistemas de comunicaciones (como por ejemplo, decidir sobre el modo de conexión a utilizar para cada transmisión). Este trabajo propone una versión mejorada del esquema de selección de modo propuesto en [7] incorporando información sobre el contexto del usuario en la decisión sobre el modo a utilizar en cada transmisión. Este trabajo evalúa la necesidad de considerar información precisa sobre el contexto actual del usuario, principalmente en sistemas MCN con retransmisores móviles, así como la mejora del rendimiento que proporciona. Además, se demuestra la capacidad del esquema propuesto para adaptar la decisión sobre el modo de conexión más adecuado para cada transmisión en escenarios con distintas densidades y distribuciones de nodos por la zona de cobertura de la BS.

II. Esquema de Selección de Modo

Este trabajo propone y estudia un esquema de selección de modo para redes MCN-MR que incorpora información sobre el contexto del usuario en el proceso de decisión sobre el modo más eficiente para llevar a cabo cada transmisión entre la BS y los DN. El esquema propuesto ha sido diseñado para transmisiones de servicios de datos en sentido descendente de manera que la BS puede decidir si establecer un enlace directo SH o una conexión MH con cada DN. Los autores de [8] muestran que la mayor parte del beneficio que puede proporcionar una conexión MCN-MR es alcanzado con un enlace de 2 saltos. Por este motivo, este trabajo se centra en el escenario de 2 saltos ilustrado en la Fig. 1, en el que la BS puede comunicar con el DN a través del enlace directo SH o a través de una conexión MH utilizando el nodo RN como nodo retransmisor. Este estudio considera que la conexión ad-hoc entre el RN y el DN es establecida utilizando tecnologías IEEE802.11. Aunque el esquema propuesto puede ser aplicado con cualquier tecnología celular, este estudio considera HSDPA (*High Speed Downlink Packet Access*) para las transmisiones celulares SH y el enlace celular entre la BS y el RN de la conexión MH. El único requisito de los terminales de usuario para actuar como RN es que tengan 2 interfaces radio para poder establecer el enlace celular con la BS y el enlace ad-hoc con el DN.

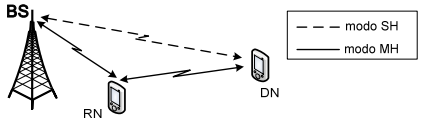


Fig. 1. Modo de conexión SH y MH entre la BS y el DN en un escenario MCN-MR de 2 saltos.

A. Beneficio y riesgo del modo MH

El esquema de selección de modo propuesto considera tanto los beneficios como los riesgos derivados de seleccionar el modo MH para llevar a cabo una comunicación entre la BS y un usuario en lugar de utilizar el enlace SH. Los beneficios que ofrece el uso del modo MH derivan de la posibilidad de encontrar un nodo RN que pueda establecer un enlace celular con la BS que proporcione un mayor rendimiento que el que podría establecer el DN, y que además pueda transferir este mayor rendimiento al DN mediante el establecimiento de un enlace ad-hoc adecuado entre el RN y el DN. Sin embargo, establecer una conexión MH implica también unos riesgos. En primer lugar, existe el riesgo de que la BS no pueda encontrar un RN con el que establecer un enlace celular con mayor rendimiento que el enlace que podría establecer con el DN. En segundo lugar, aunque se encontrara este RN, es posible que no sea posible establecer un enlace ad-hoc entre el RN y el DN con suficiente calidad para transferir el rendimiento experimentado por el RN hasta el DN. Estas circunstancias resultarían en el establecimiento de un enlace MH que proporcionaría al DN un menor rendimiento que el enlace SH que se podría haber establecido entre la BS y el DN. Además, el proceso de encontrar nodos retransmisores y establecer una conexión MCN-MR extremo a extremo tiene un coste significativo en términos de señalización, siendo importante por tanto considerar los riesgos de escoger el modo MH en la decisión del esquema de selección de modo.

Este trabajo considera un sistema celular con anillos de QoS (Fig. 2) caracterizados por distintos niveles de calidad de los enlaces y distintos modos de transmisión óptimos. Los anillos de QoS pueden ser definidos como el área de cobertura de la BS en la que un determinado modo de transmisión es utilizado en mayor porcentaje. Los anillos de QoS más interiores están caracterizados por mejores niveles de calidad de enlace y, por tanto, por el uso de modos de transmisión con mayores tasas de transmisión de datos. El anillo de QoS en el que el modo de transmisión *h* es utilizado en mayor porcentaje ha sido denotado como R*h*.

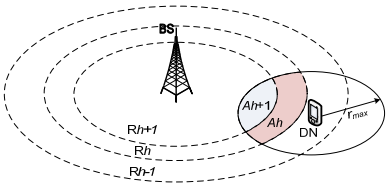


Fig. 2. Área de localización de los RN que permiten establecer al DN una conexión MH con mayor rendimiento que el enlace SH.

Un enlace MH mejoraría el rendimiento experimentado por un nodo DN a través del enlace SH si el enlace MH utiliza un RN situado en un anillo Rh^{RN} con un nivel de QoS mayor que el anillo Rh^{DN} en el que se encuentra el DN en el momento de establecer la conexión, es decir, si Rh^{RN} es tal que $h^{RN} > h^{DN}$. Además, es necesario que los nodos DN y RN se encuentren a una distancia máxima r_{max} que permita transferir el rendimiento experimentado por el RN hasta el DN [9]. Por lo tanto, una conexión MH proporcionaría al DN un rendimiento mayor que el enlace SH si la BS encontrara un RN dentro del área *A* definida como la unión de las áreas Ah^{RN} mostradas en la Fig. 2, las cuales se definen como el área de intersección entre el círculo C^{DN} (centrado en DN y con radio r_{max}) y los anillos Rh^{RN} con $h^{RN}>h^{DN}$:

$$A = \bigcup_{h^{RN},\, h^{RN} > h^{DN}} Ah^{RN} = \bigcup_{h^{RN},\, h^{RN} > h^{DN}} \left(\mathrm{R}h^{RN} \cap C^{DN} \right) \qquad (1)$$

En este contexto, el rendimiento esperado $P_{MH}(s,d)$ de una conexión MH puede definirse como:

$$P_{MH}(s,d) = Beneficio_{MH}(s,d) \cdot (1 - Riesgo_{MH}(d)) \qquad (2)$$

donde $Beneficio_{MH}$ representa el beneficio en términos de rendimiento que una conexión MH podría proporcionar al DN si se establece en condiciones adecuadas, y

$Riesgo_{MH}$ representa el riesgo de no poder establecer una conexión MH bajo dichas condiciones. El beneficio esperado por el DN de una conexión MH, $Beneficio_{MH}$, puede expresarse en función de la distancia *d* entre el DN y la BS y el número de recursos radio *s* asignados al enlace celular entre el RN y la BS según muestra la siguiente expresión:

$$Beneficio_{MH}(s,d) = \frac{\sum_{h^{RN},\, h^{RN}>h^{DN}} P_{\mathrm{SH}}(s, \mathrm{R}h^{RN}) \cdot \mathrm{Prob}(\mathrm{RN\ en}\ Ah^{RN})}{\sum_{h^{RN},\, h^{RN}>h^{DN}} \mathrm{Prob}(\mathrm{RN\ en}\ Ah^{RN})} \quad (3)$$

En (3), $P_{\mathrm{SH}}(s, \mathrm{R}h^{RN})$ representa el rendimiento del enlace celular entre la BS y un nodo RN situado en $\mathrm{R}h^{RN}$ cuando se asignan *s* recursos radio celulares a dicho enlace y Prob(RN en Ah^{RN}) representa la probabilidad de encontrar un RN dentro del área Ah^{RN} definida en (1). Es importante resaltar que $Beneficio_{MH}(s,d)$ y por tanto $P_{MH}(s,d)$, depende de la distancia *d* entre la BS y el DN que determina el área de intersección Ah^{RN} de C^{DN} con los anillos de QoS $\mathrm{R}h^{RN}$, y por tanto, que determina la probabilidad de encontrar un RN en dicha área. Por otro lado, $P_{\mathrm{SH}}(s, \mathrm{R}h)$ se define en función del anillo R*h* en el que se encuentre el nodo correspondiente ($\mathrm{R}h^{RN}$ o $\mathrm{R}h^{DN}$ para RN o DN) ya que es razonable considerar que todos los usuarios situados en el mismo anillo R*h* experimentan en media el mismo rendimiento celular al recibir el mismo número de recursos radio.

En (2), el riesgo resultante de intentar establecer una conexión MH deriva de la probabilidad de no encontrar un RN en el área *A* definida en (1):

$$Riesgo_{MH}(d) = 1 - \mathrm{Prob}(\mathrm{RN\ en}\ A) \quad (4)$$

$Riesgo_{MH}(d)$ se define en función de *d* ya que de nuevo la distancia *d* entre la BS y el DN determina el área de intersección de C^{DN} con los anillos de QoS $\mathrm{R}h^{RN}$.

B. Información de contexto del usuario

Tanto el beneficio como el riesgo de elegir el modo MH para llevar a cabo una transmisión entre la BS y un usuario DN se definen en función de la probabilidad de encontrar un nodo RN en el área *A* definida en (1). La probabilidad de encontrar un nodo en un área determinada de la zona de cobertura, Prob(RN en *A*) o Prob(RN en Ah^{RN}), depende tanto de la densidad y distribución de nodos en la celda como del tamaño del área considerada. Realizar la estimación de estas probabilidades en base a información sobre el contexto del usuario permite estimar de manera precisa el beneficio y el riesgo que supondría la elección del modo MH en el proceso de selección de modo llevado a cabo por el esquema propuesto, permitiendo elegir el modo más eficiente para cada transmisión entre la BS y los usuarios. Para ello, el esquema de selección de modo hace uso de información disponible en la BS sobre el contexto del usuario.

En primer lugar, el esquema de selección de modo utiliza información sobre la distancia del DN a la BS para estimar el rendimiento de la conexión SH. Además, en base a esta distancia, el esquema calcula el área *A* en la cual debería encontrarse el RN para establecer una conexión MH que proporcione al DN un mayor rendimiento que la conexión SH directa con la BS. En segundo lugar, el esquema de selección de modo utiliza información proporcionada por la BS sobre la densidad de nodos en la celda (información disponible pues la BS conoce el número de nodos en su área de cobertura y la distancia aproximada a la que se encuentran).

La distribución de los nodos en sistemas de comunicaciones móviles e inalámbricas es comúnmente modelada en la literatura mediante un proceso homogéneo de Poisson [10]. Según este modelo, el número de nodos en una cierta región de área *Z* se distribuye según una distribución de Poisson con parámetro ρZ, siendo ρ la densidad media de nodos. Cuando los nodos se mueven según un modelo de movilidad que mantiene la distribución homogénea de los nodos por toda la celda a lo largo del tiempo (por ejemplo, el modelo de movilidad *Random Direction* o RD), la probabilidad de encontrar al menos un nodo en un área *Z* puede ser calculada según la distribución de Poisson como:

$$\mathrm{Prob}(\mathrm{nodo\ en}\ Z) = 1 - \exp(-\rho_{0-d_{BS}} Z) \quad (5)$$

donde $\rho_{0-d_{BS}}$ es la densidad media de nodos en el área de cobertura de la BS y es calculada como el cociente entre el número total de nodos, *N*, y el valor de dicha área:

$$\rho_{0-d_{BS}} = N / \pi d_{BS}^2 \quad (6)$$

En (6), d_{BS} representa el radio de la celda. Sin embargo, el movimiento de los nodos en sistemas reales suele dar lugar a distribuciones de nodos no uniformes a lo largo del área de cobertura de la BS. En este caso, la distribución espacial de los nodos en una región con área *Z*, siendo *Z* mucho menor que el área de cobertura de la BS por la cual se desplazan los nodos, es decir, $Z << \pi d_{BS}^2$, puede de nuevo ser aproximada por una distribución de Poisson [11]. En este contexto, la probabilidad de encontrar un nodo en una región con área *Z*, $Z << \pi d_{BS}^2$, puede calcularse utilizando (5). Sin embargo, en un escenario con distribución no uniforme de los nodos, considerar la densidad media de nodos en la celda en (5) puede conllevar un error considerable en la estimación de Prob(nodo en *Z*). Por este motivo, en este trabajo se propone el uso de información sobre la densidad media de nodos en el anillo que intersecciona con el área *Z* para la cual se quiere calcular la probabilidad de encontrar al menos un nodo en ella. El esquema de selección de modo hace uso de la información sobre la densidad media de nodos en el anillo determinado por los radios interior y exterior d_{min} y d_{max}, representada por $\rho_{d_{min}-d_{max}}$. d_{min} y d_{max} corresponden a la distancia hasta la BS del punto del área *Z* más cercano y más distante a la BS respectivamente (en el caso del cálculo de Prob(RN en Ah^{RN}), $\rho_{d_{min}-d_{max}}$ corresponde a la densidad de nodos en el anillo de QoS $\mathrm{R}h^{RN}$). Si $N_{d_{min}-d_{max}}$ representa el número de nodos que se encuentran a una distancia *d* de la BS tal que $d_{min} < d \le d_{max}$, $\rho_{dmin\text{-}dmax}$ es calculada como:

$$\rho_{d_{min}-d_{max}} = N_{d_{min}-d_{max}} / \left(\pi d_{\max}^2 - \pi d_{\min}^2\right) \quad (7)$$

Es importante resaltar que tanto $\rho_{0-d_{BS}}$ como $\rho_{d_{min}-d_{max}}$ es información disponible en la BS y que ésta proporciona al esquema de selección de modo en el momento de la decisión.

C. Selección de modo

El rendimiento de los modos de conexión SH y MH dependen del número de recursos radio celulares asignados y, por tanto, de la política de gestión de recursos radio (*Radio Resource Management*, RRM) implementada. Este trabajo emplea una versión adaptada de la técnica RRM MAXIHU

(*MAXImum Homogeneous Utility values*) propuesta por los autores en [12] para redes heterogéneas. MAXIHU fue originalmente diseñada para decidir para cada usuario la tecnología de acceso radio (*Radio Access Technology*, RAT) más adecuada. En este estudio, MAXIHU ha sido adaptada para abordar el dilema de selección de modo en redes MCN-MR. De manera diferente a propuestas de selección de modo anteriores, MAXIHU no sólo decide si una nueva transmisión en sentido descendente debe realizarse en el modo SH o MH, sino que también identifica el número de recursos radio celulares a utilizar (para ambos modos SH o MH).

MAXIHU tiene como objetivo proporcionar los mayores niveles de satisfacción a todos los usuarios. Para ello, MAXIHU explota la flexibilidad que ofrece un escenario multimedia en el que los usuarios presentan diferentes demandas y requieren un número diferente de recursos radio para obtener los mismos niveles de satisfacción. En este contexto, el nivel de satisfacción del usuario es expresado por valores de utilidad que identifican el número de recursos radio requerido por cada usuario para alcanzar distintos niveles de QoS en función del servicio demandado y de la tecnología utilizada en la transmisión. Para alcanzar su objetivo, MAXIHU busca maximizar el producto de los valores de utilidad percibidos por todos los usuarios en el sistema, expresado según la siguiente función objetivo:

$$\max \prod_{i=1}^{n} u_i = \max \sum_{i=1}^{n} \ln u_i \tag{8}$$

En (8), n representa el número total de usuarios demandando servicio en la celda y u_i representa el valor de utilidad asignado al usuario i en cada reparto de recursos radio. El valor de utilidad experimentado por cada usuario u_i es expresado como $u_i = \sum_{m=1}^{2}\sum_{s=1}^{S} U_i(s,m) \cdot y_i^{s,m}$, donde $U_i(s,m)$ representa el valor de utilidad obtenido por el usuario i cuando recibe s recursos radio celulares en el modo m (en este estudio, $m \in \{SH, MH\}$) y $s \in [1,S]$ siendo S el número máximo de recursos radio celulares. $y_i^{s,m}$ es una variable binaria igual a uno si el usuario i recibe s recursos radio en el modo m, e igual a cero en caso contrario. En este contexto, el esquema de selección de modo propuesto se centra en decidir para cada usuario que variable $y_i^{s,m}$ toma el valor uno, considerando sólo variables $y_i^{s,m}$ correspondientes a asignaciones de recursos que proporcionan un valor de utilidad no nulo al usuario en el modo m. Identificar el valor de estas variables no sólo indicará el modo de conexión más apropiado (SH o MH) para cada usuario, sino que también indica el número de recursos radio celulares que deberían utilizarse en la conexión. En el modo MH, los recursos radio celulares son utilizados en el enlace entre la BS y el RN.

Para obtener la solución óptima al problema modelado, MAXIHU hace uso de técnicas de programación lineal entera. Por tanto, la función objetivo definida en (8) debe ser expresada de forma lineal, tal y como muestra la siguiente expresión (más información sobre la transformación matemática de la función objetivo puede encontrarse en [12]):

$$\max \sum_{i=1}^{n}\sum_{m=1}^{2}\sum_{s=1}^{S} \ln\left(U_i(s,m)\right) \cdot y_i^{s,m} \tag{9}$$

La solución óptima para la función objetivo de MAXIHU debe cumplir varias restricciones impuestas por el sistema, las cuales deben ser expresadas también linealmente. En primer lugar, la solución está condicionada por el número limitado de recursos radio celulares disponibles en el sistema. En el escenario analizado en este trabajo, los recursos radio celulares son utilizados tanto por las transmisiones SH como por el enlace celular entre la BS y el RN que forma parte de la conexión MH. En este contexto, la restricción sobre la cantidad de recursos radio celulares disponibles en el sistema es expresada como:

$$\sum_{i=1}^{n}\sum_{s=1}^{S} s \cdot y_i^{s,SH} + \sum_{i=1}^{n}\sum_{s=1}^{S} s \cdot y_i^{s,MH} \le S \tag{10}$$

La segundo restricción expresa el hecho de que cada usuario sólo puede tener una variable $y_i^{s,m}$ igual a uno:

$$\sum_{s=1}^{S} y_i^{s,SH} + \sum_{s=1}^{S} y_i^{s,MH} \le 1 \qquad \forall i \tag{11}$$

MAXIHU basa sus decisiones en los valores de utilidad que un usuario podría alcanzar al utilizar el modo de conexión SH o MH. En este contexto, es necesario integrar las métricas de beneficio y riesgo definidas en el apartado II.A. en la definición de los valores de utilidad utilizados por MAXIHU. Estos valores de utilidad intentan caracterizar el nivel de satisfacción del usuario en función del servicio de tráfico demandado, el modo de conexión (SH o MH) y el número de recursos radio celulares asignados. Este estudio evalúa el esquema de selección de modo propuesto en un escenario en el que todos los usuarios demandan transmisiones del servicio de navegación web. Siguiendo el análisis presentado en [12], los valores de utilidad para el servicio de navegación web $u_{web}(\cdot)$ se definen en función del *throughput* (th) experimentado por el usuario según:

$$u_{web}(th) = \begin{cases} 0 & \text{si } th \le 1\text{Mbps} \\ \text{A} \cdot \exp(\text{B} \cdot (th - 1)) + 0.24 & \text{si } th \le 2.3\text{Mbps} \\ 1 - \text{C} \cdot \exp(-\text{D} \cdot th) & \text{si } th > 2.3\text{Mbps} \end{cases} \tag{12}$$

con A = 0.00013, B = 0.0056, C = 2.13 y D = 0.0025

Para establecer la relación entre los valores de utilidad con el proceso de selección de modo, es necesario estimar el *throughput* experimentado por los usuarios en función de los distintos modos de conexión que el usuario puede establecer para llevar a cabo su transmisión (SH o MH) y el número de recursos radio celulares asignados. En el caso de una conexión SH o para el enlace entre la BS y el RN en una conexión MH, el *throughput* experimentado por el usuario que comunica con la BS depende del número de recursos radio celulares asignados y del anillo de QoS en el que se encuentre (Rh, con h igual a h^{RN} o h^{DN} para RN o DN). En este caso, el *throughput* experimentado por el usuario se denota como $th_{SH}(s,\text{R}h)$.

Este estudio considera HSDPA para las transmisiones celulares. En HSDPA, los modos de transmisión se definen por la combinación de esquemas de modulación y codificación (MCS, *Modulation and Coding Schemes*), dando lugar a diferentes tasas de transmisión. Cada modo de transmisión está asociado con un valor de CQI (*Channel Quality Indicator*). Este estudio considera los 30 modos de transmisión asociados a los CQI definidos para terminales de categoría 10 (3GPP TS 25.214). En este contexto, el

throughput experimentado por un nodo $th_{SH}(s,\mathrm{R}h)$ a través del enlace SH puede expresarse como:

$$th_{SH}(s,\mathrm{R}h) = s \cdot rate_{CQIh} / codes_{CQIh} \quad (13)$$

donde $rate_{CQIh}$ y $codes_{CQIh}$ representa la tasa de transmisión de datos y el número de códigos del modo de transmisión asociado al CQI experimentado en R*h*. Utilizando (13), el valor de utilidad que experimentaría el nodo DN *i* en el caso de comunicar con la BS a través de una conexión SH con *s* recursos radio celulares se expresa como:

$$U_i(s,SH) = U_{SH}(s,\mathrm{R}h_i^{DN}) = u_{web}(th_{SH}(s,\mathrm{R}h_i^{DN})) \quad (14)$$

Por otro lado, el valor de utilidad para el DN *i* en el caso de utilizar una conexión MH se define en función de la distancia d_i entre el usuario *i* y la BS (2):

$$U_i(s,MH) = U_{MH}(s,d_i) = Beneficio_{MH}(s,d_i) \cdot (1 - Riesgo_{MH}(d_i)) \quad (15)$$

donde $Beneficio_{MH}(s,d_i)$ y $Riesgo_{MH}(d_i)$ son calculados según las expresiones (3) y (4), sustituyendo $P_{\mathrm{SH}}(s,\mathrm{R}h)$ por el valor de utilidad $U_{SH}(s,\mathrm{R}h)$ definido en (14).

El esquema de selección de modo propuesto utiliza los valores de utilidad definidos en (14) y (15) para caracterizar el nivel de satisfacción que los usuarios pueden alcanzar utilizando los modos de conexión SH o MH. El esquema de selección de modo propuesto decide en base a estos valores el mejor modo de conexión para cada transmisión resolviendo el problema de programación lineal entera modelado, es decir, decidiendo para cada usuario, qué variable $y_i^{s,m}$ toma el valor 1. Además de decidir el mejor modo de conexión a utilizar para cada usuario, la decisión alcanzada también indica el número de recursos radio celulares a utilizar en cada conexión.

III. Entorno de Evaluación

El rendimiento del esquema de selección de modo propuesto ha sido evaluado utilizando una plataforma software propia implementada en C++ que simula un sistema con una única celda de radio 1000m. Aunque el esquema de selección de modo propuesto podría ser aplicado con cualquier tecnología celular, en la plataforma de evaluación se ha considerado HSDPA para las transmisiones SH y para el enlace entre la BS y los RNs en las conexiones MH. Para las conexiones ad-hoc entre los RNs y los DNs se considera el uso de IEEE 802.11g. Estas dos tecnologías han sido consideradas por la disponibilidad de un modelo empírico del *throughput* experimentado por enlaces MH de dos saltos propuesto en [9], y que ha sido incluido en la plataforma para modelar el *throughput* experimentado a través de conexiones MH. En base a este modelo, el valor de r_{max} se ha establecido en 150m. Este estudio considera los modos de transmisión de HSDPA asociados a los 30 CQI definidos para terminales de usuario de categoría 10 (3GPP TS 25.214). Las tasas de transmisión para los enlaces celulares (enlaces SH o enlaces BS-RN de conexiones MH) son seleccionadas en base al anillo de QoS en el que se encuentre el nodo (los anillos de QoS están asociados a los 30 CQI considerados). El objetivo de la plataforma no es modelar de forma precisa la transmisión radio, sino para medir la eficiencia del esquema propuesto bajo diferentes condiciones y escenarios. En este contexto, este estudio considera un escenario simplificado en el que no se modelan errores en la transmisión celular (el *throughput* es igual a la tasa de transmisión de datos utilizada)[1]. La BS dispone de una portadora con 14 códigos para transmisiones de datos.

Si se dispone de varios nodos que puedan actuar como RN en la zona *A* expresada en (1) en el establecimiento de ua conexión MH, el RN es seleccionado de manera aleatoria entre todos los candidatos. Si no es posible encontrar ningún RN en *A*, el nodo seleccionado como RN es aquel que se encuentre más cerca del DN y a una menor distancia de la BS que el DN. En ese caso, es posible que el *throughput* del enlace MH sea menor que el que podría haber experimentado el DN si hubiera utilizado el enlace SH entre la BS y el DN.

La plataforma simula nodos que pueden actuar solamente como RN y nodos que pueden actuar como DN. Los usuarios DN demandan sesiones del servicio de navegación web[2] según el modelo presentado en [13]. Al comienzo de la simulación, los usuarios se distribuyen por toda la celda según una distribución de Poisson homogénea con densidad media $\rho_{0-d_{BS}}$. Para analizar la capacidad del esquema de selección de modo propuesto para seleccionar el modo de conexión óptimo (SH o MH) bajo diferentes condiciones de operación, se han considerado diferentes densidades de nodos mostradas en la Tabla I (las densidades de nodos consideras pueden corresponder a densidades de usuarios en entornos sub-urbanos o urbanos). Además, se ha considerado distintos modelos de movilidad que dan como resultado distintas distribuciones de los nodos en la celda. En primer lugar, se ha considerado el modelo de movilidad *Random Direction* (RD). RD selecciona de forma aleatoria una velocidad y dirección de movimiento para cada nodo. Cuando un nodo alcanza el borde de la celda, elige una nueva dirección y velocidad para continuar desplazándose. Este modelo de movilidad resulta en una distribución uniforme de los nodos en la celda en cualquier momento de la simulación. En segundo lugar, se ha simulado también el modelo de movilidad *Random Waypoint* (RW). RW selecciona una velocidad y un punto al cual dirigirse dentro de la celda de manera aleatoria. Cuando el nodo alcanza su punto destino, selecciona otro de manera aleatoria y se dirige hacia él. RW da lugar a una distribución no homogénea de los nodos en la celda, siendo mayor la concentración de nodos a menores distancias de la BS como se muestra en la

TABLA I
Escenarios de Evaluación y Densidades de Nodos

Escenario	Número de nodos en la celda	Densidad media de nodos $\rho_{0-d_{BS}}$ (nodos/km^2)	Nodos en una circunferencia de radio 150m
50RN	50	15.9	1.13
100RN	100	31.8	2.25
400RN	400	127.3	9.00
1000RN	1000	318.3	22.50

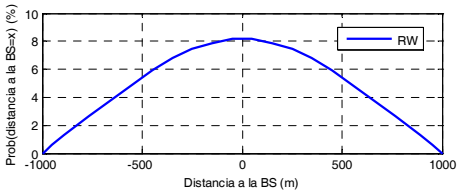


Fig. 3. Distribución de los nodos en la celda en función de la distancia a la BS con el modelo de movilidad RW (corte transversal por la BS).

[1] Este hecho no influencia la ganancia relativa alcanzada por el esquema de selección de modo propuesto.

[2] El rendimiento del esquema de selección de modo propuesto ha sido también evaluado bajo otras condiciones de tráfico multimedia mostrando las mismas tendencias en el rendimiento mostradas en este artículo.

Fig. 3. Para ambos modelos, la velocidad de los nodos es elegida de manera aleatoria entre 0 y 3m/s.

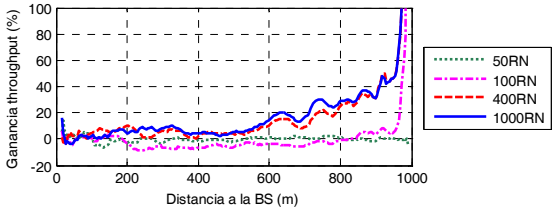
IV. Análisis de Rendimiento

El rendimiento alcanzado por el esquema propuesto ha sido evaluado en 2 escenarios distintos según la distribución de los nodos en la celda. En primer lugar, se ha realizado la evaluación del esquema propuesto en un escenario en el que los nodos se distribuyen de manera homogénea por la celda (uso del modelo de movilidad RD). Tras analizar el buen comportamiento del esquema propuesto al considerar una distribución uniforme de los nodos, se ha evaluado su rendimiento en un escenario más realista en el que los nodos se distribuyen de manera no homogénea por la celda (uso del modelo de movilidad RW). En este escenario es posible evaluar la capacidad del esquema propuesto para adaptarse a distintas condiciones de operación y despliegue del sistema. En ambos escenarios, el rendimiento alcanzado por el esquema de selección de modo propuesto ha sido comparado con el obtenido cuando sólo es posible utilizar el enlace SH directo tradicional (solo SH) y cuando sólo es posible utilizar el modo MH entre la BS y el DN (solo MH). Para realizar una comparación justa, MAXIHU es aplicado para realizar la gestión de los recursos radio celulares en ambos casos.

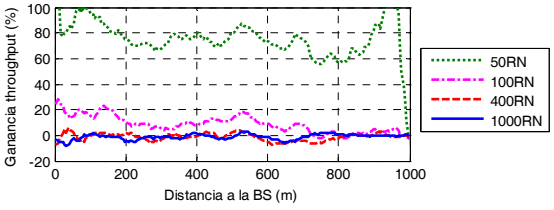
A. Escenario con distribución homogénea de los nodos

La Fig. 4 muestra la ganancia en términos de *throughput* que puede ser alcanzada utilizando el esquema de selección de modo en comparación a cuando sólo se considera el uso del modo SH y el modo MH respectivamente para llevar a cabo las transmisiones entre la BS y los DN. La ganancia obtenida es mostrada en función de la distancia entre el DN y la BS para las distintas densidades de nodos recogidas en la Tabla I. Además, la Fig. 5.a muestra el porcentaje de transmisiones satisfactorias realizadas cuando se aplica el esquema de selección de modo propuesto y para los casos en que sólo se considera el uso del modo SH y el modo MH respectivamente. Según las indicaciones dadas en 3GPP TS 22.105, la transmisión de una página web se considera satisfactoria si ésta se realiza en menos de 4 segundos. Los resultados mostrados en ambas figuras muestran que el rendimiento obtenido con el esquema de selección de modo propuesto es siempre igual o superior que cuando sólo se considera la posibilidad de establecer la comunicación a través de un único modo de conexión. La ganancia de *throughput* obtenida con el esquema de selección de modo con respecto a cuando sólo se considera el uso del modo SH (Fig. 4.a) aumenta con la distancia entre el DN y la BS para densidades de nodos medias y altas. Las ganancias son particularmente altas para DNs en el borde de la celda (ganancias superiores al 20% para usuarios situados a distancias superiores a 700m), lo cual es deseable ya que estos usuarios son los que experimentan los enlaces celulares con peor rendimiento, siendo por tanto los usuarios que más pueden beneficiarse del uso de redes MCN-MR.

De manera contraria, la ganancia que ofrece el esquema de selección de modo propuesto con respecto a cuando sólo se utilizan conexiones MH (Fig. 4.b y Fig. 5.a), es mayor cuanto menor es la densidad de nodos en la celda. En los escenarios con densidades media y alta, el rendimiento es prácticamente el mismo que al utilizar sólo el modo MH. La alta ganancia de *throughput* obtenida en los escenarios con menor densidad de nodos resalta el hecho de que el uso del enlace MH no siempre es adecuado. Cuando la densidad de nodos en el sistema es baja, la probabilidad de encontrar un RN en el área A definida en (1) es baja. En los casos en los que no se encuentra un RN en A la conexión MH se establece utilizando un RN fuera de dicha área (se elige el RN más cercano al DN y que se encuentre a una distancia menor de la BS que el DN). En estos casos, el rendimiento obtenido a través de la conexión MH es bajo, obteniendo incluso un rendimiento menor que el que se obtiene mediante el enlace SH directo entre el DN y la BS; resultado que se extrae al observar la alta ganancia obtenida en los escenarios con baja densidad de nodos con respecto al uso de solo MH y la ganancia aproximadamente igual a 1 con respecto al uso del modo tradicional SH en estos mismos escenarios. Por este motivo, el porcentaje de transmisiones para las cuales el esquema de selección de modo propuesto elige el modo MH (resultados mostrados en la Fig. 6) en los escenarios con baja densidad de nodos es muy bajo, tan sólo el 3% y el 27% de las transmisiones en los escenarios 50RN y 100RN utilizan el modo MH. Es interesante resaltar el hecho de que la ganancia de *throughput* obtenida en los escenarios con densidad baja de nodos por el esquema de selección de modo propuesto con respecto a cuando sólo se considera el modo MH es aproximadamente uniforme independientemente de la distancia del usuario a la BS. Este hecho se debe a que la distribución homogénea de los nodos en la celda resulta en una probabilidad alta de no encontrar un nodo retransmisor adecuado aproximadamente igual a lo largo de toda la celda (existen diferencias por el cálculo del área en el que se busca el nodo). Al aumentar la densidad de nodos en el sistema, la

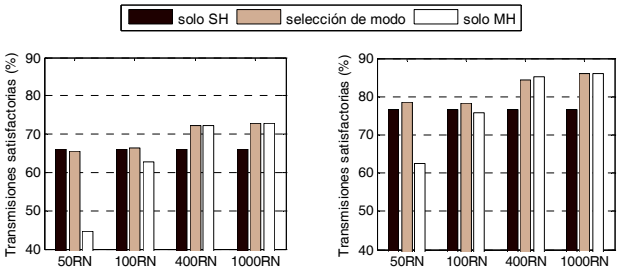


a) Ganancia con respecto al uso solamente del modo SH.



b) Ganancia con respecto al uso solamente del modo MH.

Fig. 4. Ganancia del *throughput* medio experimentado por los usuarios con el esquema de selección de modo con respecto al uso de solo modo SH y solo modo MH (escenario con distribución homogénea de los nodos).



a) Escenario con distribución de nodos homogénea.

b) Escenario con distribución de nodos no homogénea.

Fig. 5. Porcentaje de transmisiones satisfactorias.

probabilidad de encontrar un nodo retransmisor dentro del área de interés aumenta, y por tanto, los riesgos para establecer una conexión MH decrecen. En este caso, el esquema de selección de modo aumenta el porcentaje de transmisiones a través del modo MH (Fig. 6) consiguiendo un aumento del *throughput* experimentado por el usuario (Fig. 4) y de transmisiones satisfactorias (Fig. 5.a).

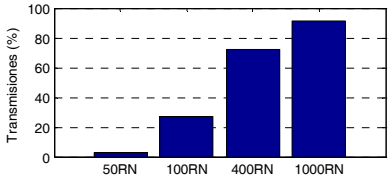


Fig. 6. Porcentaje de transmisiones a través del modo MH con el esquema de selección de modo en escenario con distribución de nodos homogénea.

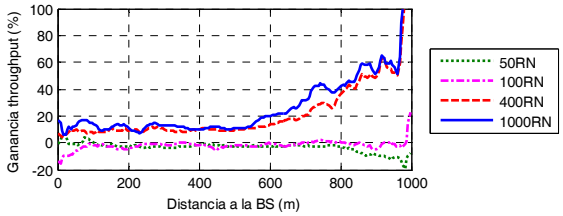
B. Escenario con distribución no homogénea de los nodos

En primer lugar, se ha evaluado el rendimiento del esquema propuesto cuando el riesgo y beneficio de seleccionar el modo MH, $Riesgo_{MH}$ y $Beneficio_{MH}$, es estimado considerando la densidad media de nodos en la celda (esquema denotado en las figuras y tablas como selección de modo-$\rho_{0-d_{BS}}$). La Fig. 7 muestra la ganancia en términos del *throughput* medio experimentado por los usuarios con el esquema de selección de modo con respecto a los casos en los que sólo se considera el uso del modo SH y del modo MH respectivamente y la Fig. 5.b muestra el porcentaje de transmisiones satisfactorias para cada caso en el escenario con distribución de nodos no homogénea. Como es posible observar en ambas figuras, a pesar de la distribución no homogénea de los nodos en la celda, el esquema de selección de modo propuesto proporciona de nuevo un rendimiento igual o superior que al considerar solamente la posibilidad de transmitir por un único modo en todos los escenarios. Al analizar la ganancia de *throughput* obtenida con el esquema de selección de modo propuesto, es posible observar que la ganancia en el escenario con distribución de nodos no homogénea es incluso mayor que cuando los nodos se distribuyen de manera homogénea. Este resultado es debido a que la mayor concentración de nodos a distancias cortas de la BS hace que la probabilidad real de establecer un enlace MH con mayor rendimiento que el enlace SH directo entre la BS y el DN sea mayor que en el escenario con distribución homogénea de los nodos (y mayor que la considerada al utilizar la densidad media de nodos en la celda). Este hecho resulta en un mayor porcentaje de transmisiones satisfactorias, tal y como muestra la Fig. 5.b.

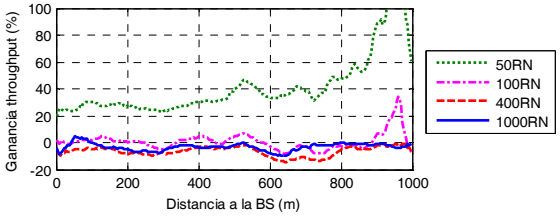
Al comparar la ganancia de *throughput* obtenida con respecto al caso en el que sólo se considera el modo MH (Fig. 7.b), la mayor concentración de nodos cerca de la BS resulta también en una reducción de la ganancia de *throughput* obtenida por el esquema propuesto en escenarios con densidad baja de nodos en comparación con el escenario en el que los nodos se distribuyen de manera homogénea. La mayor concentración de nodos cerca de la BS hace que el porcentaje de transmisiones MH que no encuentran un RN adecuado para establecer la comunicación disminuye, aumentando el *throughput* medio experimentado por los usuarios cerca de la BS en el caso en que sólo se considera el modo MH. Este hecho hace que la ganancia obtenida por el esquema de selección de modo sea menor a estas distancias.

Considerando la distribución no homogénea de nodos en la celda, es interesante analizar el porcentaje de transmisiones para las cuales el esquema propuesto elige el modo MH en función de la distancia entre el DN y la BS. Para ello, la Fig. 8 muestra el porcentaje de transmisiones realizadas a través del modo MH en función de la distancia entre la BS y los usuarios para el escenario 100RN con distribución no homogénea de los nodos (RW-$\rho_{0-d_{BS}}$). Para realizar un análisis comparativo, la figura muestra también esta misma información para el caso en que el esquema propuesto es aplicado en el mismo escenario con distribución homogénea de los nodos (RD). Como es posible observar en la figura, el esquema de selección de modo elige el modo MH para el mismo porcentaje de transmisiones independientemente de la distribución de los nodos en el escenario, es decir, la mayor o menor densidad de nodos a distintas distancias de la BS no afecta a la decisión sobre el modo de conexión a utilizar. Este hecho conlleva errores que hacen que no se obtenga el mayor beneficio posible del sistema. A distancias cortas de la BS en las que la densidad de nodos real es mayor que la densidad media de nodos en la celda (considerada en el cálculo de $Riesgo_{MH}$ y $Beneficio_{MH}$), el riesgo real de seleccionar el modo MH es sobreestimado, no eligiendo el modo MH cuando probablemente la probabilidad de encontrar un RN adecuado era alta. Por el contrario, en los bordes de la celda donde la densidad de nodos real es menor que la densidad media de nodos en la celda, $Riesgo_{MH}$ es subestimado, lo cual puede resultar en el establecimiento de enlaces MH con un rendimiento menor al del enlace SH entre el DN y la BS.

Dado el anterior resultado, se propone la estimación de $Riesgo_{MH}$ y $Beneficio_{MH}$ en función de la densidad media de nodos en el contexto más cercano al usuario o DN, es decir, en función de la densidad media de nodos en los anillos en los que se debe buscar al nodo que actúe como RN en la conexión MH, $\rho_{d_{min}-d_{max}}$ (tal y como se presentó en la sección II.B). La Fig. 8 muestra también el porcentaje de transmisiones en función de la distancia entre la BS y los usuarios realizadas con el modo MH cuando el esquema de selección de modo utiliza $\rho_{d_{min}-d_{max}}$ en el escenario con distribución no homogénea de los nodos (RW-$\rho_{d_{min}-d_{max}}$). Tal y como muestran los resultados, al considerar la densidad media de nodos por anillo, el esquema de selección de modo



a) Ganancia con respecto al uso de solo el modo SH.



b) Ganancia con respecto al uso de solo el modo MH.

Fig. 7. Ganancia del *throughput* medio experimentado por los usuarios con el esquema de selección de modo-$\rho_{0\text{-}dBS}$ con respecto al uso de solo modo SH y solo modo MH (escenario con distribución no homogénea de nodos).

elige el modo MH para un mayor porcentaje de transmisiones para usuarios cercanos a la BS (entre los 150 y 400m) al evaluar un riesgo $Riesgo_{MH}$ menor que cuando se considera la densidad media de nodos en la celda. Por el contrario, la elección del modo MH para trasmisiones en el borde de la celda disminuye, ya que al considerar información más precisa sobre la densidad media de nodos en el contexto próximo al DN se obtiene una probabilidad menor de encontrar un nodo RN en el área de interés. La elección nula del modo MH para transmisiones realizadas con usuarios entre los 400 y 550m de la BS se debe a que el beneficio que ofrece el uso del modo MH a esas distancias no compensa el riesgo de seleccionar el modo MH en el escenario con baja densidad de nodos (el aumento de *throughput* que ofrece un enlace SH al pasar de un anillo de QoS al inmediatamente superior en esas distancias es menor que en otras zonas de la celda y no compensa el riesgo que supone la elección del modo MH en el escenario 100RN).

Por último, la Tabla II compara el porcentaje de transmisiones para las que el esquema propuesto selecciona el modo que proporciona al usuario el mayor *throughput* por recurso celular asignado cuando se considera respectivamente información sobre la densidad media de nodos en la celda o por anillos en el escenario con distribución de nodos no homogénea. Los resultados muestran que incorporando información sobre la densidad media de nodos en el contexto más cercano del usuario al evaluar el riesgo y beneficio de elegir el modo MH es posible aumentar el porcentaje de transmisiones que se realizan a través del modo más eficiente. Por ejemplo, el porcentaje de transmisiones que utilizan el modo que proporciona el mayor *throughput* por recurso asignado aumenta en un 10% y un 11% en los escenarios 100RN y 400RN al considerar la densidad media de nodos por anillo. De esta manera, el esquema de selección de modo propuesto es capaz de adaptar la decisión sobre el modo a utilizar a las distintas condiciones de operación del sistema y al distinto contexto que experimentan los usuarios.

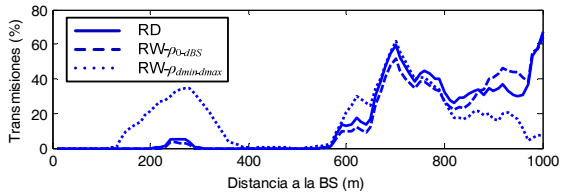


Fig. 8. Porcentaje de transmisiones que utilizan el modo MH en función de la distancia para el esquema de selección de modo propuesto.

TABLA II
PORCENTAJE DE TRANSMISIONES A TRAVÉS DEL MODO CON MAYOR THROUGHPUT POR RECURSO CELULAR EN ESCENARIO CON DISTRIBUCIÓN NO HOMOGÉNEA DE NODOS

	Selección de modo - $\rho_{0-d_{BS}}$	Selección de modo - $\rho_{d_{min}-d_{max}}$
50RN	55.37	57.69
100RN	43.04	47.43
400RN	68.00	75.52
1000RN	88.00	91.48

V. CONCLUSIONES

Este trabajo propone y evalúa un esquema de selección de modo para sistemas MCN-MR. El esquema propuesto selecciona el modo de conexión más adecuado (SH o MH) considerando información sobre la densidad de nodos y la distancia entre la BS y el DN. Esta información es utilizada para estimar tanto el beneficio como el riesgo presentes en el establecimiento de una conexión MH. Además, el esquema de selección de modo propuesto identifica el número de recursos radio celulares a utilizar según el modo de conexión seleccionado. Los resultados obtenidos muestran que el esquema de selección de modo propuesto puede mejorar significativamente el nivel de *throughput* experimentado por los usuarios principalmente en el borde de la celda en escenarios con densidad media y alta de usuarios. Además, mediante la consideración de información sobre la densidad de nodos en el contexto más cercano del DN, el esquema de selección de modo es capaz de adaptar sus decisiones y escoger en cada caso el modo más eficiente según las condiciones del contexto actual del usuario. El estudio realizado ha demostrado que el esquema de selección de modo propuesto es una herramienta válida para alcanzar los beneficios esperados de las redes MCN-MR en términos de la mejora de la capacidad y del rendimiento experimentado por los usuarios principalmente en el borde de la celda.

AGRADECIMIENTOS

Este trabajo ha sido financiado por el Ministerio de Economía y Competitividad y fondos FEDER bajo el proyecto TEC2011-26109.

REFERENCIAS

[1] L. Long and E. Hossain, "Multihop Cellular Networks: Potential Gains, Research Challenges, and a Resource Allocation Framework", *IEEE Communications Magazine,* vol.45, no.9, pp.66-73, Sept. 2007.

[2] 3GPP TR 36.806, "Evolved Universal Terrestrial Radio Access (E-UTRA); Relay architectures for E-UTRA (LTE-Advanced)", v9.0.0, Marzo 2010.

[3] J. Gozalvez and B. Coll-Perales, "Experimental Evaluation of Multi-Hop Cellular Networks using Mobile Relays", *IEEE Communications Magazine,* vol. 51, no. 1, pp. 122-129, Julio 2013.

[4] G. Fodor, et al., "Design Aspects of Network Assisted Device-to-Device Communications", *IEEE Communications Magazine*, vol. 50, no 3, pp. 170-177, 2012.

[5] S. Hakola, T. Chen, J. Lehtomaki, T. Koskela, "Device-to-Device (D2D) Communication in Cellular Network - Performance Analysis of Optimum and Practical Communication Mode Selection", *Proc. IEEE WCNC 2010*, Sydney, Australia, 2010, pp. 1-6.

[6] D. Wu, G. Zhu, L. Sun, D. Zhao, "Joint Mode/Route Selection and Power Allocation in Cellular Networks with Cooperative Relay", *Proc. IEEE ICC 2012,* Ottawa, Canada, 2012, pp. 4144-4149.

[7] M.C. Lucas-Estañ, J. Gozálvez, "Gestión de Recursos Radio en Sistemas *Multi-hop* Celular", Libro de Actas URSI 2012, Elche, 2012.

[8] S. Mukherjee, D. Avidor, K. Hartman, "Connectivity, Power, and Energy in a Multihop Cellular-Packet System", *IEEE Trans. on Vehicular Technology*, vol.56, no.2, pp.818-836, 2007.

[9] B. Coll-Perales, J. Gozalvez, J. Sanchez-Soriano, "Empirical Performance Models for P2P and Two Hops Multi-hop Cellular Networks with Mobile Relays", *Proc. 8th ACM PM2HW2N'13*, Nov. 2013, Barcelona.

[10] Z. Gong, M. Haenggi, "Interference and Outage in Mobile Random Networks: Expectation, Distribution, and Correlation", *IEEE Trans. On Mobile Computing*, early access, 2012.

[11] C. Bettstetter, "Topology properties of Ad hoc networks with random waypoint mobility", *ACM SIGMOBILE Mobile Computing and Communications Review*, v.7 n.3, Julio 2003.

[12] M.C. Lucas-Estañ and J. Gozalvez, "On the Real-Time Hardware Implementation Feasibility of Joint Radio Resource Management Policies for Heterogeneous Wireless Networks", *IEEE Trans. on Mobile Computing*, vol. 12, no. 2, pp. 193-205, 2013.

[13] R. Pries, Z. Magyari, P. Tran-Gia, "An HTTP Web Traffic Model Based on the Top One Million Visited Web Pages", *Proc. 8th EURO-NGI*, Karlskrona, Sweden, 2012, pp. 133-139.

Optimización del Tráfico P2P-TV mediante el uso de Técnicas de Compresión y Multiplexión

Idelkys Quintana-Ramirez, Jose Saldana, Jose Ruiz-Mas, Luis Sequeira, Julian Fernandez-Navajas, Luis Casadesus
Grupo de Tecnologías de las Comunicaciones (GTC) - Instituto de Investigación en Ingeniería de Aragón (I3A)
Dpt. IEC, Escuela de Ingeniería y Arquitectura, Edif. Ada Byron, Universidad de Zaragoza
50018, Zaragoza, España
Email: {idelkysq, jsaldana, jruiz, sequeira, navajas, luis.casadesus}@unizar.es

***Resumen*—En este trabajo se presenta un estudio sobre la optimización del tráfico P2P-TV, específicamente de SOPCast, una de las aplicaciones más utilizadas por los usuarios a día de hoy. En primer lugar se presenta una caracterización del tráfico, observándose que genera altas tasas de paquetes UDP de pequeño tamaño entre diferentes *peer*, presentando por tanto una eficiencia baja. Posteriormente se propone el uso de un método de optimización de ancho de banda basado en la compresión de las cabeceras y en la multiplexión de los paquetes originales. Se emplean dos políticas de multiplexión, la primera se basa en un *período* fijo y en la segunda se define un *umbral* para el tiempo entre paquetes. En las simulaciones se emplea una traza real del tráfico SOPCast, mostrándose para ambas políticas, una mejora en la eficiencia y valores significativos de ahorro de ancho de banda para el enlace de subida de un usuario (aproximadamente entre un 26% y un 35%). La cantidad de paquetes por segundo se reduce en un factor de 10 en ambos casos. Como contrapartida, se añade un retardo a los paquetes nativos, pero las pruebas muestran que no empeora la experiencia del usuario ni la calidad del vídeo percibido.**

***Palabras Clave*—P2P-TV, SOPCast, video-streaming, compresión, multiplexión, optimización del tráfico.**

I. INTRODUCCIÓN

En la actualidad, el creciente éxito de los servicios en tiempo real (ej. VoIP, juegos *online* y *video streaming*) junto con el incremento del número de usuarios que los emplean, están modificando el *"traffic mix"* presente en Internet [1], debido a la gran cantidad de paquetes pequeños que generan. P2P-TV es uno de los servicios multimedia más extendidos y prácticos en la distribución de contenidos de vídeo y TV en la red, permitiendo el intercambio entre un gran número de usuarios de manera simultánea. La filosofía del modelo *Peer-to-Peer* (P2P) es fomentar la cooperación entre usuarios (también conocidos como *peer*), que pueden actuar como clientes y servidores al mismo tiempo. De esta manera, los costes requeridos tanto en equipos como en ancho de banda se comparten entre ellos. Un *peer* puede convertirse en un emisor de contenidos sin la necesidad de un potente servidor o de un gran ancho de banda. De este modo, P2P presenta una mejor escalabilidad que el modelo cliente-servidor, usado por ejemplo en las *Content Delivery Network* (CDN) [2].

Sin embargo, las redes P2P se han convertido en uno de los más grandes desafíos para la ingeniería del tráfico y los Proveedores de Servicio de Internet (ISPs), al ser una importante fuente de tráfico en la red [3]. Las diferentes aplicaciones P2P-TV son ampliamente empleadas por usuarios residenciales con un limitado ancho de banda de subida. Al emplear *router* de gama media o baja, pueden convertirse en cuellos de botella [4]. De ahí que sea necesario estudiar con más detalle el comportamiento del tráfico P2P y evaluar su impacto en la red. Una de las aplicaciones P2P-TV más populares es SOPCast [5]. En [6] y [7] los autores estudiaron el tráfico de esta aplicación y concluyeron que los paquetes intercambiados se dividen fundamentalmente en dos tipos: $\approx 40\%$ son paquetes grandes (de vídeo) y $\approx 60\%$ son paquetes UDP pequeños (de señalización). Los paquetes pequeños son necesarios para monitorizar, controlar y reorganizar a los paquetes de vídeo (o *chunk*) desde la capa de aplicación. Como se ha mencionado, estas aplicaciones P2P-TV producen altas tasas de paquetes UDP pequeños entre *peer*, los cuales presentan una baja eficiencia debido al significativo *overhead* causado por las cabeceras IP/UDP.

En este sentido, la Fig.1 muestra un histograma del tamaño de los paquetes UDP enviados y recibidos por un *peer*, a partir de una traza SOPCast obtenida durante la transmisión de un partido de fútbol de la *Champions League* 2013, con una duración de $30\ min$ y un total de $940,000$ paquetes. Se aprecia una clara distinción en los tamaños de los paquetes, tanto en el enlace de subida como en el de bajada (*uplink* y *downlink*, respectivamente). En el primer caso, aproximadamente el 90% de los paquetes son pequeños, correspondiéndose a la señalización del nivel de aplicación, utilizados para realizar el acuse de recibo de los paquetes de vídeo. Sin embargo, se puede observar un conjunto de paquetes con un comportamiento totalmente opuesto: paquetes de gran tamaño que incluyen la información del vídeo. Esta distribución se corresponde al comportamiento típico de un *peer* que sólo recibe vídeo; en las redes P2P la mayoría de los *peer* asumen el papel de sólo consumidores de contenidos durante la mayor parte del tiempo [2].

La distribución del tamaño de los paquetes mostrada en la Fig.1, hace muy conveniente una optimización del tráfico. Si se comprimen las cabeceras y se utiliza la multiplexión para los paquetes de señalización, se pueden obtener ahorros

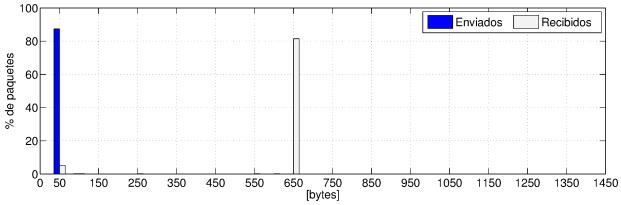


Fig. 1. Histograma del tamaño de los paquetes SOPCast intercambiados entre dos *peer*.

de ancho de banda significativos, ya que el método es especialmente interesante para flujos de paquetes pequeños. Las técnicas de multiplexión ya se han empleado en otros servicios de tiempo de real como por ejemplo VoIP [8] y juegos *online* [9], lográndose un notable ahorro de ancho de banda. Este mecanismo de optimización se podría implementar en varios lugares de la comunicación: en la propia aplicación SOPCast, en los *router* presentes entre dos *peer* o podría ser implementado por los propios proveedores de la red. Estas técnicas introducen un retardo adicional provocado por el tiempo de retención de los paquetes en el multiplexor.

En resumen, este trabajo presenta el análisis de las ventajas de optimizar el tráfico UDP de aplicaciones P2P-TV. Para ello ha sido necesario definir dos políticas de multiplexión adecuadas. El estudio cuantifica la reducción del ancho de banda y del número de paquetes por segundo, mejorando el uso de los recursos de la red. Por otro lado, se asegura que el retardo añadido no afecta a la percepción final del usuario de SOPCast.

El resto del trabajo se organiza de la siguente manera: en la Sección II se discuten los trabajos relacionados. En la Sección III se describen los métodos de compresión y multiplexión propuestos. Las pruebas realizadas y los resultados obtenidos se muestran en la Sección IV y el trabajo se cierra con las conclusiones.

II. TRABAJOS RELACIONADOS

A. Aplicaciones P2P-TV

En los últimos años ha habido un creciente interés en el análisis y caracterización del tráfico P2P-TV. Muchos investigadores se han centrado en el impacto de diferentes aplicaciones de *video streaming* en las redes de comunicaciones [10], como por ejemplo: *PPLive, TVAnts, Coolstreaming, SOPCast y PPStream*. Las mejoras que aportan a los operadores de redes IPTV [11], la calidad de experiencia aportada (*QoE*) [7], [12], los diferentes algoritmos de distribución [13] y el creciente número de usuarios que hacen uso de ellas [5], son varios de los temas fundamentales abordados en relación con los servicios P2P.

En la literatura se pueden encontrar diferentes trabajos centrados en la caracterización del tráfico, incluyendo las velocidades de *upload* y *download* de contenidos, el tipo de paquetes intercambiados y los protocolos empleados [6], así como los mecanismos empleados en algunos programas P2P-TV. Otros trabajos se centran en las características y propiedades de las estructuras de las redes P2P [14] y las implicaciones del tráfico P2P-TV para los ISPs [3], [15]. Sin embargo, en ninguno de los trabajos citados centran su atención en la optimización del tráfico y su efecto en otros servicios que comparten el mismo enlace de acceso a Internet.

B. Comportamiento del SOPCast

Entre las aplicaciones mencionadas, SOPCast se ha convertido en una de las más estudiadas debido a la gran cantidad de personas que la utilizan [5]. El estudio de su funcionamiento, el ánalisis de su rendimiento y las mediciones de la *QoE* aportada son importates temas para los investigadores, operadores y usuarios finales. Esta aplicación funciona sobre un protocolo de comunicación propietario denominado **sop** o **SoP technology** [16]. En [2] y [17] se puede encontrar una caracterización detallada de SOPCast, enfocada especialmente en el tiempo entre paquetes, el número de *peer* con los que se intercambian datos, la duración de la comunicación, entre otros. En [6] y [7] se estudian los mecanismos básicos de SOPCast y se muestra que el tráfico de señalización y vídeo es transportado fundamentalmente sobre UDP.

El sistema de *streaming* desarrollado por SOPCast se sustenta en una arquitectura de distribución no estructurada de tipo *mesh-based*, donde se posibilita que cada *peer* descargue y distribuya los contenidos, llegando a existir múltiples proveedores y consumidores de los mismos contenidos. Este mecanismo es tolerante a fallos, pues los *peer* pueden incorporarse y abandonar la red P2P en cualquier momento y sin previo aviso, asegurando que los errores sean los menos posibles en la visualización del vídeo. Se precisa un mecanismo de control del tráfico para establecer y mantener esta estructura de *peer*; siendo necesario un tráfico de señalización compuesto por paquetes UDP pequeños (menos de $100\ bytes$) [7]. Este control de flujo es necesario para gobernar el intercambio de los diferentes segmentos *(chunk)* en los que se divide el vídeo. En la bibliografía se proponen tres niveles de clasificación para los *peer* de la aplicación; una pequeña cantidad de *super peer* (aproximadamente 5) son los responsables de proveer la mayor cantidad de vídeo (casi el 90% del total) a un *peer*; los *ordinary peer* envían algún contenido y finalmente los *supplementary peer* solo intercambian paquetes de señalización [2].

Al inicio de la aplicación se necesita de un período de tiempo para realizar la búsqueda de *peer* activos, de los cuales se pueda descargar vídeo, en la estructura de distribución. Una vez que se obtiene la lista de *peer* activos y se selecciona el canal deseado, el *video stream* es almacenado en dos *buffer* consecutivos antes de comenzar su visualización. El primero se corresponde al *buffer* de la propia aplicación SOPCast, y añade un retardo desde el momento en que un canal se selecciona hasta que comienza el *streaming* del vídeo; el segundo es el *buffer* del reproductor del cliente. Como consecuencia, el tiempo total que el cliente requiere para disfrutar del *live streaming* oscila entre 30 y $40\ seg$ [7].

C. Métodos de Optimización del Tráfico

Como se ha mencionado, la gran cantidad de paquetes pequeños generados por SOPCast produce un *overhead* significativo en la red, de la misma manera que ocurre con otros servicios multimedia (VoIP, videoconferencia y juegos *online*), ya que sus requerimientos de tiempo real hacen que envíen una gran cantidad de paquetes por segundo, con lo que tienen poca eficiencia. Las técnicas de multiplexado y compresión se utilizan hace ya algún tiempo, e incluso se han estandarizado para escenarios donde varios tráficos de tiempo real comparten la misma ruta [8]. En [9] y [18], se emplea un método denominado TCM (*Tunneling, Compressing and Multiplexing*), con el que se logra ahorrar ancho de banda en el tráfico UDP de los juegos *online*. Se comprimen las cabeceras de los paquetes mediante algoritmos estándar; se multiplexa un número de paquetes en uno de mayor tamaño, y finalmente se realiza el envío extremo a extremo empleando un túnel L2TP. Los resultados muestran un ahorro de ancho de banda de hasta un 38% para juegos que emplean IPv4/UDP,

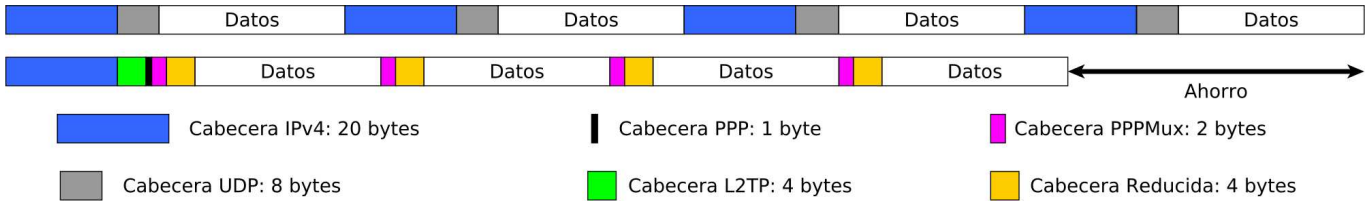


Fig. 2. Tráfico Original y Multiplexado de SOPCast (*con tamaño de paquetes a escala real*).

añadiendo un retardo a causa de la retención de los paquetes originales en el multiplexor.

Respecto al algoritmo de compresión de cabeceras, en este trabajo se precisa uno capaz de comprimir cabeceras IP/UDP, por lo que se podría utilizar IPHC [19] o ROHC [20], siendo este último más reciente y con un mejor comportamiento en redes inalámbricas, aunque conlleva más complejidad en su implementación. Estos métodos utilizan la redundancia de los campos de las cabeceras IP y UDP, para evitar el envío repetido de algunos de ellos. Utilizan también compresión *delta* para reducir el número de bits de los campos con un comportamiento incremental (ej. el número de secuencia). Se necesita por tanto un *contexto*, que se transmite inicialmente con las primeras cabeceras y que almacena los valores de los campos que no se envían, y debe estar sincronizado entre el emisor y el receptor.

Considerando lo anteriormente expuesto, las técnicas de optimización presentadas en [9] pueden ser muy útiles si se aplican al tráfico P2P-TV, caracterizado por generar altas tasas de paquetes pequeños. Se podrían multiplexar los paquetes que se envíen a mismo *peer*, por ejemplo los paquetes de acuse de recibo del nivel de aplicación. Incrementar la eficiencia de estos flujos podría ser beneficioso para las redes residenciales y de agregación, puesto que el ahorro puede llevar a una mejor utilización de los recursos de la red, y la optimización de los recursos permite que más *peer* puedan participar sin trabas en la distribución de contenidos dentro de la red P2P [21].

III. COMPRESIÓN Y MULTIPLEXIÓN

En primer lugar, necesitamos un protocolo capaz de comprimir cabeceras IP/UDP. En este caso se ha seleccionado IPHC, por ser suficiente para los própositos de este trabajo y por presentar una implementación más sencilla que la de ROHC. IPHC es capaz de comprimir las cabeceras UDP a 2 $bytes$, empleando sólo 8 $bits$ para el *Context Identifier* (CID) y evitando el campo de control opcional (*checksum*). La cabecera IPv4 puede comprimirse también a 2 $bytes$, por lo que se considerará una media de 4 $bytes$ para todas las cabeceras comprimidas, excepto para las cabeceras completas que serán de 28 $bytes$ y que, de acuerdo con la especificación de IPHC se envían cada 5 seg [22].

Para ilustrar el *overhead* que puede generar el tráfico original de SOPCast y el ahorro de ancho de banda que es posible obtener gracias a la compresión de cabeceras y la multiplexión de los paquetes, la Fig.2 muestra la reducción del tráfico alcanzado cuando cuatro paquetes P2P-TV se multiplexan en uno más grande.

En este trabajo, se utilizarán dos políticas diferentes para seleccionar qué paquetes se multiplexan juntos. Están basadas en el uso de un *período* fijo o un *umbral* de tiempo entre paquetes respectivamente (Fig.3(a) y Fig.3(b)). Los paquetes generados por la aplicación SOPCast se denominarán *nativos*, para diferenciarlos de los multiplexados o *mux*.

Ambas políticas tratan de mantener los valores del retardo añadido por debajo de una cota superior, para evitar afectar la *QoE* de los usuarios de SOPCast. Algunos servicios multimedia, como VoIP o los juegos *online* presentan restricciones muy rigurosas para el retardo añadido. Sin embargo, en el caso de P2P-TV este problema es menos severo, pues los contenidos descargados se almacenan en el *buffer* de la aplicación antes de reproducirse. En SOPCast, el *buffer* puede almacenar aproximadamente un minuto de vídeo [5], por lo que la mayor limitación en el número de paquetes a multiplexar vendrá dada por la Unidad Máxima de Transferencia (MTU) de la red.

A continuación se explican en detalle las dos políticas de multiplexión propuestas.

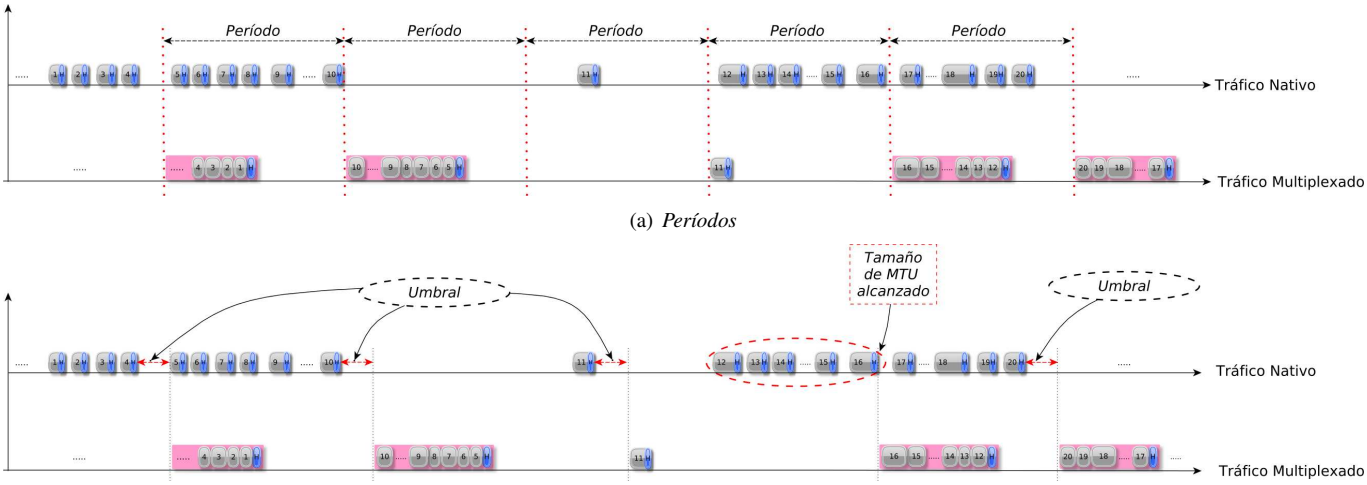
A. Multiplexión basada en un Período

En este caso se define un *período*, de forma que se envía un paquete multiplexado, incluyendo los que han llegado hasta ese momento (Fig.3(a)), al final de cada intervalo de tiempo. Hay tres excepciones: si no ha llegado ningún paquete, no se envía nada; si sólo hay un paquete, se envía en su forma original; finalmente, si se alcanza el tamaño de la MTU, se envía el paquete multiplexado y se comienza un nuevo *período*. Si el valor del *período* aumenta, el ahorro de ancho de banda (*BWS*) mejorará, pues los paquetes multiplexados serán más grandes y el *overhead* total disminuirá. Los valores seleccionados para el *período* no pueden incrementarse indefinidamente, ya que se perdería el contacto con los *peer* proveedores del vídeo.

B. Multiplexión basada en un umbral del tiempo entre paquetes

La caracterización del tráfico generado por SOPCast en [17] sugiere que el envío de paquetes entre dos *peer* sigue un patrón a ráfagas, observándose grandes grupos de paquetes consecutivos cada ciertos intervalos de tiempo. Se puede notar que los *peer* reciben la información de vídeo concentrada en bloques, es decir, en un intervalo determinado de tiempo se recibe una cantidad notable de paquetes de vídeo consecutivamente; posteriormente sólo se reciben paquetes de señalización hasta que comienza nuevamente la transmisión de información. De ahí que se puede concluir que el tráfico analizado sugiere un patrón a ráfagas (Fig.4).

Teniendo esto en cuenta, se ha definido una polítca de multiplexión capaz de adaptarse a este comportamiento (Fig.3(b)). Se define un diagrama de estados (Fig.5), que comienza en un estado de *espera* hasta que llega el primer paquete de la ráfaga. Una vez que se recibe un paquete, el sistema pasa al estado



(a) *Períodos*

(b) *Umbrales*

Fig. 3. Políticas de Multiplexión.

de *almacenamiento* (*transición A*), en el cual se acumulan los paquetes que van llegando y que presentan un tiempo entre paquetes menor o igual al *umbral* seleccionado (*transición B*). Sin embargo, si el tiempo entre dos paquetes supera el valor de dicho *umbral* o si se alcanza el valor de la MTU (*transición C*), el sistema considera que la ráfaga concluye, entonces se multiplexan los paquetes que han llegado hasta ese momento y se envían; el sistema retorna al estado de *espera*.

Para lograr que esta política se adapte al tráfico, se debe seleccionar un valor adecuado del *umbral* (tiempo entre paquetes), que nos permita discriminar claramente qué paquetes forman parte de cada ráfaga.

IV. PRUEBAS Y RESULTADOS

En esta sección se presentan algunos resultados de las simulaciones realizadas. En primer lugar, se obtuvieron trazas de tráfico de la aplicación con la herramienta Tshark, capturándose alrededor de 30 min de un partido de fútbol de la *Champions League* 2013. El cliente SOPCast se encuentra ubicado en nuestro campus universitario, con una dirección IP pública; trabajando sobre Linux (kernel $2.6.38-7$), y con un procesador $Intel® \; Core^{TM} \; i3 \; CPU \; 2.4 \; GHz$.

Para las pruebas se utiliza el tráfico intercambiado con el *peer* que nos provee con más del 90% del vídeo durante toda la comunicación y con el cual, por tanto, existe la mayor cantidad de paquetes intercambiados [6]. Analizando este tráfico, se nota que por cada paquete de vídeo aparece un paquete de confirmación del nivel de aplicación (ACK) de 28 $bytes$ de *payload* (Fig.6); esto explica la gran cantidad de paquetes pequeños generados, que presentan una gran redundancia en los campos de la cabecera, hecho que es de interés para la compresión de las mismas. Se seleccionan valores entre 10 y 50 ms para definir el *período* y los *umbrales* utilizados en las simulaciones, pues más del 84% de los paquetes presentan un intervalo de llegada en este rango.

En primer lugar, para comprobar que los retardos añadidos (en el orden de las decenas o centenas de milisegundos) por las técnicas de optimización empleadas no afectan a la visualización del vídeo, hemos realizado una prueba utilizando Netem para filtrar los paquetes ACK enviados desde la aplicación local al resto de los *peer* durante la visualización de un vídeo. A medida que los *peer* dejan de recibir las confirmaciones, asumen que se ha desconectado la sesión y por tanto dejan de enviar contenidos. Aún así, el *video streaming* se sigue reproduciendo sin problemas en el ordenador local durante casi 1 min. El comportamiento observado cuadra con [5], donde se llega a la conclusión de que el tamaño del *buffer* de SOPCast tiene esa misma duración.

Una vez comprobado que las técnicas de optimización no empeoran la experiencia del usuario, se ha utilizado MATLAB para realizar simulaciones con el fin de obtener tráfico comprimido y multiplexado para ambas políticas. En primer lugar, se separa la traza obtenida del SOPCast en dos: el tráfico de subida generado por nuestro peer (*uplink*) y el tráfico de bajada (*downlink*); y se elimina el tráfico generado por la fase de inicialización de esta aplicación P2P-TV. Los experimentos se han centrado en el tráfico de subida (*uplink*), pues es donde se presenta la mayor limitación de las redes residenciales. Para generar el nuevo tráfico se tiene en cuenta el instante de generación del paquete *nativo* y su tamaño. Posteriormente, se aplica la compresión de las cabeceras del flujo *nativo*; y finalmente se calcula el tiempo y tamaño de cada paquete multiplexado para cada política.

La Fig.7 ilustra el ahorro de ancho de banda (*BWS*) obtenido en ambas políticas. Primeramente se observa que se obtienen valores significativos de ahorro, entre el 25% y el 35% del total enviado por el *peer* local. Cuando se emplea la política basada en un *umbral* de tiempo entre paquetes, se obtiene un *BWS* entre un 33% y un 35%. Como el tiempo entre los paquetes pertenecientes a una misma ráfaga es aproximadamente 10 ms en la mayor parte de los casos, si se selecciona dicho valor como *umbral*, no se obtienen valores óptimos de *BWS*, pues se multiplexan muy pocos paquetes. Sin embargo, para *umbrales* superiores a 12.5 ms, el *BWS* presenta un mejor comportamiento y se aprecia que se mantiene prácticamente constante para el resto de los *umbrales*. Para la política basada en un *período*, el *BWS* alcanzado varía entre el 26% y el 33%. De manera similar a los resultados obtenidos en [18], los valores de *BWS* presentan un comportamiento asintótico.

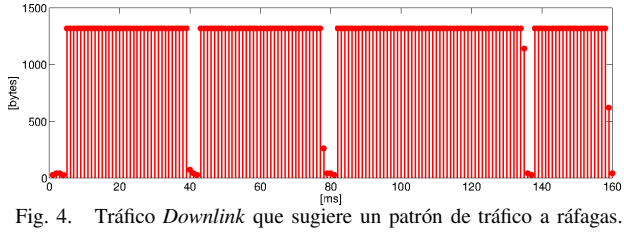


Fig. 4. Tráfico *Downlink* que sugiere un patrón de tráfico a ráfagas.

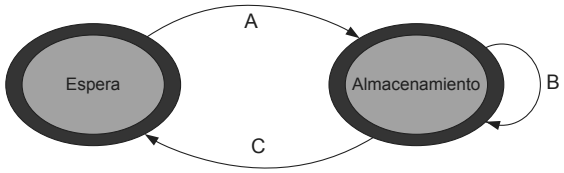


Fig. 5. Diagrama de Estado empleado en la política de *Umbrales*.

A continuación se presentan los histogramas del tamaño de los paquetes multiplexados en ambas políticas, usando un *período* y un *umbral* de 20 ms (Fig.8). Comparando los resultados obtenidos, se observa que con el uso del *período* se genera mayor cantidad de paquetes pequeños, y muy pocos paquetes grandes, con respecto a la política basada en un *umbral*. En el segundo caso, se consigue multiplexar una mayor cantidad de paquetes, al adaptarse mejor al tráfico generado. Este resultado avala los mejores resultados de *BWS* para esta política.

En la Fig.9 se presenta el número de paquetes por segundo (pps) generados en el caso del tráfico *nativo* y cuando se utiliza cada una de las políticas de multiplexión. Se observa una reducción significativa de este parámetro, que baja desde casi 50 hasta unos 5 pps al multiplexar. Como se ha explicado, esta disminución resulta interesante para reducir la carga en los *router* y al mismo tiempo, se muestra que con el aumento del *período* o el *umbral* aumenta también el número de paquetes multiplexados. Sin embargo, hay una diferencia: mientras aumenta el valor del *período*, la cantidad de pps disminuye; en el caso del *umbral*, llega un momento en que su incremento no produce ninguna mejora y la cantidad de pps

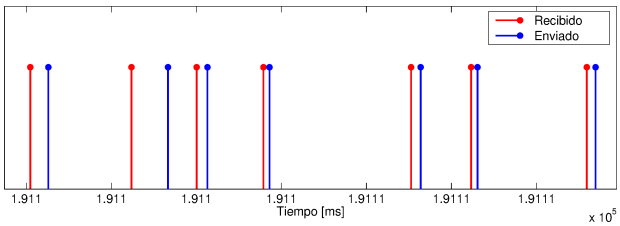


Fig. 6. Tráfico durante una comunicación entre dos peers (paquetes de vídeo y de confirmación).

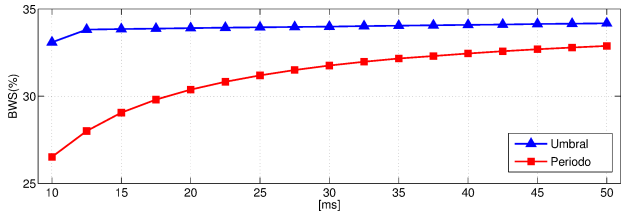
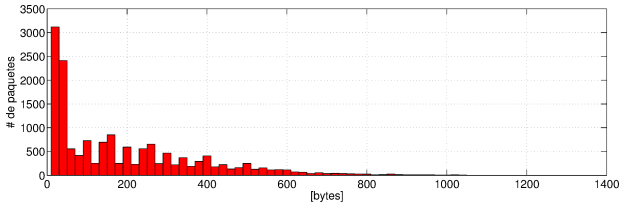
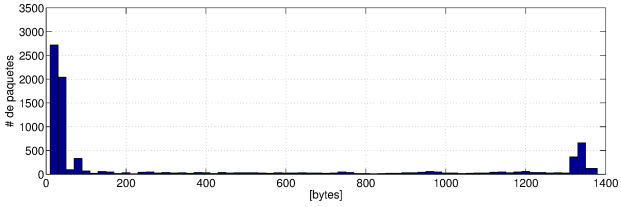


Fig. 7. *BWS* usando las dos políticas de multiplexión.



(a) *Períodos*



(b) *Umbrales*

Fig. 8. Histograma del tamaño de los paquetes *mux* para las dos políticas.

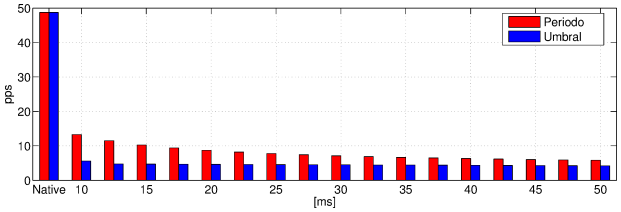


Fig. 9. Paquetes por segundo.

permanece prácticamente constante para valores superiores a 12.5 ms.

Con los resultados de las simulaciones y los valores de *BWS* y pps obtenidos, se ha mostrado que multiplexando el tráfico P2P-TV, aún cuando se considera la comunicación con un único *peer*, se logra un buen ahorro de tráfico y de paquetes por segundo, reduciendo también las necesidades de procesamiento. Estos resultados son muy prometedores para las redes residenciales, donde el *uplink* es limitado y se comparte con otros servicios. Si consideramos además que este tipo de usuarios utilizan normalmente *router* de gama media y baja con capacidad de procesamiento limitada, la reducción de pps conseguida adquiere mayor relevancia.

V. CONCLUSIONES

En este trabajo se aplica un método de compresión de cabeceras y dos políticas de multiplexión al tráfico generado por una popular aplicación P2P-TV basada en UDP. Teniendo en cuenta la cantidad de paquetes generados, se ha mostrado que se pueden obtener valores importantes de ahorro de ancho de banda en redes residenciales.

Se han desarrollado simulaciones con el propósito de estudiar el ahorro de ancho de banda para las distintas políticas de multiplexión propuestas. La primera se basa en la selección de un *período*, de forma que todos los paquetes que llegan durante ese intervalo de tiempo son multiplexados y enviados juntos. La segunda, basada en el hecho de que el tráfico SOPCast responde a un patrón de ráfagas, define un *umbral* para el tiempo de llegada entre paquetes, con el fin de multiplexar los que correspondan a la misma ráfaga. Los resultados muestran que con el empleo de las políticas propuestas se alcanzan ahorros significativos: el *uplink* puede reducirse entre un 26% y un 33% para la política basada en un *período* y entre un 33% y un 35% si se emplea un *umbral* para

el tiempo entre paquetes. Se consigue además, una importante reducción del número de paquetes por segundo. De igual manera, se ha comprobado que los retardos añadidos por el proceso de multiplexión no perjudican la experiencia del usuario con la aplicación.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por la Fundación Social Europea en colaboración con el Gobierno de Aragón, el Proyecto CPUFLIPI (MICINN TIN2010-17298), Ibercaja Obra Social, el Proyecto de la Cátedra Telefónica, la Universidad de Zaragoza, el Banco Santander y la Fundación Carolina.

REFERENCIAS

[1] C. Park, F. Hernandez-Campos, J. Marron, and F. D. Smith, "Long-range dependence in a changing internet traffic mix," *Computer Networks*, vol. 48, no. 3, pp. 401 – 422, 2005.

[2] P. Eittenberger, U. R. Krieger, and N. M. Markovich, "Measurement and analysis of live-streamed p2ptv traffic," in *Performance Modelling and Evaluation of Heterogeneous Networks in HET-NETs 2010*, January 2010, pp. 195–212.

[3] D. R. Choffnes and F. E. Bustamante, "Taming the torrent: a practical approach to reducing cross-isp traffic in peer-to-peer systems," in *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication*, ser. SIGCOMM '08, 2008, pp. 363–374.

[4] L. Sequeira, J. Fernandez-Navajas, J. Saldana, and L. Casadesus, "Empirically characterizing the buffer behaviour of real devices," in *Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2012 International Symposium on*, 2012, pp. 1–6.

[5] A. Sentinelli, G. Marfia, M. Gerla, L. Kleinrock, and S. Tewari, "Will iptv ride the peer-to-peer stream?" *Communications Magazine, IEEE*, vol. 45, no. 6, pp. 86–92, 2007.

[6] T. Silverston and O. Fourmaux, "Measuring p2p iptv systems," in *Proc. of NOSSDAV-07, International Workshop on Network and Operating Systems Support for Digital Audio and Video*, 2007.

[7] B. Fallica, Y. Lu, F. Kuipers, R. Kooij, and P. V. Mieghem, "On the quality of experience of sopcast," in *Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. The Second International Conference on*, September 2008, pp. 501–506.

[8] B. Thompson, T. Koren, and D. Wing, "Tunneling Multiplexed Compressed RTP (TCRTP)," RFC 4170, November 2005.

[9] J. M. Saldana, J. Fernandez-Navajas, J. Ruiz-Mas, J. I. Aznar, E. Viruete, and L. Casadesus, "First person shooters: can a smarter network save bandwidth without annoying the players?" *IEEE Communications Magazine*, vol. 49, no. 11, pp. 190–198, 2011.

[10] S. Tang, Y. Lu, J. M. Hernandez, F. A. Kuipers, and P. V. Mieghem, "Topology dynamics in a p2ptv network." in *Networking*, ser. Lecture Notes in Computer Science, vol. 5550. Springer, 2009, pp. 326–337.

[11] M. Cha, P. Rodriguez, S. Moon, and J. Crowcroft, "On next-generation telco-managed P2P TV architectures," in *IPTPS '08*, 2008.

[12] U. R. Krieger and R. Schwessinger, "Analysis and quality assessment of peer-to-peer iptv systems," *Consumer Electronics 2008 ISCE 2008 IEEE International Symposium on*, pp. 1–4, 2008.

[13] Y. Liu, Y. Guo, and C. Liang, *Peer-to-Peer Networking and Applications*, vol. 1, no. 1, pp. 18–28, March 2008.

[14] L. Vu, I. Gupta, J. Liang, and K. Nahrstedt, "Measurement and modeling of a large-scale overlay for multimedia streaming," in *The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness; Workshops*, ser. QSHINE-07. ACM, 2007, pp. 3:1–3:7.

[15] D. Moltchanov, Y. Koucheryavy, and B. Moltchanov, "The effect of biased choice of peers on quality provided by p2p file sharing." in *CCNC*. IEEE, 2012, pp. 608–613.

[16] http://www.sopcast.com/.

[17] A. B. Vieira, P. Gomes, J. A. M. Nacif, R. Mantini, J. M. Almeida, and S. V. A. Campos, "Characterizing sopcast client behavior." *Computer Communications*, vol. 35, no. 8, pp. 1004–1016, 2012.

[18] J. Saldana, L. Sequeira, J. Fernandez-Navajas, and J. Ruiz-Mas, "Traffic optimization for tcp-based massive multiplayer online games," in *Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2012 International Symposium on*, July, pp. 1–8.

[19] M. Degermark, B. Nordgren, and S. Pink, "IP Header Compression," RFC 2507, February 1999.

[20] G. Pelletier and K. Sandlund, "RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite," RFC 5225, April 2008.

[21] L. Sequeira, I. Quintana, J. Saldana, L. Casadesus, J. Fernández-Navajas, and J. Ruiz-Mas, "The utility of characterizing the buffer of network devices in order to improve real-time interactive services," in *Proceedings of the 7th Latin American Networking Conference*, ser. LANC '12. ACM, 2012, pp. 19–27.

[22] V. Jacobson. (1990, Feb.) RFC1144: Compressing TCP/IP headers for low-speed serial links.

YouTube Traffic Detection and Characteristics Extraction

Jorge Navarro-Ortiz, Pablo Ameigeiras, Juan J. Ramos-Munoz,
Jonathan Prados-Garzon, Juan M. Lopez-Soler
Centro de Investigación en Tecnologías de la Información y las Comunicaciones (CITIC),
Universidad de Granada
E.T.S.I. Informática y de Telecomunicación, C/ Periodista Daniel Saucedo Aranda s/n, Granada (Spain)
{jorgenavarro, pameigeiras, jjramos, jpg, juanma}@ugr.es

Abstract- **Video downloading is becoming increasingly relevant in wireless and mobile networks, being more than half of the total traffic according to the latest Cisco global mobile data forecast. In particular, YouTube is the most visited video streaming site. In this paper we propose a method to detect YouTube traffic flows and detect their main characteristics such as resolution and encoding rate. This method would be useful for operators and network administrators since the network would become service aware and e.g. the network could apply service specific policies.**

Keywords- **YouTube, traffic detection, characteristics extraction**

I. INTRODUCTION

The usage of QoS mechanisms which are present in different type of networks, such as wired (e.g. based on the DiffServ or IntServ QoS solutions) and wireless (e.g. IEEE 802.11e and 3G Long Term Evolution), makes necessary to segregate packets into different data flows and obtain their main characteristics. The user experience can be enhanced if the network becomes service aware and the network is able to apply service specific policies.

At present the video services constitute a great part of the traffic in packet switched networks (more than 50 percent of mobile traffic by the end of 2011 and accounting for 70 percent by 2016 [1]). Therefore methods for the detection of YouTube data flows from an aggregate set of packet flows with different services/applications, as well as for the extraction of the main information of the video being downloaded (e.g. resolution, duration and video data rate) will allow network operators to increase the user experience by applying some service aware policies.

The method proposed in this paper is focused on the YouTube video delivery service since it is the most representative video streaming site (3rd in the Alexas global rank [2]). This service is implemented as a video progressive download, i.e. the YouTube client (player) progressively downloads the specified video using the HTTP / TCP protocols while the playback is being performed.

The traffic generated by progressive video download from YouTube media servers [3] is carried over the HTTP protocol. This implies that a simple traffic detector based on the server's port cannot be employed since the HTTP server's port (80) is used mainly for other services, i.e. web browsing.

Existing algorithms to detect YouTube progressive video downloads are based on the statistics of this service. For example, the authors in [4] describe a traffic classifier which is based on flow similarity. Another solution is proposed in [5], using a learning classifier which utilizes logistic regression. In another work, Mori [6] detected YouTube flows based on the IP addresses of YouTube servers. Although this solution is simple and effective, it lacks the possibility of extracting the main characteristics of the downloaded media such as average encoding rate or video duration.

To the best of the authors' knowledge, there is not currently any other solution in the literature using the approach herein described.

The rest of the paper is organized as follows. Section 2 describes the basics of the proposed method, whereas Section 3 depicts the solution in detail. Section 4 presents a sample implementation with license free software and libraries. Section 5 exposes some useful use cases and, finally, Section 6 draws the main conclusions.

II. TRAFFIC DETECTION AND CHARACTERISTICS EXTRACTION

In this paper we propose a method which detects a YouTube traffic flow and extracts its main characteristics. More precisely, this method is able to detect the traffic of the YouTube progressive video download, which is carried over the HTTP protocol.

It shall be noted that our method is not intended for the YouTube video streaming service over RSTP/RTP / UDP protocols, which was previously used for mobile devices. We have checked that current smart phones (based on Android, iOS, Symbian, and Bada) receive the YouTube videos using the HTTP/TCP approach.

Our method for detecting YouTube data flows can be applied to any packet switched network that transports an aggregate set of packet flows from different services/applications. The detection of the YouTube data flow can be used in combination with packet filters to allow the network to segregate YouTube data flows and apply them a service specific treatment with the objective of enhancing both network performance and user's experienced quality.

The basic concept of our proposal is illustrated in Fig. 1. The proposed technique to detect YouTube traffic and its main characteristics, thanks to the inspection of the payloads of certain HTTP packets, provides a mechanism to control and increase the QoE perceived by the end users, and it could be installed in the terminal side or in the network side. The

method could be applied to provide a service specific treatment in order to enhance the network performance as well as the user's experienced quality.

The detection of YouTube flows is based on inspecting the contents of the payloads of the HTTP packets and finding a specific message transferred between a YouTube client and the YouTube server.

In this paper we also propose a method to a priori derive relevant information of the video clip characteristics (e.g. the video clip bit rate). This information can be conveniently exploited by the network during the progressive video download.

In this manner, QoS mechanisms such as Radio Resource Management procedures in wireless networks (e.g. admission control, packet scheduling, load balancing) will be able to discriminate among different data flows and, therefore, will be able to provide traffic differentiation. Moreover, developers / administrators / operators will be able to customize these procedures according to the flows' characteristics.

This procedure can be easily adapted to changes on the YouTube signaling, as long as:

- *For detecting the YouTube traffic*: there shall be a string that uniquely identifies the request for beginning a video progressive download. Currently all YouTube video downloads are initiated by an HTTP request containing the string "GET /videoplayback".

- *For extracting the main video characteristics*: the first packet(s) shall contain a container header with the main video characteristics (e.g. video bit rate, resolution, duration) among its metadata. Currently most YouTube videos are encapsulated onto an FLV container, but this procedure would apply to other containers as long as they have an information header with these metadata.

III. Detailed Technical Description

Our proposal is based on the procedure depicted in Fig. 2 to view a YouTube video based on the HTTP protocol.

Before the user starts viewing a YouTube video, the browser sends an HTTP request to the YouTube web server after clicking on a video link.

The downloaded web page includes the video player (in an SWF container) and the required configuration parameters for the selected video. The player further interchanges signalling messages with the YouTube web server, which finally sends the parameters required to download the video from a YouTube media server (from a farm of servers [3]).

Finally, the player requests the video to the YouTube media server by using an HTTP request. More precisely, the request always starts with the following string:

```
GET /videoplayback?sparams=id
```

which is followed by a number of parameters and their corresponding values.

This TCP packet (hereafter designated *get_videoplayback_packet*) is used to carry this HTTP message and contains the **source IP address**, the **destination IP address**, the **source port** and the **destination port**. Therefore, this packet will be used to obtain these values, which uniquely identifies the data flow used to download the YouTube video.

Most YouTube videos are encapsulated into an FLV container, whose format is specified in [7]. The FLV header contains some tags with information about the video, being some of the main tags:

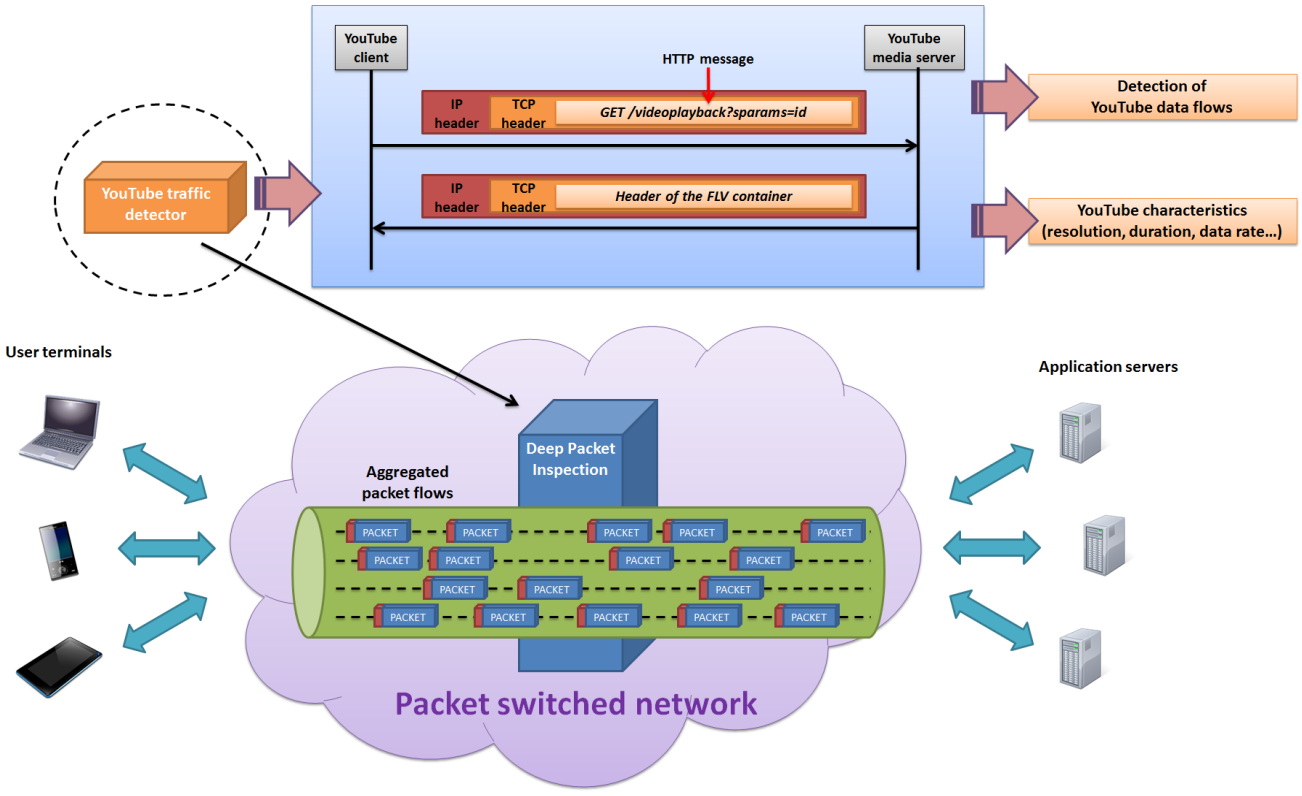


Fig. 1. Basic concept of the YouTube traffic detection method.

- `totalduration`
- `width`
- `height`
- `videodatarate`
- `audiodatarate`
- `totaldatarate`
- `framerate`
- `bytelength`
- `httphostheader`

The first packet from the YouTube media server after the get_videoplayback_packet contains the beginning of the FLV file, i.e., the FLV header. The FLV header starts with a string "FLV" [7] , which can be used to determine whether the video is encapsulated into an FLV container and therefore an FLV header parsing can take place.

If the YouTube video is not encapsulated into an FLV file, then it is encapsulated into an MP4 container [8]. The MP4 container is specified in [9]. The metadata also contains information about the video, e.g. the resolution and the data rate. This information is present in the *moov* atom which can be present in different parts of the video [10]. However, in the case of streaming, the *moov* atom shall be present at the beginning of the video [11] and therefore the methodology used in this paper is also valid for videos in MP4 format.

It is important to note that the string "*videoplayback*" has been searched in packet traces (obtained with *Wireshark* [12]) when viewing videos from the following sites, not being found in any of those traces: hulu.com, metacafe.com, vimeo.com, mtv.com, dailymotion.com, megavideo.com, adobe.com, msn.com, aol.com, myspace.com, yahoo.com, warnerbros.com, disney.com, cbs.com, elmundo.es, elpais.com, 20minutos.es, nbc.com, thetimes.co.uk, tv.tv, citytv.com, spike.com, pandora.tv, muzu.tv, wideo.fr, clarin.com, myvideo.de, wat.tv, kewego.com, brightcove.com, photobucket.com, viddler.com, grindtv.com, liveleak.com, and stupidvideos.com.

IV. Sample Implementation

Our proposal can be implemented by software development, based on a packet sniffing library such as *libpcap* [13]. A sample implementation of YouTube traffic detector is presented in Fig. 3, which is based on the *Python* programming language [14] and the *Scapy* packet manipulation environment [15] . Both *Python* and *Scapy* are available for Windows, Linux, UNIX and MAC OS. *Python* has an OSI approved open source license, and *Scapy* is license free software (GPLv2+). One library available for FLV header parsing (to extract the main characteristics of the flow, e.g. the data rate) is *FLVLib* [16], which is release under a free license (MIT license). The FLV format is specified in [7].

A description of the sample implementation (Fig. 3) is provided next:

- The `main()` function sniffs packets on the chosen network interface, e.g. *eth0*, filtering packets on the TCP port for HTTP (80). If the network interface is not provided as a parameter, the `printUsage()` function prints the syntax for using this application.
- Packets fulfilling the filter criterion are passed to the `callback()` function. If the packet contains data and

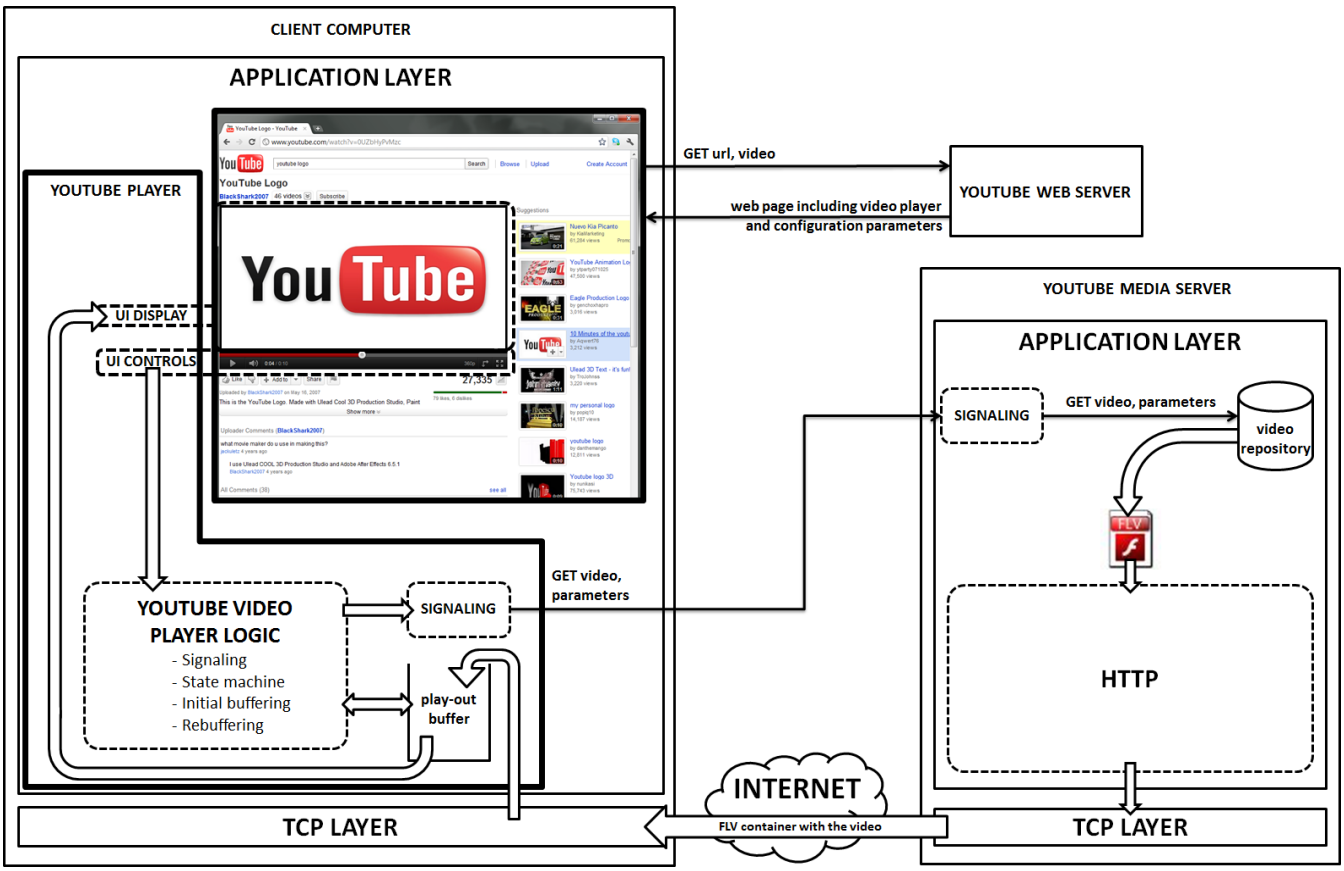


Fig. 2. YouTube video progressive download session.

```
#!/usr/bin/python
#######################################################################
### YouTube server discovery                                        ###
### Copyright (C) 2013 Jorge Navarro-Ortiz et.al.                   ###
### University of Granada                                           ###
#######################################################################

from scapy.all import *
import os
import sys

## Global variables
stringToSearch="'GET /videoplayback?sparams=id" # Request string to the media server

## Initial configuration
conf.verb=0
conf.promisc=0

####################################
### printUsage: display short help ###
####################################
def printUsage():
   print "YouTube sniffer."
   print "Usage: " + sys.argv[0] + " <interface>"
   print "E.g.:  " + sys.argv[0] + " eth0"
   print "NOTE: run 'ifaces' on Scapy to check the available interfaces."

#############################################################################################
### checkYouTubeGetVideoPacket: look for the packet sent to the YouTube video server ###
#############################################################################################
def checkYouTubeGetVideoPacket(pkt):
   global stringToSearch

   src=pkt.sprintf("%IP.src%")
   dst=pkt.sprintf("%IP.dst%")
   sport=pkt.sprintf("%IP.sport%")
   dport=pkt.sprintf("%IP.dport%")
   raw=pkt.sprintf("%Raw.load%")

   if raw[0:len(stringToSearch)]==stringToSearch:
      print "IP.src: " + src
      print "IP.dst: " + dst
      print "TCP.sport: " + sport
      print "TCP.dport: " + dport
      print "Raw: " + raw

      nextPacket=sniff(filter="tcp port 80 and host %dst%", count=1)
      FLVHeaderParsingFromPacket(nextPkt)
      exit(0)

################################################
### callback: called for each packet received ###
################################################
def callback(pkt):
   sport=pkt.sprintf("%IP.sport%")
   dport=pkt.sprintf("%IP.dport%")
   raw=pkt.sprintf("%Raw.load%")

   if raw!='??':
      if dport == '80':
         checkYouTubeGetVideoPacket(pkt)

############
### main ###
############
def main():
   if (len(sys.argv) < 2):
      printUsage()
      exit(0)

   ## Command line parameters
   conf.iface=sys.argv[1]
   expr='tcp port 80'

   try:
      sniff(filter=expr, prn=callback, store=0)
   except KeyboardInterrupt:
      exit(0)

if __name__ == "__main__":
    main()
```

Fig. 3. YouTube video progressive download session.

the destination port is 80, then the `checkYouTubeGetVideoPacket()` function is called.

- The `checkYouTubeGetVideoPacket()` function checks whether the payload information of the TCP packet matches the string "`GET /videoplayback?sparams=id`". If this is the case, then this is the first packet sent from the YouTube player (in the client device) to the specific YouTube media server (from a farm of servers). The information for detecting this YouTube traffic flow is composed by the source IP address (`src`), the destination IP address (`dst`), the source TCP port (`sport`) and the destination TCP port (`dport`). All these data can be extracted from this TCP packet (see Fig. 4).
- After that, the `sniff()` function is called to obtain the following packet, sent from the YouTube media server to the YouTube player, i.e. the source IP address is `dst`, the destination IP address is `src`, the source TCP port is `dport` and the destination TCP port is `sport`.
- This packet is then analyzed to get the metadata on the FLV header, i.e. for extracting the main video characteristics such as the video data rate, the resolution or the video duration. This analysis is performed in the `FLVHeaderParsingFromPacket()` function. This function is not included for the sake of clarity and readibility. It can be easily implemented with the *FLVLib* [16] library or following the FLV format specifications [7].

V. Examples of Use Cases

One use case for our solution is the detection of YouTube traffic in the Deep Packet Inspector (DPI) functionality in 3G Long Term Evolution (LTE) networks. The Deep Packet Inspection requires creating packet classifiers which, in conjunction with the subscriber's profile, will allow the Policy and Charging Rules Function (PCRF) to initiate the establishment of a dedicated bearer. The parameters of this dedicated bearer (QoS Class Identifier (QCI), Guaranteed Bit Rate (GBR), Maximum Bit Rate (MBR), and Allocation and Retention Priority (ARP)) will be used in the Radio Resource Management (RRM) algorithms to assign the required resources for that specific data flow. Our proposal provides the method to generate such packet classifiers and tune these parameters (e.g. GBR and MBR can be computed considering the flow's data rate) for the case of YouTube traffic. A sample scenario considering this use case is shown in Fig. 5.

A second use case of this solution is the traffic classification when a computer, e.g. a laptop, is connected to a 3G network through a modem. In this situation, the modem's connection software –which is executed at the computer– could implement the traffic classifier proposed in this document, marking the packets (e.g. with the TOS field [17] or the DSCP field [18] of the IP header). In addition, it may signal the flow's data rate to the network for reserving the required resources. Similarly, this packet classification could also be used in Wi-Fi networks supporting the EDCA and/or the HCCA medium access mechanisms [19] for QoS support.

A third use case could be the identification of YouTube streams in order to characterize their traffic profiles in terms of throughput requirements and load generation. This characterization would be very useful for network planning and design but also for resource management mechanisms such as admission control and scheduling.

Another use case is the capability of reducing the bandwidth requirements for video streams in congested networks by transforming the bitrates of video streams. This could be done by transforming the HTTP requests from users' equipment to the YouTube servers so that the computer appears to ask for the same video stream but in lower quality.

This procedure may be also used for the discrimination of YouTube traffic flows when entering a DiffServ network, so the packets belonging to those flows can be marked and treated according to their QoS requirements. Those QoS requirements could be computed from the FLV metadata, e.g. considering the video clip data rate.

Similarly, the detection of YouTube traffic could be used in firewalls in order to block (or boost) this service in specific networks, e.g. in an enterprise environment.

VI. Conclusions

The YouTube video delivery service is highly influenced by network QoS metrics such as delay and throughput, which may cause playback interruptions and therefore negatively impact on the end-user experienced quality. Our proposal provides the means to differentiate YouTube traffic flows from other types of traffic flows, therefore being able to provide a differentiated treatment, e.g. in QoS-related mechanisms / algorithms.

Furthermore, the metadata extracted from the FLV header can be used for collecting video statistics (e.g. resolution, video encoding rate, audio encoding rate, video duration, etcetera) and for tuning QoS mechanisms (e.g. to compute the QoS requirements such as average throughput, average

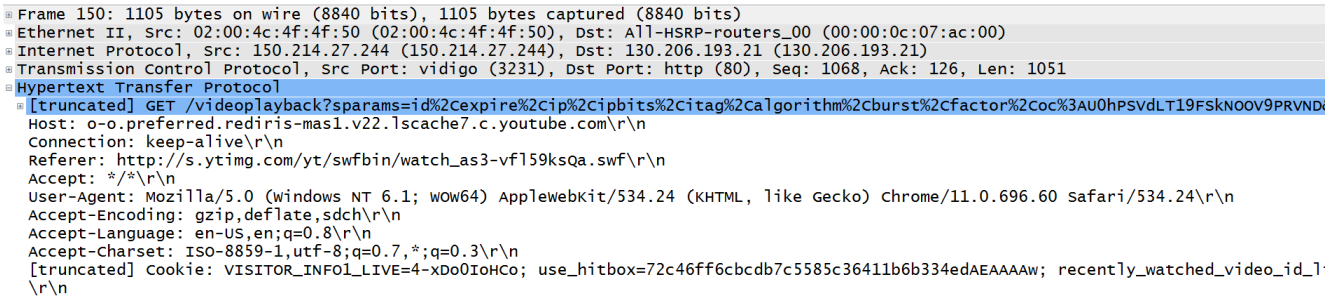


Fig. 4. Sample *get_videoplayback_packet* packet captured with *WireShark*.

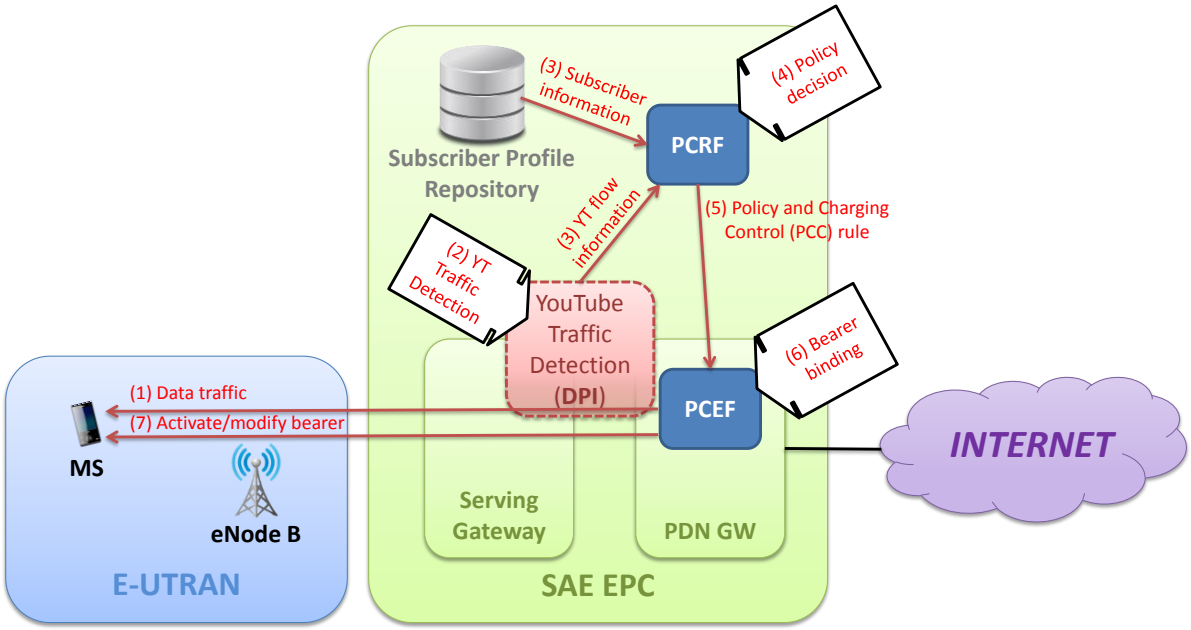


Fig. 5. Sample scenario with an LTE network using the proposed YouTube traffic detector.

packet delay, etcetera).

Both the traffic differentiation and the video characterization can be used by operators and/or network administrators to guarantee the YouTube service requirements.

The technical advantages of the proposed method, compared to other approaches, are:

- This procedure is based on the existing signaling for the YouTube service, not on traffic patterns / statistics. For that reason, it is not possible to have false positives or false negatives when detecting the YouTube traffic. Therefore, our proposal improves the accuracy of the YouTube traffic detection compared to other existing solutions, which are based on traffic patterns / statistics.
- In addition, its implementation is simple but effective, as shown in the sample code included, compared to other existing solutions which require complex statistical computations.
- Moreover, these solutions do not extract information from the video such as resolution, video data rate, duration, etcetera. Our proposal obtains these metadata which could be used for RRM mechanisms such as admission control, resource reservation, resource assignment or for collecting traffic statistics which can be used later for traffic engineering, network planning or troubleshooting.

ACKNOWLEDGMENTS

This work was supported by the Ministerio de Ciencia e Innovación of Spain (project TIN2010-20323).

REFERENCES

[1] Cisco Corporation, Cisco visual networking index: global mobile data traffic forecast update, 2011-2016. white paper. Available: http://www.cisco.com/

[2] Alexa, The Web Information Company. Available: http://www.alexa.com/siteinfo/youtube.com

[3] V. K. Adhikari, S. ain, G. Ranjan, and Z. Zhang, "Understanding data-center driven content distribution", proceedings of the ACM CoNEXT Student Workshop (CoNEXT '10 Student Workshop), New York, USA, December 2010.

[4] J. Y. Chung, B. Park, Y. J. Won, J. Strassner, and J. W. Hong, "Traffic classification based on flow similarity", proceedings of the 9th IEEE International Workshop on IP Operations and Management (IPOM '09), Venice, Italy, October 2009.

[5] T. En-Najjary, M. Pietrzyk, "Application-based feature selection for Internet traffic classification", proceedings of the 22nd International Teletraffic Congress (ITC 2010), Amsterdam, Netherlands, September 2010.

[6] T. Mori, R. Kawahara, H. Hasegawa, S. Shimogawa, "Characterizing Traffic Flows Originating from Large-Scale Video Sharing Services," Proceedings of the Second international conference on Traffic Monitoring and Analysis (TMA'10), Zurich, Switzerland, April 7, 2010.

[7] Adobe Flash Video File format specification, version 10.1, 2010. Available: http://download.macromedia.com/f4v/video_file_format_spec_v10_1.pdf

[8] P. Ameigeiras, J.J. Ramos-Munoz, J. Navarro-Ortiz, J.M. Lopez-Soler, "Analysis and Modeling of YouTube Traffic," Transactions on Emerging Telecommunications Tecnologies, June 2012.

[9] M. Levkov, "Understanding the MPEG-4 movie atom". Available: http://www.adobe.com/devnet/video/articles/mp4_movie_atom.html

[10] ISO/IEC 14496-14:2003, "Part 14: MP4 file format", 2003.

[11] Android Supported Media Formats. Available: http://developer.android.com/guide/appendix/media-formats.html

[12] Wireshark network protocol analyzer. Available: http://www.wireshark.org/

[13] LibPCap, a portable C++ library for network traffic capture. Available: http://www.tcpdump.org/

[14] Python Programming Language – Official Website. Available: http://www.python.org/

[15] Scapy, an interactive packet manipulation program. Available: http://www.secdev.org/projects/scapy/

[16] FLVLib, a library for parsing, modifying and verifying FLV files. Available: http://wulczer.org/flvlib/

[17] P. Almquist, "RFC 1349: Type of Services in the Internet Protocol suite", July 1992. Available: http://tools.ietf.org/html/rfc1349

[18] K. Nichols, S. Blake, F. Baker, and D. Black, "RFC 2474: Definition of the Differentiated Services field (DS field) in the IPv4 and IPv6 headers", December 1998. Available: http://tools.ietf.org/html/rfc2474

[19] IEEE 802.11-2012, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", March 2012.

Testbed para el análisis del impacto de la movilidad en redes de acceso

Javier Carmona-Murillo*, David Cortés-Polo†, Pedro Rodríguez-Cubero†,
Francisco J. Rodríguez-Pérez*, José-Luis González-Sánchez†
*Departamento de Ingeniería de Sistemas Informáticos y Telemáticos
Universidad de Extremadura
Av. Universidad s/n. 10003, Cáceres.
{jcarmur,fjrodri}@unex.es
†Centro Extremeño de Investigación, Innovación Tecnológica y Supercomputación (CénitS)
Carretera N-521, km 41,8. 10071, Cáceres.
{david.cortes,pedro.rodriguez,joseluis.gonzalez}@cenits.com

***Abstract*—La gestión de la movilidad y la Calidad del Servicio (QoS) son dos de los objetivos más importantes en el desarrollo de las redes inalámbricas. Estas metas no sólo involucran al dominio inalámbrico, sino que, en gran medida, la red de acceso que interconecta al dispositivo móvil con Internet también es responsable de conseguir unas comunicaciones eficientes y con QoS. Este área de trabajo que busca la integración del dominio inalámbrico con la red de acceso se conoce como Convergencia Fija Móvil (FMC). El objetivo final de esta convergencia es la integración y la creación de una infraestructura unificada de red, fija y móvil. En ella, los usuarios pueden moverse a través de las diferentes redes y acceder a los servicios sin interrumpir su conexión a la red. La red de acceso juega un papel muy importante en los parámetros de QoS que se proporcionan a los diferentes nodos móviles. En este trabajo se presenta un *testbed* para analizar la influencia de la movilidad en la red de acceso. Este *testbed* permite medir de manera real y no simulada la influencia del tráfico de los usuarios móviles en la comunicación.**

***Index Terms*—testbed, Red de Acceso, FMC, QoS, MPLS, movilidad**

I. INTRODUCCIÓN

En los últimos años, la creciente demanda de interconexión por parte de los dispositivos móviles cuyas aplicaciones y servicios requieren cada vez de mayores recursos en la red, está cambiando la simplicidad y transparencia con la que fue concebida la arquitectura de Internet. En un principio, el principal cometido de Internet era interconectar host fijos. Con la aparición de los dispositivos móviles, se ha hecho necesario adaptar los protocolos tradicionales y las redes de acceso para acomodar a los usuarios móviles.

La cuarta generación (4G) de redes inalámbricas propone integrar redes heterogéneas de manera continua. De esta forma, se intenta satisfacer la creciente demanda de los usuarios en términos de QoS y ancho de banda [1].

De esta manera, las tradicionales redes de acceso E1/T1 y ATM desplegadas en 2G y 3G no son viables debido al coste asociado para adaptar estas redes a los nuevos requerimientos de QoS, sincronización, menor pérdida de paquetes y alta disponibilidad [2].

La integración de redes heterogéneas en 4G, se obtiene mediante el uso arquitecturas *All-IP* en la red de acceso. Para favorecer este despliegue, se han desarrollado varias soluciones basadas en IP/MPLS que son implementadas en la red de acceso [3]-[5].

Así mismo, la integración de las redes inalámbricas se consigue mediante protocolos de gestión de la movilidad basados en IP. Estos protocolos gestionan la movilidad del nodo móvil (MN) y permiten mantener la conectividad allá donde el dispositivo tenga acceso a una interfaz radio. Por lo tanto, los protocolos de gestión de movilidad basados en IP se pueden dividir en dos grandes grupos: centralizados y distribuidos. Los primeros tienen una estructura jerárquica bien definida dentro de la red de acceso, mientras los segundos permiten que diferentes nodos dentro de la red de acceso puedan realizar las funciones para la gestión de la movilidad permitiendo así una mayor flexibilidad dentro de la red.

Todos estos protocolos generan una gran cantidad de señalización cada vez que un nodo móvil realiza un *handover* entre diferentes puntos de acceso. Se hace, por tanto, necesario un estudio de las implicaciones que esto provoca dentro de la red, ya que este cambio de punto de interconexión conlleva modificaciones en el routing, lo que genera retardos debido a nuevos cómputos de rutas en la red, paquetes perdidos mientras se realiza el *handover* o recursos reservados debido a las diferentes rutas de respaldo creadas para mejorar los parámetros de QoS en la red de acceso.

Este trabajo tiene como principal objetivo analizar el comportamiento de una red de acceso que da servicio a terminales móviles, evaluando los mecanismos de *tunneling* más adecuandos, la señalización generada y las pérdidas de paquetes provocadas por los movimientos del usuario móvil.

El resto del artículo se estructura de la siguiente manera: la sección 2 presenta una breve descripción del estado del arte y los diferentes protocolos de movilidad existentes, así como los elementos de red que deben ser incorporados en la red de acceso. La sección 3 presenta el *testbed* desarrollado para realizar las pruebas de gestión de movilidad en la red de acceso. La sección 4 muestra los resultados obtenidos en la realización de las pruebas sobre el *testbed*. Por último, en la sección 5 se exponen las conclusiones de este trabajo.

II. ESTADO DEL ARTE

A. IP OSPF y MPLS-TE

Open Shortest Path First (OSPF) es un protocolo de enrutamiento en redes IP, englobado dentro de los algoritmos IGP (Interior Gateway Protocol) para el cálculo de rutas dentro de un dominio.

OSPF usa un algoritmo de estado el enlace (Link State Algorithm) para calcular las posibles rutas más cortas dentro del dominio. Para ello se basará en métricas que serán configuradas en los nodos.

Todos los routers del dominio construyen una base de datos con la información recabada de todos los nodos adyacente que se mantiene actualizada para realizar el cálculo de la ruta.

Por su parte, MPLS (Multi-Protocol Label Switching) [6] es una técnica que se ha utilizado hasta ahora ampliamente en redes troncales. Se le considera una tecnología de nivel 2+ al estar por debajo del nivel de red y por encima del nivel de enlace. MPLS permite establecer un camino llamado LSP (Label Switched Path) desde un extremo a otro de un dominio MPLS, por el que el tráfico va a ser enviado.

MPLS con ingeniería de tráfico (TE, Traffic Engineering) [7] tiene un funcionamiento similar a MPLS con la diferencia que los protocolos de encaminamiento interior (OSPF e IS-IS) han sido extendidos para soportar la ingeniería de tráfico. Del mismo modo, el funcionamiento de RSVP (Resource Reservation Protocol) también ha sido extendido para permitir a MPLS la creación de túneles LSP con ingeniería de tráfico (RSVP-TE).

Según las características del tráfico y de la situación de la red, los túneles LSP pueden ser adaptados en función de las necesidades y de los recursos de la red. Por tanto, cuando nos referimos a MPLS-TE son varias las tecnologías que funcionan de manera conjunta. Además de MPLS se necesita un protocolo de encaminamiento y un protocolo de reserva de recursos, cada uno con extensiones de ingeniería de tráfico. La situación más común es encontrarnos: MPLS, RSVP-TE [8] y OSPF-TE [9]. A continuación se explica brevemente cada uno de los componentes de MPLS-TE y su funcionamiento conjunto:

- OSPF-TE: Ofrece a MPLS la capacidad de calcular rutas con restricciones de ingenieria de trafico. Rellena las tablas de encaminamiento de cada router.
- RSVP-TE: Reserva los recursos necesarios y crea los túneles LSP rellenando las tablas FIB (Forwarding Information Base) de cada conmutador MPLS de la red.
- MPLS: Se encarga de clasificar el tráfico, reparte las etiquetas y organiza los FEC (Forwarding Equivalence Class).

El funcionamiento conjunto de una red MPLS con ingeniería de tráfico es la siguiente: Un LER (Label Edge Router) utiliza OSPF-TE para calcular una ruta con restricciones de ingeniería de tráfico. Tras calcular esta ruta, las tablas de encaminamiento se rellenan con la información de nivel de red que se obtiene del protocolo de encaminamiento. Una vez calculada la ruta, se utiliza RSVP-TE para reservar recursos en el camino calculado por OSPF-TE y para repartir las etiquetas con las que se rellenan las tablas FIB, de forma que el túnel LSP está creado. El LER finalmente clasifica el tráfico, lo etiqueta y lo reenvía por el túnel LSP establecido.

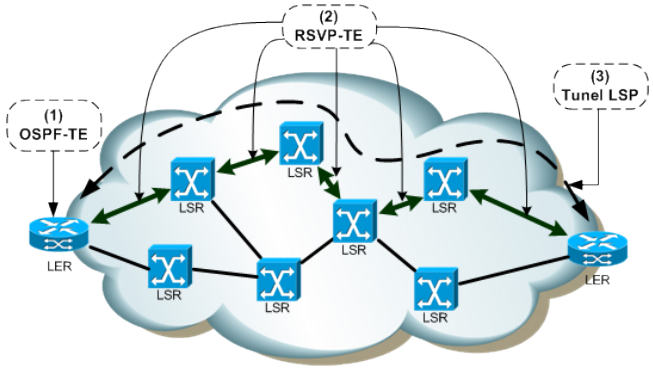


Fig. 1: Funcionamiento basico de MPLS-TE

Este funcionamiento puede observarse en la Fig. 1. Una de las ventajas fundamentales que se consiguen con la extensión de ingeniería de tráfico en OSPF es que se extienden el número de restricciones a utilizar durante el cálculo de las rutas.

B. Gestión de la movilidad en redes de próxima generación

La gestión de la movilidad en Internet es un aspecto clave en las comunicaciones móviles y es uno de los retos en la evolución de Internet debido a la gran demanda de tráfico y al incremento exponencial de usuarios de estas tecnologías. En 2012 el crecimiento del trafico de datos móviles fue de un 70% con respecto al año anterior. Este volumen de datos está provocado por servicios como la navegación web, mensajería instantánea, juegos on-line, servicios de redes sociales o, principalmente, servicios de video *streaming* (p. ej. Youtube, Vimeo, Netflix) que por primera vez en 2012 ha supuesto mas del 50 % del trafico total de datos en redes móviles [10].

Para dar soporte a esta creciente demanda de tráfico y a la propia movilidad de los usuarios, las operadoras de telecomunicaciones diseñan arquitecturas que proporcionan servicios móviles en banda ancha *All-IP* donde los datos de usuario se intercambian a través de paquetes IP que se envían sobre distintas tecnologías de niveles inferiores. En estas redes, en las que los usuarios se mueven frecuentemente, cambiando su punto de conexión a la red, la gestión de la movilidad IP es una función clave para permitir a los nodos móviles continuar con una conexión ininterrumpida ofreciendo movilidad transparente.

En este entorno de convergencia hacia arquitecturas *All-IP*, el IETF ha desarrollado varios protocolos de gestión de la movilidad que se pueden clasificar en dos familias: los protocolos de gestión de la movilidad basados en *host* y los basados en red. La mayor parte de las soluciones son extensiones o modificaciones del protocolo MIPv6.

Las propuestas basadas en *host* como Mobile IPv6 o Dual Stack Mobile IPv6 (DSMIPv6) [11] ofrecen movilidad al nodo móvil (MN, Mobile Node). Este nodo móvil es el elemento principal del protocolo y corresponde al usuario que se mueve a través de Internet; la red origen (Home Network, HN) es aquella desde donde parte el nodo móvil y cuyo prefijo coincide con el de la dirección permanente (Home Address, HoA) del nodo.

El agente origen (Home Agent, HA) es un router IPv6 situado en la red origen responsable de interceptar y de hacer llegar al nodo móvil aquellos paquetes dirigidos a él

mientras se encuentra fuera de su red origen; la red visitada (Foreign Network, FN) es la red IPv6 en la que se encuentra actualmente el nodo móvil y en la cual ha adquirido una dirección IP auxiliar (Care-of Address, CoA) a través de uno de los mecanismos de IPv6; el nodo con el que el nodo móvil se comunica se denomina CN (Correspondant Node).

Cuando el nodo móvil está fuera de su red origen, se establece un túnel entre él y su agente origen, de forma que el camino de los datos pasan por dicho túnel. Cuando el MN cambia su punto de conexión a la red al realizar un movimiento, durante un corto periodo de tiempo, la comunicación se interrumpe, provocando pérdidas de paquetes. Este proceso de movimiento de una red a otra se denomina *handover*, *handoff* o, simplemente, traspaso. Proporcionar un *handover* transparente para un nodo móvil que se mueve a una nueva subred IP mientras su sesión permanece activa, junto con mantener la QoS durante este movimiento, son los principales problemas del protocolo MIPv6.

Con respecto a los protocolos de gestión de la movilidad basados en red, como Proxy Mobile IPv6, la principal diferencia con respecto a los basados en *host* es que los MN podrán realizar los movimientos sin participar en la señalización de la movilidad, es decir, no es necesario modificar la pila de protocolos del dispositivo móvil. En este caso, la detección del movimiento y y la señalización son realizados por una nueva entidad denominada MAG (Mobile Access Gateway), que normalmente se sitúa en el router de acceso que da servicio al MN.

Por tanto, en el dominio en el que se ofrece la movilidad basada en red (LMD, Local Mobility Domain) existen multitud de MAGs que, a través de los mecanismos propios de IPv6 como Router Discovery y Neighbour Discovery o mediante información de nivel de enlace, es capaz de detectar los movimientos del MN. Dentro del dominio de Proxy Mobile IPv6, el MN tendrá una dirección IPv6 permanente cuyo prefijo corresponderá a la de su red origen, que será gestionada por otro agente que debe estar presente en la red que es el LMA (Local Mobility Anchor). Este es el agente que gestiona la movilidad de los dispositivos móviles del LMD y tiene un rol similar al del *Home Agent* en Mobile IPv6.

Al igual que en las soluciones basadas en *host*, la información que va destinada al MN desde el CN es interceptada por el agente de movilidad, en este caso el LMA, que se encarga de enviar los datos a través de un túnel al MAG que da servicio al MN. Del mismo modo, cuando el MN envía datos al CN, los enviará al router de acceso (MAG), que los reenvía al LMA mediante un túnel. El LMA encamina el trafico fuera del LMD hasta el CN mediante IP.

En el despliegue de las tecnologías de comunicaciones móviles, MIPv6 y PMIPv6 han sido los mecanismos de gestión de la movilidad de referencia. Para el diseño de GPRS (General Packet Radio System), el 3GPP (3rd Generation Partnership Project) adoptó una variante de la movilidad IP basada en red y para el núcleo de red de LTE (Long Term Evolution), el 3GPP ha adoptado PMIPv6 y DSMIPv6 como mecanismos de gestión de la movilidad basada en la red y en *host* respectivamente[12].

Por tanto, los despliegues de las redes móviles actuales como UMTS (Universal Mobile Telecommunications System) y 4G EPS (Evolved Packet System) utilizan una gestión de la movilidad en el que toda la información, tanto de señalización como de datos, con origen o destino el usuario móvil, tenga que pasar por un punto concreto del núcleo de la red, que es el nodo que gestiona la movilidad. Esos agentes son el HA en Mobile IPv6 y el LMA en PMIPv6, como se observa en las Fig. 2 y 3 respectivamente. Estos diseños centralizados no son eficientes cuando se transmiten grandes volúmenes de datos y tienen algunas limitaciones [13]:

- No permite movilidad dinámica.
- Alto *overhead* de señalización.
- *Routing* poco óptimo.
- Baja escalabilidad.
- Único punto de fallo y vulnerabilidad a ataques.

La necesidad de una red más dinámica y flexible ante los nuevos escenarios que requieren las redes de próxima generación está llevando a las organizaciones estandarizadoras a desarrollar protocolos de gestión de la movilidad distribuidos. Recientemente, tanto el IETF como el 3GPP están proponiendo iniciativas que resuelvan estos problemas. [14].

En el caso del IETF, se ha creado recientemente un grupo de trabajo denominado DMM (Distributed Mobility Managment) para proporcionar soluciones distribuidas que resuelvan las nuevas necesidades de los operadores de red. El 3GPP, por su parte, está evolucionando hacia una gestión de la movilidad más flexible y dinámica en sus núcleos de red.

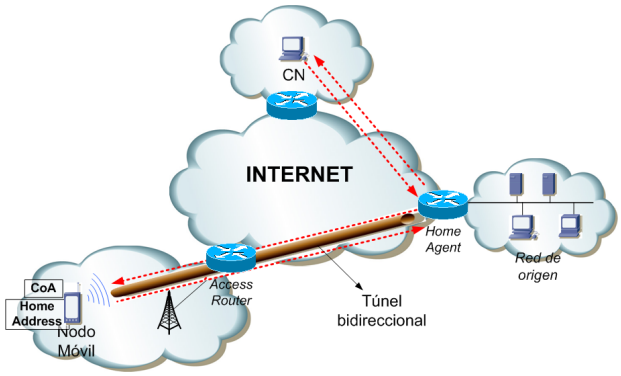


Fig. 2: Gestión de la movilidad mediante MIPv6

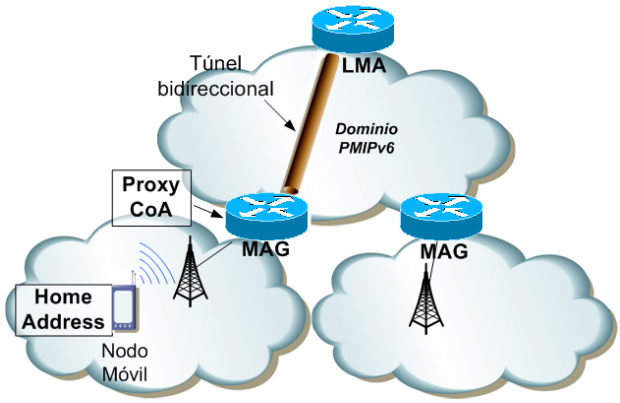


Fig. 3: Gestión de la movilidad mediante PMIPv6

C. Integración de MPLS con protocolos de gestión de la movilidad

Desde que se comenzaron a desarrollar los primeros protocolos de gestión de la movilidad, uno de los principales retos ha sido mantener la conectividad durante el movimiento del usuario. Sin embargo un protocolo de gestión de la movilidad eficiente debe ser capaz, además, de proporcionar los recursos que el usuario espera de la red.

Con este planteamiento, existen trabajos que tratan de ofrecer calidad de servicio en redes de comunicaciones móviles, extendiendo los mecanismos que resuelven esta situación en las redes cableadas. Los primeros trabajos que trataban de ofrecer QoS en redes móviles se centraron en extensiones a RSVP.

Sin embargo, MPLS es la tecnología que actualmente trata de forma más eficiente los recursos de la red, ya que proporciona una solución que mejora el rendimiento en el reenvío de paquetes y garantiza la QoS en determinados caminos [15].

Con respecto a Mobile IP, MPLS puede ser visto como una tecnología de tunneling que supera las técnicas propuestas en Mobile IP (por ejemplo IP sobre IP) o como una tecnología con la que mejorar el *handover* de Mobile IP. Una revisión de soporte de QoS en redes móviles puede encontrarse en [16], [17].

En los últimos años, la tendencia está llevando a la introducción de MPLS en entornos inalámbricos [18]. Los principales organismos de estandarización como el IETF, el ITU-T (Internacional Union's Telecommunication Standarization Sector) o el MPLS Forum están trabajando en propuestas en las que Mobile IP y MPLS interactúan en un entorno de movilidad [19].

Desde el MPLS Forum se ha estado trabajando en la primera especificación integral para solventar el principal obstáculo en el despliegue de los servicios móviles y que han definido como la Red de Acceso de la Red Inalámbrica (Fig. 4).

En esta especificación, se proporciona un entorno basado en MPLS para los operadores móviles y se establece un conjunto de requisitos para el acceso inalámbrico y para el total de redes que utilizan diferentes interfaces de radio y protocolos como GSM, UMTS, HSPA, LTE o Mobile WiMAX.

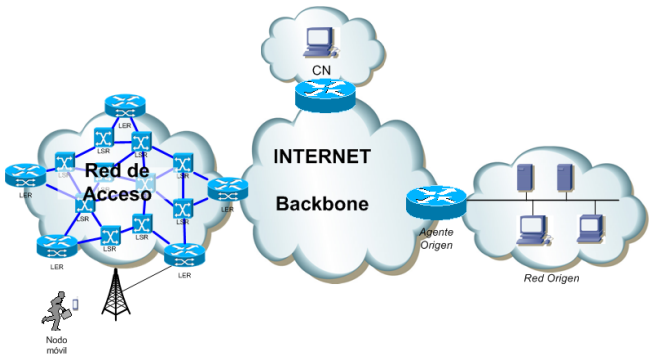


Fig. 4: Red de Acceso de la Red Inalámbrica

III. DESCRIPCIÓN DEL ESCENARIO DE PRUEBAS

En esta sección se describe el *testbed* que se ha usado para llevar a cabo los experimentos presentados en este artículo y el equipamiento *hardware* utilizado. La fig. 5 muestra la topología de red utilizada para las pruebas.

A. Diseño del testbed

La necesidad de evolución de las tecnologías de comunicaciones inalámbricas, que deben dar soporte a un mayor número de usuarios y cuyos requerimientos en cantidad y calidad de los servicios ofrecidos son cada vez mas elevados, obliga también a evolucionar a las tecnologías de la red fija que soportan dichas comunicaciones. Aunque estemos tratando con comunicaciones móviles, la red fija y, en concreto, la red de acceso a la red inalámbrica, juega un papel fundamental en el rendimiento del servicio ofrecido a los usuarios móviles.

Este artículo se centra en el análisis y en la evaluación del rendimiento de la red de acceso que da soporte a usuarios móviles. Por tanto, el *testbed* se ha diseñado como una estructura jerárquica de varios niveles y sobre la que se puedan evaluar las características propias de una red de comunicaciones móviles. Cabe indicar que no es el objetivo de este trabajo evaluar el rendimiento de ningún protocolo de gestión de la movilidad concreto, sino de la red de acceso.

B. Equipamiento hardware

Este escenario consta de 6 routers Cisco 1921/K9 con capacidades IP y MPLS-TE para construir la red de acceso. Estos routers se interconectan tal y como se muestra en la Fig. 5, de manera que permita analizar el *routing* de la red de acceso una vez que se ha producido un movimiento entre dos routers de salida.

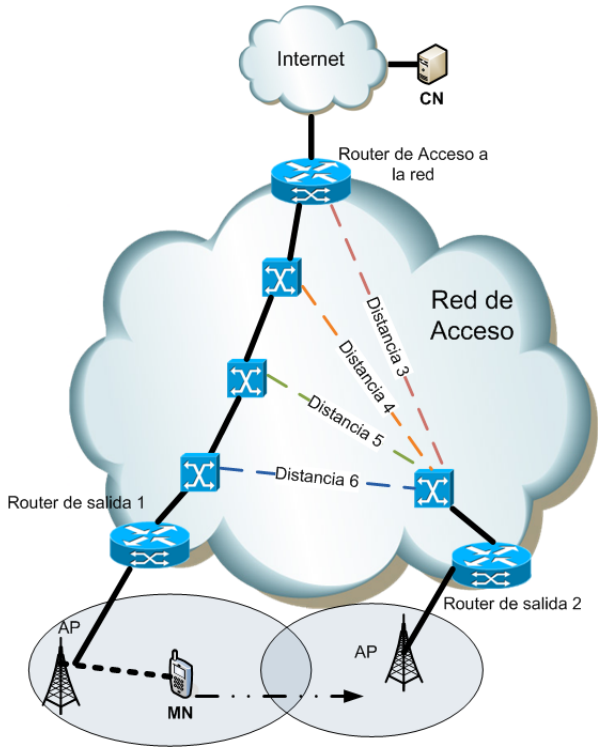


Fig. 5: Topología de la red

Dicho movimiento afecta al routing establecido para el transporte de los paquetes dentro de la red de acceso y por lo tanto, necesita que los algoritmos recalculen el camino tanto de MPLS como de IP dependiendo del protocolo usado.

El hardware utilizado para los dispositivos de comunicación del *testbed* son los siguientes: el nodo corresponsal es un Mac Book Pro i7 a 2,4 Ghz, 4 Gb de Ram, mientras el nodo móvil es un PC i3 a 2,53 Ghz con 4 Gb de memoria.

El tráfico que se ha usado para las pruebas es generado con la herramienta ostinato [20], los parámetros que se han usado para las pruebas, es un flujo de 60000 paquetes de 60 bytes cada uno, usando enlaces de 100 Mbps en el escenario. No se ha realizado reserva de recursos en la red de acceso cuando el escenario de la red de acceso estaba configurado usando MPLS-TE. De esta manera todo el tráfico que circula por la red será tomado como tráfico best-effort.

En este *testbed* se ha propuesto la configuración de diferentes túneles entre el nodo de entrada a la red de acceso y los nodos que van a servir como punto de anclaje para los dispositivos móviles para medir diferentes parámetros de QoS.

IV. RESULTADOS

En esta sección se describen los experimentos realizados en el *testbed* descrito en la sección anterior.

Los esfuerzos de estandarización que están realizando tanto el 3GPP como el IETF para los nuevos diseños de redes móviles, indican una tendencia hacia una gestión de la movilidad más flexible, dinámica y distribuida que solventen de forma eficiente el crecimiento exponencial en la demanda de tráfico de datos a través de dispositivos móviles. Las soluciones de movilidad distribuida proponen que las funciones de movilidad no recaigan sobre un único nodo en la red, y sean varios agentes los que puedan proporcionar, de forma coordinada y distribuida, la funcionalidad que en MIP y PMIP ofrecen el HA y el LMA respectivamente.

En este caso, la ubicación topológica del agente de movilidad puede afectar al rendimiento del *handover* y al retardo del paquete extremo a extremo. Por otra parte, desde el punto de vista de la arquitectura de red, estos nuevos mecanismos de gestión de la movilidad distribuida proponen también diseños de red con menos niveles de jerarquía (*flat networks*)[21]

Por otra parte, los protocolos de gestión de la movilidad establecen túneles para enviar el tráfico. En las pruebas realizadas, consideramos distintos mecanismos de *tunneling* como son IP sobre IP, GRE (Generic Routing Encapsulation) y MPLS.

IP sobre IP es un protocolo en el que un datagrama IP puede ser encapsulado dentro de otro datagrama IP. Un túnel configurado con el modo IP-IP tiene 20 bytes extra de *overhead*, por tanto, en una red con MTU de 1500 bytes, un paquete enviado por el túnel puede tener un tamaño máximo de 1480 Bytes. GRE, por su parte, requiere la encapsulación IP-IP (con su correspondiente cabecera extra de 20 bytes), pero ademas añade otros 4 bytes de la cabecera GRE al paquete, resultando un *overhead* de 24 bytes. Por último, un túnel MPLS tiene una etiqueta de 4 bytes que se añade de *overhead* a un datagrama IP.

La fig. 6 muestra la cantidad de información de señalización y de datos que se envían en una sesión de 60 segundos utilizando IP-IP, GRE y MPLS como métodos de *tunneling*. Ademas, se muestran los valores para distintos niveles de jerarquía para la red de acceso.

Como se puede observar en la figura, el *overhead* de señalización que introduce en la red MPLS es un 80% más pequeña que el introducido por los túneles IP-IP y por GRE en cualquiera de los niveles de jerarquía de la red. A raíz de estos datos, se puede observar la importancia de la señalización en la red de acceso en el que las rutas cambian dinámicamente dependiendo del movimiento del nodo móvil.

Así mismo, se comprueba que los niveles de jerarquía dentro de la red de acceso influyen en la cantidad de *overhead* que se manda a la red. En estas pruebas se ha usado un único flujo que se transmitiría por la red de acceso hasta un nodo móvil. Si esto se reproduce para un conjunto de nodos móviles a los que la red de acceso estuviera dando servicio, el *overhead* introducido por IP-IP y por GRE aumentaría por cada uno de los móviles que estuvieran conectados. Las organizaciones de estandarización, fundamentalmente el IETF, plantea disminuir el tamaño de jerarquía de los nodos de la red de acceso y llegar a una red con los menores niveles de jerarquía posible.

En estos experimentos se ha realizado el análisis del tiempo de *handover* en función de los mensajes de señalización necesarios para detectar la movilidad.

Estos mensajes son intercambiados entre los nodos vecinos de la red para detectar los cambios producidos en el transcurso de la comunicación y poder actuar en consecuencia. En [22] se especifican los mensajes de señalización que se intercambian entre los LSR (Label Switch Router) de una red MPLS-TE para mantener el estado de los enlaces. Se intercambia un mensaje *Hello* cada cierto tiempo, configurable, entre los nodos vecinos. Si este mensaje de 60 bytes se pierde un número predefinido de veces, el vecino adyacente detectará y notificará el error y se liberarán los LSP que pasen por ese conmutador. Así mismo, se intercambiará otros dos mensajes en todo el LSP, para el refresco de la tabla LFIB (Label Forwarding Information Based) del LSP completo. Estos mensajes son *PATH* y *RESV* y se intercambian con una frecuencia bastante menor a la de los *Hello* en los nodos intermedios.

Por otro lado, en [23] se especifican los mensajes que se intercambian los nodos de una red IP para mantener las tablas de rutas RIB (Routing Information Based) actualizadas y detectar que se produce algún cambio. Estos mensajes son

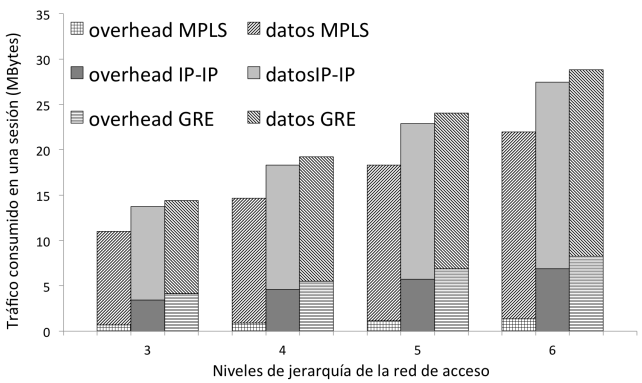


Fig. 6: *Overhead en función de los niveles de jerarquía*

también llamados mensajes *Hello*, los cuales se envían en un intervalo configurable y tienen un tamaño de 96 bytes. Si se produce algún error en algún nodo o enlace de la red, el nodo adyacente lo detectaría a través de este mensaje y mandaría un mensaje *LS Update* actualizando tanto su tabla de rutas como la tabla de rutas de sus nodos adyacentes. Estos mensajes serán replicados por todos los nodos de la red IP hasta que llegan al nodo de entrada de la red de acceso que deberá cambiar la ruta, seguida por los paquetes hasta el nodo móvil. Por tanto es necesario un tiempo de convergencia entre todos los nodos para que actualicen sus tablas de rutas.

La fig. 7 y la fig. 8 comparan la cantidad de señalización que se debe intercambiar entre los nodos de la red para el reenrutamiento de los paquetes desde el nodo de entrada a la red de acceso hasta el router de salida, y el tiempo que pasa en la red para detectar que se ha producido un cambio de router de acceso del nodo móvil. Los tiempos mostrados son la media obtenida tras la ejecución de 5 repeticiones por experimento.

Como se puede observar en la comparativa, MPLS introduce menor *overhead* de señalización en la red y disminuye el tiempo del cálculo de la ruta aún con un intervalo de 1 segundo. Esto es debido a los túneles *detour* que permiten el reenrutamiento de los paquetes hacia el nuevo destino. Usando IP, aumenta tanto el *overhead* de señalización ya que el tamaño de los paquetes *Hello* de OSPF es mucho mayor así como el tiempo de convergencia de OSPF para notificar el cambio en el routing incrementa el tiempo de *handover*.

De igual manera, el intervalo de señalización tanto en MPLS como en IP influye en el tiempo de *handover* ya que a un mayor tiempo de señalización, aumenta el tiempo que se tarda en detectar un cambio en el routing de la red y por lo tanto en propagar las nuevas rutas.

La fig. 9 muestra la comparativa de la pérdida de paquetes usando un túnel MPLS y un túnel basado en IP.

Como se ha explicado en la prueba anterior, el intervalo de señalización influye en el tiempo de propagación de rutas y esto conlleva una mayor pérdida de paquetes mientras no se señalice el nuevo camino por el que retransmitir paquetes.

En la fig. 9 también se puede observar que el porcentaje de pérdidas de MPLS sobre IP es un 10% aproximadamente menor, con lo que se favorece una comunicación con menor número de pérdidas, además de las ventajas que ya se conocen

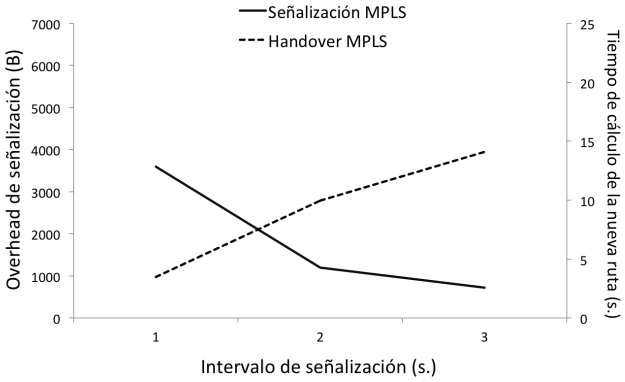


Fig. 7: *Overhead* vs Tiempo para el cálculo de la nueva ruta usando túneles MPLS

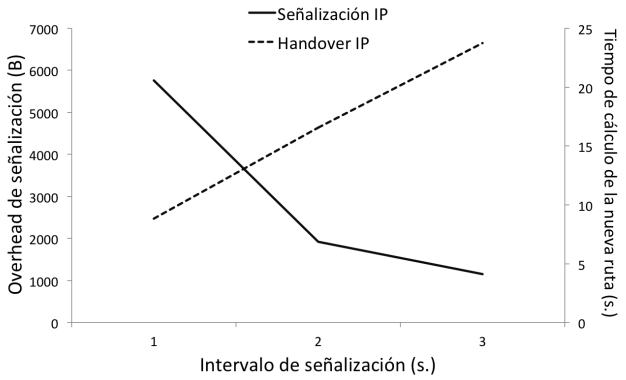


Fig. 8: *Overhead* vs Tiempo para el cálculo de la nueva ruta usando túneles IP

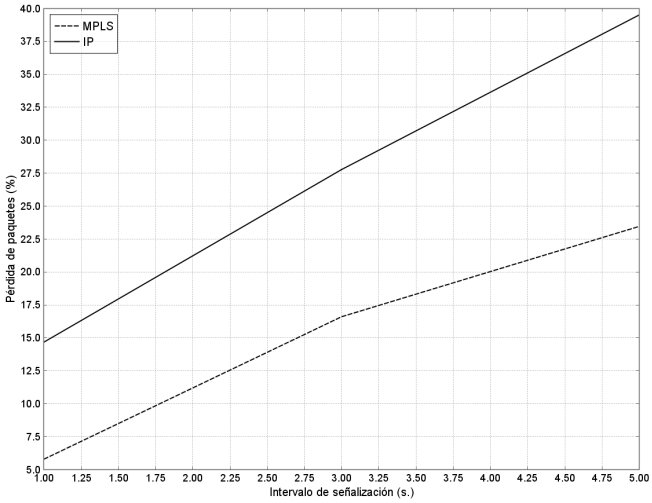


Fig. 9: Pérdida de paquetes utilizando IP y MPLS

de MPLS-TE en cuanto a la QoS ofrecida, como la reserva de recursos en la red de acceso.

Por último, se puede destacar, que el tiempo de señalización es el tiempo que tardará la red en recuperarse del cambio de routing sobre la red de acceso. En estas pruebas se han realizado únicamente en mecanismos basados en nivel 3. Se pueden utilizar mecanismos de nivel 2 para poder acelerar el cambio de las tablas de routing y switching de la red.

V. CONCLUSIONES

En este artículo se ha presentado un *testbed* que representa una red de acceso de un proveedor de servicios en el que se analiza el impacto que supone incluir la movilidad en la misma. Además se han comparado diferentes mecanismos de *tunneling* entre el nodo acceso a la red y los nodos que dan conectividad al nodo móvil. En estas comparativas se observa cómo MPLS-TE además de proporcionar QoS a las comunicaciones, introduce un menor *overhead* en la red, lo cual es beneficioso si se gestionan múltiples flujos.

Así mismo, este *overhead* es proporcional al tiempo de detección y recálculo de las rutas en la red de acceso. Por tanto, es necesario llegar a un equilibrio entre la cantidad de *overhead* introducido en la red y el tiempo de cálculo de la nueva ruta.

Esto, además, es importante ya que cuanto mayor sea el tiempo de cálculo de la nueva ruta, mayor sera el número de paquetes perdidos en la red. Esto también provoca un mayor *overhead* debido a reenvíos si se usa TCP como protocolo de transporte. En este caso, con técnicas de nivel 2, se podrían reducir estos problemas en la red de acceso.

Este trabajo se centra en un aspecto relevante que está por llegar a los proveedores de servicio como es la integración de la red fija y móvil. Las redes de próxima generación requerirán que los proveedores de servicio integren en sus redes la movilidad de los nodos. Por tanto, la red de acceso deberá gestionar los *handovers* de los dispositivos móviles y el enrutamiento de sus paquetes, lo que supone un importante reto en el mundo de las telecomunicaciones.

AGRADECIMIENTOS

Este trabajo ha sido financiado, en parte, por el Gobierno de Extremadura gracias a la ayuda con referencia GRU10116.

REFERENCES

[1] Frattasi S., Fathi H., Fitzek F., Prasad R., Katz M.: Defining 4G technology from the users perspective, IEEE Network, 2006.
[2] Tipmongkolsilp O., Zaghloul S., JukanFrattasi A.: The Evolution of Cellular Backhaul Technologies: Current Issues and Future Trends, IEEE Communications Surveys & Tutorials, 2011
[3] Ghebretensa Z., Harmatos J., Gustafsson K.: Mobile Broadband Backhaul Network Migration from TDM to Carrier Ethernet, IEEE Communications Magazine, October 2010
[4] The Broadband Forum, Technical Specifications for MPLS in Mobile Backhaul Networks, Tech. Rep. TR-221, The Broadband Forum, October 2011.
[5] Francesco P., ”An MPLS-based architecture for scalable QoS and traffic engineering in converged multiservice mobile IP networks,” Comput. netw., vol. 47, pp. 257-269, 2005.
[6] E. Rosen, A. Viswanathan, R. Callon. ?Multiprotocol Label Switching Architecture. IETF RFC 3031. January 2001.
[7] D. Awduche, J. Malcolm, J. Agogbua, M. O?Dell, J. McManus. ?Requirements for Traffic Engineering Over MPLS?. IETF RFC 2702. September 2009.
[8] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow. ?RSVP-TE: Extensions to RSVP for LSP Tunnels?. IETF RFC 3209. December 2001.
[9] D. Katz, K. Kompella, D. Yeung. ?Traffic Engineering (TE) Extensions to OSPF version 2?. IETF RFC 3630. September 2003.
[10] Cisco, ”Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017”
[11] H. Soliman, ?Mobile IPv6 Support for Dual Stack Hosts and Routers,? IETF RFC 5555 June 2009.
[12] Dong-Hoon Shin, D. Moses, M. Venkatachalam, and S. Bagchi. Distributed mobility management for efficient video delivery over all-ip mobile networks: Competing approaches. Network, IEEE, 27(2):28-33, 2013.
[13] H. Chan, D. Liu, P. Seite, H. Yokota, and J. Korhonen. Requirements for Distributed Mobility Management. Internet-Draft, December 2012.
[14] J. C. Zuniga, C. J. Bernardos, A. de la Oliva, T. Melia, R. Costa, and A. Reznik. Distributed mobility management: a standards landscape. Communications Magazine, IEEE, 51(3):80-87, 2013.
[15] R. G. Garroppo, S. Giordano, and L. Tavanti. Network-based micromobility in wireless mesh networks: Is mpls convenient? In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pages 1-5, 2009.
[16] Taha, A.-E.M.; Hassanein, H.S.; Mouftah, H.T., ”Extensions for Internet QoS paradigms to mobile IP: a survey,” Communications Magazine, IEEE , vol.43, no.5, pp. 132-139, May 2005.
[17] Konstantinos Samdanis and A. Hamid Aghvami. Qos provision in wireless access networks: a routing perspective considering mobility. International Journal of Network Management, 19(5):445-456, 2009
[18] Langar, R., Bouabdallah, N., and Boutaba, R. 2008. ?A comprehensive analysis of mobility management in MPLS-based wireless access networks?. IEEE/ACM Trans. Netw. 16, 4 (Aug. 2008), 918-931
[19] IP/MPLS Forum. ?Mobile backhaul Standard?. October 2008.
[20] Packet/Traffic Generator and Analyzer Ostinato. Ref: https://code.google.com/p/ostinato/ Ult. Visita: 28 Mayo 2013
[21] H. Chan, H. Yokota, J. Xie, P. Seite, and D. Liu, ”Distributed and Dynamic mobility management in mobile internet: Current approaches and issues,” Journal of Communications, vol. 6, no.1, pp. 4-15, February 2011.
[22] D. Awduche; L. Berger; D. Gan; T. Li; V. Srinivasan; G. Swallow;, RSVP-TE: Extensions to RSVP for LSP Tunnels, RFC 3209, December 2001
[23] J. Moy;, OSPF Version 2, RFC 2328, April 1998

Abordando la heterogeneidad en la Internet de las cosas: una solución de agentes auto-configurables

Inmaculada Ayala, Mercedes Amor, Lidia Fuentes
Departamento de Lenguajes y Ciencias de la Computación
Universidad de Málaga
Bulevar Louis Pasteur, 35, Málaga
{ayala,pinilla,lff}@lcc.uma.es

***Resumen*—La Internet de las Cosas concibe un mundo en el que un conjunto heterogéneo de dispositivos están interconectados y colaboran utilizando Internet para proporcionar servicios a los usuarios. Desde el punto de vista del desarrollador, estas aplicaciones requieren abordar y gestionar una gran diversidad de dispositivos, que deben comunicarse de forma efectiva a través de diferentes tecnologías y protocolos de comunicación. Esto supone hacer frente a las incompatibilidades y diferencias que puedan surgir entre las tecnologías subyacentes, incluso durante la ejecución. La tecnología de agentes proporciona los medios necesarios para abordar esta heterogeneidad que impone la IoT de forma satisfactoria. Sin embargo, aquellas plataformas de agentes disponibles para dispositivos ligeros y de recursos limitados como sensores, presentan mayores limitaciones e incompatibilidades a la hora de facilitar la comunicación de dispositivos que soporten diferentes tecnologías y protocolos de comunicación, característico de estos entornos. En este trabajo veremos como el uso combinado Sol, una plataforma de agentes para la IoT, y la familia de agentes Self-StarMAS, permite resolver resuelven de manera efectiva la comunicación de aplicaciones basadas en agentes que se ejecutan en un conjunto heterogéneo de dispositivos típicos de la IoT. Para ilustrar las bondades de nuestra propuesta, utilizaremos como caso de estudio un museo inteligente.**

***Palabras Clave*—Internet de las Cosas, Inteligencia Ambiental, Dispositivos ligeros, Agentes Software**

I. INTRODUCCIÓN

La Internet de las Cosas (*Internet of Things* en inglés, o IoT) concibe un mundo en el que los objetos de la vida diaria (como por ejemplo, teléfonos móviles, vehículos, aparatos electrodomésticos etc.) están interconectados y colaboran a través de Internet para proporcionar servicios útiles a los usuarios [1]. Las posibilidades ofrecidas por la IoT permiten el desarrollo de una gran cantidad de nuevas aplicaciones cuyo propósito es mejorar la calidad de nuestras vidas, tanto en casa, como mientras viajamos, en visitas turísticas, en el hospital o mientras trabajamos [2]. Para ello la IoT tiene como objetivo proporcionar una infraestructura de red global y dinámica donde los *objetos*, tanto virtuales como físicos, se identifican y localizan mediante identificadores únicos, y están integrados de forma transparente en una red de información. Varias tecnologías contribuyen a hacer realidad esta visión: entornos de Inteligencia Ambiental (*Ambient Intelligence*, AmI), sistemas empotrados, identificación automática de objetos, como RFC (*Radio Frequency Communication*) y NFC (*Near Field Communication*), o la computación ubicua (*Ubiquitous Computing*), sólo por mencionar algunos ejemplos [2].

Cualquier sistema software desarrollados para la IoT, como los entornos AmI, deben tener en cuenta una serie de requisitos inherentes de este tipo de sistemas en cuanto a: (i) la heterogeneidad de dispositivos que los componen (ej. sensores, teléfonos móviles, dispositivos integrados, etc.); (ii) la diversidad de tecnologías de comunicación, mayoritariamente inalámbricas, utilizadas por estos dispositivos (ej. Bluetooth, ZigBee, WiFi, etc.); (iii) y la sensibilidad al contexto (ej. Los sistemas deben adaptar su modo de operación a los recursos de que dispongan los dispositivos, cómo la batería o la memoria interna). Es decir, para llevar a cabo la visión de la IoT, los servicios y aplicaciones se debe poder ejecutar en una gran variedad de dispositivos, adaptándose de forma adecuada a la disponibilidad de recursos (computacionales o del sistema operativo). Además, dado que continuamente aparecen innovaciones tecnologías en los dispositivos y tecnologías de comunicación inalámbricas de este tipo de sistemas, es necesario proporcionar los medios y mecanismos necesarios para poder actualizar e incorporar estas novedades a las aplicaciones de la IoT, incluso a las que ya están desplegadas.

Por tanto, hemos de tener en cuenta que si no tratamos de manera adecuada la heterogeneidad a nivel de comunicaciones permitiendo la incorporación de cualquier tecnología de comunicación con el soporte adecuado se limitará enormemente el desarrollo de aplicaciones y servicios para IoT, ya que el intercambio de información y por tanto la comunicación entre dispositivos es un elemento vital de tipo de sistemas. Además, dado que la mayoría de sistemas AmI en entornos de IoT están compuestos por dispositivos con recursos limitados (ej. energía, capacidad de procesamiento, etc.), es necesario gestionar la degradación que sufren estos dispositivos con el tiempo. Por ejemplo en una red de sensores (*Wireless Sensor Network*, WSN), cuyos elementos se encargan de proporcionar información acerca del entorno del usuario, los nodos pierden energía, o simplemente pueden dejar de funcionar, pero el sistema global del que forman parte debería de poder seguir funcionando aunque su calidad de servicio disminuya. Sería por tanto muy beneficioso que el sistema fuera capaz de realizar, de forma autónoma, acciones y tareas orientadas gestionar de forma eficiente los recursos de los dispositivos (por ejemplo para ahorrar energía y alargar la vida de la batería, o que permitan al sistema recuperarse del fallo de alguno de sus nodos). Esta auto-adaptación del funcionamiento interno en respuesta a diferentes tipos de cambios significa que sistemas AmI se deberían comportar como sistemas autónomos con capacidad de autogestión [3].

Dado que las propiedades de autogestión (*self-management* en inglés) están inspiradas en las propiedades de los agentes software [4], el uso de la tecnología de agentes software y los Sistemas Multi-Agente (SMA) facilita enormemente y de

forma eficaz el diseño e implementación de aplicaciones para entornos de AmI con capacidad de autogestión. De hecho el 38.64% de los sistemas AmI se basan en agentes y SMA para la realización de muchas de sus funciones más complejas [5]. Así, agentes software ejecutándose directamente en los dispositivos, serían los encargados de incorporar las funciones de auto-adaptación necesarias para gestionar sistema AmI en respuesta a los cambios en su entorno (es decir, sensibilidad al contexto).

En este trabajo veremos como el uso combinado de: (i) *Sol*, una plataforma de agentes para la IoT [6], y (ii) *Self-StarMAS* [7], [8], una familia de agentes con capacidades de auto-gestión que pueden ser ejecutados sobre una gran variedad de dispositivos ligeros, se puede resolver de forma efectiva la heterogeneidad de tecnologías de comunicación de la IoT. Para ilustrar nuestra propuesta hemos desarrollado una aplicación real para gestionar el museo de Informática de la E.T.S.I. Informática de la Universidad de Málaga, utilizando tecnologías de la IoT. En este artículo nos vamos a centrar en la presentación de una serie de escenarios que ponen de relieve cómo la heterogeneidad limita la interacción entre agentes, y cómo se resuelve de forma efectiva y en muchos casos de forma eficiente, con nuestra propuesta.

El artículo está organizado de la siguiente forma: la siguiente sección describe cuales son las principales características de la plataforma de agentes *Sol* y de la familia de agentes *Self-StarMAS*. La sección III describe la aplicación de gestión del museo y una descripción de los agentes que forma parte de la misma, además aborda cómo resolvemos la heterogeneidad a nivel de dispositivos y comunicaciones mediante la presentación de varios escenarios que se dan en la aplicación. La sección IV muestra los resultados obtenidos en los experimentos realizados para comprobar la validez de nuestra propuesta. Finalmente, en la última sección, presentamos nuestras conclusiones y el trabajo futuro.

II. AGENTES PARA LA IOT

En la actualidad, la tecnología de agentes proporciona los medios necesarios para gestionar muchos de los requisitos de identificación, localización, interacción y comunicación que impone la IoT de forma satisfactoria: los agentes software son entidades reactivas, proactivas, que se identifican, localizan y comunican a través de los servicios proporcionados por una plataforma de agentes distribuida. En la actualidad, existen varias plataformas de agentes que facilitan el desarrollo, despliegue, ejecución y comunicación de agentes software sobre dispositivos propios de la IoT (como teléfonos móviles, dispositivos personales ligeros e incluso motas) [9], [10], [11], [12], [13]. Los agentes que se ejecutan en nodos de la IoT encapsulan y proporcionan funcionalidad y servicios, separándolos de los detalles hardware y software dependientes del dispositivo en el que se está ejecutando. De esta forma, si un objeto o nodo de la IoT está representado por un agente software, la localización de objetos, nodos servicios y funciones puede abordarse a través del servicio de directorio (DF por sus siglas en inglés, *Directory Facilitator*) que proporciona la plataforma de agentes, resolviendo de forma adecuada y natural la identificación y localización de objetos en la IoT.

Sin embargo, las plataformas de agentes disponibles para dispositivos ligeros no abordan de forma adecuada el problema de la heterogeneidad, imponiendo fuertes limitaciones que impiden la interoperabilidad y la comunicación, tal y cómo requiere la IoT. Por ejemplo, la plataforma de agentes Jade-Leap [9] facilita la ejecución y comunicación entre agentes que se ejecuten sobre dispositivos Android y sobre dispositivos que soporten J2ME, usando TCP/IP. Estos dispositivos suelen incorporar interfaces de acceso a redes inalámbricas Wi-Fi, 3G y Bluetooth. Por otro lado, AFME (*Agent Factory Micro Edition*) [14] permite la ejecución de agentes deliberativos sobre dispositivos móviles, y motas con sensores Sun SPOT [10], que se comunican utilizando como tecnologías inalámbricas Wi-Fi y ZigBee. Sin embargo, los agentes Jade-Leap y AFME no pueden comunicarse entre si (a pesar de compartir el uso de una red Wi-Fi) e incluso un agente AFME de un dispositivos móvil no puede comunicarse con otro agente AFME que se ejecute en un nodo Sun SPOT (ya que no comparten la misma tecnología de acceso a red).

Otra limitación encontrada en el uso de la tecnología de agentes cómo infraestructura de comunicaciones para la IoT es que no facilitan la difusión de información a un grupo de nodos. En aplicaciones para Internet, la gestión y comunicación de grupos está soportada por IGMP e IP multicast respectivamente, siendo servicios proporcionados por la capa de red. Sin embargo en los sistemas de agentes, la comunicación uno-a-muchos (incluida la definición, gestión y comunicación de grupos de agentes) debe realizarse a nivel de aplicación por cada agente. Es decir cada agente tiene que mantener el grupo de nodos de la IoT (o sea, el grupo de agentes) que están interesados en sus datos, y diseminar (a través de mensajes individuales o con varios destinatarios) nuevos datos cuando estén disponibles. Esta solución es una tarea que consume recursos cuando el número de destinatarios es alto o dinámico, además de que complica el diseño e implementación de la funcionalidad de los agentes. Al igual que ocurre con TCP/IP, la gestión y comunicación de grupos debería ser soportada por la infraestructura, en este caso por la plataforma de agentes. Sin embargo, sólo unas pocas plataformas de agentes soportan la comunicación multicast a nivel de infraestructura, pero apoyándose en IGMP e IP multicast, por lo que ninguna de éstas aborda además el problema de la heterogeneidad en cuanto a las tecnologías de acceso a red [15], [16].

Nuestra propuesta es resolver estas limitaciones de la tecnología de agentes para la IoT en dos niveles diferentes: (i) a nivel de agente, mejorando el diseño del subsistema responsable de la comunicación dentro de su arquitectura; y (ii) a nivel de infraestructura, dotando al servicio de comunicación de la plataforma de agentes con los mecanismos necesarios para abordar la heterogeneidad de tecnologías y protocolos de acceso a la red, y la gestión y comunicación a grupos.

A. Sol, *una plataforma para agentes de la IoT*

La plataforma de agentes *Sol* implementa parcialmente la arquitectura abstracta especificada por la asociación de estándares para agentes FIPA [17] para dispositivos ligeros. El objetivo principal de los servicios de esta plataforma es facilitar la interoperabilidad de agentes desplegados en diferentes dispositivos a través de diferentes tecnologías de

acceso a red y protocolos de comunicación. La versión actual de la plataforma soporta la comunicación de dispositivos móviles con perfil MIDP, dispositivos Android, y motas Sun SPOT de Oracle Lab y Waspmotes de Libelium (Wifi/3G, Bluetooth y dos versiones de Zigbee). La plataforma ejerce de middleware proporcionando un servicio de localización y comunicación a los agentes, a la vez que internamente actúa como pasarela, haciendo transparente el uso heterogéneo tecnologías de acceso a red.

En concreto, nuestra plataforma *Sol* soporta: (1) el registro y descubrimiento de agentes (*Agent Management Service* o AMS por sus siglas en inglés), (2) el registro y descubrimiento de los servicios proporcionados por los agentes (DF), (3) la creación y la pertenencia a grupos (GMS por sus siglas en inglés, *Group Management System*), y (4) Servicio de distribución de mensajes (MTS por *Message Transport System*), que permite la comunicación entre los agentes registrados en la plataforma de agentes. Este servicio ha sido extendido para facilitar la distribución de datos en grupos de agentes. La distribución de mensajes en la comunicación a grupos se realiza internamente por el servicio interno de transporte de mensajes de la plataforma (IPMT por sus siglas en inglés, *Internal Platform Message Transport*) de *Sol*. La extensión realizada sobre este servicio contempla que los agentes puedan estar empotrados en dispositivos heterogéneos, y por tanto es capaz de resolver el problema de la interoperabilidad realizando las tareas de interconexión y adaptación necesarias. Los servicios AMS, DF y MTS son servicios clásicos proporcionados por cualquier plataforma de agentes y vienen definidos por FIPA. Nuestra plataforma incorpora además los servicios GMS y el IPMT extendido.

Al igual que todas las plataformas de agentes, el acceso a los servicios de la plataforma está basado en el intercambio de mensajes ACL (de *Agent Communication Language*), un lenguaje para la comunicación de agentes. En nuestra propuesta los mensajes ACL se representan en un formato especial basado en cadenas de bytes denominado *Sol-Message*. Para poder beneficiarse de los servicios de *Sol*, los agentes han de registrarse en su AMS intercambiando mensajes ACL con ella. Una vez que el registro se ha completado, interactuará con el servicio DF para registrar sus servicios, o consultar y buscar servicios ofrecidos por otros agentes.

B. Self-StarMAS*, una una familia de agentes autogestionables para sistemas AmI heterogéneos*

La principal característica de la arquitectura interna de un agente de la familia *Self-StarMAS* es que se compone de un conjunto de entidades independientes que ayudan a mantener separada la funcionalidad específica de la aplicación, de las funciones y mecanismos relacionadas con la comunicación. Estas funciones de comunicación están encapsuladas en entidades denominadas aspectos se encargan del formato de los mensajes (aspecto de *Representación*) y la distribución de los mensajes de comunicación a través de la plataforma de agentes (aspecto de *Distribución*), entre otros. Las ventajas de separar estos aspectos[1] se pueden encontrar de forma más detallada en [5]. El beneficio más relevante de la orientación a aspectos es que se mejora la modularización interna del sistema mediante la definición de arquitecturas débilmente acopladas, que son más fáciles de reconfigurar, incluso en tiempo de ejecución. De esta forma, los agentes *Self-StarMAS* tienen la capacidad de adaptar sus comunicaciones con facilidad, mediante el uso de diferentes implementaciones de los aspectos de representación y distribución. Estos aspectos pueden sustituirse entiempo de ejecución y varios de ellos pueden incluso ser utilizados de forma simultánea, cómo si fueran un *proxy*, siempre que sea necesario.

Aprovechando esta capacidad de adaptación, los agentes *Self-StarMAS* llevan a cabo, junto con las funciones y tareas propias de la aplicación, un conjunto de tareas dirigidas a su propia gestión, como la recuperación de errores (autosanación o *self-healing* en inglés), la optimización del modo de operación y del rendimiento (auto-optimización o *self-optimizing* en inglés) por mencionar algunas. Para poder realizar esta adaptación, los agentes son sensibles al contexto (monitorizan el estado del entorno y su propio estado interno, como el nivel de batería) y son conscientes de su arquitectura interna (que tareas están en ejecución y que componentes están instanciados así como las relaciones entre ellos en un momento dado). A partir de la monitorización del entorno y de su propio estado, los agentes son capaces de detectar cambios en el contexto (por ejemplo, el fallo de un nodo proveedor de un servicio o el funcionamiento incorrecto de alguno de sus componentes internos) y ajustar su funcionamiento automáticamente para adaptarse a estos cambios. Estos comportamientos son especificados utilizando un conjunto de políticas de auto-gestión. Una política describe una situación que requiere que el sistema sea ajustado (descrita mediante una condición) y las acciones que tiene que llevar a cabo el agente para resolverla. Las condiciones son detectadas mediante la monitorización tanto interna (ej. número de componentes instanciados en la arquitectura) como externa (ej. condiciones de otro agente del SMA) al agente. Las acciones para ajustar el agente son agrupadas en planes. Así, si la batería baja de un determinado nivel, el agente llevará a cabo acciones que le ayuden a alargar la vida de la batería (cómo minimizar las comunicaciones disminuyendo la frecuencia de muestreo). Si detecta la caída de un agente proveedor de un servicio (deja de recibir información), buscará otros agentes que le proporcionen el mismo servicio; y si detecta un fallo o una interrupción en la comunicación, buscará un mecanismo de distribución alternativo de entre los soportados por el dispositivo sobre el que se ejecuta.

En algunos casos, los planes incluyen acciones orientadas a cambiar la configuración de los componentes y aspectos que integran el agente (por ejemplo, modificar la frecuencia de muestreo) mientras que en otros casos las acciones requieren reconfigurar su arquitectura interna añadiendo y eliminado los componentes y aspectos, o cambiando las relaciones de composición entre ellos.

III. MUSEO INTELIGENTE Y ESCENARIOS

Como se ha mencionado en la introducción, vamos a ilustrar la diversidad de tecnologías de acceso a red presente en la IoT y como nuestra plataforma la resuelve los problemas de comunicación con una serie de escenarios en un Museo Inteligente. Concretamente, nos referiremos al “Museo de la

[1] http://aosd.net/

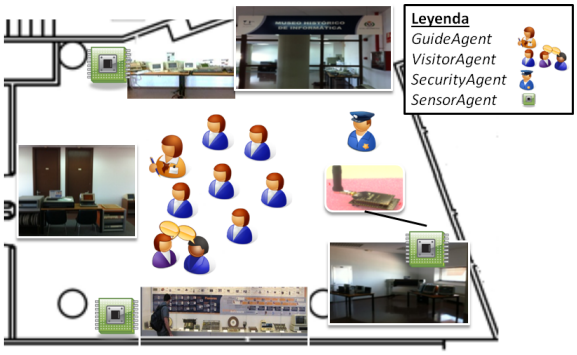


Fig. 1. Plano de la Sala 2 del Museo de Informática. Incluye la ubicación de los agentes software.

Informática" situado en la E.T.S.I. Informática de la Universidad de Málaga. Las salas de este museo (ver Fig. 1) incorporan un conjunto de dispositivos electrónicos denominados motas, cada uno de los cuales incluye un conjunto de sensores que proporcionan datos del entorno (luminosidad, temperatura, presencia, ruido). Estos dispositivos carecen de interfaz gráfica y cada cierto tiempo, los datos sensados son enviados a otros dispositivos (deniminados nodos *sink*) o a dispositivos ligeros personales inalámbricos con el fin de proporcionar servicios sensibles al contexto a los usuarios del museo (personal de seguridad, guías y visitantes) o a los administradores del sistema. En la actualidad, tenemos desplegadas varias motas WaspMotes de Libelium y Sun SPOT de Oracle Labs. Ambos tipos de motas incorporan diversos sensores y son capaces de transmitir los datos sensados utilizando como protocolo de acceso a red Zigbee. Los servicios para los diferentes usuarios se despliegan sobre dispositivos Android, que soportan comunicación a través de Wi-Fi y Bluetooth, extensibles para otros tipos de teléfonos móviles.

Este museo proporciona diferentes servicios sensibles al contexto a sus usuarios: (i) al guía del museo le ofrece soporte para la organización de la ruta entre las salas del museo, teniendo en cuenta la presencia de otros grupos en el edificio o el estado de la estancia, y le facilita la difusion de información a su grupo de visitantes; (ii) en el caso del personal de seguridad, los dispositivos del sistema (nodos sensores y dispositivos portátiles personales) proporcionan información acerca de las salas del museo (condiciones ambientales y localización de los grupos y visitantes) y les facilita un servicio de envío de notificaciones a diferentes grupos de personas que visitan el museo; y (iii) en el caso de los visitantes, y aprovechando el hecho de que la mayoría de la gente suele llevar un teléfono móvil o incluso una tableta, el museo les proporciona información contextual basada en la ubicación, cómo por ejemplo, detalles acerca de los objetos expuestosen la sala en la que se encuentran.

Este sistema está diseñado como un SMA con cuatro tipos de agentes: *GuideAgent*, *SecurityAgent*, *VisitorAgent* y *SensorAgent* (ver Fig. 1). Los 3 primeros se ejecutan integrados en los dispositivos que los usuarios del museo (tabletas y teléfonos móviles) traen con ellos: el agente *GuideAgent* para los guías de museo, el agente *SecurityAgent*, que asiste los miembros del personal de seguridad y el agente *VisitorAgent* a los visitantes. Por último, el agente *SensorAgent* se ejecuta

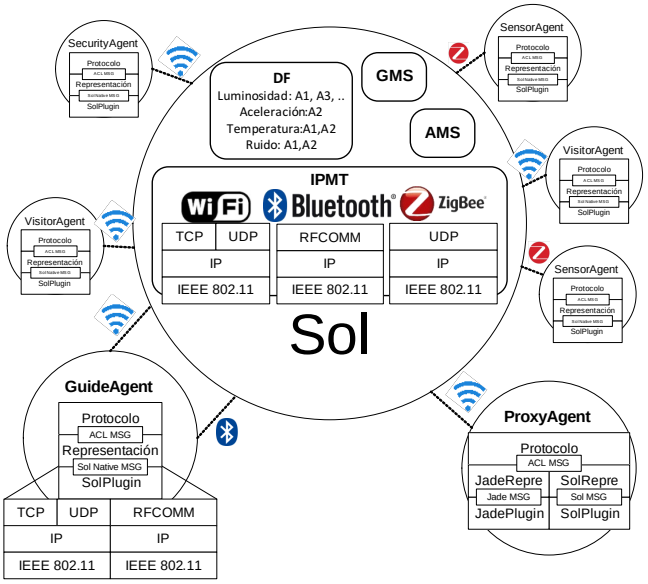


Fig. 2. Agentes del museo y la plataforma *Sol*.

en motas y proporciona información ambiental y contextual a los otros agentes.

Todos los agentes están implementados como agentes *SelfStarMAS* y se adaptan a las características del dispositivo sobre el que se ejecutan. Además, se comunican a través de la plataforma de agentes *Sol*, que se ejecuta en un ordenador de sobremesa y en un router multiprotocolo Meshlium de Libelium (ver Fig. 2). Además, ofrece los servicios AMS, DF, GMS e IPMT.

En el museo, cada agente registra en el servicio DF los servicios que puede proporcionar. Por ejemplo, cada agente *SensorAgent* se registra como proveedor de un determinado tipo de datos (luminosidad, presencia, temperatura) en alguna de las salas del museo (dónde esté ubicado). Cuando un *SecurityAgent* necesite uno de estos servicios de datos, consultará el DF para localizar agentes que lo presten. Finalmente, este agente enviará una solicitud de suscripción de datos al *SensorAgent* elegido, que se encargará de enviar datos de presencia periódicamente. Además, cada agente lleva a cabo un conjunto de políticas de auto-gestión que dependerán del tipo de agente, de los servicios que ofrece al museo, y de los recursos del dispositivo sobre el que se ejecuta. En la Tabla I podemos ver la descripción de algunas las políticas del agente de seguridad orientadas a la recuperación de fallos, y a las que nos referiremos en la sección siguiente. La política denominada "Obtener Proveedor de Servicio" se aplica cuando alguno de los agentes de sensor que proporcionan información del museo a este agente interrumpe. En este caso, *SecurityAgent* iniciará por sí mismo, la búsqueda de un nuevo agente que le proporcione estos datos a través del DF de la plataforma.

La segunda política tiene que ver con la recuperación de un fallo de comunicación interno. En este caso, si por diversos motivos (por ejemplo, una mala cobertura) la interfaz WiFi del dispositivo no funcionara, el agente, ante la situación de fallo en comunicación, cambiaría a otra interfaz de red, utilizando como mecanismo de distribución la interfaz Bluetooth.

Tabla I
POLÍTICAS DEL AGENTE SECURITY AGENT.

Objetivo	Condición	Plan
Obtener Proveedor de Servicio	$\exists e \in Environment \vert e.value == Null$	1: List(AID) id=queryDF(Service) 2: send(CFP) and wait(ANSWER) 3: if receive(BAT_LIFE) then candidates.store(sensor) 4: if candidates.isEmpty() then send(FAILURE) else send(ACCEPT) to sensorX where $sensorX = \{sensor \in candidates \wedge !\exists sensorY \in candidates \vert sensorY(BAT\_LIFE) > sensor(BAT\_LIFE)\}$ and wait(ANSWER) 5: if receive(DONE) then knowledge.update() else restart
Recuperar fallo de comunicación	CommunicationException	1: removeAspect(SolPlugin) 2: addAspect(BluetoothPlugin)

A. *Escenarios de interacción entre agentes del museo*

Este caso de estudio nos proporciona diferentes escenarios que muestran la heterogeneidad típica de los sistemas IoT (a nivel de comunicación y dispositivos) y se utilizará para describir como nuestra propuesta la resuelve. Los escenarios tienen lugar en la Sala 2 del museo, que está dedicada exclusivamente a la exposición de piezas.

Escenario 1. En nuestro museo, la Sala 2 incluye un conjunto de motas con sensores y un *SensorAgent* incorporados, que pueden medir y proporcionar datos sobre la aceleración, la luminosidad, detección de personas, la temperatura y el ruido en la estancia. Consideremos que es cerca de la hora de cierre, por lo que el personal de seguridad al cargo tiene que cerrar esta habitación, pero antes debe comprobar si la Sala 2 está vacía o no. Para ello solicitará el servicio de detección de presencia de esa sala a alguno de los *SensorAgent* que haya registrado este servicio en el DF de *Sol*. Con esta monitorización, cuando el agente de seguridad detecte que el museo está completamente vacío indicará que se puede cerrar.

Este escenario es un ejemplo de comunicación entre el dispositivo Android y las motas a través de la plataforma *Sol*. De otra manera la comunicación sería imposible. En este caso, el agente del sensor envía los datos en un datagrama UDP encapsulado en *radiogramas*. Estos son recibidos y procesados por la interfaz ZigBee de nuestra plataforma. A partir de la información incluida en el mensaje ACL (que incluye en su cabecera el agente destino), consulta la información de registro y envía el mensaje de ACL al agente a través de la interfaz WiFi. El mensaje ACL es ahora transportado a través de una conexión TCP.

Escenario 2. En el museo los agentes del SMA pueden pertenecer a distintos grupos de comunicación. Por defecto, hay un grupo para cada tipo de agente desplegado en la plataforma (un grupo para todos los *SensorAgent*, otro para los *SecurityAgent*,...). Además, los sensores desplegados en una determinada estancia forman parte de un grupo que aglutina a todos los agentes que ofrecen servicio en ese lugar. Por otro lado, los agentes que prestan servicio a un determinado grupo de visitantes forman parte también de grupos específicos. La pertenencia a este último tipo de grupo es independiente de realizar la visita con guía. Los agentes de los visitantes que no realizan la visita acompañados de un guía sino de forma individual, sólo pertenecen al grupo de visitantes global, mientras que los agentes de los visitantes que son acompañados por un guía en grupos organizados (por ejemplo, el grupo del Instituto Teatinos) forman un grupo independiente compuesto por el agente de su guía (por ejemplo Inmaculada) y los agentes de los visitantes (los estudiantes del instituto que han venido a ver el museo). Además, la pertenencia a un grupo puede variar con el tiempo y según el contexto: Los agentes miembros del grupo "usuarios en la Sala 2" dependen de la ubicación actual de los agentes Guía, agentes Visitantes (de grupo e individuales), y agentes del personal de seguridad. Además, la creación de grupos se puede hacer en cualquier momento.

A través del servicio de comunicación que proporciona la plataforma *Sol* es más eficiente enviar notificaciones e información relevante a todos los agentes del museo, cómo por ejemplo, "la hora de cierre está cerca", o "hay una oferta especial en la cafetería".

Escenario 3. Como se ha mencionado anteriormente, en el museo, hay un grupo para todos los agentes de los sensores que están ubicados en una misma sala. Aunque estos agentes monitorizan y proporcionan diferentes datos (por ejemplo, presencia, humedad o temperatura), se considera cómo característica que define la pertenencia al grupo su ubicación en el museo junto con "ser un agente de sensor". De esta manera, cuando la Sala 2 del museo está vacía (es decir, los usuarios no están en ella), se puede enviar un mensaje "Habitación vacía" para que los agentes sensores puedan disminuir su actividad con el fin de ahorrar energía, crucial para que el sistema sea sostenible en términos de energía. Con los escenarios 2 y 3, podemos ver la necesidad y ventajas que ofrece la creación y comunicación a grupos en aplicaciones IoT. La creación y el mantenimiento de grupos se dejan al servicio GMS de la plataforma *Sol*, y permite a los agentes a unirse y dejar los grupos. La plataforma ofrece una interfaz gráfica que permite al administrador monitorizar visualizar, crear y gestionar los grupos de la plataforma (ver Fig. 3).

Escenario 4. Juan ha decidido visitar el museo. Cuando entra en la recepción, se le invita a descargar e instalar la aplicación del museo en el teléfono móvil que permite solamente conectividad Bluetooth. Cuando se inicia la aplicación, se crea un agente visitante (*VisitorAgent*). El nuevo agente se registra en el AMS y se une al grupo de los agentes visitantes. Un minuto después, un mensaje le indica que una visita comenzará en pocos minutos y lo invita a unirse. El agente del usuario no es consciente de cómo se difunde esta información, pero el hecho es que la plataforma consigue que el agente de Juan se comunique con otros agentes aunque su

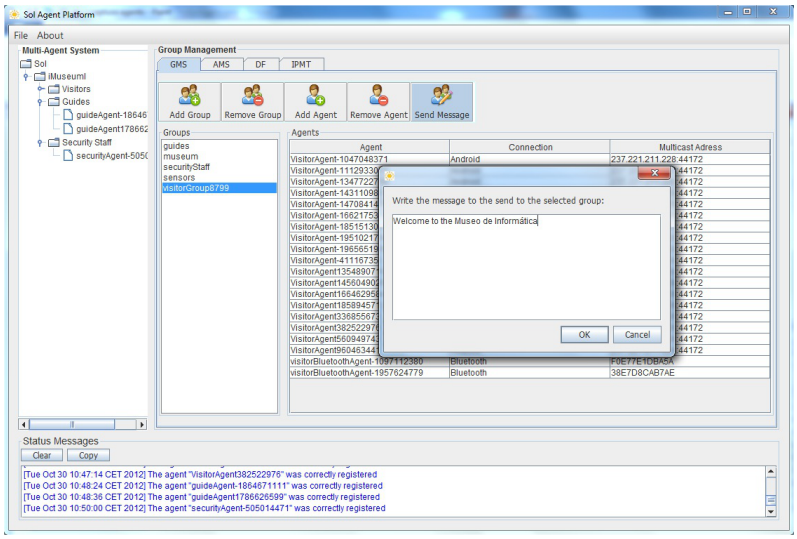


Fig. 3. Agentes del museo y la plataforma *Sol*.

móvil sólo soporte Bluetooth. Si acepta la invitación, el agente visitante de Juan transmiten en datagramas UDP especiales denominados datagramas de radio (*radiogramas*). El agente que se ejecutará en este nuevo sensor es programado para unirse al grupo de los "sensores en la habitación 2".

Sin embargo, la unión del nuevo agente no requiere cualquier tipo especial de conexión debido a que los agentes del sensor ya utilizan datagramas UDP para comunicarse, por lo que sólo necesita obtener la dirección de multidifusión IP y el puerto correspondiente para configurar correctamente su aspecto de distribución.

Escenario 6. Uno de los dispositivos con detección de presencia de la Sala 2 se ha quedado sin batería. El agente sensor ha dejado de proporcionar esta información al agente de seguridad de Luis. Pero el agente detecta esta situación (aplicando la política "Obtener Proveedor de servicio") e inicia la búsqueda de un nuevo agente proveedor de datos de presencia que se encuentre ubicado en la Sala 2. Los agentes que proporcionan ese servicio se encuentran agrupados en el mismo grupo. Así que el agente del guardia de seguridad solo tiene que mandar un mensaje para consulta que *SensorAgent* puede proporcionarle la información presencia en esta estancia.

Escenario 7. El agente de seguridad desplegado en el móvil de Luis ha detectado un fallo de comunicación que le impide enviar o recibir mensajes a través de la interfaz WiFi del dispositivo (probablemente se encuentre en una zona sin cobertura). Este evento interno hace que se active la política de recuperación de fallos, activando el uso de la interfaz Bluetooth para no permanecer incomunicado. El cambio es notificado a la plataforma que actualizará adecuadamente la información relativa a la conectividad del agente en todos grupos de los que fuera miembro.

IV. VALIDACIÓN

Como ya hemos dicho, la plataforma de agentes *Sol* ha sido diseñada y desarrollada para conseguir la interoperabilidad de la familia de agentes *Self-StarMAS* para su uso en sistemas típicos de la IoT. En esta sección vamos a validar el funcionamiento de la plataforma respecto a sus dos funciones principales no presentes en el resto de plataformas de agentes: el soporte para la transmisión de mensajes a un grupo de nodos/agentes relacionados a través de la plataforma, y sus funciones de pasarela para resolver la interoperabilidad entre agentes desplegados en un sistema de dispositivos heterogéneos. Todos los experimentos presentados en esta sección se han repetido cincuenta veces, mostrando los tiempos medios y la desviación estándar para cada caso. El tiempo se mide en milisegundos (ms) y para llevar a cabo estos experimentos hemos utilizado dispositivos Android Google Nexus y sensores Sun SPOT y las plataformas de agentes *Sol* y Jade-Leap.

A. Comunicación a grupos

Como parte de las tareas que los agentes *Self-StarMAS* pueden realizar relacionadas con la auto-configuración, algunas afectan a la comunicación, como por ejemplo cambiar el aspecto de distribución en tiempo de ejecución, o solicitar un nuevo (agente) proveedor de servicios de datos en caso de fallo del proveedor actual. La primera está relacionada con el escenario 7 y en una contribución previa demostramos que los tiempos de reconfiguración para esta tarea son razonables [19]. La segunda de las tareas está presente en muchos de los escenarios presentados y está directamente relacionada con los servicios de la plataforma y la capacidad de autoconfiguración del agente, descritos en secciones anteriores [8].

Para comprobar la carga que esto supone hemos realizado una serie de experimentos que compara la distribución de mensajes individuales (TCP, UDP/ZigBee sobre Sun SPOT, o conexión Bluetooth) con la distribución de mensajes a grupos proporcionado por la plataforma. En concreto, se compara la distribución a grupos de la plataforma frente al uso de un conjunto de comunicaciones individuales para ver los beneficios que proporciona la comunicación a grupos.

En el caso del escenario 6 y con el fin de evaluar cómo se gestiona la heterogeneidad de dispositivos y cómo influye en la comunicación, hemos implementado diferentes escenarios del museo, compuesto principalmente por un agente *SecurityAgent* (ejecutándose en un teléfono Android) y número

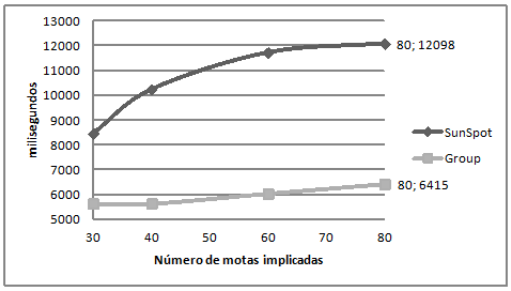


Fig. 4. Resultados de la evaluación de la comunicación a grupos multicast (Group) vs. la comunicación de uno a muchos (SunSPOT) mediante mensajes individuales..

variable de agentes *SensorAgent*. El número de agentes *SensorAgent* puede variar de sólo un dispositivo (por ejemplo, proporcionando datos de luminosidad) a varios. Todos los agentes *SensorAgent* están registrados como proveedores de servicios en el DF. El fallo de uno de estos dispositivos (y consiguientemente del agente que se ejecuta en él) provoca la ejecución de la política "Obtener Proveedor de Servicio" (descrita en la primera fila de la Tabla I).

Los resultados de este experimento (media de los tiempos obtenidos) están representados en la gráfica de la Fig. 4, siendo la desviación estándar de aproximadamente 2 ms para todos los casos. Los resultados muestran que el tiempo de dedicado a la comunicación de la búsqueda de un proveedor de servicio aumenta con el número de agentes (proveedores de servicio) siguiendo una función logarítmica en el caso del conjunto de comunicación ZigBee de las Sun SPOT (etiqueta SunSpot). Mientras que el aumento del tiempo es lineal en el caso del uso de un grupo aumentando el número de agentes del grupo. Los tiempos obtenidos son asequibles y la escalabilidad es buena, mostrando claramente la ventaja de utilizar el nuevo mecanismo de comunicación a grupos soportado por la plataforma *Sol*. El tiempo cuando se utiliza la información recogida por la plataforma específica para la comunicación a grupos (etiqueta *Group*) es menor en todos los experimentados realizados.

Además, hay que tener en cuenta que, cuando el número de sensores y agentes aumenta en más de 250%, el tiempo necesario para la comunicación aumenta el 140% en el caso del conjunto de mensajes individuales y el 120% en el caso de utilizar la comunicación a grupos soportada por el servicio IPMT de la plataforma *Sol*.

Tal como se ha ilustrado en el escenario 2, el mecanismo de grupo ofrece una gran ventaja para comunicar SMA dinámicos, cuyos agentes pueden variar en tiempo de ejecución. En nuestro caso de estudio, el *GuideAgent* puede enviar información a su grupo de agentes visitantes sin que sea necesario saber cuál es el número de agentes o su identificador en un momento dado, o cuando los miembros se unen o abandonar el grupo. Además, no es necesario que el agente controle la presencia en el SMA de los miembros del grupo (de eso se encarga el servicio GSM de la plataforma). Hemos validado el rendimiento del mecanismo de grupo para Android y comparación con la comunicación individual (unicast). El experimento consistió en medir los tiempos de comunicación de un grupo de agentes de un grupo compuesto por 20 *VisitorAgent*s (17 de ellos se ejecutan en los dispositivos

Tabla II
TIEMPOS DE IDA Y VUELTA (RTT) EN MILISEGUNDOS PARA LA COMUNICACIÓN A GRUPOS DE AGENTES.

Escenario	Experimento 2	Experimento 3
Escenario 1	935	413
Escenario 2	1023	647

virtuales y 3 agentes en dispositivos reales) y un *GuideAgent*. Hemos medido el tiempo de ida y vuelta (RTT por sus siglas en Inglés, Round Trip Delay Time) de un mensaje enviado por el *GuideAgent* utilizando 3 mecanismos de comunicación diferentes (tres escenarios distintos): (E1) envío a un grupo; (E2) el envío de un mensaje único con 20 agentes destinatarios en el campo receptor (los identificadores de los miembros del grupo), y (E3) el envío de 20 mensajes diferentes (con los mismos datos de contenido) de la *GuideAgent* a cada miembro del grupo. La diferencia entre los escenarios E2 y E3 es que en E2 la plataforma *Sol* recibe un único mensaje y luego lo envía a través de cada una de las conexiones TCP de los agentes indicados en el campo receptor del mensaje (1 + 20 envíos en total), mientras que en el escenario E3 el *GuideAgent* envía 20 mensajes diferentes a *Sol* que sólo tienen un agente representados en sus campos receptores (20+20 envíos en total). En el escenario E1 el número de envíos es 2, ya que el envío de mensajes individuales a los miembros del grupo se resuelve con IP multicast.

Los resultados promedio y desviación estándar en ms son 935 y 93 para (E1), 1023 y 214 para (E2) y 1340 y 312 para (E3) (ver gráfica de la Tabla II). Estos resultados son ligeramente mejores para la distribución a través del servicio GMS y la distribución a grupos proporcionada por la plataforma, pero como se dijo antes, las ventajas de su uso no son sólo la mejora en el rendimiento.

Los resultados para los escenarios E2 y E3 muestran que hay una penalización en el rendimiento si el agente envía mensajes con un único receptor. Esto se debe a que en los agentes *Self-StarMAS*, los aspectos encargados de las tareas de comunicación se componen (tejen, según el vocabulario seguido en la orientación a aspectos) cada vez que un mensaje es enviado o recibido. Así que en E3, internamente los aspectos se componen 20 veces (uno para cada mensaje que es enviado a los 20 agentes miembros del grupo), mientras que en E2 los aspectos se componen una sola vez. Sin embargo, esta sobrecarga se puede evitar fácilmente mediante el envío de un único mensajes con múltiples receptores, tal y como se realiza en el escenario E2.

B. Funciones de pasarela

Nuestro segundo conjunto de experimentos valida la interoperabilidad presente en el escenarios 4. Concretamente, nos hemos ocupado de validar la interoperabilidad entre agentes residentes en dispositivos con diferentes tecnologías de comunicación inalámbrica, a través de la plataforma *Sol*. En concreto, se midió el rendimiento de la comunicación entre un agente que utiliza WiFi y otro agente que utiliza Bluetooth (entre un agente *GuideAgent* y un agente *VisitorAgent*). En este tercer experimento, medimos el tiempo de retardo de ida y vuelta de un mensaje (RTT) enviado por el *GuideAgent* a un *VisitorAgent*. El objetivo de este experimento es doble: (1)

demostrar que el tiempo dedicado a la comunicación a través de *Sol* es razonable y (2) mostrar que la comunicación a través de *Sol* no introduce una sobrecarga importante. El tiempo de ida y vuelta de un mensaje con un tamaño de 207 Bytes (E1) es 413 ms con una desviación estándar de 157 ms. En esta situación, la comunicación requiere una conexión RFCOMM utilizando la misma tecnología de red (Bluetooth). Por otro lado, el RTT medido cuando el agente *GuideAgent* utiliza su interfaz WiFi es de 647 ms con una desviación estándar de 115 ms (ver Tabla II). Estos resultados muestran que los tiempos de ida y vuelta en los dos escenarios son razonables, y ponen de manifiesto que la comunicación entre agentes a través de la plataforma *Sol* utilizando diferentes protocolos de transporte no introduce un retardo crítico.

Sin embargo, durante la realización de estos experimentos hemos encontrado situaciones en las que estas soluciones no bastan para resolver todos los casos. Por ejemplo, las motas se basan en el estándar IEEE 802.15.4 para comunicarse (ZigBee se basa en él), éstos no son interoperables entre si, ni son soportados por la mayoría de los dispositivos ligeros. Con el fin de lograr la interoperabilidad necesitamos soluciones adicionales, siendo una de ellas el uso de nodos intermedios que actúen de proxy. En esta situación nuestro enfoque puede permitir que el interoperabilidad incorporando un agente que actúe de proxy. Esto tiene un gran valor si consideramos que van a seguir surgiendo nuevos dispositivos y protocolos de comunicación, especialmente de corto alcance, dentro del contexto de la IoT.

V. CONCLUSIONES Y TRABAJO FUTURO

En este trabajo nos hemos centrado en la presentación y validación de una serie de escenarios que muestran como la diversidad de tecnologías de comunicación inalámbricas en el entorno de la IoT puede limitar el desarrollo de aplicaciones de la IoT y como puede resolverse utilizando la plataforma *Sol* y la familia de agentes *Self-StarMAS*. Por un lado, la plataforma de agentes *Sol* extiende la funcionalidad de las plataformas de agentes (i) facilitando la comunicación entre agentes que se ejecutan sobre un conjunto heterogéneo de dispositivos y tecnologías de red, y (ii) realizando la gestión y distribución de mensajes a grupos de una manera eficiente. La plataforma de agentes *Sol* soporta diversos protocolos de acceso a red inalámbricos (Wi-Fi, ZigBee, Bluetooth) y actúa como pasarela con el fin de asegurar la comunicación entre agentes que utilicen diferentes tecnologías de acceso. Además para asegurar una distribución de mensajes a grupo, la plataforma proporciona soporte para la definición y gestión de grupos, así como para la distribución de mensajes en el medio más adecuado (como por ejemplo, IP multicast).

Por otro lado, los agentes *Self-StarMAS* son una familia de arquitecturas de agentes con capacidad de auto-gestión para dispositivos ligeros. Esos agentes se caracterizan por poder ser desplegados sobre un variado conjunto de dispositivos típicos de la IoT; y por poder adaptar su comportamiento a los recursos y capacidad del dispositivo, incluso en tiempo de ejecución, incluyendo la posibilidad de utilizar diferentes mecanismos de comunicación, incluso de forma simultánea.

Los resultados de los experimentos presentados muestran la viabilidad del uso de agentes para resolver los problemas de comunicación en términos de los tiempos de reconfiguración e intercambio de datos a través de un conjunto de tecnologías de acceso inalámbricas diferentes.

Nuestro trabajo futuro se centra en la ampliación del conjunto de dispositivos y tecnologías soportadas por la plataforma *Sol*, con el fin de desarrollar más aplicaciones reales en las que validar nuestra propuesta y enriquecer la creación y definición de grupos con sensibilidad al contexto.

AGRADECIMIENTOS

Este proyecto ha sido subvencionado por los proyectos FamWare P09-TIC-5231, INTER-TRUST FP7-317731, RAP TIN2008-01942 y MAVI TIN2012-34840.

REFERENCIAS

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010.

[2] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer *et al.*, "Internet of things strategic research roadmap," *Internet of Things: Global Technological and Societal Trends*, pp. 9–52, 2011.

[3] J. Kephart, J. Kephart, D. Chess, C. Boutilier, R. Das, J. O. Kephart, and W. E. Walsh, "An architectural blueprint for autonomic computing," *IEEE internet computing*, vol. 18, no. 21, 2007.

[4] M. C. Huebscher and J. A. McCann, "A survey of autonomic computingdegrees, models, and applications," *ACM Comput. Surv.*, vol. 40, no. 3, pp. 7:1–7:28, Aug. 2008.

[5] I. Ayala, M. Amor, and L. Fuentes, "A model driven engineering process of platform neutral agents for ambient intelligence devices," *Autonomous Agents and Multi-Agent Systems*, pp. 1–42, 2013.

[6] ——, "An agent platform for self-configuring agents in the internet of things," in *Proceedings of the Thirds International Workshop on Infrastructures and Tools for Multiagent Systems.* Universidad Politècnica de València, Jun. 2012, pp. 65–78.

[7] ——, "Self-management of ambient intelligence systems: a pure agent-based approach," in *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems*, ser. AAMAS '12. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems, 2012, pp. 1427–1428.

[8] ——, "Self-configuring agents for ambient assisted living applications," *Personal and Ubiquitous Computing*, vol. 17, no. 6, pp. 1159–1169, 2013.

[9] F. Bergenti and A. Poggi, "Leap: A fipa platform for handheld and mobile devices," in *Intelligent Agents VIII*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2002, vol. 2333, pp. 436–446.

[10] C. Muldoon, G. O'Hare, M. J. O'Grady, and R. Tynan, "Agent migration and communication in wsns," in *Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2008.*, dec. 2008, pp. 425 –430.

[11] F. Koch, J.-J. C. Meyer, F. Dignum, and I. Rahwan, "Programming deliberative agents for mobile services: The 3apl-m platform," in *Programming Multi-Agent Systems*, ser. Lecture Notes in Computer Science, vol. 3862. Springer Berlin Heidelberg, 2006, pp. 222–235.

[12] T. C. Lech and L. W. M. Wienhofen, "Ambieagents: a scalable infrastructure for mobile and context-aware information services," in *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, ser. AAMAS '05. New York, NY, USA: ACM, 2005, pp. 625–631.

[13] R. Lopes, F. Assis, and C. Montez, "Maspot: A mobile agent system for sun spot," in *10th International Symposium on Autonomous Decentralized Systems*, march 2011, pp. 25 –31.

[14] C. Muldoon, G. O'Hare, R. Collier, and M. O'Grady, "Agent factory micro edition: A framework for ambient applications," in *Computational Science*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2006, vol. 3993, pp. 727–734.

[15] P. Gotthelf, A. Zunino, C. Mateos, and M. Campo, "Gmac: An overlay multicast network for mobile agent platforms," *Journal of Parallel and Distributed Computing*, vol. 68, no. 8, pp. 1081 – 1096, 2008.

[16] A. Macias-Estrada, O.-I. Lepe-Aldama, and J. Garcia-Macias, "Implementing true multicast communications support for the jade/leap agent framework," in *Sixth Mexican International Conference on Computer Science, 2005.*, 2005, pp. 206–213.

[17] F. for Intelligent Physical Agents, "Fipa abstract architecture specification," Foundation for Intelligent Physical Agents, Geneva, Switzerland, Tech. Rep. SC00001L, December 2002.

Una Nueva Herramienta para Testear el Rendimiento de una Red IP

Carlos Barambones, David Pascual, Juan R. Diaz, Jaime Lloret
Instituto de Investigación para la Gestión Integrada de Zonas Costeras (IGIC)
Universidad Politécnica de Valencia
C/ Paranimf Nº1, 46730, Grao de Gandía, Gandía (Spain)
carbafer@teleco.upv.es, dapasgon@gmail.com, juadasan@dcom.upv.es, jlloret@dcom.upv.es

***Resumen*- Una de las mayores necesidades que hay en las redes de IP es la falta de herramientas que permitan testear el rendimiento de la red cuando ya está implementada. Cuando se quiere probar qué ocurre en la red cuando existe un fallo en esta y cuánto tiempo tarda en recuperarse ante eventos inesperados, los administradores suelen recurrir a herramientas de gestión de red. Pero esta solución no permite hacer pruebas del tráfico que se distribuye dentro de ésta, ni medir el tiempo exacto que tarda la red en recuperarse ante un fallo. En este artículo presentamos una nueva herramienta para realizar pruebas de rendimiento de la red cuando ya está implementada. Los parámetros que muestra es jitter, delay, mensajes recibidos, mensajes perdidos, % de mensajes perdidos, y ancho de banda. Para poder probar su efectividad realizaremos una serie de medidas sobre una red real.**

***Palabras Clave*- rendimiento, herramienta de test, monitorización de red, test de red de datos.**

I. INTRODUCCIÓN

La proliferación de las redes de datos en entornos empresariales, administraciones públicas e incluso en los hogares, ha provocado que a día de hoy sea inconcebible estar en un lugar sin conectividad con otros dispositivos. Además, el hecho de existir múltiples fabricantes de electrónica de red con un gran abanico de modelos, hace que sea muy complicado realizar un test de rendimiento de red cuando ésta ya está implementada [1].

Una de las mayores necesidades que hay en las redes de datos es la falta de herramientas que permitan comprobar el rendimiento de la red cuando está funcionando correctamente así como su evolución cuando existen fallos.

Las primeras herramientas aparecieron a principio de los años 80 junto con el protocolo IP. La primera de ellas es el ping (Packet Internet Groper), definido por primera vez en Abril de 1981 en la RFC 777 y actualizado posteriormente ese mismo año en la RFC 792 [2], que hace uso del protocolo ICMP. El ping es una utilidad que permite que comprobar el estado de la comunicación entre 2 dispositivos que utilicen el protocolo IP por medio del envío de paquetes ICMP de solicitud y de respuesta. Ésta nos permite medir si existe comunicación entre los equipos y el tiempo que se tarda desde que se envía el paquete, hasta que se obtiene la respuesta. La otra herramienta es Traceroute, que permite seguir los saltos de los paquetes que vienen desde un dispositivo de la red. Traceroute también da una estadística del RTT (Round Trip Time) o latencia de red de esos paquetes. Éste utiliza el campo Time To Live (TTL) de la cabecera IP para contar el número de saltos que lleva hasta alcanzar el destino.

Con el objetivo de gestionar la red de forma más detallada, incluyendo las características de los dispositivos de la red, no sólo el tráfico, se creó el protocolo de gestión SNMP (Simple Network Management Protocol) [3] y RMON (Remote Monitor) [4]. SNMP es un protocolo que permite intercambiar información de gestión entre dispositivos de una red IP. Actualmente está soportado por múltiples tipos de dispositivos de red como los encaminadores, conmutadores, concentradores, servidores, ordenadores, impresoras, etc. Permite a los administradores monitorizar y supervisar el funcionamiento de la red, y buscar y resolver los problemas que pudiera haber. Lo definió el Engineering Task Force (IETF) como un conjunto de estándares que incluyen el protocolo de capa de aplicación, el esquema de la base de datos y un conjunto de objetos de datos. A lo largo de los años ha evolucionado hasta la actual SNMPv3, que posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad. Remote Network MONitoring (RMON) fue desarrollado por el IETF con el objetivo de ayudar en la monitorización y análisis de los protocolos en la red de área local. La versión 1 de RMON estaba enfocada principalmente a la capa 1 y capa 2 del modelo OSI. La versión 2 de RMON añadió soporte para la monitorización de la capa de red y de aplicación. Los agentes RMON están principalmente incluidos en conmutadores y encaminadores.

En ocasiones es necesario probar que ocurre en la red cuando existe un fallo y cuánto tiempo tarda en recuperarse ante eventos inesperados, pero desde el punto de vista del usuario final. Para obtener esta información, los administradores suelen recurrir a herramientas de gestión de red como las anteriormente citadas. Pero esta solución no permite hacer pruebas del tráfico que se distribuye dentro de ésta (por ejemplo, el tiempo que tarda en transmitirse la información entre dos dispositivos finales, el tiempo que un dispositivo final está sin recibir datos, etc.), sólo reciben la información de los dispositivos de la red. Sin embargo en ocasiones es necesario obtener los valores de los parámetros que se obtienen en el receptor. Generalmente este tipo de test se realiza con simuladores de red, por ejemplo NS-2, OPNET, OMNET++, etc.

Dada la necesidad de herramientas que permitan probar el rendimiento de una red desarrollada desde el punto vista del usuario final, en este trabajo presentamos una nueva herramienta que permite realizar test de rendimientos de red. Primero explicaremos cómo obtenemos los valores para cada una de las variables. Después mostraremos algunas capturas

de pantalla de la aplicación, para mostrar las variables que se pueden medir. Finalmente mostraremos las medidas obtenidas en una red con 5 encaminadores y 2 conmutadores.

El resto del artículo está estructurado como sigue. En la sección 2 se muestran las herramientas que hemos encontrado parecidas a la herramienta desarrollada por nosotros. La explicación del desarrollo de la herramienta se incluye en la sección 3. La sección 4 muestra el entorno gráfico de la herramienta. Las medidas realizadas con la herramienta en varios tests se muestran en la sección 5. Finalmente, en la sección 6, las conclusiones exponen la contribución de nuestro trabajo y los futuros trabajos.

II. Trabajos Relacionados

En la actualidad existen algunas herramientas que permiten generar tráfico en la red. Pero ninguna de estas tiene una aplicación en el cliente final que permita ver que ha ocurrido con el tráfico tras haber atravesado la red.

El primer tipo de herramientas que hemos encontrado que se asemejan a la desarrollada por nosotros son los generadores de tráfico. A continuación se muestran algunos de las más comunes.

Mike Ricketts, ingeniero de software de IBM, dentro del proyecto Purple, creó SendIP [6]. SendIP es una herramienta con gran número de opciones, que se ejecuta en línea de comandos y permite enviar paquetes de red de manera arbitraria. Además, las opciones permiten especificar el contenido de cada encabezado de una NTP, BGP, RIP, TCP, UDP, ICMP o paquetes IPv4 e IPv6. Sólo se puede ejecutar en Linux y tiene licencia GPL. La gran desventaja es que la última vez que fue actualizada, fue en el 2003.

En 2003, W. Feng y otros presentaron TCPivo [7]. Es una herramienta que proporciona una alta velocidad de repetición de paquetes desde un archivo de trazas. TCPivo es capaz de reproducir con precisión trazas de red a alta velocidad utilizando el hardware estándar de un PC. Este software es de código abierto y actualmente está desarrollado exclusivamente en Linux.

Rude&Crude es un conjunto de programas desarrollados en Linux que se distribuye bajo la licencia GPL V2 [8]. Rude es un programa pequeño y flexible, que generador de tráfico de red. Los paquetes emitidos pueden ser recibidos y registrados en el otro lado de la red con el programa Crude. Actualmente, estos programas solo pueden generar y medir el tráfico UDP.

Scapy es un programa que permite manipular paquetes [9]. Es capaz de crear o decodificar paquetes de muchos protocolos, realizar peticiones y respuestas, y mucho más. Es capaz de realizar acciones más clásicas como escanear, traza de rutas, sondeo, pruebas sobre un solo destino, ataques o descubrimiento de la red. También es capaz de hacer otras acciones que la mayoría de las otras herramientas no pueden realizar, como por ejemplo el envío de tramas no válidas, la inyección de tramas 802.11, o combinar técnicas como VLAN hopping + ARP envenenamiento de caché, VOIP decodificación de canal cifrado WEP, etc.

PKTgen es una herramienta de pruebas de alto rendimiento incluido en el propio kernel de Linux [10]. Al ser parte del kernel se transmite mejor al controlador de la tarjeta de red. PKTgen también se puede utilizar para generar paquetes ordinarios con el objetivo de probar otros dispositivos de la red como encaminadores, conmutadores o puentes. También es capaz de generar altas tasas de paquetes con el objetivo de saturar los dispositivos.

Joel. E Sommers y otros, de la universidad de Wisconsin, USA, crearon un conjunto de 5 programas denominado Harpoon [11]. Harpoon es un generador de tráfico que trabaja en las capas de transporte y sesión (atendiendo al modelo de referencia OSI) que es capaz de medir el flujo de datos en la red. Éste utiliza un conjunto de parámetros de distribución (temporales y espaciales) que pueden extraerse automáticamente de las trazas Netflow para generar flujos de tráfico. Se puede utilizar para generar tráfico de fondo, para una aplicación o protocolo de prueba, o para probar el hardware de conmutación de red. Harpoon está formado por una combinación de cinco modelos de distribución para las sesiones TCP: tamaño de fichero, tiempo de interconexión, rangos IP origen y destino, y número de sesiones activas. Hay tres modelos de distribución para sesiones UDP: bitrate constante, periódico o exponencial. Cada una de estas distribuciones se puede configurar manualmente o de manera automática. Harpoon es un software libre que se puede redistribuir y/o modificar bajo los términos de la Licencia Pública General GNU.

Nemesis, desarrollada por Jeff Nathan, es una aplicación capaz de enviar la información que se quiera en una red utilizando TCP/IP [12]. Esta aplicación es muy utilizada para probar y depurar los sistemas de detección de intrusiones de red, cortafuegos, etc. Es una herramienta habitual a la hora de auditar redes y servicios. Nemesis puede crear e inyectar ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF, RIP, TCP y UDP. Ha sido desarrollada para Linux y Windows. La versión de Windows requiere la instalación previa de Winpcap, sin embargo, la versión de Linux requiere libnet 1.0.2a.

Packet Excalibur es un generador de paquetes y sniffer multiplataforma.Tiene entorno grafico y scripts con extensibles descripciones de protocolo basados en texto [13]. Es una herramienta de red diseñada para crear y recibir paquetes personalizados de la red. Además, es capaz de rastrear y detectar paquetes falsos, mostrándolos en una única interfaz gráfica. Esta herramienta es muy útil para auditar cortafuegos, encaminadores, o cualquier equipo de red.

packETH es una herramienta gráfica generadora de paquetes Ethernet [14]. Permite crear y enviar cualquier posible paquete o secuencia de paquetes en la red Ethernet. Admite los protocolos Ethernet II, Ethernet 802.3, 802.1Q QinQ, ARP, Ipv4, IPv6, UDP, TCP, ICMP, ICMPv6, e IGMP. Además, el usuario puede definir la carga de la capa de red y permite retardar el envío de paquetes, numero de paquetes a enviar, etc. Las principales ventajas de esta herramienta son que es muy fácil de usar y soporta muchas características personalizadas.

Mike Frantzen, y otros, crearon un conjunto de herramientas, denominada ISIC-IP Stack Integrity Checker [15], para probar la estabilidad de una pila IPv4 e Ipv6 y sus pilas de componentes (TCP, UDP, ICMP, etc). Para ello, se generan muchos paquetes aleatorios del protocolo objeto de estudio. De todo este flujo generado, el 50% de los paquetes generados puede tener opciones IP. 25% de los paquetes pueden ser fragmentos IP. Sin embargo, los porcentajes son arbitrarios y la mayoría de los campos de paquetes tienen una

tendencia totalmente configurable. Los paquetes se envían hacia el equipo de destino con el objetivo de testearlo. Sirve para detectar vulnerabilidades en el cortafuegos, observar si existe fuga de paquetes o para encontrar errores en la pila IP. ISIC también dispone de una utilidad para examinar las configuraciones del hardware implementado en la red.

Netperf es una herramienta que puede utilizarse para medir el rendimiento de muchos tipos de redes [16]. Permite realizar pruebas tanto para el rendimiento unidirecional, como medir la latencia de extremo a extremo. Las variables actualmente medibles por netperf incluyen TCP y UDP a través de sockets BSD para IPv4 e Ipv6, DLPI, Unix Domain Sockets y SCTP para IPv4 e Ipv6. Sólo está disponible para Linux.

Roel Jonkman, de la universidad de Kansas, USA, creó la utilidad NetSpec [17]. Es una herramienta diseñada, y desarrollada en Linux, para simplificar el proceso de las pruebas rendimiento y funcionalidad de la red. NetSpec proporciona un marco bastante genérico que permite al usuario controlar múltiples procesos a través de múltiples hosts, todo ello controlado desde un punto central de control. Se compone de demonios que implementan las fuentes de tráfico además de diversas herramientas de medición pasiva. NetSpec utiliza un lenguaje de scripting que permite al usuario definir múltiples flujos de tráfico desde/hacia varios equipos de manera automática.

Bit-Twist [18] es un generador de paquetes Ethernet basado en libpcap que está diseñado para complementar tcpdump. Los paquetes se generan a partir de un archivo de trazas tcpdump (archivo. Pcap). Bit-Twist viene con un completo editor de archivo de trazas para permitir cambiar el contenido del mismo. Es muy útil para probar cortafuegos, sistemas de detección de intrusión y sistemas de prevención de intrusión, además de permitir resolver diversos problemas de red.

A. Dainotti y otros, de la universidad de degli Studi di Napoli "Federico II" (Italia), han creado recientemente D-ITG (Distributed Internet Traffic Generator) [19]. D-ITG es una plataforma que puede generar tráfico tanto IPv4 como IPv6. Además, permite generar tráfico en las capas de red, transporte y aplicación. Es multiplataforma (soporta Windows, Linux y OSX).

Tras listar los generadores y receptores de tráfico existentes, hemos comprobado que no existe ningún generador de tráfico desarrollado en Windows, que también tenga un receptor para poder analizar los paquetes recibidos a nivel de IP, TCP y UDP. Por tanto hemos desarrollado la herramienta que proponemos en este artículo con ese objetivo.

III. Herramienta de Test

Hemos desarrollado una herramienta de test utilizando programación Java con el objetivo de cumplir los requisitos previamente descritos. La programación orientada a objetos nos permite desarrollarlo por módulos, y por tanto se pueden hacer cambios fácilmente y añadir más cosas en caso de requerirlo. En esta sección explicamos los diferentes componentes desarrollados.

A. Cabecera Personalizada

La aplicación envía un mensaje con una cabecera personalizada sobre UDP que nos permite realizar medidas sobre diferentes parámetros de la red. Hemos prescindido de la cabecera RTP. De esta manera, cuando el programa envía los datos según requiere el usuario, a estos se les incluye la cabecera que se describe a continuación y se encapsulan en mensajes UDP que posteriormente son encapsulados en IP y transmitidos a la red. En la Figura 1 se muestra el mensaje de Audio (arriba) y Video (abajo) que se envían para testear el rendimiento de la red. Se puede observar con detalle cada uno de los campos de la cabecera. Ambos mensajes tienen un identificador que permite distinguirlos. Además tienen, el número de mensaje, el tiempo en el origen, la frecuencia de envío y la dirección IP y el puerto del Cliente.

La principal diferencia entre ellos es debida a que la información de video requiere que se envíen varios mensajes para transportar los datos, se ha creado tres campos expresamente para indicar qué número de mensaje se está transmitiendo, cuantos hay y si es el último mensaje, que son identificados con "Numero de SubMensaje", "Último Mensaje" y "Mensajes Totales". El tamaño total que puede tener este mensaje, dado que está encapsulado sobre UDP, es de 65535 bytes. Las capas inferiores (IP y Ethernet) serán las que dividirán este contenido en paquetes y tramas más pequeñas para poder transmitirlo a la red.

Para poder encapsular los datos, se han utilizado unos comandos específicos en Java que permiten encapsular la información recibida en UDP. Inicialmente asociamos un número de puerto al objeto socket, que es del tipo DatagramSocket, tal como se muestra a continuación:

```
socket = new
DatagramSocket(Integer.parseInt(CampoPuerto.getTex
t()));
```

Seguidamente rellenamos la cabecera del mensaje UDP, que es del objeto, y separamos cada campo con "/". En el caso de envío de audio, eso se realiza de la siguiente forma:

```
mensajeUDP="A/"+numeromensaje+"/"+Long.toString(ti
empoOrigen)+"/"+frecuenciaEnvio+"/"+InetAddress.ge
tLocalHost().getHostAddress()+"/"+CampoPuertoField
.getText()+"/"+relleno;
```

Seguidamente creamos un objeto llamado "enviarmensaje" para poder enviarlo a la red, al cual debemos indicarle su longitud, la dirección IP destino y el puerto destino. Éste se muestra a continuación:

```
DatagramPacket enviarmensaje = new
DatagramPacket(datos,datos.length,InetAddress.getB
yName(CampoIPField.getText()),Integer.parseInt(Cam
poPuertoField.getText()));
```

B. Calculo de Jitter

Para calcular el jitter, la herramienta registra cada tiempo de llegada de cada mensaje y lo compara con el tiempo del mensaje anterior, para ello utilizando los campos "Numero de mensaje" y "Numero de submensaje" de la cabecera según se trate de audio o video.

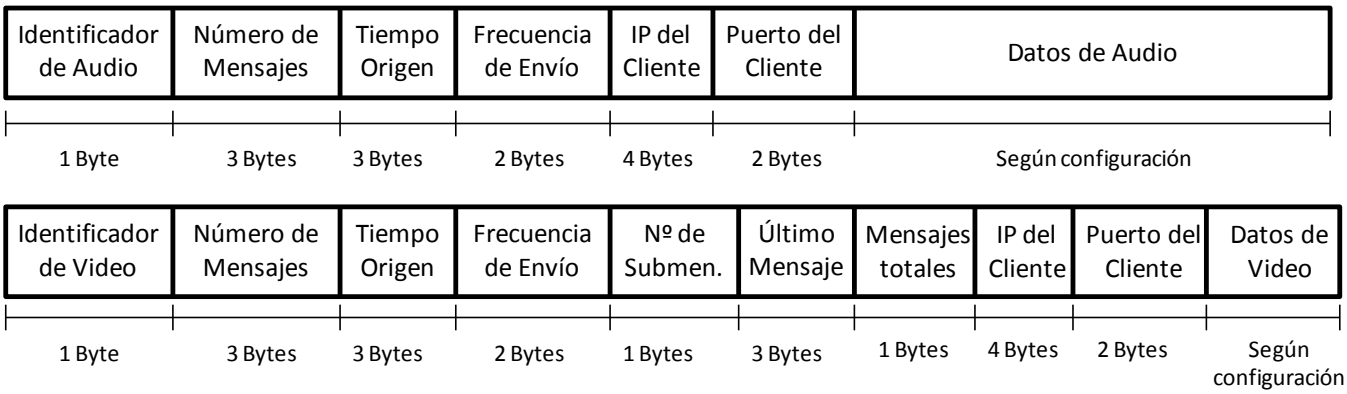


Fig. 1. Mensajes de Audio y Video que se envían para testear el rendimiento de la red.

```
Para AUDIO:

if(recibidos>1){
       if(NumeroMensaje==(mensajeAnterior+1) )
   jitter=Long.toString(tiempoLlegada-
tiempoJitter-frecuenciaEnvio)
        else
   jitter="ERROR"
}

Para VIDEO:

if(recibidos>1){
if(SubMensaje>1){
if((NumeroMensaje==mensajeAnterior) &&
(SubMensaje==subMensajeAnterior+1))
jitter=Long.toString(tiempoLlegada-tiempoJitter);
else{
if(NumeroMensaje==(mensajeAnterior+1) &&
(mensajeFinalAnterior==1) )
jitter=Long.toString(tiempoLlegada-tiempoJitter-
frecuenciaEnvio);
else
jitter="ERROR2";
}
}
```

Fig. 2. Código para estimar jitter en audio y en video.

Si no coincide el "número de mensaje" (para audio) o "número de submensaje" (para video) recibido con el anterior +1, el programa indica ERROR en el campo del jitter. Esto puede ser debido a la pérdida del mensaje.

En la figura 2 se muestra el código utilizado para estimar el jitter tanto en audio como en video.

C. Calculo de Delay

Para calcular el retraso de la red, la herramienta utiliza el campo "tiempo origen" del mensaje. Toma el valor del tiempo de llegada del mensaje y resta ambos tiempos para calcular dicho retraso. Para poder hacer esta estimación, es necesario que ambos ordenadores estén completamente sincronizados. Para ello, hemos instalado en uno de los ordenadores un servidor NTP (Network Time Protocol) y en el otro el cliente NTP. Con la siguiente instrucción obtenemos el tiempo de llegada del mensaje en milisegundos:

```
tiempoLlegada=Calendar.getInstance().getTimeInMill
is();
```

Seguidamente seleccionamos el campo adecuado del Tiempo Origen:

```
tiempoOrigen=Long.parseLong(tokens.nextToken());
```

Y calculamos la diferencia para saber el delay:

```
delay = (tiempoLlegada-tiempoOrigen);
```

D. Calculo de mensajes perdidos

El cálculo de mensajes perdidos es diferente para el caso de audio que para el video. La diferencia principal es que en el audio cada mensaje es capaz de contener los datos enviados de audio, sin embargo en el video los datos son divididos en varios mensajes, por tanto, para poder contar el número de mensajes totales en audio, basta con contar el número de mensajes recibidos, sin embargo en el caso del video es necesario saber cuántos mensajes se han enviado completos a través del campo "mensajes totales".

Para el cálculo del porcentaje de mensajes perdidos, basta con tener en cuenta la cantidad de mensajes perdidos y la cantidad de mensajes transmitidos.

E. Calculo del Ancho de Banda

Para calcular el ancho de banda, sólo es necesario extraer la longitud del mensajeUDP, con la función "lenght", pues nos da el numero de bytes del Paquete, y lo multiplicamos por 8 para representarlo en bits.

IV. Interfaz Gráfico de la Herramienta de Test

Se ha desarrollado una aplicación que una vez ejecutada, se puede elegir que sea cliente o servidor. El cliente permite elegir el tipo de tráfico que envía al servidor (Audio o Video) y el servidor reenvía dicho tráfico hasta el Cliente. En el cliente se calcula y registra el jitter, delay, mensajes perdidos, porcentajes de mensajes perdidos, ancho de banda, etc. El cliente muestra todos estos datos por segundo en una interfaz gráfica muy intuitiva y de fácil uso. Además, muestra los últimos 20 paquetes recibidos en una tabla. Estos datos también pueden ser exportados en formato cvs, que puede ser interpretado por programas de tratamiento de datos como Microsoft Excel.

En la aplicación el usuario debe introducir un valor de carga útil para cada mensaje y su frecuencia de envío. Cuando el usuario selecciona "audio", se envía un ancho de banda constante y tiene un valor marcado por los dos

parámetros anteriormente introducidos. Para el caso del video, el usuario debe introducir un intervalo con los valores máximo y mínimo de datos (en Bits/s) que desea enviar junto con la frecuencia de envío de mensajes por segundo (FPS). El programa se encarga de generar los mensajes de tamaño aleatorio entre los márgenes dados por el usuario. En este caso la aplicación tiene en cuenta que los datos pueden ser divididos en varios mensajes, llamados "SubMensajes". Este interfaz gráfico se puede ver en la Figura 3.

Cuando se elige el modo servidor (seleccionándolo en la parte superior izquierda), el programa solo nos deja introducir el número de puerto por el cual recibiremos los mensajes del Cliente. A continuación le damos a "encender" y el Servidor se activa, quedándose a la escucha de los paquetes. Se puede observar la configuración del modo Servidor en la Figura 4.

El modo Cliente es el que viene por defecto en la aplicación, pero se puede pasar de modo Cliente a modo servidor simplemente seleccionándolo. En el modo Cliente el usuario debe rellenar las casillas de "Direccion IP" y "Puerto" del servidor destino. La forma de proceder para utilizar el programa, e la que sigue a continuación. El usuario elige el modo de envío, ya sean datos de "Video" o "Audio". Si elige Video, debe rellenar el intervalo de "Máximo" y "Mínimo" en Bits/s de carga útil de video que se enviará al servidor. También debe seleccionar los FPS (Frames por Segundo) para determinar el tamaño y el período de envío de cada paquete. Se puede ver la configuración del modo cliente para video en la Figura 5. Si elige Audio, debe rellenar la carga útil en Bytes y el período de envío entre cada paquete. Si se prefiere, se puede seleccionar en la pestaña derecha un tipo de Codec de Audio el cual nos rellenara la carga útil y el período de los paquetes que debemos enviar. Finalmente, debe pinchar en el botón "Enviar Paquetes" para comenzar el envío.

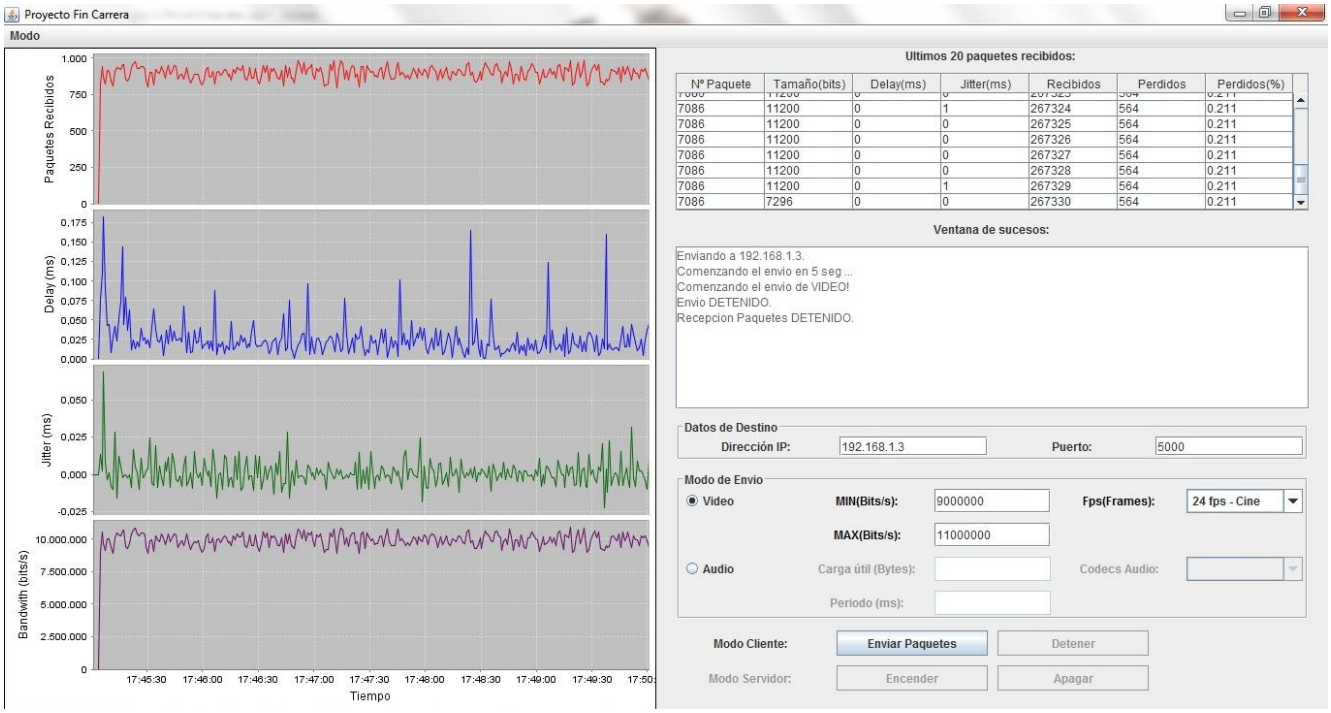


Fig. 3. Interfaz gráfico de la herramienta desarrollada.

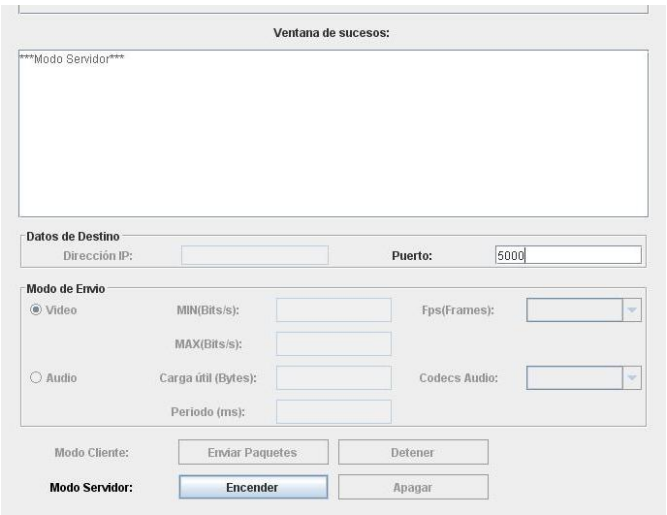


Fig. 4. Configuración del modo Servidor

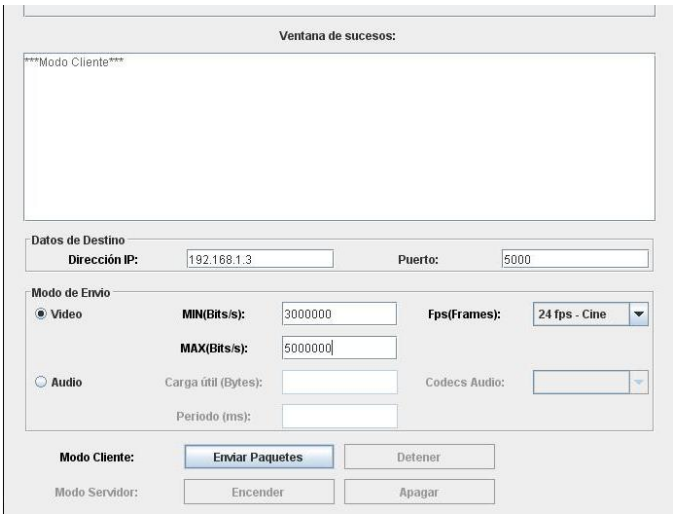


Fig. 5. Configuración del modo Cliente

V. Test realizado con la Herramienta Desarrollada

Con el objetivo de poner a prueba la herramienta desarrollada, hemos realizado varias pruebas.

A. *Prueba en una red local*

Primero hemos probado la herramienta entre 2 ordenadores que pertenecían a la misma red y estaban conectados al mismo conmutador. Ambos ordenadores utilizaban FastEthernet.

La figura 6 muestra los parámetros que se obtienen cuando se está emitiendo VoIP utilizando la norma G728. Tal como se puede ver, el ancho de banda que se utiliza es prácticamente constante, y no se percibe ningún paquete perdido. Los valores de jitter y delay son muy bajos, debido a que están conectados al mismo conmutador, pero apreciables.

La figura 7 muestra los resultados obtenidos cuando se está emitiendo video de alta definición entre los 2 ordenadores. En este caso, tanto el ancho de banda de utilización de la red ha subido considerablemente, así como el número de paquetes recibidos. Sin embargo tanto el jitter como el delay se siguen manteniendo bajos.

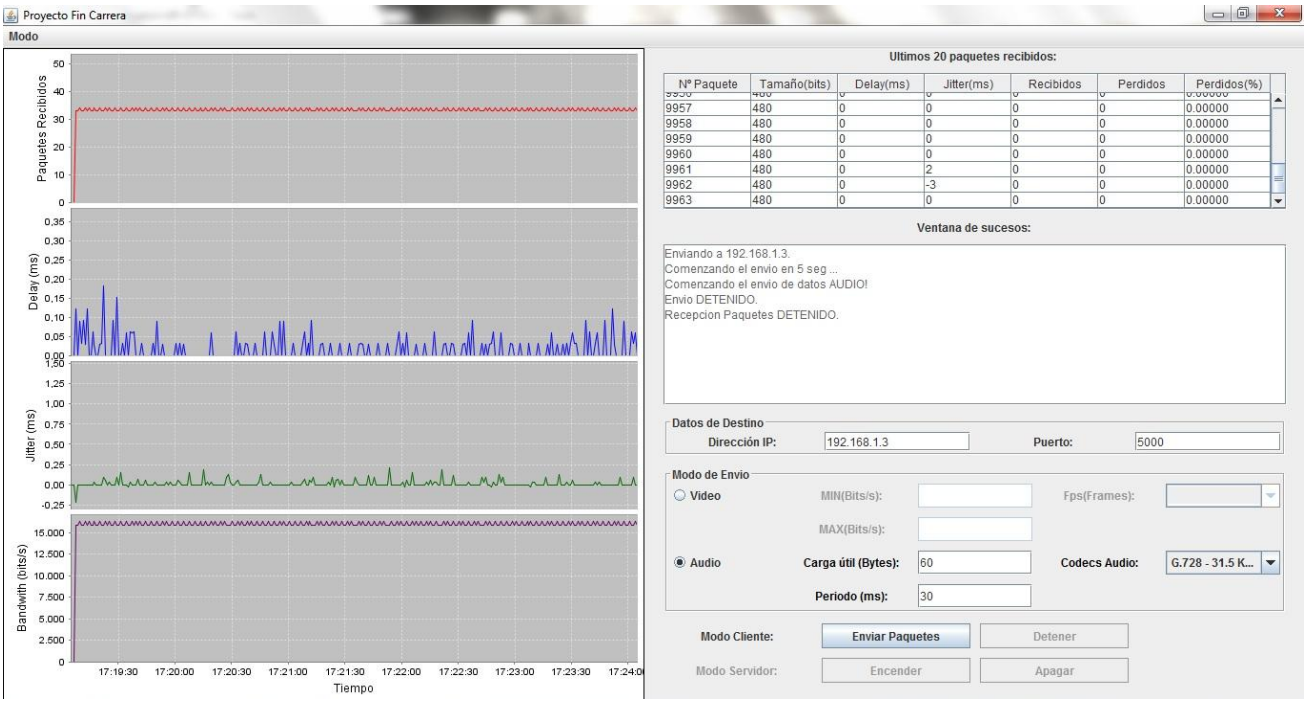


Fig. 6. Test cuando se transmite VoIP utilizando la norma G.728.

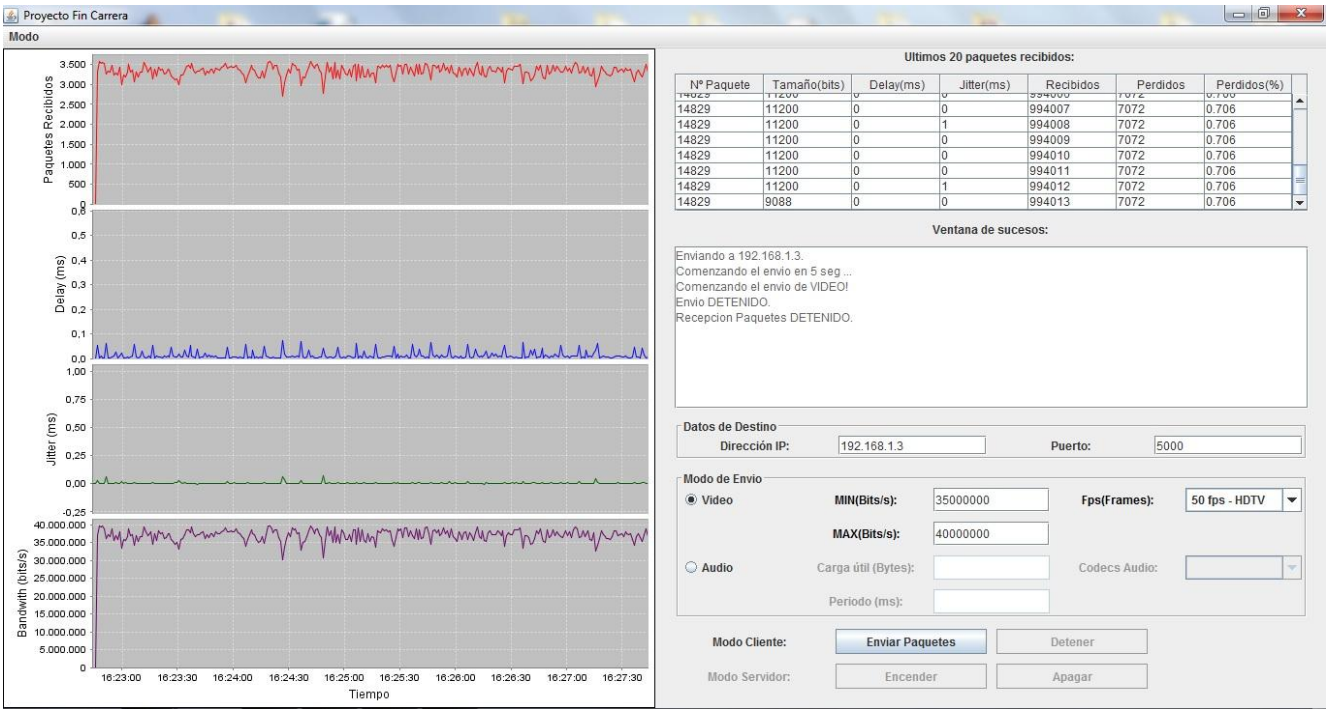


Fig. 7. Test cuando se transmite Televisión de alta definición.

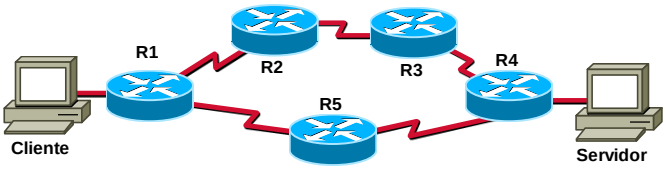


Fig. 8. Topología utilizada para realizar el test.

B. *Prueba de rendimiento cuando existen varias redes*

Seguidamente hemos configurado en el laboratorio la topología que se muestra en la Figura 8. El protocolo de encaminamiento configurado en los routers es RIPv2. Los enlaces WAN tienen una ancho de banda de 64 Kbps El objetivo de esta prueba es determinar el tiempo de convergencia del protocolo de enrutamiento. Para ello, inicialmente comprobamos que la información es transmitida desde el cliente al servidor a través de la ruta del router R5. Seguidamente, apagamos R5 y comprobamos cuanto tiempo tarda la red en converger y por tanto empieza a recibirse datos de nuevo.

La figura 9 muestra el tiempo de convergencia cuando se realiza la prueba descrita anteriormente mientras se envía VoIP utilizando la norma G.728. En esta figura se muestra claramente el tiempo que dejó de recibirse mensajes. Sin embargo se puede observar un efecto interesante. Tras la convergencia de la red, el delay entre ambos ordenadores es durante un tiempo considerablemente diferente. Creemos que esto es debido a que toda vía existen mensajes de convergencia entre los routers. Tras este breve tiempo, cuando se ha estabilizado la red, el delay pasa a ser prácticamente el mismo (aunque un poquito superior, debido a que la información pasa por un camino más largo), pero casi inapreciable.

En la figura 10 mostramos la misma prueba explicada anteriormente, pero esta vez realizada con video de con características estándar (24fps a un bitrate de entre 30Kb y 50Kb). En este caso también se observa el mismo efecto de retraso observado en VoIP. Podemos observar en este caso que el ancho de banda utilizado es bastante superiory que el delay también se ha incrementado (principalmente por el retraso que se genera debido al poco ancho de banda que se ha configurado entre los enlaces WAN). Sin embargo el número de paquetes de video que se reciben es menor (pero contienen mas Bytes) y el jitter que se obtiene es muy parecido.

VI. Conclusiones

En este artículo hemos presentado una herramienta que nos permite medir diversos parámetros de red de manera intuitiva utilizando el sistema operativo Windows. Comparándola con las herramientas existentes, podemos decir que la mayor contribución está en la creación de la primera herramienta gráfica para medir el rendimiento de red que ofrece resultados y permite almacenarlos para su posterior estudio.

Las medidas de jitter, delay, paquetes perdidos y ancho de banda se calculan sin la necesidad de que exista ninguna cabecera RTP (la mayoría de programas, como por ejemplo Wireshark, requieren de RTP para poder calcularlo, en caso contrario, no son capaces de hacerlo).

Los futuros trabajos que van a derivar del presente trabajo están enfocados en comprobar la fiabilidad, ventajas y desventajas de nuestra herramienta comparándola con las herramientas existentes. Además, se pretende comprobar su rendimiento cuando se utiliza para testear la red, con respecto a otros protocolos como por ejemplo RTP.

Agradecimientos

Este trabajo está parcialmente financiado por el "Ministerio de Ciencia e Innovación", a través del Plan Nacional de I+D+I 2008-2011, proyecto TEC2011-27516 y por la Universitat Politècnica de Valencia a través del PAID-05-12.

Referencias

[1] IBM Corporation, "IBM Study Related to the NEP Industry", 2007. http://www-935.ibm.com/services/us/gbs/bus/pdf/g510-7870-01-nep.pdf
[2] J. Postel, Internet Control Message Protocol, RFC 792, Septiembre 1981. Disponible en http://www.ietf.org/rfc/rfc0792.txt
[3] J. Case, M. Fedor, M. Schoffstall, J. Davin, A Simple Network Management Protocol (SNMP), RFC 1157. May 1990. http://tools.ietf.org/html/rfc1157
[4] S. Waldbusser, Remote Network Monitoring Management Information Base, RFC 2819. May 2000. http://tools.ietf.org/html/rfc2819
[5] S. Waldbusser, Remote Network Monitoring Management Information Base Version 2 using SMIv2. RFC 4502. May 2006. http://tools.ietf.org/html/rfc4502
[6] SendIP. Disponible en: http://www.earth.li/projectpurple/progs/sendip.html
[7] W. Feng, A. Goel, A. Bezzaz, W. Feng, J. Walpole, "TCPivo: A High-Performance Packet Replay Engine", ACM SIGCOMM 2003 Workshop on Models, Methods, and Tools for Reproducible Network Research (MoMeTools), August 2003.
[8] Rude&Crude, disponible en: http://rude.sourceforge.net/
[9] Scapy Project, en: http://www.secdev.org/projects/scapy/doc/index.html
[10] Daniel Turrull Torrents, Open Source Traffic Analyzer. Master of Science Thesis. Stockholm, Sweden. June, 2010. Available at: http://people.kth.se/~danieltt/pktgen/docs/DanielTurull-thesis.pdf
[11] Joel Sommers, Hyungsuk Kim and Paul Barford, Harpoon: a flow-level traffic generator for router and network tests, ACM SIGMETRICS Performance Evaluation Review, Volume 32 Issue 1, June 2004. Pages 392-392
[12] Nemesis. Disponible en: http://nemesis.sourceforge.net/
[13] Packet Excalibur. Disponible en http://freecode.com/projects/packetexcalibur
[14] PackETH. Disponible en http://packeth.sourceforge.net/packeth/Home.html
[15] ISIC -- IP Stack Integrity Checker, disponible en http://isic.sourceforge.net/
[16] Netperf Homepage, disponible en: http://www.netperf.org/netperf/
[17] NetSpec: A Tool for Network Experimentation and Measurement. Disponible en: http://www.ittc.ku.edu/netspec/
[18] Bit-Twist website. Disponible en: http://bittwist.sourceforge.net/
[19] A. Dainotti, A. Botta, A. Pescapè, "A tool for the generation of realistic network workload for emerging networking scenarios", Computer Networks, 2012, Volume 56, Issue 15, pp 3531-3547.

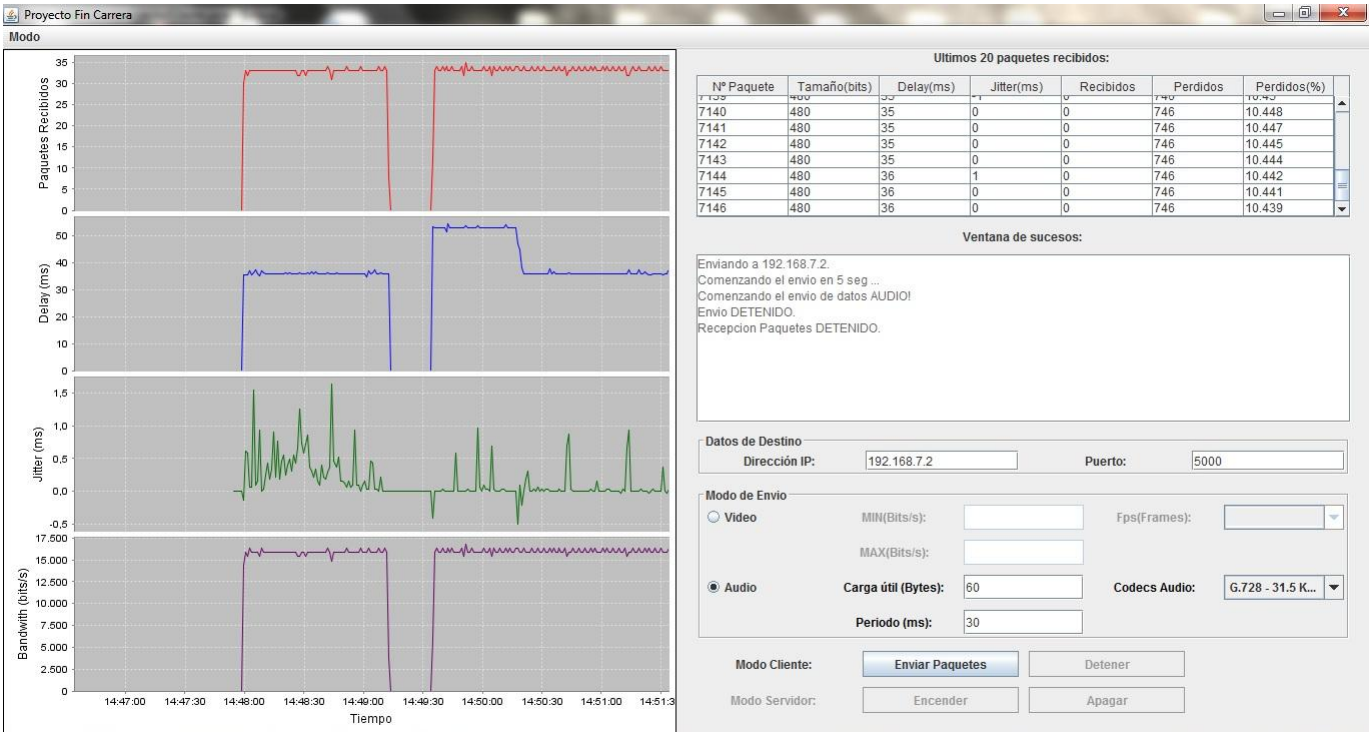


Fig. 9. Prueba de convergencia de red cuando se está transmitiendo VoIP con la norma G.728.

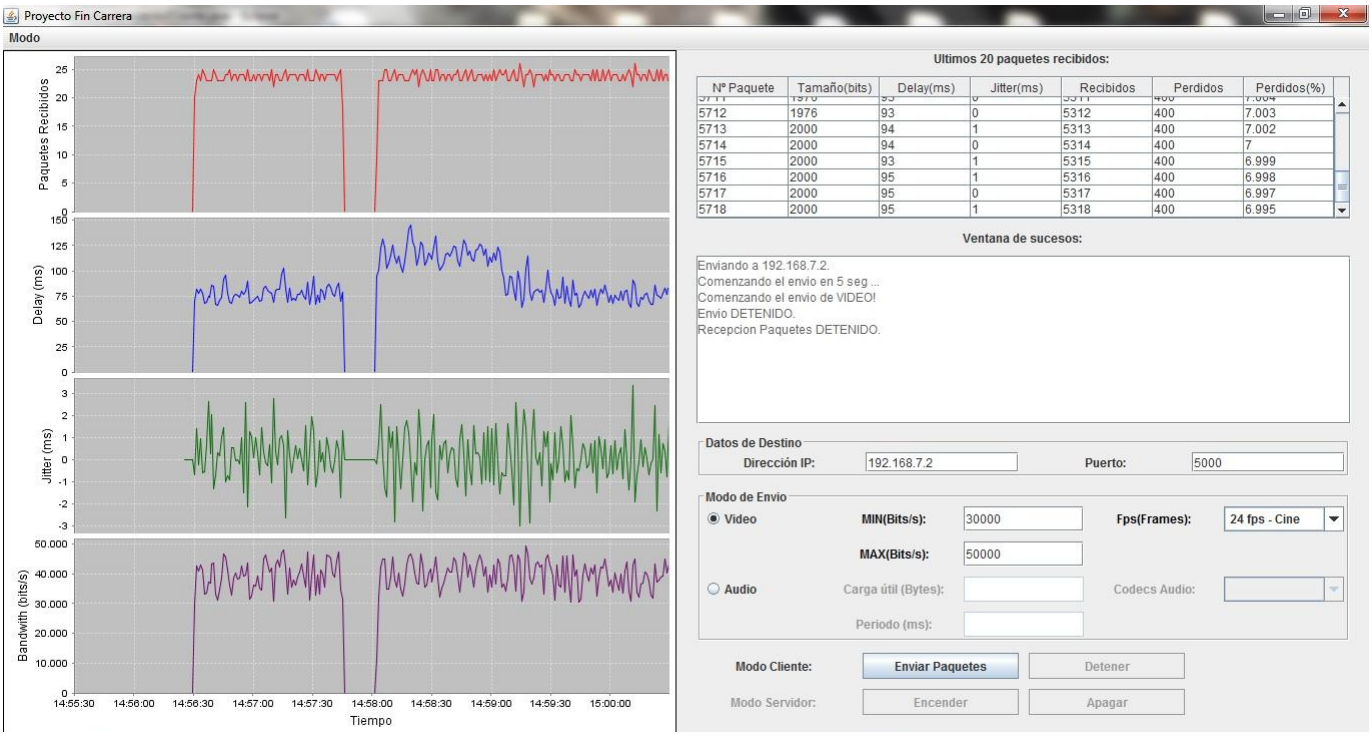


Fig. 10. Prueba de convergencia de red cuando se está transmitiendo Televisión Estándar.

Estudio Energético en el estándar 802.11

F^{co} Cárdenas Capitán[1], José M. Fornés Rumbao[1], F^{co} Rodríguez Rubio[2], Rafael M. Estepa Alonso[1].
[1]Departamento de Telemática, [2]Departamento de Automática
Escuela Superior de Ingenieros - Universidad de Sevilla
Caminos de los Descubrimientos, s/n Isla de la Cartuja 41092.
fcardenas2@us.es, fornes@trajano.us.es, rubio@us.es, rafaestepa@us.es

***Resumen*- La eficiencia energética es una de las preocupaciones más importantes de las redes inalámbricas ya que los dispositivos que conforman estas redes suelen tener una batería limitada. Además; estas interfaces inalámbricas son grandes consumidores de energía en los sistemas móviles. Por tanto, planteamos un estudio profundo sobre el consumo energético en dispositivos que utilizan el protocolo 802.11. Esta norma es muy popular y extendida. Este artículo presenta conclusiones muy interesantes para el diseño de algoritmos que persiguen ese objetivo de ahorro energético. La principal aportación de este artículo es el estudio del comportamiento de la energía consumida en transmisión en función del régimen binario, potencia de transmisión y la probabilidad de error de paquete. Se puede lograr la optimización del consumo energético a través de la elección conjunta de estas tres variables. Estos resultados han sido evaluados además en una plataforma real.**

***Palabras Clave*- potencia de transmisión, régimen binario, consumo de energía, 802.11.**

I. INTRODUCCIÓN

El consumo energético en el estándar 802.11 se ha convertido en una de las cuestiones clave debido a que la mayoría de los dispositivos con este estándar operan con baterías. Por ello, la eficiencia energética es estudiada en numerosas investigaciones, demostrando que el control de la potencia de transmisión y la capa física (tasas binarias) junto con la aplicación del modo sueño en los periodos inactivos han sido reconocidas como las mejores soluciones para perseguir el ahorro en el consumo energético.

Existen numerosas investigaciones sobre el estudio de la eficiencia energética en el estándar 802.11. En [8] se estudia la eficiencia de energía en el transceptor para medir la relación entre el coste de comunicación y el electrónico. En [9] se realiza un modelado de transceptores para aplicaciones inalámbricas y muestra que la vida de las baterías puede mejorarse significativamente con el aumento de la velocidad de datos. En estos dos artículos [8] y [9], se estudia la eficiencia desde el punto de vista de parámetros electrónicos, en cambio nosotros estudiamos el consumo de energía con parámetros utilizados directamente por el estándar.

Por otro lado [1], [4] y [5] hacen una comparación energética entre las distintas técnicas de modulación para analizar la más óptima, sin embargo no se propone una conclusión que pueda ayudar a crear nuevos algoritmos de eficiencia energética.

Además [6], [2] y [3] comparan varios protocolos en el consumo energético en modo ad-hoc. [2] compara varios protocolos para demostrar que es más óptimo aquel que reduce el número de contenciones. [3] demuestra que la energía de startup puede dominar sobre la energía total consumida en las estaciones cuando la longitud de paquete es pequeña. Por el contrario, aquí estudiamos esta magnitud en modo infraestructura.

Entre estos artículos, también es destacable el algoritmo MiSer [19], el cual busca la mejor combinación de potencia de emisión de paquete (P_e) y tasa (Rb) para reducir el consumo energético. Este algoritmo se basa en la estimación de las condiciones del canal y conocimiento previo del número de estaciones que componen la red. La elección es realizada entre elementos de una tabla con elementos calculados offline y los resultados son obtenidos con simulación en ns-2. En cambio, aquí se estudia la energía con información registrada en tiempo real y muestra su comportamiento a través del cual se pueden diseñar algoritmos sin utilizar estimaciones ni datos previos. Además, los resultados de este artículo son realizados en una plataforma real.

En este artículo presentamos un estudio profundo sobre el consumo de la energía en el periodo de transmisión que sirve para sacar conclusiones que ayudan a diseñar algoritmos de eficiencia energética. Demostraremos que existe una solución conjunta de potencia de transmisión (P_{Tx}), régimen binario (Rb) y probabilidad de error de paquete (per) que minimizan el consumo de energía de transmisión. Con este análisis desarrollado en el presente artículo, sería interesante el diseño de algoritmos de eficiencia energética que busquen de manera dinámica la solución conjunta de P_{Tx}, Rb y per.

Las secciones en las que se dividirá el presente artículo son las siguientes: La sección II analiza la magnitud del consumo energético de una manera general y justifica el motivo de centrarnos en el periodo de transmisión. La sección III estudia la potencia consumida en transmisión en una tarjeta 802.11 desde el punto de vista radioeléctrico y electrónico. El tiempo de transmisión y sus variables implicadas es estudiado en la sección IV. Del mismo modo se estudia la influencia de la probabilidad de error en la sección V. La sección VI muestra la validación real de los resultados teóricos expuestos. Por último la sección VI muestra las conclusiones.

II. ANÁLISIS DEL CONSUMO DE ENERGÍA

La energía consumida por una estación viene determinada por la siguiente fórmula:

$$E = P_{Tx} \cdot T_{Tx} + P_{Rx} \cdot T_{Rx} + P_L \cdot T_L + P_S \cdot T_S \quad (1)$$

Donde:

P_{Tx} = *Potencia consumida en transmisión.*
T_{Tx} = *Tiempo de transmisión.*
P_{Rx} = *Potencia consumida en recepción.*
T_{Rx} = *Tiempo de recepción.*
P_L = *Potencia consumida en escucha.*
T_L = *Tiempo de escucha.*
P_S = *Potencia consumida en sueño.*
T_S = *Tiempo de sueño.*

Si tenemos en cuenta que los valores típicos de potencia proporcionados por los fabricantes para estas potencias son los que se presentan a continuación; podremos observar como el valor más alto corresponde a la potencia de transmisión:

Tabla 1. Consumo de potencia de una tarjeta 802.11 (dlink g520)

Potencia consumida por la tarjeta en:	Watios
Transmisión (P_{Tx})	1,65
Recepción (P_{Rx})	0,95
Escucha (P_L)	0,8
Sleep (P_S)	0,04

Debemos notar que el valor de potencia más alto corresponde a la transmisión y el más bajo a sueño.

Por otra parte en cuanto a la división de los tiempos; una estación que utiliza la norma 802.11 empleando además el u-apsd (Unscheduled Automatic Power Save Delivery) [18] dividirá su tiempo en transmisión, recepción, escucha y sueño. Atendiendo a ello; la división del tiempo en una estación puede ser representado mediante el siguiente esquema:

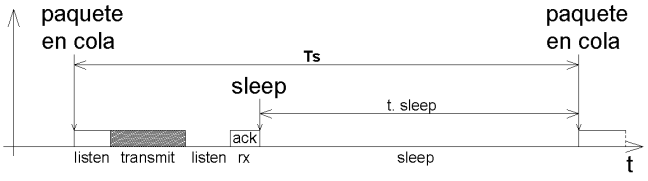


Fig. 1. División del tiempo en el nodo estación.

El periodo de **escucha** y **recepción** suelen permanecer aproximadamente constantes y dependen en parte del número de tramas a transmitir. El periodo de **sueño** comienza cuando se recibe el asentimiento de la última trama enviada y termina cuando exista un nuevo paquete en cola o bien se prevea la recepción de la trama beacon de nuestra red. En ese caso se recibirá la trama beacon y posteriormente vuelve al estado de reposo. Y por último el periodo de **transmisión** depende de la tasa con la que el paquete es enviado. Por otro lado; el tiempo de transmisión completa o tiempo de transferencia de paquete depende, además de la tasa, del número medio de intentos de transmisión, es decir, de la probabilidad de error. **Minimizar este tiempo de transmisión completa significa aumentar el tiempo de sueño.**

Por tanto, el factor de potencia de transmisión (P_{Tx}) multiplicado por el tiempo de transmisión contribuirá como sumando en el consumo de energía según la formula (1). Por ello; atendiendo al hecho de que el factor de potencia de transmisión es notablemente mayor que el resto y que la optimización del tiempo de transmisión implica maximizar el tiempo en reposo; es lógico centrarse en la transmisión y estudiar sus dos magnitudes asociadas, P_{Tx} y T_{Tx}.

$$E_{Tx} = P_{Tx} \cdot T_{Tx} \quad (2)$$

Ahora analizaremos estas dos magnitudes (y sus variables directas) para estudiar como afectan al consumo energético.

III. Potencia de transmisión

Procedemos a detallar el consumo energético de una tarjeta 802.11 para obtener el porcentaje de ahorro que se puede obtener mediante la variación de la potencia de emisión de un paquete. Es conveniente diferenciar entre potencia consumida en transmisión (P_{Tx}) y potencia de emisión (P_e) que va desde 0 a 18 dbm (sin incluir la ganancia de la antena).

Representaremos mediante el siguiente esquema una tarjeta PCI wlan 802.11; destacando la parte de electrónica, la antena, el índice de reflexión producido entre las dos anteriores, la potencia radiada y la potencia disipada.

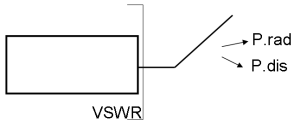


Fig. 2. Esquema de una tarjeta pci wlan 802.11

En dicho esquema hemos indicado la relación de onda estacionaria (VSWR), la cual es una variable relacionada con el índice de reflexión producido por la adaptación entre la tarjeta y la antena.

$$VSWR = (1+|\Gamma|) / (1-|\Gamma|) \quad (3)$$

Where Γ es el coeficiente de reflexión. La potencia de reflexión sería:

$$\text{Potencia reflejada (\%)} = 100 \cdot \Gamma^2 \quad (4)$$

En el esquema, se muestra además la potencia radiada y disipada que tienen lugar en la antena cuando esta está transmitiendo.

Conociendo que dicha antena es un dipolo fácilmente caracterizable en muchas fichas técnicas; podemos extraer de ellas sus parámetros; los cuales nos serán útiles para el estudio de su consumo de potencia. Los datos que nos interesan son los siguientes:

Tabla 2. Características de una antena dipolo

Antena dipolo	
Ganancia	2
VSWR	2
HPBW	65º
Polarización	Lineal

Además de ello; sabemos que según la normativa europea; la potencia radiada isotrópica equivalente (pire = potencia radiada más la ganancia) en esta banda de frecuencias no debe superar los 100 mW (20 dbm). Por ello,

si la ganancia de la antena (G) es 2, la potencia radiada es 18 dbm:

$$Pire < 20\ dbm = P.\ Rad + G = 18\ dbm + 2 = 20\ dbm \quad (5)$$

Conocemos que la eficiencia de una antena es:

$$\eta = \frac{P_{rad}}{P_{rad} + P_{dis}} \quad (6)$$

Por otro lado; sabemos que para calcular la eficiencia de una antena podemos aplicar la siguiente fórmula [7]:

$$\eta = G/D \quad (7)$$

donde G = 1,585 (2 db en unidades naturales).

La directividad (D) podríamos extraerla de la siguiente fórmula válida para antenas omnidireccionales [7]:

$$D = \frac{101}{HPBW(^{o}) - 0.0027[HPBW(^{o})]^2} \quad (8)$$

Conociendo HPBW de las especificaciones anteriores; **D = 1.897**, podríamos calcular la eficiencia de la antena:

$$\eta = G/D = 1.585 / 1.897 = 0.8355$$

Con esto podríamos calcular la potencia disipada en la antena ya que sabemos la potencia radiada:

$$\eta = \frac{P_{rad}}{P_{rad} + P_{disp}} \rightarrow P_{disp} = 0.1969 \cdot 63.1 = 12.42mW$$

Por tanto la potencia radiada más la disipada es igual a:

Pot. radiada + Pot. disipada= 63,1 + 12,42 = 75.52 mW.

Por otro lado; hay que tener en cuenta las pérdidas en la adaptación de la antena a su entrada. Estas pérdidas vienen dadas por el parámetro VSWR. En nuestro caso dicho dato es igual a 2. Este dato aplicando la tabla de conversión de potencia transmitida y potencia reflejada; obtenemos el resultado de que el 89 % es potencia transmitida y el 11 % es potencia reflejada.

Por tanto; sabiendo que la potencia total que gasta la antena (P.rad + P.dis) es igual a 75,52 mW y que esto pertenece al 89 % de la potencia total que se gasta la tarjeta en alimentar a la antena podríamos calcular la potencia total que se consume justo antes de la antena cuando está transmitiendo (P_{out}):

P_{out} = 100 · (75,52 mW) / 89 = **84.85 mW**

Esta potencia total es la potencia que debe existir en el interior de la tarjeta; concretamente en la parte de electrónica que hay justo antes de la antena cuando se están transmitiendo datos.

A partir de aquí; debemos profundizar en el consumo interno de la electrónica. La electrónica de este tipo de tarjetas se divide en partes y elementos que son comunes tal y como muestran los artículos [8], [9], [10], [11] y [12]. Estudiando esto podemos simplificar la electrónica de un transceptor 802.11 mediante cuatro bloques tal y como muestra la siguiente figura. Éstos son el bloque de transmisión (TX); el cual es responsable de la modulación y la conversión de la señal de información en banda base a la de radiofrecuencia; el bloque de recepción (RX) que se encarga de la demodulación y la conversión de radiofrecuencia a banda base; el bloque de oscilador local (LO) que genera la frecuencia portadora requerida y el bloque del amplificador de potencia (PA) que amplifica la señal.

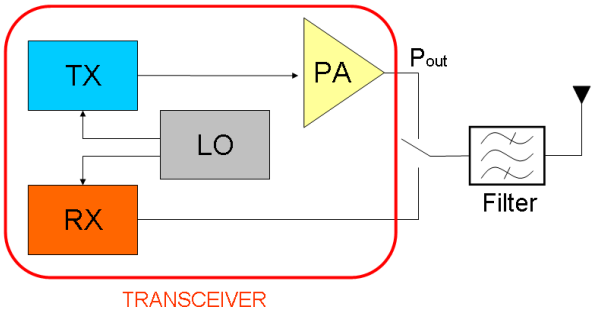


Fig. 3. Transceptor dividido en bloques

Atendiendo a este esquema podemos concluir que la potencia consumida en electrónica, cuando la tarjeta está en modo transmisión se debe a los tres bloques: oscilador, transmisión (modulación) y amplificador; que intervienen en el proceso:

$$P_{Tx} = P_{Lo} + P_{Tx} + P_{Pa} \quad (9)$$

Tanto el consumo del oscilador como la parte de transmisión encargada de otras tareas como la modulación pueden considerarse constantes. En cambio el bloque PA corresponde a un amplificador de ganancia variable cuya potencia total consumida depende de la potencia que esté aportando a su salida y su eficiencia:

$$P_{PA} = \frac{1}{\eta_{amp}} \cdot P_{out} \quad (10)$$

Donde P_{out} es la potencia proporcionada a la antena ya calculada anteriormente; es decir; la potencia a la salida del amplificador. El parámetro η_{amp} es la eficiencia del amplificador.

La eficiencia de un amplificador viene dado en sus características técnicas; proporcionadas por el fabricante. En este caso, cuando el amplificador puede tener distintas potencias de salida es necesario utilizar (en lugar de η_{amp}) la eficiencia de potencia añadida (pae), la cual es una medida para relacionar la eficiencia de un amplificador de potencia con su ganancia.

$$pae = (P_{out} - P_{in}) / P_{total} \quad (11)$$

Donde P_{out} es la potencia de salida del amplificador, P_{in} la potencia de entrada y P_{total} la potencia total consumida por el amplificador.

Esta variable se utiliza para considerar la potencia consumida por un amplificador cuando la potencia de salida es variable. Cuando la ganancia del amplificador es relativamente alta; las dos magnitudes (η_{amp} y pae) son similares. En nuestro caso hemos de utilizar la variable pae para tener en cuenta la ganancia.

Si analizamos dicha magnitud en las especificaciones de un amplificador similar al utilizado internamente en nuestra tarjeta [13] podremos caracterizarla. En dicha ficha técnica observamos su comportamiento frente a la potencia de salida:

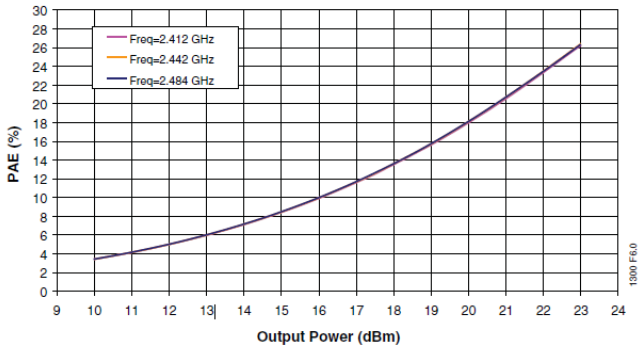


Fig. 4. Pae en función de la potencia de salida

A partir de esta gráfica debemos obtener el pae para las distintas potencias de salida que tengamos en cada momento. Teniendo en cuenta que la potencia de entrada al amplificador es despreciable, que la potencia de salida tomará valores discretos y que además son pocos, podemos caracterizar la función pae mediante una tabla con los siguientes valores:

Tabla 3. Relación entre Potencia de Radiación y pae

P_{rad}(db)	P_{rad}(mw)	P_{out}(mw)	P_{out}(db)	pae
-2	0,6309	0,8485	-0,7133	0,01
-1	0,7943	1,0682	0,2866	0,01
0	1	1,34	1,28	0,01
1	1,2589	1,69	2,28	0,01
2	1,5848	2,13	3,28	0,01
3	1,9952	2,68	4,28	0,011
4	2,5118	3,37	5,28	0,013
5	3,1622	4,25	6,28	0,017
6	3,9810	5,35	7,28	0,019
7	5,0118	6,74	8,28	0,022
8	6,3095	8,48	9,28	0,029
9	7,9432	10,68	10,28	0,035
10	10	13,44	11,28	0,042
11	12,589	16,93	12,28	0,052
12	15,848	21,31	13,28	0,062
13	19,952	26,83	14,28	0,073
14	25,118	33,78	15,28	0,087
15	31,622	42,52	16,28	0,105
16	39,810	53,53	17,28	0,12
17	50,118	67,40	18,28	0,14
18	63,095	84,85	19,28	0,17

Para conocer el consumo del amplificador en el caso de máxima potencia de emisión tomamos el valor de P_{out} = 84,85 mW = 19,28 dbm; su pae asociado (0,17) y podemos calcular la potencia consumida de la siguiente forma:

$$P_{PA} = \frac{1}{0.17} \cdot 84.85 = 499.12\,\text{mW}.$$

Esta es la potencia consumida por el amplificador cuando se está transmitiendo paquetes a 20 dbm (100 mw). En caso de transmitir un paquete a 0 dbm (1 mw):

$$P_{rad} = 0\ dbm - 2\ dbm = -2dbm = 0.631\ mw$$

$$((0.631 \cdot 0.1969) + 0.631) \cdot 100/89 = 0.8485\ mw$$

$$P_{PA} = 1/0.01 \cdot 0.8485 = 84.85\ mw$$

Por tanto el ahorro máximo que se podría obtener sería la diferencia: **414.27 mW.** Esta cantidad supone un **25.11 %** del total consumido (1650 mW).

Por ello; de acuerdo con esto, se obtiene que el ahorro máximo que se podría obtener (diferencia entre transmitir a 18 db y 0 db) es de 414,27 mW. Lo que significa el 25,11 % del total consumido (1650 mW).

IV. Tiempo de transmisión

Por otro lado las variables que afectan directamente al **tiempo de transmisión** son el número de intentos de una trama (r), la frecuencia de muestreo o de llegada (o envío) de paquetes (fs), el régimen binario (Rb) y la longitud de paquetes (L).

Así el tiempo de transmisión de un paquete se define como:

$$T_{Tx} = P_f + \frac{L}{Rb} \quad (12)$$

Donde P_f es la parte fija correspondiente a la cabecera (enviada siempre a la menor tasa de modulación). Rb es el régimen binario al que puede enviarse una trama (en el estándar 802.11 existen 12 posibilidades: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps). Para demostrar el grado de influencia sobre el tiempo de transmisión cuando L>> debemos notar que la gestión entre tasas contiguas podría conseguir un ahorro mínimo en tiempo de aproximadamente el 10% (de 5.5 a 6 Mpbs) o un ahorro máximo de un 64% (de 2 a 5.5 Mbps) entre tasas binarias contiguas. En el caso de L<<; este efecto se diluye proporcionalmente en relación a su peso relativo respecto a la cabecera, la cual es transmitida siempre a la tasa mínima de modulación.

Si multiplicamos este tiempo con la potencia de transmisión obtendríamos la energía empleada en enviar ese paquete. Si ahora hablamos de periodos de tiempo en los que tenemos que enviar N paquetes y con una probabilidad de error de paquete per, el tiempo de transmisión en ese periodo lo podríamos definir de la siguiente manera [16]:

$$T_{Tx-P} = T_{Tx} \cdot N \cdot r \quad (13)$$

Siendo r el número medio de transmisiones de cada paquete para que la transmisión sea correcta.

$$r = \frac{1}{(1 - per)} \quad (14)$$

Por tanto comprobamos la influencia del régimen binario y de la probabilidad de error sobre el tiempo de transmisión.

Para definir finalmente el comportamiento de la energía consumida en transmisión falta estudiar la probabilidad de error, lo cual se presenta en la próxima sección.

V. PROBABILIDAD DE ERROR

Mediante consideraciones anteriores, definimos la energía de transmisión en un periodo de tiempo del modo siguiente:

$$E_{Tx} = P_{Tx} \cdot T_{Tx-P} = P_{Tx} \cdot T_{Tx} \cdot N \cdot r = \frac{P_{Tx} \cdot T_{Tx} \cdot N}{1 - per} \quad (15)$$

Siendo P_{Tx} la potencia gastada en transmisión en ese periodo, T_{Tx} el tiempo de transmisión de un paquete, N el número de paquetes a enviar en ese periodo, per la probabilidad de error de paquete durante ese periodo y r el número medio de veces que se intenta enviar la trama.

Debemos tener en cuenta que la variación directa de P_{Tx} cambia la snr con la que llega un paquete y esta última variable afecta directamente a la probabilidad de error de paquete. Por tanto, aplicando cambios en la P_{Tx} a través de la potencia de emisión de los paquetes (P_e) como describe la sección III, da lugar a determinadas relaciones señal/ruido y esto a su vez a variaciones en la probabilidad de error. Dicha relación la explicaremos a continuación.

La probabilidad de error de bit o paquete puede desarrollarse a nivel teórico sin mayor complejidad. Dicha probabilidad de error depende de la modulación con la que se lleva a cabo la transmisión. En la norma que nos ocupa, las modulaciones son OFDM y CCK. La modulación ODFM consiste en enviar un conjunto de ondas portadoras en diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o en PSK. En la siguiente tabla se indica la correspondencia entre estas modulaciones y el régimen binario en el estándar 802.11g:

Tabla 4. Modulaciones de tasas

Régimen binario (Mbps)	Modulation type
6	BPSK
9	BPSK
12	QPSK
18	QPSK
24	16-QAM
36	16-QAM
48	64-QAM
54	64-QAM

Si tomamos como ejemplo la modulación M-QAM; la probabilidad de error de paquete quedaría expresada de la siguiente manera [17], [14] y [15]:

$$per = 1 - (1 - ber)^L \text{ con L = nº bits del paquete. (16)}$$

Donde:

$$ber = \frac{P_s}{\log_2 M} \quad (17)$$

En el que P_s es:

$$P_s = 1 - (1 - P_{\sqrt{M}})^2 \quad (18)$$

$$P_{\sqrt{M}} = 2(1 - \frac{1}{\sqrt{M}})Q(\sqrt{\frac{3 \cdot \log_2 M \cdot snr \cdot BW}{Rb \cdot R_c \cdot (M-1)}} \quad (19)$$

Y donde snr es:

$$snr = \frac{E_b}{N_0} \cdot (\frac{Rb \cdot R_c}{BW}) \quad \text{con} \quad \frac{E_s}{N_o} = \frac{E_b}{N_o} \cdot \log_2 M \quad (20) \text{ y } (21)$$

Siendo M el tipo de modulación empleada, No es el ruido y Q la función estándar de distribución gaussiana que representa la densidad de probabilidad a la derecha de un valor determinado. Es y Eb corresponde a la energía de símbolo y de bit, BW = 20 Mhz, Rc es el Coding rate definido en la norma para cada régimen binario y data_rate es la tasa o régimen binario.

Realizando dicho cálculo, podemos representar la probabilidad de error de paquete (per) frente a la relación señal/ruido (snr). Para representar con una gráfica esta relación tomamos un caso específico para dar valores a snr. Tomamos como ejemplo un régimen binario de 36 Mbps al que corresponde la modulación 16-QAM y un Rc=¾, y suponiendo L=50, 500 o 1500 bytes; obtenemos la siguiente gráfica:

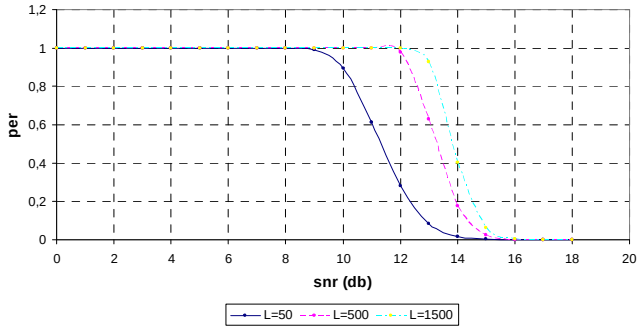


Fig. 5. per vs snr

Y a continuación representaremos la relación a nivel teórico de la expresión con la que iniciamos el apartado (15), para representar la energía de transmisión frente a la probabilidad de error de paquete. Tomando el caso de Rb = 36 Mbps, No = -95dbm, L = 500 bytes, N = 2000 paquetes y atenuación = 95 dbm tenemos lo siguiente:

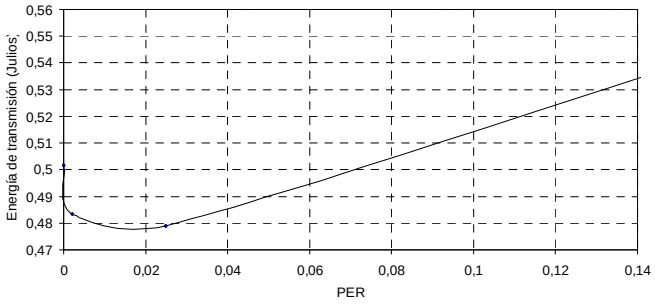


Fig. 6. Energía de transmisión vs per

En esta gráfica podemos observar el comportamiento a nivel teórico de la energía de transmisión frente a per (en

tanto por uno). En dicha relación se prueba la existencia de una probabilidad de error que hace mínima la energía de transmisión y por tanto **existe una potencia de transmisión que minimiza dicha energía de transmisión.**

VI. Representación de la energía gastada en transmisión frente a Per en un escenario real

A continuación mostramos las representaciones de la energía de transmisión (en milijulios) frente a la probabilidad de error de paquete de las 12 posibles tasas binarias obtenidas por medio de pruebas reales. La probabilidad de error utilizada, contiene además los errores por colisión ya que esta per es un cálculo derivado a partir de la media del número de intentos de transmisión de los paquetes a través de la ecuación 14. Los valores de estas representaciones son obtenidos de forma experimental a través de un escenario real descrito a continuación.

La plataforma sobre la que se llevarán a cabo las pruebas; estará formada por dos elementos; un punto de acceso y una estación asociada al anterior mediante el modo infraestructura. Dichos elementos se corresponden físicamente con dos PC´s equipados con dos tarjetas pci D-Link DWL-G520 con chipset Atheros AR5001X y espaciados tres metros entre sí.

Madwifi será el driver elegido para estas tarjetas. Para implementar las pruebas es útil y necesaria la creación de otro software de más alto nivel que gestione las estadísticas de cada una de las estaciones. Será escrito en lenguaje C. La comunicación entre ambas capas software (Madwifi y aplicación C) es fundamental y se realizará mediante llamadas IOCTL.

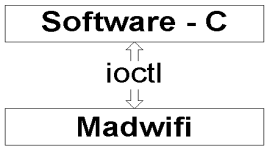


Fig. 7. Capas software de la plataforma

Para la comunicación entre la estación y el punto de acceso se utilizará el canal 3 (de los 14 posibles). Por dicho canal el punto de acceso enviará una trama Beacon cada 1000 ms. Por otro lado; la estación hará uso de la norma 802.11 en sus versiones b, g y e.

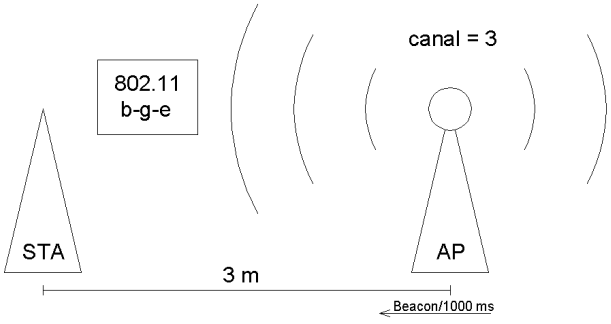


Fig. 8. Escenario físico de la plataforma.

Además la prioridad asociada a los paquetes enviados por la estación será Best Effort y sus parámetros asociados son los siguientes: CWmin = 7, CWmax = 1023, AIFS = 28 μs y Txop = 0 (por lo que no se permitirá agregación de paquetes).

Las siguientes gráficas muestran la energía consumida por la tarjeta en transmitir 100 paquetes con una determinada longitud. El cálculo de esta energía se realiza del siguiente modo: El driver Madwifi registra multitud de parámetros del estándar 802.11. Entre estos parámetros se encuentra el número de intentos de envío de un paquete para que sea recibido correctamente (r). Si enviamos 100 paquetes, registramos su parámetro r y hacemos la media de r podemos calcular la probabilidad de error de paquete durante ese periodo mediante la ecuación 14. Si además, sabemos la longitud del paquete, la tasa y potencia con la que son emitidos estos 100 paquetes, podemos saber la energía gastada en ese periodo a través de la ecuación (15).

Resumiendo, si definimos un periodo como el tiempo en transmitir 100 paquetes; el proceso seguido en la prueba para calcular la energía de transmisión se puede describir mediante estos pasos: Comenzamos iniciando la potencia de emisión de los paquetes (P_e) a 18 db y el régimen binario (rb) a 54 Mbps, posteriormente se realizan los siguientes pasos de forma cíclica, (1) calcular la media del número de intentos de envío de paquetes cada periodo (100 paquetes transmitidos) (2) calcular la probabilidad de error de paquete mediante la ecuación 14, (3) calcular la energía de transmisión consumida mediante la ecuación 15, (4) Este valor de energía junto con el régimen binario, la potencia de emisión, la atenuación (calculado con la aplicación del principio de reciprocidad [20]) y la probabilidad de error son comunicadas a través de una llamada ioctl a la aplicación del nivel superior. Por último, (5) si la potencia de emisión es mayor que 0 disminuye la potencia de transmisión cada cinco periodos, en caso contrario, la potencia de emisión se inicia a 18 db y el régimen binario es bajado un nivel respecto su capacidad.

A continuación mostramos el pseudocódigo que resume lo anterior. Notar que Rb [] se refiere a una tabla de 12 elementos que almacena las distintas tasas ordenadas de mayor a menor y la i representa el elemento específico de la tabla.

```
Pe = 18 dbm
rb = 54 Mbps
If (paquetes_transmitidos = 100) {
        contador++
        rb = Rb [i]
        calcular r
        calcular per
        calcular energía de transmisión (ETX)
        calcular atenuación
        IOCTL (r, per, ETX, atenuación)
If (contador = 5) {
        If (Pe > 0) {
        Pe = Pe - 1
     }
else {
        Pe = 18 dbm
        rb = Rb [i-1]
        }
}
```

Fig. 9. Pseudocódigo del proceso para calcular la energía de transmisión

Esta última medida de esperar cinco periodos hasta disminuir la potencia de emisión tiene el objetivo de hacer una media entre los cinco valores de energía de transmisión y probabilidad de error y así aumentar la fiabilidad de los resultados.

A. *Longitud de paquete de 80 bytes*

Las siguientes gráficas corresponden a una longitud de paquete pequeña (80 bytes aprox). Han sido representadas en distintas gráficas para apreciar mejor sus escalas:

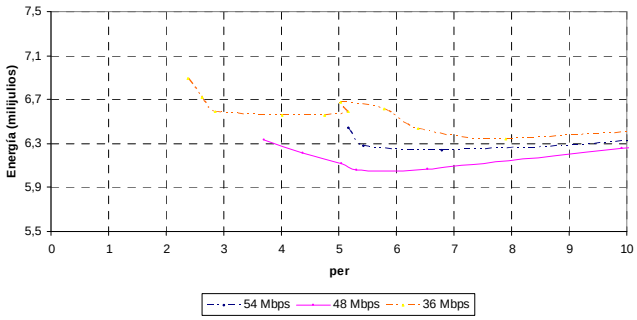


Fig. 10. Energía – per para 54, 48 y 36 Mbps

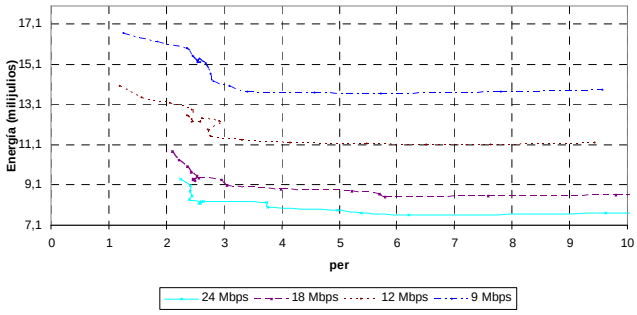


Fig. 11. Energía – per para 24, 18, 12 y 9 Mbps

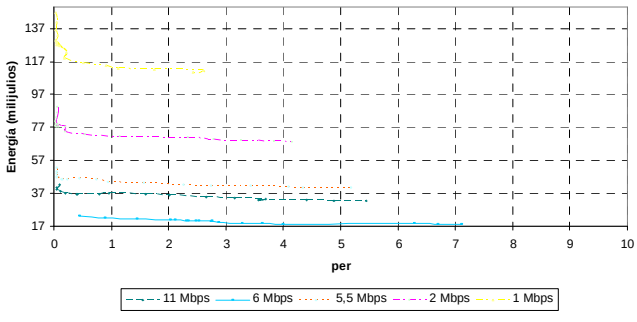


Fig. 12. Energía – per para 11, 6, 5.5, 2 y 1 Mbps

En este caso el orden de tasa de mayor a menor consumo de energía de transmisión con una probabilidad de error determinada, es 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 54, 48 Mbps. Podemos comprobar que este orden no coincide con el orden establecido por la capacidad de la tasa. Esto se debe a que cuando el tamaño de paquete es pequeño, la cabecera que es enviada a la mínima tasa de modulación es dominante frente al resto del paquete. Por ello, el factor dominante sobre la energía de transmisión es el tiempo de transmisión de la cabecera (por ejemplo el envío del paquete a 11 Mbps con modulación CCK requiere enviar la cabecera a 1Mbps y el envío del paquete a 6 Mbps con modulación OFDM manda la cabecera a 6 Mbps por lo que el tiempo de transmisión de la cabecera con 6 Mbps es menor) o bien la potencia de transmisión (por ejemplo, el tiempo de transmisión a tasa 48 y 54 Mbps es igual por tanto como la tasa de 48 Mbps requiere menos potencia de transmisión para el envío con un mismo per, la energía de transmisión es menor).

B. *Longitud de paquete de 1864 bytes*

Para una longitud de paquete igual a 1864 bytes (1800 bytes de datos más 64 de distintas cabeceras) tenemos las siguientes representaciones de energía de transmisión frente a la probabilidad de error:

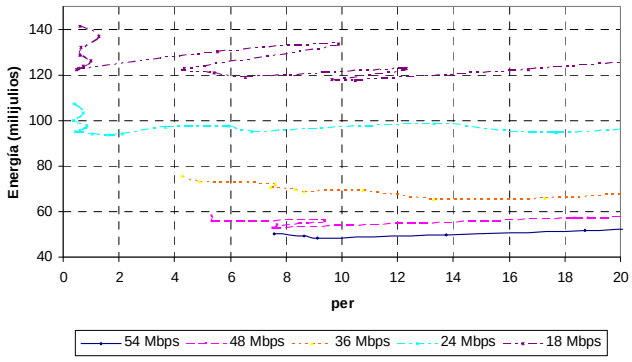


Fig. 13. Energía – per para 54, 48, 36 , 24 y 18 Mbps

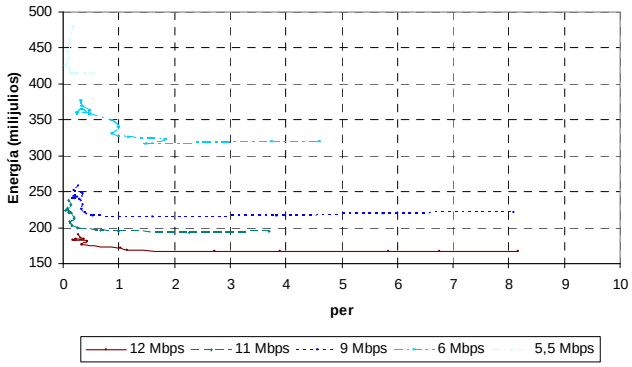


Fig. 14. Energía – per para 12, 11, 9 , 6 y 5.5 Mbps

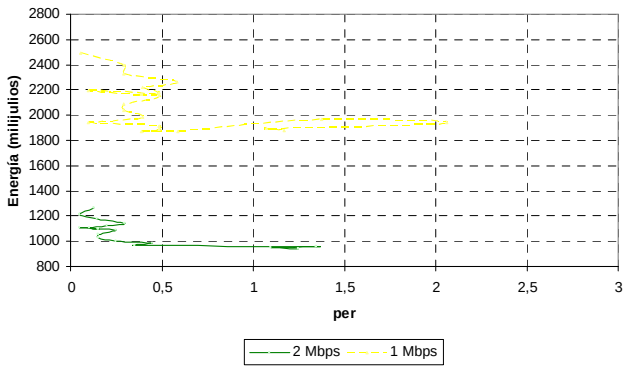


Fig. 15. Energía – per para 2 y 1 Mbps

Podemos notar que aquí el orden de tasa de mayor a menor consumo de energía es 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 y 54 Mbps. Este orden coincide con el orden establecido por la capacidad del régimen binario debido a que el factor dominante en la energía de transmisión es el tiempo en transmitir el paquete.

En estas gráficas se observan mínimos en el consumo de energía en cada curva dependiendo del Rb y per. La variación de per se obtiene de cambiar la snr a través de la variación de la potencia de transmisión. Por ello, **se pueden obtener mínimos en la energía de transmisión con la correcta elección de Rb, per y P_{Tx}.** Otra conclusión importante que se extrae es que **para longitudes de paquete pequeñas el orden de las tasas binarias ordenadas de menor a mayor consumo de energía** (48, 54, 36, 24, 18, 12, 9, 6, 11, 5, 2 y 1) **no coincide con el orden de mayor a menor tasa**. Esto no es considerado por algoritmos de eficiencia energética que utilizan mecanismos de elección de tasas basados en el orden de su capacidad y no en el del consumo de energía.

VII. CONCLUSIONES

En el presente artículo, se analiza en profundidad los parámetros que influyen en el consumo energético en transmisión de un dispositivo 802.11. Tras ese estudio se comprueba de forma teórica la existencia de un mínimo en la energía de transmisión consumida en función del régimen binario, la probabilidad de error y la potencia de transmisión. Además se ha implementado un escenario real para obtener el comportamiento de la energía consumida en las distintas soluciones. Las pruebas realizadas confirman la existencia de puntos óptimos de energía. También concluimos que para longitudes de paquete pequeñas, las tasas ordenadas en función de su consumo de energía no coinciden con el orden establecido según su capacidad.

Con este estudio se pueden definir algoritmos de eficiencia energética basados en la búsqueda de los valores óptimos (P_{Tx}, Rb, y per) que optimizan el gasto energético.

AGRADECIMIENTOS

Los autores agradecen al Proyecto de Excelencia de la Junta de Andalucía. (P09-AGR-4785) y al Proyecto de Investigación y Desarrollo Tecnológico del Ministerio de Ciencia e Innovación (DPI2010-19154) por subvencionar este trabajo.

REFERENCES

[1] A. Wang, S. Cho, C. Sodini, and A. Chandrakasan, “Energy efficient modulation and MAC for asymmetric RF microsensor systems” in Proc. Int. Low Power Design (ISLPED), 2001 pp.106-111.

[2] J. C. Chen, K. Sivalingam, P. Agrawal, and S. Kishore, “A comparison of MAC protocols for wireless local networks based on battery power consumption,” in Proc. Conf. IEEE COmput. Commun. Societies, 2000 pp. 150-157

[3] S.Cho and A. Chandrakasan, “Energy efficient protocols for low duty cycle wireless microsensor networks,” in Proc. Int. Conf. Acoustics, Speech and Signal Processing, 2001, pp. 2041-2044.

[4] S.Cui, A. Goldsmith, and A. Bahai, “Energy-constrained modulation optimization for coded systems,” in Proc. IEEE Global Telecomm. Conf., 2003, pp. 372-376.

[5] A. Wang and C. Sodini, “A simple energy model for wireless microsensor transceivers,” in Proc.IEEE Global Telecomm. Conf., November 2005, pp. 3205-3209

[6] Laura Marie Feeney, Martin Nilsson, “Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment,” in Proc. IEEE Conference of the IEEE Computer and Communications Societies, 2001, pp 1548-1557 vol. 3

[7] Fundamental Parameters of Antennas. Jhon Wiley. http://es.scribd.com/doc/76045379/11/Omnidirectional-Patterns

[8] Andrew Y. Wang and Charles G. Sodini, “On the Energy Efficiency of Wireless Transceivers”, Massachussets Institute of Technology, Cambridge. IEEE International Conference on Communications, 2006.

[9] Andrew Y. Wang and Charles G. Sodini, “A Simple Energy Model for Wireless Microsensor Transceivers”, Massachussets Institute of Technology, Cambridge. IEEE Global Telecommunications Conference, 2004.

[10] Integrated Transceiver Modules for WLAN 802.11 b/g/n, Bluetooth. http://www.mouser.com/ds/0/LS-Research/tiwi_r2_datasheet-1381.pdf

[11] Ana González, “INVESTIGATION OF RF POWER AMPLIFIERS FOR 802.11a MOBILE TERMINALS, Norkoping Sweden. http://www.ep.liu.se/ecp/008/posters/015/ecp00815p.pdf

[12] Qcom “Specifications 802.11b/g Wireless PCI Express Mini Card”. http://resources.mini-box.com/online/AOC-QCOM-PCIE/AOC-QCOM-PCIE-specs.pdf

[13] 2.4 Ghz High-Power, High-Gain Power Amplifier (SST12LP14A), http://ww1.microchip.com/downloads/en/DeviceDoc/S71300.pdf

[14] Brage Ellingsaeter and Torleiv Maseng “Adaptive M-QAM Signaling for Dynamic Spectrum Access”, Norwegian Defense Research Establishment. IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications, 2011

[15] Pierre-François Morlat, Guillaume Villemaud, Jaques Verdier, Jean-Marie Gorce, “On Relaxing constraints on Multi-branches RF Front-End for a SIMO OFDM Receiver”, Centre d´Innovarion en Telecom et Integration de services, Lyon, France, Pervasive Mobile & Ambient Wireless Communications, 2008

[16] Dra. Isabel Román Martínez, “El nivel de enlace”, 2010.

[17] CITI, Centre dÍnnovarion en Telecom et Intégration de services, “On Relaxing constraints on Multi-branches RF Front-End for a SIMO OFDM Receiver – A Global System evaluation Scheme”. European Cooperation in the field of scientific and technical research, France, October 2008.

[18] Xavier Pérez-Costa, Albert Vidal and Daniel Camps-Mur, “SU-APSD: Static IEEE 802.11e Unscheduled Automatic Power Save Delivery” Wireless Conference 2006 - Enabling Technologies for Wireless Multimedia Communications (European Wireless), 12th European. Athens, Greece, April 2006.

[19] Daji Qiao, Sunghyun Choi, Amit Jain, Kang G. Shin, , “MiSer: an optimal low-energy transmission strategy for IEEE802.11a/h” MobiCom 2003 - Proceedings of the 9th annual international conference on Mobile computing and networking, pp: 161

[20] Glenn Judd, Xiaohui Wang and Peter Steenkiste, “Efficient Channel-aware Rate Adaption in Dynamic Environments“ Carnegie Mellon Universtity. 6th International Conference on Mobile Systems, applications and services

Impacto de la seguridad en el rendimiento de los protocolos de enrutamiento seguro para MANETs

J.L. Tornos y J.L. Salazar
Grupo de Tecnologías de las Comunicaciones – Instituto de Investigación en Ingeniería de Aragón
Dpt. IEC. Centro Politécnico Superior Universidad de Zaragoza
Edif. Ada Byron, 50018, Zaragoza
{jltornos, jsalazar}@unizar.es

***Resumen*- Las MANET tienen unas características que hacen que los protocolos de enrutamiento cobren especial relevancia. Debido a la falta de una infraestructura predeterminada, la movilidad de los nodos y la necesidad de que todos los nodos realicen funciones de retransmisión de paquetes es especialmente importante realizar una correcta elección del protocolo de enrutamiento para que se adecúe a las necesidades de la red. Dentro de estas necesidades, se encuentra la seguridad la cual se vuelve esencial en determinados entornos. Los protocolos seguros de enrutamiento para MANETs, basados normalmente en protocolos de enrutamiento previos, centran su desarrollo en la seguridad y obvian en la mayoría de los casos el impacto en el rendimiento del protocolo. En este artículo mostramos varios ejemplos del impacto de la seguridad en el rendimiento de los protocolos de enrutamiento y como puede paliarse este descenso mediante un correcto diseño del protocolo seguro.**

***Palabras Clave*- MANET, enrutamiento seguro, DSR**

I. INTRODUCCIÓN

Los protocolos de enrutamiento para MANETs tienen que hacer frente a características distintas a las encontradas en las redes cableadas. A la falta de una infraestructura predeterminada y la necesidad de colaboración por parte de los nodos para la retransmisión de los paquetes, se une la movilidad de los nodos. Todo esto requiere que se puedan realizar ajustes en las rutas de comunicación de una manera rápida y que se adapten a las variaciones en la topología de red. Dando solución a estas características se han desarrollado multitud de protocolos de enrutamiento que intentan obtener el mejor rendimiento para las MANET [1-3].

Los distintos protocolos de enrutamiento hacen uso de una gran variedad de técnicas para conseguir minimizar el impacto en los recursos de los nodos que componen la red: ancho de banda, consumo de energía, tiempo de procesado… De esta manera algunos protocolos se centran en disminuir el número de paquetes que se transmiten, otros intentan que estos paquetes tengan un menor tamaño, que el tiempo de procesado sea el menor posible o minimizar el tiempo de descubrimiento de ruta.

Los protocolos clásicos de enrutamiento en MANETs obvian la seguridad, por lo que ha sido necesario desarrollar protocolos seguros [4] para aquellos entornos en los que la seguridad es un requisito fundamental. La gran mayoría de los protocolos seguros se basan en los protocolos clásicos para realizar el enrutamiento. Por ejemplo encontramos los protocolos seguros ADSR [5], ARIADNE [6], SDSR [7], SRD [8] y SRDP [9] basados DSR [10]; ARAN [11], SAODV [12] y SEAR [13] basados en AODV [14]; SEAD [15] basado en DSDV [16]; o SOLSR [17] basado en OLSR [18].

El problema al añadir seguridad a estos protocolos es que su rendimiento original decrece en alguno, o varios, de los recursos de los que disponen la red y los nodos: consumo de energía, tiempo de descubrimiento de ruta, tiempo de procesado, ancho de banda… Por tanto, la QoS original que el protocolo de enrutamiento ofrecía se ve afectada ya que el hecho de añadir seguridad al protocolo requiere del uso de un mayor ancho de banda y necesidad de un mayor procesado y análisis de los paquetes.

Los protocolos de enrutamiento seguros normalmente se centran en la seguridad del protocolo y no intentan dar un paso más allá del funcionamiento básico del protocolo original, lo cual suele reducir su rendimiento. De esta manera, las características adicionales que acompañan al protocolo no suelen ser planteadas en el desarrollo inicial del problema. En el mejor de los casos, estas características quedan pendientes de desarrollo. En otros casos su empleo en el protocolo seguro no será posible debido a restricciones impuestas por el propio diseño del protocolo seguro.

Varios de estos protocolos seguros emplean criptografía simétrica para asegurar los mensajes de enrutamiento mientras que otros se decantan por la criptografía asimétrica. El uso de un tipo de criptografía u otro afectará en uno o varios aspectos al rendimiento del protocolo de enrutamiento (ancho de banda, tiempo de procesado y tiempo de descubrimiento de ruta) y también a que haya una mayor o menor complejidad en el despliegue de la PKI [19] en la que se apoyará la seguridad del sistema.

En este artículo nos vamos a centrar en los protocolos seguros basados en DSR. Analizaremos cuales de ellos permiten el despliegue de las características adicionales del protocolo y de qué manera varía su rendimiento cuando se habilitan estas características. Centraremos la atención sobre todo en el número de paquetes que tiene que transmitir la red para procesar los paquetes de descubrimiento de ruta y en el tiempo necesario para que el nodo que inicia el descubrimiento de ruta pueda iniciar la comunicación con el nodo destino. También se hará un análisis de las distintas características adicionales y de qué manera restringen el planteamiento inicial de los protocolos si se quiere hacer uso de ellas.

En la Sección II se hace un repaso sobre los principales protocolos de enrutamiento para MANETs mostrando las diferentes características que tienen los protocolos. En la

Sección III se describe más en detalle el funcionamiento del protocolo DSR y de los protocolos seguros basado en él. En la Sección IV se muestran las pruebas y los resultados obtenidos. En la Sección V se muestran las conclusiones y las líneas futuras de trabajo.

II. Protocolos de Enrutamiento Para MANETs

El enrutamiento en las redes ad hoc debe hacer frente a problemas inexistentes en los protocolos de enrutamiento clásicos de las redes cableadas. A la falta de una infraestructura predeterminada se une la movilidad de los nodos que componen la red. Así pues, un nodo que accede a una red no sabe de inicio la topología ni la composición de la red. Y además, una vez iniciada la comunicación, tampoco se garantiza que la topología se mantenga constante y no cambie debido al desplazamiento de uno o varios nodos en la red.

Planteados, encontrados y detectados todos estos problemas se desarrollaron diversos protocolos de enrutamiento empleando diversas funcionalidades para intentar paliar al máximo las dificultades para realizar el enrutamiento en este tipo de redes. De esta manera podemos dividir los protocolos según pertenezcan a uno o varios de los siguientes grupos:

- **Reactivos, proactivos e híbridos**: los protocolos reactivos son protocolos bajo demanda y las nuevas rutas se descubrirán cuando sean necesarias para establecer una comunicación. Un ejemplo de este tipo de protocolos es DSR. Los protocolos proactivos, envían de manera periódica mensajes a la red para conocer su estado. Como contrapunto, envían más paquetes de control a la red que los primeros, lo que implica que el throughput de datos del sistema disminuirá. Como ejemplo de este tipo de encaminamiento podemos poner Destination-Sequenced Distance Vector (DSDV). Existen también protocolos híbridos, que mantienen una actitud proactiva a nivel local y reactiva a nivel global, como es el caso de Zone Routing Protocol (ZRP) [20].

- **Encaminamiento en el origen o encaminamiento salto a salto**: el encaminamiento en el origen se caracteriza porque cada paquete de datos incorpora la ruta que va atravesar hasta alcanzar su destino. Esto se consigue empleando una lista con los nodos intermedios por los que deberá pasar el paquete hasta su destino. Un ejemplo de este protocolo es DSR. El encaminamiento salto a salto únicamente especifica el destino y son los nodos intermedios los encargados de seleccionar el siguiente nodo al que será enviado el paquete. De esta manera se reduce el tamaño de los paquetes al no incluir la lista de nodos, pero aumenta el tiempo de procesamiento de los paquetes. Un ejemplo seria el protocolo DSDV.

- **Jerárquico o plano:** los protocolos jerárquicos establecen niveles, cada uno con unas funciones determinadas. Suelen realizar agrupaciones en clusters, de manera que los nodos se repartan las funciones. Unos harán de Gateway para comunicarse con otros clusters. También habrá un nodo cabecera de cluster, encargado de recopilar la información del cluster y comunicarla a otros clusters vía Gateway. Como ejemplo de protocolo jerárquico podemos poner Cluster-Head Gateway Switch Routing Protocol (CGSR) [21]. Los protocolos planos son aquellos en los que no existen niveles en las funcionalidades sino que todos los nodos realizan las mismas funciones.

- **Multipath o singlepath**: los protocolos singlepath tan solo emplean una ruta para cada destino, como DSDV. Los multipath [22] permiten almacenar varias rutas para cada nodo de la red, tal y como hace MP- DSR [23].

Los diferentes protocolos de enrutamiento se diseñan basándose en las características descritas. A continuación se describen varios protocolos de enrutamiento indicando las características previas de las que hace uso cada uno de ellos:

- **AODV**: Ad-hoc On-Demand Distance Vector, es un protocolo bajo demanda, con encaminamiento salto a salto. Cada nodo solo conoce el siguiente salto para un destino dado. Consigue una adaptación rápida a las variaciones de los enlaces y emplea un contador para evitar la formación de bucles.

- **CGSR**: Cluster head Gateway Switching Routing. Los nodos se agrupan en clusters de manera que todos los nodos dentro de la cobertura de unos nodos específicos, clusterhead, forman un cluster. Los nodos que están dentro del área de cobertura de dos clusterhead son conocidos como nodos Gateway. Estos son los encargados de realizar las comunicaciones entre los clusterhead transmitiendo los paquetes entre los distintos clusters.

- **DSDV**: Destination-Sequenced Distance Vector. Este esquema de encaminamiento está basado en el algoritmo de Bellman-Ford. Fue desarrollado en 1994 por Perkins y Bhagwat. De manera periódica, los nodos comunican a sus vecinos su tabla de rutas, de este modo los nodos actualizan su propia tabla de rutas.

- **DSR**: Dynamic Source Routing. En este protocolo de encaminamiento el nodo origen establece la ruta a seguir en la red hasta alcanzar el nodo destino. Los nodos tan solo realizan búsquedas de rutas cuando tienen datos que enviar a un nodo para el que no tienen una ruta almacenada, protocolo reactivo.

- **OLSR**: Optimized Link State Routing. Se trata de un protocolo proactivo que proporciona la ruta óptima, en cuanto a número de saltos, y está especialmente diseñado para redes extensas y densas. Emplean paquetes Hello para comunicarse con sus vecinos y paquetes Topology Control (TC) para conocer el estado general de la red. Los paquetes TC son transmitidos por la red únicamente por los nodos llamados Multipoints Relays (MPR's), con lo que se consigue reducir significativamente el número de paquetes de control que circulan por la red.

- **TORA**: Temporally Ordered Routing Algorithm [24]. Este protocolo fue diseñado para realizar funciones de encaminamiento en redes muy dinámicas. Esta especialmente diseñado para reaccionar de manera rápida a los cambios en la topología de la red.

- **ZRP**: Zone Routing Protocol. Este protocolo está formado por dos subprotocolos: Intra-zone Routing Protocol (IARP) e Inter-zone Routing Protocol (IERP). Cuando opera IARP, el protocolo es proactivo, mientras que en IERP el protocolo es reactivo. ZRP no especifica los protocolos IERP ni IARP. El diámetro de la zona de actuación IARP es variable y se seleccionará el óptimo de manera individual para cada red.

III. DSR y Protocolos Seguros Basados en DSR

A. DSR

El protocolo DSR está definido en el RFC 4728 [25] y queda definido de la siguiente manera: "DSR is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration".

Dentro de DSR tenemos dos protocolos distintos, uno para realizar el descubrimiento de ruta y otro para el mantenimiento de ruta.

- **Route Discovery**: cuando un nodo quiere iniciar una transmisión de datos y desconoce la ruta para alcanzar el nodo destino transmite en modo broadcast un paquete de descubrimiento de ruta (RR). Los nodos que reciben el paquete comprueban si son ellos el destino, si no es así añaden su dirección a la lista de nodos intermedios y retransmiten el paquete. Cuando el nodo destino recibe el paquete RR guarda la ruta en su Route Cache y envía un paquete de respuesta (REP) en sentido inverso por la ruta indicada. El paquete, enviado en modo unicast, seguirá la ruta inversa hasta llegar al nodo que originó el descubrimiento de ruta. Este nodo almacenará la ruta y podrá iniciar la transmisión de datos.
- **Route Maintenance**: las rutas almacenadas en la Route Cache de cada nodo tienen un periodo de validez. Para que las rutas no caduquen y sean borradas, se deberán emplear dentro del periodo de validez, el cual se actualizará cada vez que se emplee la ruta. Si una ruta es borrada de la Route Cache, por que haya pasado el tiempo de validez o debido a errores de conexión, y vuelve ser necesaria se iniciará un nuevo descubrimiento de ruta.

Las características del protocolo descritas hasta ahora permiten realizar el descubrimiento y mantenimiento de las rutas. Además de estas características básicas del protocolo existen diversas opciones que permiten variar en parte la forma de trabajar del protocolo de manera que se adapte a las necesidades de la red. Estas opciones se puedan emplear para mejorar parámetros de QoS de la red en función de las necesidades de la propia red. Se podrá intentar reducir el tiempo de descubrimiento de ruta; evitar la saturación excesiva de la red con paquetes de descubrimiento de ruta; reducir el número de paquetes descartados…

En este artículo nos centraremos en el protocolo de descubrimiento de ruta ya que es el "goal" de los protocolos de enrutamiento seguro. Las tres opciones adicionales de DSR en el descubrimiento de ruta son: Replying to Route Requests Using Cached Routes, Route Request Hop Limits, Caching Overheard Routing Information.

Replying to Route Requests Using Cached Routes: Esta opción otorga al protocolo la opción de que un paquete de descubrimiento de ruta no tenga que atravesar todos los nodos que componen la ruta. De esta manera se consigue no saturar la red en exceso y también acortar el tiempo de descubrimiento de ruta. Cuando un paquete RR llega a un nodo, lo procesa de manera que si no es el nodo destino, busca en su tabla de rutas si conoce una ruta que permita alcanzar el nodo destino. Si es así, crea un paquete de respuesta REP añadiendo a la ruta marcada en el paquete RR la ruta que él tiene almacenada. Esta opción permitirá acortar el tiempo de respuesta y evitar la saturación de la red. Habrá que tener en cuenta las condiciones de la red ya que si la movilidad de la red es alta puede que estas rutas estén ya caducadas lo que obligará al nodo origen a volver a iniciar un descubrimiento de ruta.

Route Request Hop Limits: Esta opción limita el Time-To-Live (TTL) de los paquetes de descubrimiento de ruta a 1. Se emplea cuando se quiere evitar saturar la red con paquetes de descubrimiento de ruta y primero se hace una petición a todos los nodos que están a distancia 1. De esta manera, si alguno de los nodos con los que existe comunicación directa son el nodo destino, o tienen un ruta almacenada para alcanzar el nodo destino y se permite el uso de las rutas cacheadas para responder a paquetes RR, se evita la saturación de la red ya que los nodos no retransmiten el paquete RR. En caso de que ninguno de los nodos con distancia 1 pueda responder a la solicitud, el nodo que inicio el RR, volverá a enviar un paquete de descubrimiento de ruta desmarcando la opción Route Request Hop Limits, e iniciando de esta manera un descubrimiento de ruta normal. Existe otra alternativa todavía más conservadora de esta opción que incrementa en una unidad el TTL del paquete cada vez que no obtiene respuesta. Esta opción se asemeja a una búsqueda "circular", ya que partiendo del nodo origen, o central, se va aumentando el radio de búsqueda.

Caching Overheard Routing Information: Mediante esta opción se permite a los nodos "aprender" información de enrutamiento de los paquetes que escuchen en la red aunque no estén dirigidos a ellos. Para poder realizar esto los nodos deberán tener activado el modo promiscuo. De esta manera "escucharán" la red y añadirán la información de enrutamiento de los paquetes que circulan por la red a su Route Cache. Esta opción permitirá a un nodo aprender rutas de una manera indirecta, gracias a la información que circula por la red, y que se reduzcan las solicitudes de descubrimiento de ruta. Por el contrario también obligará a los nodos a procesar un mayor nodo de paquetes, ya que al trabajar en modo promiscuo analizará todos los paquetes, sean ellos los destinatarios o no.

B. Protocolos seguros basados en DSR

Existen diversos protocolos de seguridad basados en DSR [5 – 9]. Vamos a proceder a describir el funcionamiento y las características que añaden al protocolo para dotarlo de seguridad:

ADSR: El protocolo ADSR (Authenticated DSR) [5] emplea criptografía de curvas elípticas y firmas agregadas para añadir la capa de seguridad al protocolo DSR. La distribución de claves se basa en una PKI preestablecida que se ha encargado de entregar los certificados a cada nodo. En el descubrimiento de ruta se añade una firma al mensaje que será verificada por los nodos que lo reciban y, si no son el destino, añadirán su identidad a la lista de nodos intermedios, firmarán el paquete y agregarán su firma a la anterior. Cuando el paquete llegue al nodo destino, este verificará la firma agregada, y, si es correcta, almacenará la ruta y enviará el paquete REP de vuelta al nodo origen, también firmado, por la ruta inversa a la que recibió el RR. Los nodos intermedios de la ruta verificarán la firma anterior y agregarán la suya hasta que el paquete llegue al nodo origen que verificará la firma y, si es correcta, añadirá la ruta a su Route Cache e iniciará la comunicación con el nodo destino.

Al emplear criptografía de curvas elípticas se reduce la longitud de las claves (160 bits para un nivel de seguridad comparable a RSA [26] con 1024 bits), pero aumenta el tiempo de verificación de las firmas. También se emplea el protocolo de firmas agregadas por lo que el campo de firma de los mensajes se mantendrá constante independientemente del número de firmantes.

ARIADNE: El protocolo Ariadne [6] emplea un Message Authenticacion Code (MAC), para que el nodo que recibe un paquete pueda verificar el origen del paquete. Para que esto se pueda llevar a cabo, los nodos deben tener un par de claves compartidas entre cada nodo para poder realizar las verificaciones de los paquetes. Ariadne emplea el protocolo TESLA [27] para implementar el descubrimiento de ruta. Los nodos crean los paquetes RR al iniciar el descubrimiento de ruta hacia el nodo objetivo y calculan un MAC mediante la clave compartida con el nodo destino. Cuando un nodo intermedio recibe un paquete RR y no es el nodo destino, agrega su dirección a la lista de nodos y calcula un nuevo valor de MAC que deberá ser enviado junto con los anteriores. Una vez que el paquete RR alcanza el nodo objetivo, este verifica el contenido del paquete e inicia la respuesta mediante un paquete REP. Envía además el MAC asociado a dicho paquete. Los nodos intermedios retransmitirán el paquete e irán añadiendo las claves intermedias con las que cada uno calculo el valor del MAC asociados a ellos. De esta manera, el nodo origen podrá verificar la validez de todo el paquete y agregar la ruta. El protocolo ARIADNE también admite la opción de emplear digital signatures en lugar de MACs. En este caso el protocolo variaría ya que no será necesario enviar de vuelta las claves intermedias si no que se podría verificar el proceso en cada nodo intermedio.

SDSR: El protocolo Secure DSR (SDSR) [7] emplea criptografía asimétrica para asegurar los paquetes de descubrimiento de ruta (RR y REP). También envía los valores iniciales necesarios para poder establecer una clave de sesión entre los nodos origen y destino mediante el intercambio de claves públicas Diffie-Hellman. Emplea también criptografía simétrica para calcular el testigo con el que se acompaña el descubrimiento de ruta y asegurar que las identidades de los nodos intermedios no han sido modificadas. Al tener que realizar el intercambio de las claves públicas de sesión entre los nodos, y sus correspondientes firmas, el ancho de banda necesario para transmitir el mensaje aumenta conforme aumenta el número de nodos que componen la ruta. El protocolo consume más ancho de banda que otros y aumenta el tiempo de procesado pero consigue establecer ya en el enrutamiento un intercambio de clave de sesión que será empleada por los nodos que van a establecer la comunicación.

SRD: El protocolo Secure Route Discovery [8] emplea criptografía simétrica para asegurar los paquetes de enrutamiento. Cifra todo el paquete de enrutamiento a excepción de la identidad del nodo emisor. De esta manera, empleando un protocolo de identificación de vecinos, distribuye de manera segura los paquetes de enrutamiento a lo largo de la red. Asegura el paquete tanto extremo a extremo como salto a salto mediante dos HMAC. Este último variará salto a salto para poder ser verificada por todos los

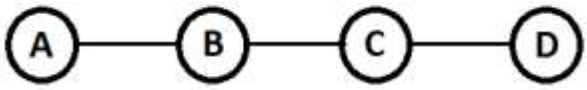


Figura 1.- Red lineal de cuatro nodos

nodos que componen la ruta. Gracias a que realiza un enlace entre los distintos valores enviados por los nodos previos, empleando un hash enlazado, se evita tener que enviar todas las firmas anteriores y un nodo que recibe un paquete REQ puede verificar que el paquete recibido es correcto al enviado dos saltos atrás.

SRDP: El protocolo Secure Route Discovery Protocol (SRDP) [9] es un protocolo genérico que trabaja con un conjunto de primitivas criptográficas basadas en MACs agregadas y otros tipos de firmas susceptibles de ser agregadas. Para los esquemas que emplean MACs se asume la existencia de un mecanismo seguro de distribución de claves. Emplea autenticación backward, por lo que la autenticación de la ruta se realiza únicamente mediante los paquetes REP. Al emplear mecanismos agregados consigue reducir el tamaño de la firma que acompaña a los paquetes de descubrimiento de ruta. Cuando emplea MACs el tiempo de cómputo es bajo ya que emplea mecanismos de firma simétrica.

IV. Impacto de las Características Adicionales en el Rendimiento del Protocolo de Enrutamiento

Para conocer el impacto que tienen en el rendimiento de los protocolos seguros el empleo de las características adicionales primero se debe seleccionar un protocolo en el que puedan ser implementadas. El empleo de estas características es directo en el protocolo original DSR, pero cuando se añade seguridad al protocolo, las nuevas restricciones pueden hacer más complicado el uso de estas características o directamente que no sea compatible su uso.

La premisa de la que se parte en los protocolos seguros para poder emplear las características adicionales es que el nivel de seguridad se vea alterado. El uso de la característica *Route Request Hop Limits* limita el TTL a 1 en su primer intento de realizar el descubrimiento de ruta. Esta opción tiene un impacto muy limitado ya que depende en gran medida de la opción *Replying to Route Requests Using Cached Routes.* Así, si un nodo intermedio de la ruta conoce una ruta para alcanzar el destino, responde al nodo origen con la ruta sin necesidad de esperar a que el paquete de descubrimiento de ruta llegue al destino.

Esta característica, en un protocolo seguro en el que todos los saltos intermedios deben ser validados, implica que un nodo intermedio pueda verificar la ruta del paquete que ha procesado. Este requisito no se cumple en los protocolos que emplean criptografía simétrica entre cada par de nodos. Si los paquetes de enrutamiento se cifran o firman de manera que tan solo los nodos extremos, o los nodos dos a dos, puedan verificar la validez de la ruta, se imposibilita que el resto de nodos intermedios aprendan de manera segura la ruta y que puedan verificarla. Lo mismo ocurre en los protocolos en los que se cifra la información (SRD), los nodos intermedios no pueden extraer ningún tipo de información ya que ni siquiera son capaces de conocer el nodo destino.

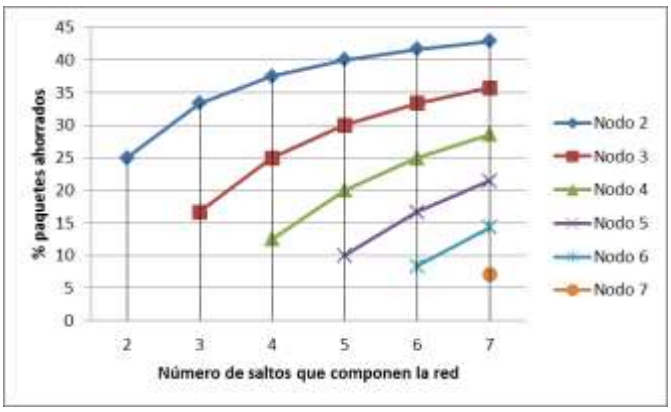


Figura 2.- Porcentaje de paquetes

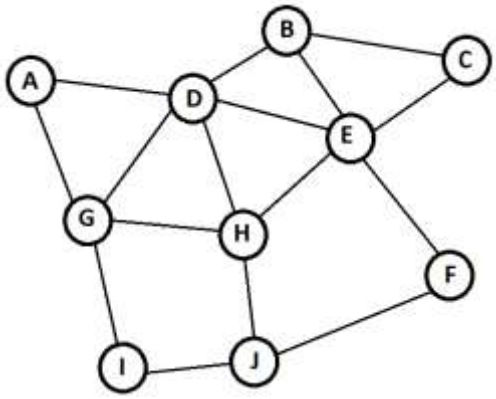


Figura 3.- Red de 10 nodos

Sin embargo, los protocolos que emplean únicamente criptografía asimétrica, donde cualquier nodo que conozca la clave pública de un nodo puede verificar los paquetes que ha firmado, y donde se incluya la firma de todos los nodos que componen la ruta, puede emplear dichos paquetes para retransmitirlos y usarlos para responder a un paquete REQ aunque sea un nodo intermedio.

El protocolo ADSR cumple todos los requisitos anteriores. Emplea únicamente criptografía asimétrica, todos los paquetes que forman parte de la ruta firman el paquete de descubrimiento de ruta y los datos de enrutamiento no están cifrados. Tomando como ejemplo la red de la Fig. 1, si el nodo A inicia el protocolo de descubrimiento de ruta hacia el nodo D se tendría el siguiente intercambio de paquetes, notación detallada en [5]:

A ➔ *broadcast*: RR || [$N_{A,}$ *t*, IP_A, IP_D] K_{MA-}
B ➔ *broadcast*: RR || [$N_{A,}$ *t*, IP_A, IP_D, IP_B] K_{MAB-}
C ➔ *broadcast*: RR || [$N_{A,}$ *t*, IP_A, IP_D, IP_B, IP_C] K_{MABC-}
D ➔ *C*: REP || [$N_{D,}$ *t*, IP_D, IP_A, IP_B, IP_C] K_{MD-}
C ➔ *B*: REP || [$N_{D,}$ *t*, IP_D, IP_A, IP_B, IP_C, IP_C] K_{MDC-}
B ➔ *A*: REP || [$N_{D,}$ *t*, IP_D, IP_A, IP_B, IP_C, IP_B] K_{MDCB-}

Mientras que si se habilitase la opción *Replying to Route Requests Using Cached Routes* y el nodo B conociese una la ruta para alcanzar el nodo D, los paquetes que habría que enviar se reducirían a:

A ➔ *broadcast*: RR || [$N_{A,}$ *t*, IP_A, IP_X] K_{MA-}
B ➔ *A*: REPC || [$N_{B,}$ *t*, IP_B, IP_A [*CR*]] $K_{MB\&CRnodes-}$
B ➔ C: REPC || [$N_{B,}$ *t*, IP_B, IP_A [*CR*]] $K_{MB\&CRnodes-}$
C ➔ *D*: REPC || [$N_{B,}$ *t*, IP_B, IP_A [*CR*]] $K_{MB\&CRnodes-}$

El nodo B al conocer una ruta para alcanzar el nodo D envía un paquete con la ruta cacheada (REPC) tanto al nodo origen A como al nodo destino, ya que puede ser que el nodo destino tampoco conozca la manera de alcanzar el nodo origen y las rutas tienen que estar aseguradas por la firma de todos los nodos intermedios. En la Fig. 2 podemos ver los resultado obtenidos al emplear la opción en una red lineal formada por 8 nodos cuando son los responden los distintos nodos intermedios. Los datos obtenidos reducen siempre el número de paquetes necesarios para establecer la comunicación, lo cual reduce la saturación del espectro.

Si se realiza la misma prueba en una red un poco más compleja se aprecia que los resultados obtenidos también mejoran al resultado inicial. Partiendo de la red mostrada en la Figura 3, el nodo A inicia un descubrimiento de ruta hasta alcanzar el nodo F. Hay que recordar que un nodo no procesa dos veces el mismo paquete de descubrimiento de ruta. Es decir, cada nodo mantiene una tabla en la que se almacenan los paquetes REQ procesados previamente identificándolos mediante los datos nodo origen – nodo destino - número de secuencia. Antes de procesar el paquete verifica que el identificador relacionado con el nodo origen es mayor que el que tiene almacenado y que ha pasado un tiempo predeterminado desde la última búsqueda de ruta de ese nodo origen para el nodo destino indicado.

En la Tabla 1 se muestran los valores obtenidos para esta red. Se indican tanto el número de paquetes que recorren la red como el tiempo necesario para iniciarse la comunicación, cuantificado en el número de saltos intermedios necesarios para realizar la comunicación.

Las rutas que se establecen son dos: A-D-E-F y A-G-I-J-F. Se muestra también que cuando se emplea el protocolo de descubrimiento de ruta se consigue una mejora en el rendimiento del protocolo que puede ir desde un 25% de paquetes que son enviados por los nodos y también conseguir reducir el número de saltos intermedios necesarios para que el nodo origen conozca la ruta a emplear y pueda empezar la transmisión de los paquetes de datos. Este tiempo se reduce, en el mejor de los casos, de requerir 6 saltos en el protocolo original a necesitar únicamente 2 saltos, algo que también es interesante porque reduce en gran medida el tiempo necesario para establecer la comunicación.

Las mejoras que se obtienen al permitir a los nodos intermedios responder con una ruta cacheada, sin reducir la seguridad del protocolo, dependerán en gran medida de la topología de la red y de los nodos que realizan el descubrimiento de ruta.

Si en el ejemplo anterior el nodo A iniciase un descubrimiento de ruta hacia el nodo J, se descubrirían tres rutas distintas: A-D-H-J; A-G-I-J; y A-D-E-F-J. En este caso, serían necesarios 19 paquetes para que la red procesase por completo el paquete de descubrimiento de ruta. Sin embargo, incluso siendo mayor el número de paquetes que se necesitaría en el protocolo original, si el nodo D respondiese con la ruta cacheada A-D-H-J al nodo origen, el número de paquetes que procesaría la red serían nueve, consiguiendo un

Tabla 1.- Paquetes transmitidos por la red para realizar el descubrimiento de ruta

Nodo intermedio que responde con una ruta cacheada	Paquetes necesarios	% paquetes ahorrados	Saltos necesarios para iniciar la comunicación	Rutas descubiertas
Protocolo original	16	0	6	A-D-E-F; A-G-I-J-F
Nodo D	12	25	2	A-D-E-F; A-G-I-J-F
Nodo E	15	6.25	4	A-D-E-F; A-G-I-J-F
Nodo G	13	18.75	2	A-D-E-F; A-G-I-J-F
Nodo I	14	12.5	4	A-D-E-F; A-G-I-J-F
Nodo J	15	6.25	6	A-D-E-F; A-G-I-J-F

ahorro mayor a un 52% de paquetes que circulan por la red y reduciendo a dos el número de saltos para que el nodo A pudiese iniciar la comunicación con el nodo destino, lo que conllevaría un importante ahorro en tiempo.

Como contrapunto, la ruta A-D-E-F-J no llegaría a ser descubierta por el nodo A. Esto se debe a que el nodo D no propaga en modo broadcast el paquete REPC que contiene la ruta cacheada sino que emplea una transmisión unicast. De esta manera se consigue que el número de paquetes que la red necesita para procesar por completo el paquete de descubrimiento de ruta se reduzca a menos de la mitad de los necesarios inicialmente.

Otro de los resultados que pueden llamar la atención se da cuando el nodo D responde con la ruta cacheada A-D-E-F-J. En este caso, al nodo H le llega el paquete de descubrimiento de ruta no desde el nodo D, como en el protocolo original, sino desde el nodo G. De esta manera, se descubre una nueva ruta A-G-H-J, que antes quedaba enmascarado por la ruta A-D-H-J. En la Tabla 2 se muestra el resto de los resultados que se obtendrían al realizar este descubrimiento de ruta.

Con estos dos ejemplos se muestra que el empleo de la opción *Replying to Route Requests Using Cached Routes* reduce el número de paquetes necesarios para procesar los paquetes de descubrimiento de ruta. Cuanto más cercano al nodo origen esté el nodo que responde con la ruta cacheada, mejores resultados se obtendrá. De todos modos, en el peor de los casos, cuando el nodo que responde es el inmediatamente anterior al nodo destino, el número de paquetes se reduce en una unidad. Además, a parte de reducir el número de paquetes que tiene que procesar la red, también se reduce el tiempo necesario para establecer la comunicación. Habrá redes en las que las que sea primordial que la comunicación se establezca de la manera más rápida posible, ya sea por la necesidad de que la comunicación sea en tiempo real o porque exista una alta movilidad de los nodos de manera que la disponibilidad de los nodos sea muy reducida en el tiempo. Además, en el caso del protocolo estudiado, tal y como se muestra en [5], el tiempo de descubrimiento de ruta aumenta considerablemente conforme aumenta el número de nodos intermedios.

Otro aspecto muy relevante que afecta al empleo de las rutas cacheadas es durante cuánto tiempo es válida una ruta. Este dato dependerá de la red en la que se estén desarrollando las comunicaciones ya que si existe una alta movilidad, el tiempo de almacenamiento de las rutas en la tabla de rutas cacheadas deberá ser menor que si la movilidad de los nodos en la red es más limitada. De todas maneras, este hecho afectará al protocolo de descubrimiento de ruta se empleen o no se empleen las características adicionales que ofrece el protocolo DSR ya que en el protocolo básico de descubrimiento de ruta, puede ocurrir que un nodo se desplace después de que se haya completado el descubrimiento de ruta y haya que volver a iniciarlo para poder establecer una comunicación entre los nodos origen y destino.

V. Conclusiones

El desarrollo de los protocolos de enrutamiento seguro para redes MANET era un desarrollo necesario. Los protocolos originales en los que se suelen basarse los protocolos seguros, incluyen una serie de posibilidades de enrutamiento que, al añadir la capa de seguridad, pueden no ser usadas por los protocolos seguros. Este hecho hace que el impacto sobre el rendimiento del protocolo de enrutamiento vaya más allá del estrictamente necesario al añadir la capa de seguridad.

El protocolo ADSR es uno de los protocolos de enrutamiento seguro basado en DSR. La peculiaridad de este protocolo seguro respecto a otros protocolos es que el diseño original del mismo se planteó para que se pudiesen implementar la mayor cantidad posible de posibilidades del protocolo DSR. De esta manera se ha mostrado como el empleo de la característica adicional *Replying to Route Requests Using Cached Routes*, permite que el rendimiento del protocolo se acerque más al del protocolo original, todo esto sin reducir el nivel de seguridad que aporta el protocolo ADSR en su funcionamiento original.

Los resultados han mostrado que se puede reducir tanto el número de paquetes necesarios que deben ser procesados por la red como el tiempo necesario para que el nodo origen conozca la ruta que le permita establecer la comunicación con el nodo destino.

Como futura línea de trabajo se están desarrollando las medidas posibles que se pueden realizar para reducir el impacto de la seguridad en el rendimiento de otros protocolos de enrutamiento seguro para MANETs. Así como realizar un estudio mayor de casos en los que se pueda apreciar el efecto de la movilidad de los nodos en la caducidad de las rutas almacenadas en la tabla de rutas cacheadas y como afecta esto al rendimiento del protocolo.

Tabla 2.- Paquetes transmitidos por la red para realizar el descubrimiento de ruta

Nodo intermedio que responde con una ruta cacheada / ruta	Paquetes necesarios	% paquetes ahorrados	Saltos necesarios para iniciar la comunicación	Rutas descubiertas
Protocolo original	19	0	6	[A-D-H-J]; [A-G-I-J]; [A-D-E-F-J]
Nodo D / A-D-H-J	9	52.63	2	[A-D-H-J]; [A-G-I-J]
Nodo H / A-D-H-J	18	5.26	4	[A-D-H-J]; [A-G-I-J]; [A-D-E-F-J]
Nodo G / A-G-I-J	17	10.52	2	[A-D-H-J]; [A-G-I-J]; [A-D-E-F-J]
Nodo I / A-G-I-J	18	5.26	4	[A-D-H-J]; [A-G-I-J]; [A-D-E-F-J]
Nodo D / A-D-E-F-J	14	26.31	2	[A-G-H-J]; [A-G-I-J]; [A-D-E-F-J]
Nodo E / A-D-E-F-J	17	10.52	4	[A-D-H-J]; [A-G-I-J]; [A-D-E-F-J]
Nodo F / A-D-E-F-J	18	5.26	6	[A-D-H-J]; [A-G-I-J]; [A-D-E-F-J]

AGRADECIMIENTOS

Este trabajo ha sido parcialmente subvencionado por el proyecto CPUFLIPI (MICINN TIN2010-17298) del Gobierno de España, la Cátedra Telefónica-Universidad de Zaragoza y el Fondo Social Europeo en colaboración con el Gobierno de Aragón.

REFERENCIAS

[1] Royer, E.M. and Toh, C.-K. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, 6 (2) (1999), pp. 46–55

[2] Abolhasan, M., Wysocki, T., Dutkiewicz, E. A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, 2 (1) (2004), pp. 1–22

[3] Boukerche, A., Turgut, B., Aydin, N., Ahmad, M., Boloni, L., Turgut, D. Routing Protocols in Ad Hoc Networks: A survey. *Computer Networks* (55), 2011, pp 3032-3072.

[4] Argyroudis, P. G. and O'Mahony, D. Secure Routing for Mobile Ad Hoc Networks. *IEEE Commun.Surveys & Tutorials*, (7) (3) 2005, pp.2–21.

[5] Tornos, J.L., Piles, J.J. and Salazar, J.L. ADSR: Authenticated DSR. *6th International Conference on Risk and Security of Internet and Systems (CRiSIS), 2011*, pp.1-8,

[6] Hu, Y.C., Perrig, A. and Johnson, D.B. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Proceedings of the 8th annual international conference on Mobile computing and networking*, ACM Press, 2002, MobiCom, pp. 12–23.

[7] Kargl, F., Geiβ, A., Schlott, S. and Weber, M. Secure Dynamic Source Routing. *Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS'05).* 2005.

[8] Sivakumar K.A. and Ramkumar M.: An Efficient Secure Route Discovery Protocol for DSR, IEEE Globecom (2007), pp. 458 - 463

[9] Kim, J., Tsudik, G. SRDP: Secure route discovery for dynamic source routing in MANETs. *Ad Hoc Networks, Volume 7, Issue 6.* 2009, pp. 1097-1109.

[10] Johnson, D.B., Maltz, D.A. Imielinski, Korth. Dynamic source routing in ad hoc wireless networks. *Mobile Computing*. Volume 353. Kluwer Academic Publishers. 1996.

[11] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., Belding-Royer, E.M. A secure routing protocol for ad hoc networks. *10th IEEE International Conference on Network Protocols.* 2002, pp. 78-89.

[12] Zapata, M.G., Asokan, N. Securing ad hoc routing protocols. *3rd ACM workshop on Wireless security (WiSE '02)*, 2002, pp, 1-10.

[13] Li, Q., Zhao, M., Walker, J., Hu, Y-C., Perrig, A., Trappe, W. SEAR: a secure efficient *ad hoc* on demand routing protocol for wireless networks. *Security and Communication Networks* Volume 2, Issue 4, 2009, pp 325–340.

[14] Perkins, C.E., Royer, E.M. Ad-hoc on-demand distance vector routing. Proceedings of the *Second IEEE Workshop on Mobile Computer Systems and Applications (WMCSA*), IEEE Computer Society, 1999, pages. 90–100.

[15] Hu, Y.-C., Johnson, D. B., Perrig, A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1, (2003), pp. 175-192.

[16] Perkins, C.E., Bhagwat, P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *Proceedings of the conference on Communications architectures, protocols and applications*, ACM Press (SIGCOMM), 1994, pp. 234–244

[17] Hafslund, A., Tonnesen, A., Rotvik, R.B., Andersson, J. and Kure, O. Secure extension to the OLSR protocol. *OLSR Interop and Workshop*, 2004, pp. 1–4.

[18] Jacquet, P., Muhlethaler, P., Clausen, T.; Laouiti, A., Qayyum, A., Viennot, L. Optimized link state routing protocol for ad hoc networks. *IEEE INMIC 2001*. pp. 62- 68.

[19] Adams, C. and Lloyd, S.: "Understanding Public-Key Infrastructure – Concepts, Standards, and Deployment Considerations". Macmillan, Indianapolis (1999)

[20] Haas, Z., Pearlman, M. and Samar, P. The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft, July 2002.

[21] Chiang, C.-C., Wu, H.K., Liu, W. Gerla, M. Routing in clustered multihop mobile wireless networks with fading channel. *IEEE SICON_97*, 1997, pp. 197–211.

[22] Nasipuri A., Castaneda, R. and Das, S.R. "Performance of multipath routing for on-demand protocols in mobile ad hoc networks", *ACM/Kluwer Mobile Networks and Applications (MONET*), vol. 6, no. 4, pp.339 -349 2001

[23] Leung, R., Liu, J., Poon, E., Chan, A.-L.C., Li, B.: MP-DSR: A QoS-aware Multi- path Dynamic Source Routing Protocol for Wireless Ad-hoc Networks. Proceedings of the 26th IEEE Annual Conference on Local Computer Networks (2001) 132-141

[24] Park, V., Corson, M. A highly adaptive distributed routing algorithm for mobile wireless networks. *Proceedings of the Conference on Computer Communications Infocom* 1997, pp. 1405-1413.

[25] David B. Johnson, Yih-Chun Hu, and David A. Maltz, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. Internet Request for Comments 4728. 2007.

[26] Rivest, R. L., Shamir, A., Adleman, L. A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, v.21 n.2, pp.120-126. 1978.

[27] Perrig, A., Canetti, R., Tygar, J.D., Song, D. Efficient authentication and signing of multicast streams over lossy channels. *IEEE Symposium on Security and Privacy* 2000 pp. 56–73.

Aplicación de EDA en datos de redes de comunicación

Elena Jiménez Mañas, José Camacho-Páez, Jesús E. Díaz-Verdejo
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada
C/Periodista Daniel Saucedo Aranda s/n - 18071
elenajm@correo.ugr.es, josecamacho@ugr.es, jedv@ugr.es

***Resumen*- Las técnicas de análisis exploratorio de datos (EDA) constituyen una potente herramienta para el análisis de las características y propiedades de conjuntos de datos, siendo recomendable su utilización como paso previo en problemas de detección de anomalías, clasificación y optimización, entre otros. En particular, resultan de interés para analizar el tráfico capturado en una red. Para facilitar la aplicación de estas técnicas se ha desarrollado una herramienta software, EDA 2.0, cuya aplicación se describe en el presente artículo. Este software se ha diseñado teniendo como objetivo principal su sencillez de uso, de forma que el usuario solo tendrá que interpretar las gráficas proporcionadas, pudiendo trabajar con una gran variedad de problemas y situaciones de diferente naturaleza. Se ha desarrollado también una interfaz gráfica que facilita aún más su utilización. Las capacidades de la técnica EDA y de la herramienta se muestran en un caso de estudio centrado en el análisis de un conjunto de datos formado por el tráfico generado en una red de comunicaciones.**

***Palabras Clave*-análisis exploratorio de datos, componentes principales, análisis por componentes principales.**

I. INTRODUCCIÓN

Son múltiples los escenarios en los que se dispone de un conjunto de datos que deben ser modelados o representados de alguna forma compacta como parte del proceso a realizar para resolver un problema. A modo de ejemplo, la detección de anomalías en el tráfico de red puede abordarse a partir del establecimiento de un modelo de tráfico normal y la evaluación de las desviaciones respecto del mismo. El modelo se establecería a partir de un conjunto de datos bidimensional, con N observaciones (p.e. flujos de tráfico, paquetes, intervalos temporales de muestreo, …) sobre M variables (estadísticas, características calculadas, …), compuesto por el tráfico capturado en un escenario libre de anomalías. Las técnicas para establecer el modelo pueden ser de muy diversa naturaleza y complejidad [1], pudiendo incluir técnicas relativamente simples, como un modelado estadístico de algunas variables, o realmente complejas, como la aplicación de técnicas de agrupamiento, redes neuronales, etc. En la aproximación habitual, los investigadores seleccionan una técnica válida y evalúan su rendimiento cuando se aplica al escenario considerado. Esta aproximación, que podríamos denominar "ciega", puede considerarse, en cierta medida, una aproximación de prueba y error, ya que se evalúan diferentes técnicas a fin de seleccionar la que proporcione mejores resultados.

Aunque esta metodología es válida y extensamente utilizada, genera algunos problemas con la generalización de las soluciones y resulta altamente costosa. Una aproximación más adecuada incluiría una fase previa de análisis y caracterización de las propiedades del o de los conjuntos de datos sobre los que se trabaja, a fin de determinar qué soluciones tecnológicas resultan más adecuadas a priori. Así, p.e., si existiese una variable cuyos valores fuesen claramente diferentes en el caso de una anomalía, un simple detector de umbral sobre esa variable podría ser suficiente para detectar la ocurrencia de anomalías.

El análisis exploratorio de datos (Exploratory Data Analysis, EDA) proporciona un conjunto de técnicas y herramientas que permiten analizar las propiedades de un conjunto de datos. El EDA sobre conjuntos de datos de alta dimensionalidad (gran número de variables) se basa principalmente en modelos de proyección, como son el Análisis por Componentes Principales (Principal Component Analysis, PCA) [2] y los Mínimos Cuadrados Parciales (Partial Least Squares, PLS) [3]. Dichos modelos permiten comprimir el conjunto de variables originales de los datos en un conjunto mucho más reducido, denominadas variables latentes. La transformación de los datos a estas variables latentes permite simplificar mucho la visualización e interpretación de los mismos, facilitando la identificación de patrones. Finalmente, dichos patrones pueden ser de gran utilidad para abordar un problema de clasificación, optimización, etc.

A pesar de su clara utilidad, estas técnicas no son empleadas habitualmente debido a la complejidad asociada y a la ausencia de herramientas automatizadas que faciliten esta labor. Por este motivo, se ha desarrollado una herramienta software basada en Matlab que implementa las funcionalidades requeridas para EDA, proporcionando las gráficas correspondientes a la aplicación de las diversas técnicas sobre un conjunto de datos. A fin de facilitar aún más la tarea, se ha desarrollado también una interfaz gráfica de muy fácil utilización. De esta forma, el investigador o analista únicamente debe centrarse en la interpretación de las gráficas obtenidas, ocultándose así los detalles de las técnicas utilizadas.

En el presente artículo se describe brevemente la herramienta y se aplica a un caso de estudio en el que se analiza el tráfico capturado en una red.

La estructura del artículo se indica a continuación. En primer lugar, en la Sección II se describe la herramienta desarrollada

y se relacionan las técnicas que implementa. A continuación, en la Sección III, se presenta el escenario experimental así como las características más relevantes del tráfico capturado. En la Sección IV se ilustra el uso de la metodología EDA mediante PCA en el marco del análisis forense en red, mediante la aplicación de la herramienta desarrollada. Finalmente, en la Sección V se presentan las conclusiones del presente trabajo así como algunas indicaciones respecto del trabajo futuro.

II. Trabajos Relacionados

Los modelos multivariantes como PCA o PLS poseen dos características que los hace especialmente interesantes para el análisis de datos en redes de comunicación: permiten el manejo de conjuntos de datos de alta dimensión y permiten la identificación de patrones en los datos, con especial sensibilidad para la detección de anómalos.

La capacidad de tratar datos de alta dimensión es fundamental para combinar un gran número de variables o características de distintas y variadas fuentes (tráfico, logs de firewalls, IPS/IDS o sistemas, etc.) En comparación, otras herramientas de análisis están limitadas a una variable o un número reducido de variables medidas en el tiempo [4]. Adicionalmente, las técnicas de visualización suelen ser muy específicas para el tipo de datos analizado (por ejemplo, trazas de tráfico en red) [5]. Por otro lado, si bien el uso de técnicas como PCA no es nuevo en el análisis y detección de anomalías en tráfico [6,7], su empleo automático en la detección tiene importantes limitaciones [8]. La propuesta de este artículo no es el uso de PCA y técnicas asociadas para la detección automática de anomalías, sino para la visualización y análisis de los datos, donde podemos encontrar su mayor potencial.

En el contexto de EDA, PCA y PLS se utilizan en combinación con un conjunto de herramientas para la detección de anomalías, grupos de observaciones, grupos de variables y relaciones entre observaciones y variables. Las herramientas más utilizadas en este contexto son los gráficos de dispersión de puntuaciones (score plots), los gráficos de dispersión de cargas (loading plots) y los gráficos combinados (biplots) [9]. Sin embargo, recientes estudios demuestran que estas herramientas tienen importantes limitaciones, con el potencial riesgo de equivocar al analista [10,11]. En [12], se propone una estrategia EDA basada principalmente en tres herramientas: scores plot, MEDA (Missing Data Methods for Exploratory Data Analysis) [10] y oMEDA (observation-based MEDA) [11]. Dicho trabajo es el germen a partir del cual ha sido desarrollada la herramienta EDA 2.0.

III. La Herramienta EDA 2.0

A continuación se describen las técnicas implementadas y el funcionamiento de la herramienta EDA 2.0, descargable de http://wdb.ugr.es/~josecamacho/downloads.php.

Las principales técnicas para el análisis exploratorio de datos son los *modelos de proyección*: PCA y PLS. Ambos modelos de proyección pretenden solucionar el problema que supone la colinealidad de los datos, presente en la mayoría de conjuntos de datos de gran dimensión. La elección de uno u otro modelo de proyección, PCA o PLS, dependerá de la naturaleza del problema a tratar. De cualquier forma, cabe señalar que PCA resulta más adecuado en problemas no supervisados mientras que PLS se emplea en problemas supervisados.

En el contexto de los modelos de proyección se utilizan diversas herramientas para la visualización de los datos y resultados. En la herramienta software desarrollada, EDA 2.0, se han incluido las siguientes:

- ***Score Plots* [9].** Los gráficos de dispersión de puntuaciones o *score plots* son de gran utilidad en el análisis exploratorio de datos. Estos gráficos son una herramienta de visualización que muestra la distribución espacial del conjunto de observaciones. Para ello se representa en una gráfica de 2 dimensiones una variable latente frente a otra, dando lugar a la representación gráfica de la distribución de las observaciones. Esta representación permitirá advertir la distribución de los datos del conjunto y la consecuente existencia de tendencias, patrones, *clusters*, *outliers*, etc.
- ***Loading Plots* [9]**. Los gráficos de cargas o *loading plots* son de aspecto similares a los anteriores *score plots*. La principal diferencia estriba en que, en este caso, se representa la distribución espacial de las variables originales del conjunto. De nuevo, se trata de un gráfico bidimensional donde cada uno de sus dos ejes representa una variable latente.
- ***MEDA* [10].** La herramienta MEDA permite mostrar en un sencillo gráfico el grado de relación que existe entre las variables que caracterizan a las observaciones de un conjunto de datos. La relación entre variables se obtiene calculando un índice que permite estimar una relación de carácter predictivo entre cada par de variables del conjunto de datos. Dicha relación permite distinguir mejor entre estructura y ruido que el cálculo estándar de la correlación. El gráfico MEDA está formado por una cuadrícula detamaño *MxM* siendo *M* el número de variables del conjunto de datos. Cada cuadro corresponde a la relación entre un par de variables. Según el color de la cuadrícula correspondiente, las variables estarán más o menos correlacionadas. De esta forma la relación varía de 1 a -1 según la intensidad del color y si la relación es directa o inversa.
- ***oMEDA* [11].** Esta herramienta es una variante de la anterior que pretende relacionar entre sí observaciones y variables. El interés se centra en descubrir qué variables, y con qué peso, influyen sobre determinados patrones (tendencias, *clusters*, *outliers*, etc.) en las observaciones.
- ***Squared Residuals* [9].** Consiste en la representación gráfica (gráfico de barras) de los residuos tanto de las observaciones como de las variables. Se representa la suma cuadrática de residuos. El residuo corresponde a la variabilidad que no se ha incluido en el modelo. Por tanto, en aquellas observaciones/variables donde se observe un residuo alto se deduce que no siguen el modelo establecido.

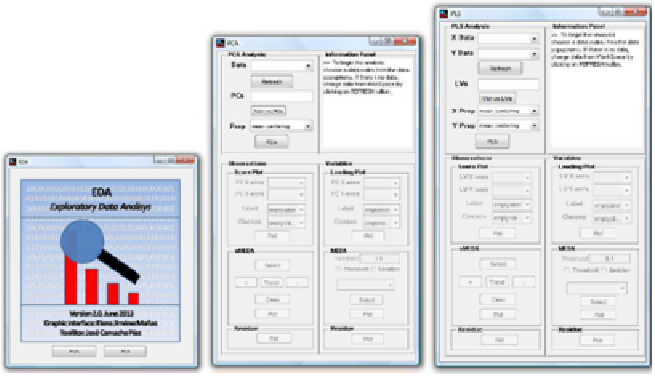


Fig. 1. Interfaces gráficas que forman la herramienta EDA 2.0

Además de las herramientas indicadas, se incluyen funciones complementarias para la normalización y preprocesamiento de los datos, de gran utilidad en el desarrollo de un EDA.

Interfaz gráfica

Junto con las funciones para el análisis y visualización indicadas previamente, se ha desarrollado una interfaz gráfica para facilitar su utilización. Ésta, a su vez, está constituida por tres interfaces gráficas, llamadas EDA, PCA y PLS respectivamente (véase la Fig.1). Como característica más reseñable hemos de indicar que las interfaces permiten una fácil selección de los parámetros/funciones/opciones posibles en cada herramienta de las mencionadas en el apartado anterior. Así, el usuario sólo tendrá que seleccionar de un menú desplegable una de las opciones posibles en cada escenario concreto. Por tanto, puede centrar toda su atención en el análisis de las gráficas que vaya proporcionando el sistema en lugar de tener que ocuparse de ejecutar las secuencias de comandos con todas sus opciones.

El procedimiento estándar de uso de la herramienta es el siguiente. El analista parte del conjunto de datos disponible, posiblemente formado por diversas fuentes como tráfico en red, logs de IDS y firewalls, syslog, SNMP, etc. Estos datos son convertidos en una matriz bidimensional que contiene un conjunto de observaciones, típicamente ordenadas en el tiempo, de un conjunto de variables o características. Por poner un ejemplo, las observaciones pueden corresponder a intervalos de muestreo en el tiempo y las variables al número de veces que ocurre algún evento reseñable durante ese intervalo (por ejemplo, número de paquetes ICMP, número de accesos al puerto 465, etc.) Estos datos se visualizan con la herramienta, con lo que podemos detectar relaciones entre variables y observaciones que nos permitan dilucidar los episodios comunes y anómalos que tienen lugar en nuestra red.

IV. Caso de estudio: Anomalías en tráfico de red

Para ilustrar de forma sencilla las capacidades de la herramienta y cómo se realizaría un análisis de un conjunto de datos con la misma se ha considerado un escenario simplificado consistente en la caracterización del tráfico normal observado en una red y la detección de anomalías. Para el lector interesado, otros ejemplos aparecen disponibles en http://wdb.ugr.es/~josecamacho/downloads.php.

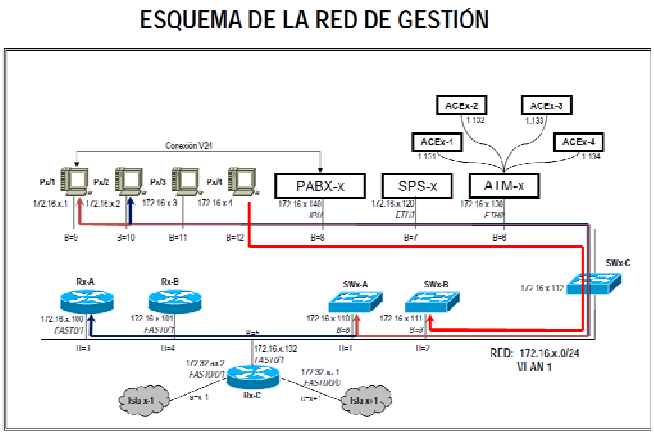


Fig. 2. Diagrama de red de una de las tres redes del laboratorio y flujos generados por el trabajo de los estudiantes (Estudiante 1 en marrón y Estudiante 2 en azul) y ataques *Neptune* (en rojo). La interfaz n del *switch* C se representa por B=n bajo las líneas horizontales del esquema. Las interfaces correspondientes de los *switches* A y B conectados al *switch* C también se muestran.

Los datos a analizar fueron capturados en el laboratorio de redes de la ETS de Ingenierías Informática y Telecomunicación de la Universidad de Granada [7] durante una sesión de prácticas de 2 horas de la asignatura Gestión de Redes. Esta asignatura corresponde al grado en Ingeniería de Telecomunicaciones de la Universidad de Granada. Durante la sesión monitorizada, los estudiantes estaban configurando el sondeo (*polling*) y los avisos (*traps*) del protocolo *Simple Network Managment Protocol* (SNMP) en dispositivos conmutadores y encaminadores *Cisco*[1].

El laboratorio de telemática está formado por 24 puestos de trabajo, todos ellos conectados a las 3 redes configuradas en el laboratorio (Fig. 2). Los 24 puestos se organizan en 6 islas de 4 terminales cada una. Las islas están numeradas de la 1 a la 6, y están preparadas para funcionar de forma independiente del resto de islas. Los 4 puestos de trabajo de una isla se etiquetan como Px/1, Px/2, Px/3 y Px/4, donde x se refiere al número de isla. Cada isla dispone de tres interfaces de red conectadas a las tres redes disponibles. Además cada isla dispone de una serie de dispositivos de interconexión como son: tres encaminadores (routers) Cisco 1841, designados como Rx-A, Rx-B y Rx-C, tres conmutadores (switches) Catalyst 2950, designados como SWx-A, SWx-B y SWx-C, además de dispositivos ATM, FrameRelay, X.25, PBX, etc. Una descripción más detallada del laboratorio puede encontrarse en [14].

Durante parte de la sesión de laboratorio se capturó información SNMP de los conmutadores de la isla 4 en intervalos de un minuto, utilizando para ello el comando *snmpwalk* [15]. Los datos capturados corresponden a los

[1] Si bien por simplicidad en la introducción de la herramienta, en este ejemplo no se han combinado datos de diversas fuentes, entre los ejemplo disponibles para su descarga se encuentran análisis de datos más complejos, como son los datos del VAST Challenge 2012 [13], donde se combinan datos de firewall, IDS y tráfico.

octetos de entrada y salida de las 14 interfaces de los tres conmutadores de la isla 4. Durante la captura de datos, únicamente dos estudiantes se encontraban trabajando en la isla. El Estudiante 1, en el puesto de trabajo P4/1, estaba configurando vía telnet el conmutador SW4-A. El Estudiante 2, en el puesto de trabajo P4/2, estaba configurando, también vía telnet, el encaminador R4-A. Además, durante ciertos intervalos de tiempo a lo largo de la práctica, se realizaron ataques *Neptune* (*SYN flooding*) al SW4-C desde el puesto de trabajo P4/4. El experimento no influyó en ningún momento sobre el trabajo de los alumnos.

Tabla I. VARIABLES SNMP OBTENIDAS CON EL COMANDO *SNMPWALK* DE LOS TRES CONMUTADORES DE LA ISLA 4.

Núm. variable	Nombre	Núm. variable	Nombre	Núm. variable	Nombre
1	A.ifIn1	18	B.ifIn9	35	C.ifIn9
2	A.ifIn2	19	B.ifIn10	36	C.ifIn10
3	A.ifIn8	20	B.ifIn4	37	C.ifIn12
4	A.ifIn14	21	B.ifOut1	38	C.ifIn14
5	A.ifOut1	22	B.ifOut2	39	C.ifOut1
6	A.ifOut2	23	B.ifOut3	40	C.ifOut2
7	A.ifOut3	24	B.ifOut4	41	C.ifOut3
8	A.ifOut4	25	B.ifOut8	42	C.ifOut4
9	A.ifOut8	26	B.ifOut9	43	C.ifOut5
10	A.ifOut9	27	B.ifOut10	44	C.ifOut7
11	A.ifOut10	28	B.ifOut11	45	C.ifOut9
12	A.ifOut11	29	B.ifOut12	46	C.ifOut10
13	A.ifOut12	30	B.ifOut14	47	C.ifOut11
14	A.ifOut14	31	C.ifIn1	48	C.ifOut12
15	B.ifIn1	32	C.ifIn2	49	C.ifOut14
16	B.ifIn2	33	C.ifIn3		
17	B.ifIn8	34	C.ifIn5		

Durante la captura se obtuvieron un total de 108 observaciones sobre 84 variables. Tras procesar los datos para calcular incrementos en los contadores y eliminar variables que no representaban tráfico, quedaron un total de 101 observaciones sobre 49 variables. Las 101 observaciones se dividen en dos conjuntos de datos. El primero de ellos, con 48 observaciones, está constituido solo por tráfico normal y se utilizará para el EDA inicial. El segundo conjunto de datos a considerar contiene 53 observaciones e incluye tráfico normal y ataques *Neptune*. La lista de variables consideradas se muestra en la Tabla I.

V. Análisis del tráfico

El objetivo del experimento es ilustrar el correcto funcionamiento de la interfaz gráfica PCA basada en la metodología EDA para detectar anomalías y para interpretar e identificar el origen del tráfico. En particular para llevar a cabo un análisis forense en red con el objetivo de detectar el origen de los ataques. La metodología EDA se utiliza teniendo en cuenta el contexto en el que se desarrolla el análisis, para poder interpretar de forma adecuada los resultados. En este ejemplo la interpretación de las gráficas proporcionadas por las herramientas EDA se llevará a cabo considerando la red presente en la Fig.2.

A. Modelo PCA

Para obtener el modelo PCA a partir del conjunto de calibración es necesario, en primer lugar, seleccionar el número de variables latentes, llamadas componentes principales (Principal Components o PCs) en el contexto de PCA, de forma que se capture gran parte de la variabilidad. Para ello, EDA 2.0 permite obtener una gráfica con la variabilidad residual según el número de componentes principales consideradas para el modelo. El gráfico obtenido (Fig.3) muestra que con las 2 primeras componentes principales se captura aproximadamente el 90% de la variabilidad. De aquí se deduce que las 49 variables que componen el conjunto de datos con el que se trabaja (Tabla I) están muy correlacionadas, ya que con tan sólo dos componentes se captura la mayor parte de la variabilidad del modelo. Por tanto la información puede comprimirse de forma efectiva para simplificar la visualización. Adicionalmente, las siguientes componentes capturan bastante menos porcentaje de variabilidad, por lo que en principio las dos primeras componentes parecen ser las más relevantes para el EDA. Si bien en este ejemplo nos centraremos en investigar dichas componentes, EDAs más detallados podrían incluir el análisis individual de otros componentes.

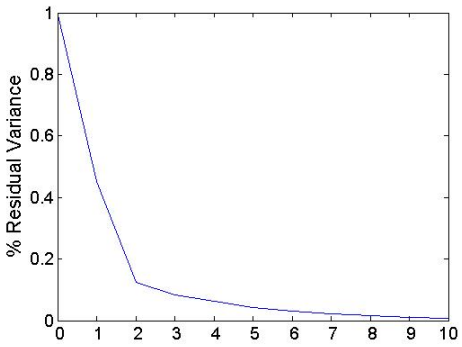


Fig. 3. Variabilidad capturada para 10 componentes.

B. Análisis de las variables

En este punto, es posible centrarse en el estudio de las variables o bien de las observaciones a partir del modelo PCA. En este ejemplo concreto, en primer lugar, se estudian las variables que caracterizan al conjunto de datos. Para ello se obtiene el gráfico de cargas o *Loading Plot* (Fig. 4) en el que nos centramos en los puntos lejanos al origen de coordenadas. Descartaremos las variables cercanas al origen, lo que denota baja variabilidad y, por tanto, ausencia de información de interés en el diagrama. En la Fig. 4. resulta

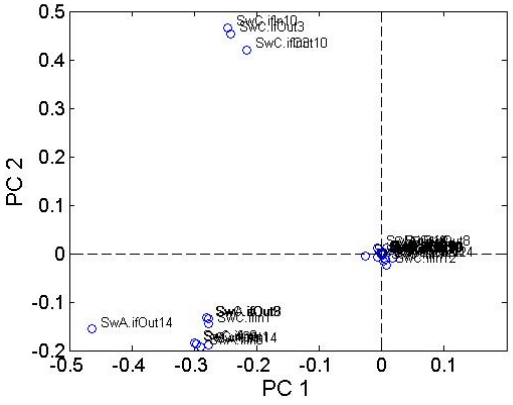


Fig. 4.*Loading Plot* de PC1 vs PC2.

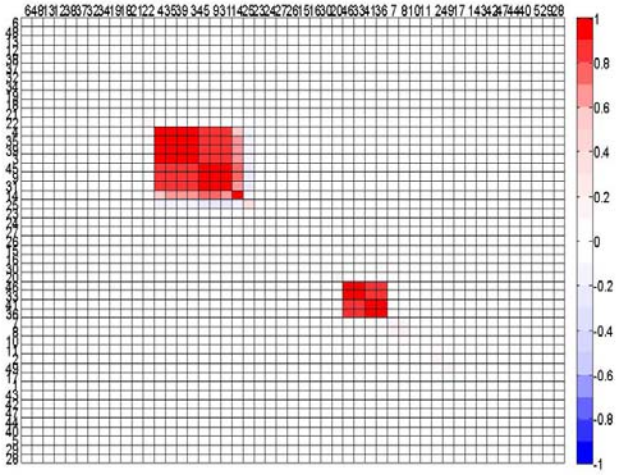


Fig. 5. Matriz MEDA con las dos fuentes de variabilidad generadas por el tráfico de cada uno de los estudiantes.

fácil observar dos grupos de variables alejados del origen. Dicha agrupación de variables refleja una potencial correlación entre las mismas, correlación que puede comprobarse con MEDA.

Si se representa el gráfico MEDA (Fig. 5), podemos observar dos cuadrados de alta correlación positiva, que denotan de nuevo los mismos dos grupos de variables correlacionadas anteriores. La correlación entre variables en sí misma no es informativa. Para obtener información de utilidad necesitamos contextualizar dichas variables. Para ello, se puede hacer zoom sobre cada uno de los grupos de variables de esta gráfica y añadir las etiquetas de las variables (Fig. 6). En la Fig.6(a) se ha hecho zoom sobre el primer conjunto de variables que aparecía en la Fig. 5. Se observa que las variables destacadas aquí son las interfaces de entrada y salida 8 y 14 del *switch* A y 1 y 9 del *switch* C. Si se considera el esquema de la red de la Fig.2, que representa nuestro contexto, se observa que las interfaces 8 del *switch* A y 1 del *switch* C están conectadas, y que la interfaz 9 del *switch* C se conecta con el ordenador P4/1 donde se encuentra trabajando el Estudiante 1 que, como sabemos, está configurando el *switch* A. Por lo tanto, se deduce que las variables destacadas en este conjunto son las referentes al tráfico generado por el Estudiante 1, que conecta el P4/1 con el *switch* A. Éstas son también el primer grupo de variables que se ha observado en el *Loading Plot* de la Fig.4.

Del mismo modo, si se hace zoom sobre el segundo conjunto de variables de la Fig. 5, se obtiene el gráfico MEDA de la Fig. 6 (b). Las variables destacadas en este caso son las interfaces 3 y 10 del *switch* C, que conectan, la primera de ellas, el *switch* C con el *router* A y la segunda el *switch* C con el ordenador P4/2. Estas interfaces se pueden relacionar con el Estudiante 2, ya que es éste el que genera el tráfico en dichas interfaces, puesto que está configurando desde el ordenador 2 el *router* A. Por tanto, este segundo grupo de variables corresponden al tráfico generado por el Estudiante 2. De nuevo podemos relacionar esto con el segundo conjunto del *Loading Plot* de la Fig. 4 y asociar los grupos de datos a las dos fuentes de variabilidad correspondientes al tráfico generado por cada uno de los estudiantes –Fig. 7.a)–. En la Tabla II se listan las variables asociadas a cada uno de los estudiantes.

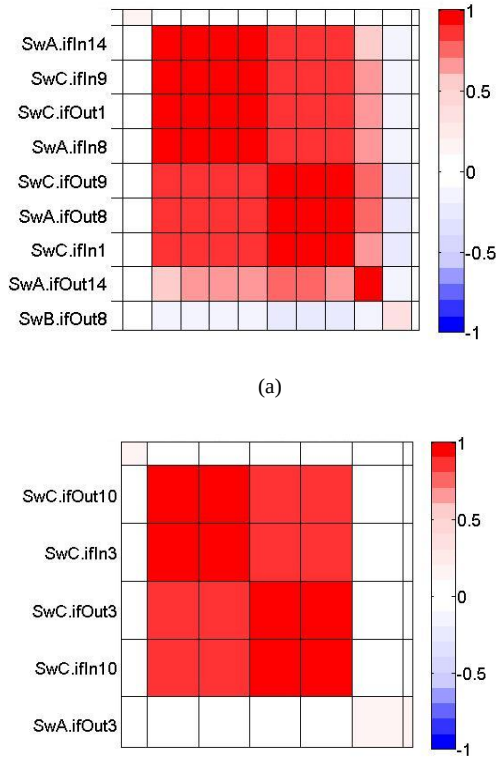


Fig 6. Matrices MEDA donde se visualizan los dos grupos de variables, (a) grupo 1 y (b) grupo 2.

C. **Análisis de las observaciones**

Una vez que se ha estudiado la relación que existe entre las variables del conjunto de datos, haciendo uso de los *Loading Plots* y MEDA, es posible también estudiar las observaciones mediante los *Score Plots* (gráfico de dispersión de puntuaciones) y oMEDA. Para ello obtiene el gráfico de dispersión de puntuaciones (*Score Plot*) del conjunto de calibración –Fig. 7.b)–, es decir, del primer conjunto de datos formado por el tráfico normal. Recordemos que en este diagrama, cada observación representa el tráfico (número de octetos) que transita por las interfaces de los conmutadores en un intervalo de 1 minuto. El índice en las observaciones representa el orden cronológico. Por tanto, la distribución de las observaciones nos permite caracterizar el tráfico de la red en el tiempo.

Es posible interpretar de forma conjunta los *Loading Plots* y los *Score Plots* [4]. Si en el *Score Plot* vemos una observación desviada en la misma dirección que una variable en el *Loading Plot*, es probable que eso signifique que la observación representa un valor alto de dicha variable. En

Tabla II. GRUPO DE VARIABLES MOSTRADOS EN LA FIG. 5.

Grupo	Variables	Descripción
Estudiante 1	A.ifIn14(4), C.ifIn9(35), C.ifOut1(39), A.ifIn8(3), C.ifOut9(45), A.ifOut8(9), C.ifIn1(31), A.ifOut14(14).	Configuración telnet del SW-A desde PC-1
Estudiante 2	C.ifOut10(46), C.ifIn3(33), C.ifOut3(41), C.ifIn10(36).	Configuración telnet del R-A desde PC-2

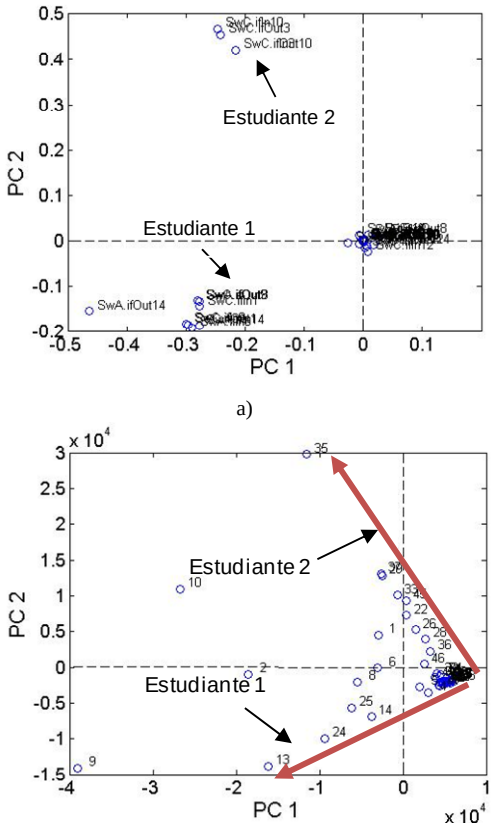


Fig. 7. Las dos fuentes de variabilidad originadas por el tráfico de cada uno de los estudiantes: a) *LoadingPlot*, b) *Score Plot.*

todo caso, esto es sólo una hipótesis que se debe confirmar con un estudio más detallado, por ejemplo con oMEDA. Como ocurría en el caso del estudio de las variables, conocer que una o varias observaciones tienen un valor especialmente alto o bajo de una o varias observaciones no aporta información de por sí sino se aplica el contexto. En nuestro caso, el contexto viene determinado por la identificación de las variables relacionadas con el tráfico de los dos estudiantes. Así, interpretando conjuntamente ambos diagramas en la Fig. 7, podemos determinar qué intervalos de tiempo presentaron un tráfico predominante del Estudiante 1, y qué intervalos tuvieron mayor peso del tráfico del Estudiante 2. Para facilitar dicha interpretación, la Fig. 7 b) ha sido anotada con dos flechas coherentes con las direcciones observadas en los grupos de variables de la Fig. 7 a). Así, a modo de ejemplo, la observación 35, correspondiente aproximadamente al minuto 35 de la sesión práctica, presenta principalmente un alto flujo de tráfico del Estudiante 2. De nuevo, esto es una hipótesis que debe confirmarse con oMEDA.

Para confirmar la hipótesis realizada sobre el *Score Plot* de la Fig.7.b) al asociar las dos direcciones de variabilidad de las observaciones con el tráfico de cada uno de los estudiantes, se obtienen los gráficos oMEDA que se presentan en la Fig. 8 y 9. Estos gráficos permiten estudiar las variables que influyen sobre las observaciones de cada una de las dos direcciones de variabilidad. Así, oMEDA muestra el grado de influencia de cada variable sobre las tendencias en las observaciones que seleccione el usuario, lo que resulta de gran utilidad como se verá a continuación.

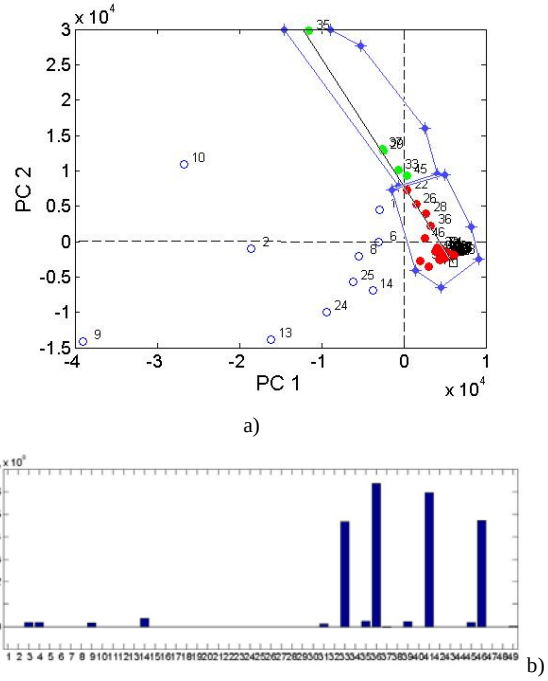


Fig. 8. Primera dirección de variabilidad correspondiente al tráfico generado por el estudiante 2: a) *Score Plot*, b) *Gráfico oMEDA.*

En primer lugar se obtiene el gráfico oMEDA para la supuesta dirección de variabilidad del Estudiante 2. La interfaz gráfica de EDA 2.0 ha sido especialmente diseñada para poder facilitar el uso de oMEDA, permitiendo una selección interactiva de las observaciones en un *Score Plot*. En el ejemplo de la Fig. 8.a) se definen dos conjuntos de observaciones a lo largo de la tendencia, el primero de ellos (verde) está formado por las observaciones de uno de los extremos, el segundo conjunto (rojo) está formado por las observaciones el otro extremo de la tendencia. Finalmente se incluye la línea de tendencia para asignar pesos a los valores de las observaciones. El diagrama oMEDA establece una comparación entre ambos grupos de observaciones de acuerdo a la tendencia marcada. En la gráfica oMEDA de la Fig. 8.b) se observa que las variables relacionadas con la tendencia, es decir, en esta dirección de variabilidad son: *C.ifOut10*(46), *C.ifIn3*(33), *C.ifOut3*(41) y *C.ifIn10*(36). Si observamos la Tabla II, obtenida tras el análisis MEDA, se observa que estas variables son las correspondientes al Estudiante 2. Por tanto, la hipótesis realizada al representar el *Score Plot* de la Fig.7.b) y relacionarlo con el *Loading Plot* de la Fig.7.a) para determinar que la dirección de variabilidad correspondía al tráfico del Estudiante 2 queda confirmada.

De igual forma se procede a estudiar la segunda dirección de variabilidad. En este caso las variables destacadas en oMEDA –Fig. 9.a)– son: *A.ifIn14*(4), *C.ifIn9*(35), *C.ifOut1*(39), *A.ifIn8*(3), *C.ifOut9*(45), *A.ifOut8*(9), *C.ifIn1*(31) y*A.ifOut14*(14), que, de acuerdo a la Tabla II, corresponden al Estudiante 1. Por tanto, se confirma que esta dirección de variabilidad hace referencia al tráfico del Estudiante 1.

Por último, se deben estudiar adicionalmente los *outliers*, que son las observaciones que están alejadas del resto de datos al representar el gráfico de dispersión de puntuaciones de la Fig.

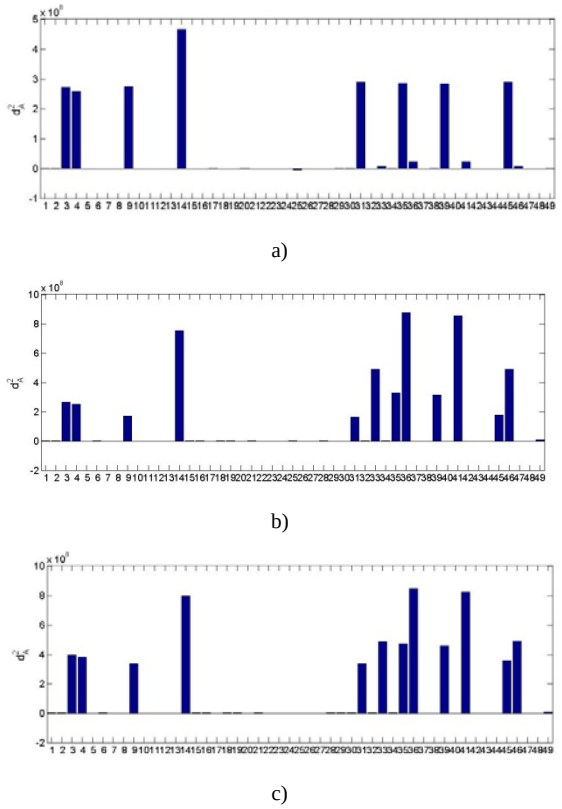


Fig. 9. Gráficos *oMEDA* de (a) la primera dirección de variabilidad correspondiente al tráfico generado por el estudiante 1, (b) estudio del *outlier 2 y* (c) Estudio del *outlier 9*

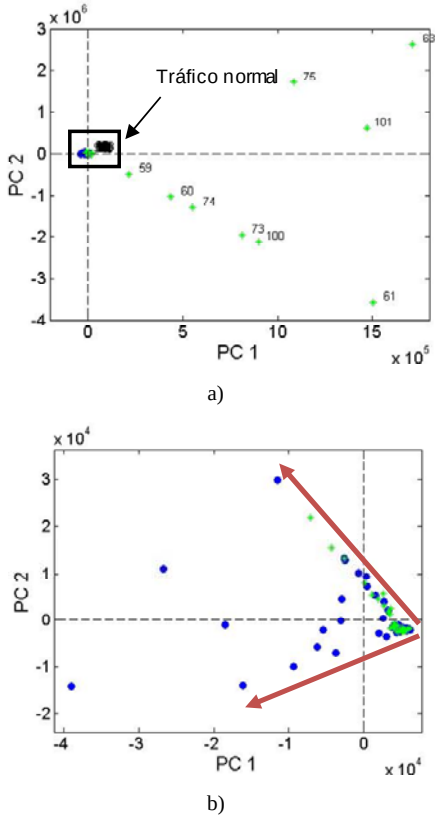


Fig.10. *Score Plot* de los conjuntos *de datos*. (a) Normal y (b) Rectángulo ampliado.

7.b). Éstas son las observaciones 2, 9 y 10. Para estudiar estos puntos se hace uso, de nuevo, de la herramienta oMEDA.

Para el estudio realizado sobre el *outlier* 2 (Fig. 9.b)) se observa que las variables correspondientes al tráfico del Estudiante 2 –*C.ifOut10*(46), *C.ifIn3*(35), *C.ifOut3*(41) y *C.ifIn10*(36)– son especialmente altas, además de la variable *A.ifOut14*, que es una variable referente al tráfico de mantenimiento de la VLAN que se añade al tráfico del *switch* A.

Para el *outlier* 9, en la Fig. 9.c), se observa que tanto las variables referentes al Estudiante 1 como las del Estudiante 2 toman valores muy altos en la observación 9. Se considera que esa observación se refiere a un minuto de tiempo en el que el tráfico generado por ambos estudiantes fue especialmente alto, en especial para el Estudiante 2.
Antes de dar por concluido el análisis también es interesante estudiar el residuo para comprobar si existen observaciones o variables especialmente mal modeladas. En el presente ejemplo no se encontraron elementos relevantes en dicho estudio, por lo que, por brevedad, no ha sido incluido en este documento.

D. **Análisis de las anomalías**

A continuación se incluye el segundo conjunto de datos (formado por tráfico normal y los ataques *Neptune*) para completar el estudio. La interfaz gráfica no contempla la posibilidad de analizar este conjunto frente al primero, aunque dicha funcionalidad será añadida en el futuro. Se realiza la acción por línea de comandos haciendo uso de la *toolbox*. Se obtiene el gráfico de dispersión de cargas mostrado en la Fig. 10. En verde se representa el tráfico del segundo conjunto de datos, que incluye los ataques, y en azul se muestra el tráfico normal original. En la Fig.10.a) puede verse cómo el tráfico utilizado en el estudio inicial queda confinado en un espacio pequeño del gráfico, mientras que los ataques están distanciados de la zona de tráfico normal, lo que facilita su detección. Si se hace zoom sobre la zona de tráfico normal – Fig.10.b) –, se observa que éste sigue manteniendo la estructura que se observó en el inicio de este análisis, es decir, se distinguen las dos direcciones de variabilidad que corresponden al tráfico correspondiente a cada uno de los dos estudiantes.

Las observaciones correspondientes a los ataques, Fig.10.a), parecen de nuevo tener cierta estructura y pueden distinguirse dos tendencias. La primera de ellas la forman las observaciones 59, 60, 74, 73, 100 y 61 y La segunda las observaciones 75, 101 y 63. Si se realiza un análisis oMEDA sobre el gráfico de dispersión de puntuaciones de la Fig.10.a) para cada una de estas direcciones, se obtienen los resultados mostrados en la Fig. 14. Así, se obtiene el gráfico oMEDA de la Fig.14.a), donde puede verse que las variables que influyen sobre las observaciones consideradas son las número 37 y 40. Éstas corresponden a la interfaz de entrada 12 y a la interfaz de salida 2 del *switch* C (*C.ifIn12*(37) y *C.ifOut2*(40)). La variable 37 es la interfaz de entrada del *switch* C (véase la Fig. 2), que se conecta con el puesto de trabajo 4 desde el que el profesor ha realizado los ataques. Asimismo, la variable 40 es la interfaz de salida del *switch* C, que conecta con el *switch* B hacia el que se han realizado los ataques. En el gráfico oMEDA de la Fig.14, la variable 37 toma valores mucho más altos que la 40. Teniendo en cuenta que la cola del *switch* C

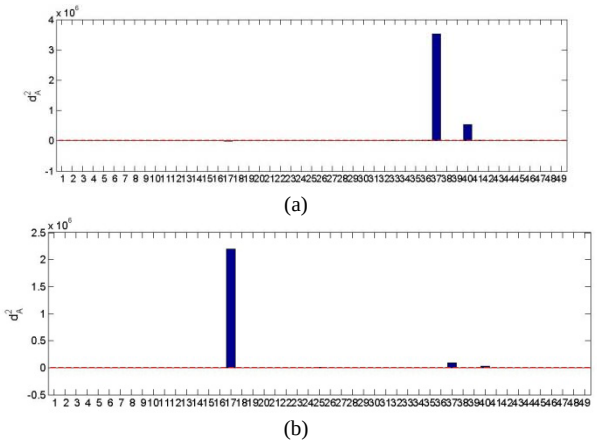


Fig.14. Gráfico oMEDA relacionado con el inicio (a) y el final (b) de los ataques *Neptune.*

introduce retardos en el tráfico de salida, se considera que las observaciones estudiadas en este caso corresponden al inicio de los ataques, ya que el tráfico entre el ordenador desde el que se realizan los ataques y el *switch* C (que cursa dicho tráfico) es muy alto.

El gráfico oMEDA obtenido para la segunda tendencia, observaciones 63, 75 y 101. se muestra en la Fig.14.b), en la que la variable destacada es la 17. Ésta corresponde a la interfaz 8 del *switch* B, que conecta el *switch* C con el *switch* B que está siendo atacado. Por su parte la variable 37 correspondiente al tráfico de entrada al *switch* C es ahora muy pequeña, a diferencia de lo que se acaba de mostrar en la Fig.14. Este hecho se debe a que el tráfico correspondiente a las observaciones estudiadas aquí se refiere al final de los ataques, cuando el tráfico es mayor entre los *switches* C y B y menor entre el ordenador 4 y el *switch* C.
Podemos observar que el patrón de los ataques queda claro, también, en los índices de las observaciones. Por ejemplo, el ataque que empieza en la observación 59 acaba terminando en la observación 63. Todas estas herramientas permiten focalizar la búsqueda del análisis forense, reduciendo mucho su complejidad.

VI. Conclusiones

La aplicación de EDA en los procesos de modelado y/o clasificación de datos se revela como una valiosa herramienta que facilita la selección a priori de la técnica a utilizar. Una correcta interpretación de las gráficas proporcionadas permite conocer la estructura subyacente en los datos y las relaciones entre las distintas dimensiones o variables involucradas, posibilitando, incluso, la eliminación de variables no relevantes para el problema considerado.

Este artículo muestra un caso de estudio sencillo para simplificar su compresión, donde la aplicación e interpretación de distintas herramientas de EDA lleva a una adecuada caracterización del tráfico normal y anómalo.

Para facilitar la aplicación de EDA por parte de investigadores no expertos en el campo, ya sea en problemas relacionados con la telemática como en otros variados ámbitos, se ha desarrollado una *toolbox* de Matlab, junto con una interfaz gráfica.

La principal línea futura relacionada con este artículo es la extensión de EDA a grandes conjuntos de datos, dentro del problema conocido como Big Data. Dicho problema introduce un conjunto de retos singulares, donde una adecuada visualización de los datos puede ser de una ventaja competitiva.

Referencias

[1] P. García Teodoro, J. E. Díaz Verdejo, G. Maciá Fernández y E. Vazquez. Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers & Security, Vol. 29. 2009, pp. 18-28.

[2] J. Jackson, A user's guide to principal components, Wiley series in probability and mathematical statistics. Probability and mathematical statistics, Wiley-Interscience, 2003.

[3] S.Wold, M. Sjöström, L. Eriksson, PLS-regression: a basic tool of chemometrics, Chemometrics and Intelligent Laboratory Systems 58 (2001) 109–130.

[4] R. Marty. Applied Security Visualization. Pearson Education, USA, 2008.

[5] K. Cook, G. Grinstein, M. Whiting, M. Cooper, P. Havig, K. Liggett, B. Nebesh, C.L. Paul. VAST Challenge 2012: Visual Analytics for Big Data. IEEE Conference on Visual Analytics Science and Technology, 2012.

[6] A. Lakhina, M. Crovella, C. Diot. Diagnosing Network-wide Traffic Anomalies. SIGCOMM 2004.

[7] W. Wang, R. Battiti. Identifying intrusions in computer networks with principal component analysis. Proceedings of the First International Conference on Availability, Reliability and Security (IEEE). 2006

[8] R. Sommer, V. Paxson. Outside the Close World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy. 2010.

[9] Kim H. Esbensen. Multivariate Data Analysis: in practice. Camo. ISBN: 82-993330-3-2.

[10] J. Camacho, Missing-data theory in the context of exploratory data analysis, Chemometrics and Intelligent Laboratory Systems 103 (2010) 8–18.

[11] J. Camacho, Observation-based missing data methods for exploratory data analysis to unveil the connection between observations and variables in latent subspace models. Journal of Chemometrics, 2011, 25 (11): 592-600.

[12] J. Camacho. Exploratory Data Analysis using latent subspace models. INTECH. ISBN 978-953-51-0438-4. Pages 63 - 90. 2012

[13] VAST Challenge 2012. http://www.vacommunity.org/VAST+Challenge+2012

[14] G. Maciá-Fernández, J.E. Díaz-Verdejo, P. García-Teodoro, J.M. López, J.J. Ramos, F. Toro-Negro, P. Ameigeiras, J. Navarro: Diseño e Implementación de un Laboratorio para la Docencia en Redes. VI Jornadas Ingeniería Telemática, JITEL 2007, Málaga (Spain), Sept. 2007.

[15] http://www.net-snmp.org/

Information security audit of WhatsApp

Júlia Ferràndiz, Joan S. Pujol, Gil Triginer, Alba Xifra, Miguel Soriano
ETSETB
Universitat Politècnica de Catalunya
Jordi Girona, 1-3 08034 Barcelona.
jjuliaf11@gmail.com, joan.sebastia.pujol@gmail.com,
gil.triginer@gmail.com, axifra@gmail.com, soriano@entel.upc.edu

***Abstract*—WhatsApp is the most popular instant messaging application for smartphones, managing more than 20,000 million messages every day generated by 200 million users worldwide. Consequently, this service handles important sensitive material. Therefore, it is essential that WhatsApp fulfils security requirements to protect personal information. Some of the challenges that this application should face are a) data privacy, b) prevention of user impersonation and c) reliable management of the information stored on the servers of this company.**

However, security requirements were not incorporated into the initial development of the application. Actually, WhatsApp has been known and criticized for its weaknesses in this area. Especially, in the first deployments of the application many security holes were identified and later covered, but not always with the best possible solutions. These weaknesses caught the attention of Canadian and Dutch governments, which launched a joint investigation, causing WhatsApp to significantly improve its security to satisfy the requirements of these two countries.

The objective of this paper is to analyse the security mechanisms that have been implemented by WhatsApp to provide the mentioned security services throughout time.
Also, a description of the attacks performed against the application is provided, along with a report of the measures that were taken to counter them. In this way, a picture of the current security situation of the company is given.

***Key words*—WhatsApp, security, audit, privacy, confidencial-lity, evolution**

I. INTRODUCTION

In the last years, many claims were raised that the security provided by WhatsApp was not meeting the standard security requirements. Given the popularity of this application, weaknesses of this kind represented an important opportunity to take advantage of the situation. However, due to the proprietary-software nature of WhatsApp, no official literature was available and it was difficult to differentiate between real insight on the application workings and inconsistent information. Regarding this, the present paper intends to gather trustworthy information that allows the reader to have a first impression of how this application works.

One of the most active fields of research in this subject was the development desktop clients for WhatsApp[1]. The result of this research was that applications like WhatsAPI or Yowsup achieved to connect to WhatsApp servers and exchange messages with WhatsApp users. Given the success of these attempts, the analysis of the developed code stood as a relevant source of information about the security implemented. Also, the reports of an investigation launched by the Canadian and Dutch governments were used to gather valuable information on the procedures of WhatsApp, particularly regarding privacy issues.

In this paper we first provide in section 2 an overview of XMPP, the protocol used by WhatsApp, and then in section 3 the desired security services are regarded. In section 4, confidentiality is examined, reporting the different implementations that the application has provided throughout time. In section 5 it is noticed that neither integrity nor non-repudiation is provided and, in section 6 the authentication methods are analyzed. At this point, in section 7, some relevant attacks are described, also explaining how the company countered them. Regarding the last security service, in section 8, some privacy issues are discussed, based on the findings of the Canadian-Dutch investigation. Finally there is a last section with some conclusions.

II. BRIEF EXPLANATION OF THE PROTOCOL

To understand the mechanisms that will provide the security services it is useful to know how WhatsApp messages are exchanged. For that purpose we will briefly describe the main features of the protocol used.

WhatsApp is based on the standard protocol XMPP (eXtensible Messaging and Presence Protocol) but includes some modifications. XMPP was designed to provide nearly real-time message exchanging, based on a client-server architecture. In this setup, users connect to a server to be able to exchange messages with other users who can be connected to the same network or to a different one.

In an XMPP connection, the main steps are the following:

1) Determine the IP address and the port of the server to which you want to connect.
2) Open a TCP connection between client and server.
3) Open an XMPP stream over the TCP connection.
4) Preferably, negotiate TLS for security mechanisms.
5) Authenticate using the SASL (Simple Authentication and Security Layer).
6) Bind resources to the connection.
7) Exchange messages.
8) Close the XMPP stream.
9) Close the TCP connection.

WhatsApp does not follow this scheme entirely. The main changes that WhatsApp's protocol (FunXMPP) introduces are:

1) Some variations in the security mechanisms that are used.
2) Modifications of the programming language. Instead of using standard XML, WhatsApp has compressed some instructions that are carried in the headers of the messages to get lighter traffic. To do so, a dictionary is used that maps the most used commands to single bytes. In addition, this makes the messages harder to read by an external programmer, which seems to be part of a security-through-obscurity policy carried out by the company.

III. ANALYSIS OF THE DESIRED SECURITY SERVICES

An instant messaging application would be required to fulfill several conditions:

- Confidentiality: No other users should have access to the contents that are sent.
- Integrity: The message received should be the same as the message sent.
- Authentication: no one should be able to impersonate your identity.
- Non-repudiation: a user can not deny being the author of a message that she has written.
- Privacy: an individual has the right to control what information about him is collected, how it is used and who uses it.

From now we're going to discuss if WhatsApp fullfills these features.

IV. CONFIDENTIALITY

The only way to provide confidentiality is by using cryptographic techniques. In this aspect, WhatsApp not always has met the expectations.

From its inception in 2009 until May 2012, WhatsApp did not use any encryption so messages were sent and received in unencrypted plain-text format, meaning that messages could easily be read, especially in a public WiFi network, where everybody is able to sniff incoming and outgoing messages. It was only after receiving the first complaints that security mechanisms were introduced to pursue confidentiality.

Then, in May 2012 security researchers noted that new updates of WhatsApp no longer sent messages as plaintext, and three months later WhatsApp Support Staff claims messages are encrypted in the "latest version" of the WhatsApp software for iOS and Android.
The encryption algorithm was the same in both Android and iOS devices, the RC4 algorithm.

A. ENCRYPTION ALGORITHM: RC4

RC4 is a stream cipher system, similar to the Vernam cipher, but in this case it uses a pseudo-random sequence (keystream), that is generated with an initial key. Once generated this sequence, we combine the keystream with the plaintext using bit-wise exclusive-or. This encryption is used in some of the most popular protocols such as Transport Layer Security (TLS / SSL), WEP (Wired Equivalent Privacy) and WhatsApp.
It uses two different algorithms to generate the keystream:

```
8⊖    public function __construct($key, $drop)
9     {
10        $this->s = range(0, 255);
11        for ($i = 0, $j = 0; $i < 256; $i++) {
12            $k = ord($key{$i % strlen($key)});
13            $j = ($j + $k + $this->s[$i]) & 255;
14            $this->swap($i, $j);
15        }
16
17        $this->i = 0;
18        $this->j = 0;
19        $this->cipher(range(0, $drop), 0, $drop);
20    }
```

Fig. 1. Function *_construct* [1].

1) KSA (Key Scheduling Algorithm).
2) PRGA (Pseudo-Random Generation Algorithm).

We are going to describe how those algorithms are implemented in WhatsApp protocol, using the WhatsApp Api[1], that was made by inverse engineering.

1) KSA: As many ciphers do, RC4 relies on the use of Sbox to provide randomness to its outcome. Similarly to what AES or DES do, RC4 creates a matrix structure on which various operations are performed to randomized its content. The main difference is that, unlike DES, the initial content of this Sbox is not the message itself, but a definite sequence of numbers that will be subsequently reordered to obtain a pseudo-random sequence. The key-scheduling algorithm is used to initialize the permutation in the array *S*[2].First, a vector of 256 positions *S* is generated and in each position is saved the value of their own position, for instance, S [153] = 153. The key is a vector KEY and "keylength" is defined as the number of bytes in the key and can be in the range $1 \leq keylength \leq 256$, typically between 5 and 16, corresponding to a key length of $key \in [40 \sim 128]$ bits. Once we have initialized all the variables values, we can perform the permutation.

Let's analyze how they do it in WhatsApp. As can be seen in the figure 1 the array *s* is first initialized. Once the array is initialized they obtain a number from the *key*. As the *key* can be a character they use the function *ord* that returns the ASCII value of the char. However, the *key* length can be shorter than the algorithm iteration (256) for this reason we have to access to the *key* in the position $i \ \% \ strlen(key)$. After that, the value of *j* can be calculated, therefore we can do the permutation from $s[i] = s[j]$.
To end the process, the function cipher is being called to perform the pseudo-random generation algorithm.

Notes that variable $\$drops$ indicates the length of the message that's need to be encrypted. In the figure 2 this behaviour can be understood. As the function cipher is the one that has to cipher all the message this function needs to know the length to implement the loop.

```php
public function cipher($data, $offset, $length)
{
    $r = '';
    for ($n = $length; $n > 0; $n--) {
        $this->i = ($this->i + 1) & 255;
        $this->j = ($this->j + $this->s[$this->i]) & 255;
        $this->swap($this->i, $this->j);
        $d = ord($data{$offset++});
        $r .= chr($d ^ $this->s[($this->s[$this->i] + $this->s[$this->j]) & 255]);
    }

    return $r;
}

protected function swap($i, $j)
{
    $c = $this->s[$i];
    $this->s[$i] = $this->s[$j];
    $this->s[$j] = $c;
}
```

Fig. 2. Function cipher[1].

```php
$key = pbkdf2('sha1', base64_decode($this->password), $this->challengeData, 16, 20, true);
```

Fig. 3. A generic function to cipher with PBKDF

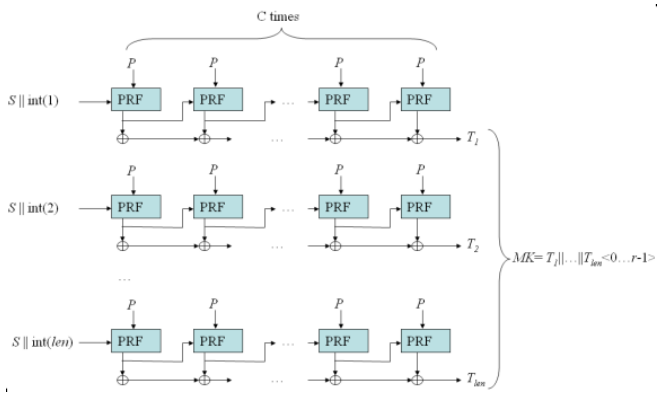


Fig. 4. A general diagram of the PBKDF

2) PRGA: PRGA is responsible for generating a keystream of the same length as the message to be encrypted out of the 256 bytes Sbox that has been previously initialized.
For as many iterations as are needed, the PRGA modifies the state and outputs bytes of the keystream.
First of all, two variables i and j are created, both initialized to 0, and then in each iteration PRGA follows the next steps:

1) Increments i: $i = (i + 1)\%256$
2) Looks up the i^{th} element of S, S[i], and adds that to j:
3) Exchanges the values of S[i] and S[j]
4) The output is the value of the S vector at the position of S[i]+S[j] module 256.
5) Then, K is XORed with the next byte of the message to produce the next byte of either ciphertext (if we are encrypting) or plaintext (if we are decrypting).

This functionality can be seen in the figure 2.

B. KEY GENERATION

1) PBKDF2: As we have just explained, RC4 algorithm needs an encryption key. This key is generated using an algorithm called PBKDF2 (RFC2898[3]).
PBKDF2 is a key derivation function. This algorithm applies a pseudorandom function, such as a cryptographic hash, cipher, or HMAC to the input password or passphrase along with a salt value (set of random bits) and repeats the process many times to produce a derived key, which will be used for encryption and decryption. The PBKDF2 key derivation function has five input parameters:

$$Dk = PBKDF_{(PRF,C)}(P, S, kLen)$$

Where DK is the derived key, PRF is a pseudorandom function of two parameters with output length hLen, P is the master password from which a derived key is generated, S is the salt value, c is the number of iterations desired and dkLen is the desired length of the derived key. The dkLen value shall be at least 112 bits in length[4].

In WhatsApp, the function responsible for encryption can be seen in the figure 3. The dkLen is 20 bytes (160 bits), so WhatsApp fulfills the recommendations. The salt value or (”challenge”) is provided by the server in session negotiation and is used for all following crypto operations. This token is changed regularly on each session negotiation. The password is the security key provided by WhatsApp using the procedure of the figure 4.

The output length of the random function PRF is hLen but the key should be dkLen, so PBKDF concatenates (||) dkLen/hLen T_i blocks of hLen:

$$DK = T1||T2||...||Tdklen/hlen$$

Each T_i block is the output of an F function:

$$T_i = F(Password, Salt, Iterations, i)$$

And the function F is the xor ($\oplus$) of c iterations of chained PRFs:

$$F(Password, Salt, Iterations, i) = U1 \oplus U2 \oplus ... \oplus Uc$$

The first iteration of PRF uses Password as the PRF key and Salt concatenated to i encoded as a big-endian 32-bit integer. Subsequent iterations of PRF use Password as the PRF key and the output of the previous PRF computation as the salt:

$$U1 = PRF(Password, Salt||INT_msb(i))$$

$$U2 = PRF(Password, U1)$$

$$...$$

$$Uc = PRF(Password, Uc - 1)$$

The number of iterations, PBKDF2 iterations, is 16, although the recommended minimum number of iterations is 1000.

2) MD5: Until now it seems that the security is quite accurate, but how is the password generated?
To generate the password, WhatsApp crew chose to make the MD5 function of a number. This number, as we will see later, depends on the operating system that the device uses. First we are going to analyze how MD5 works.

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512.

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D.

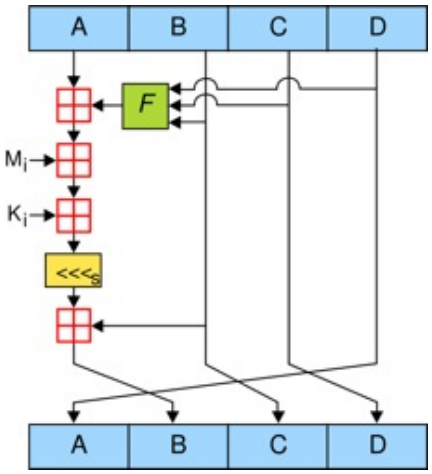


Fig. 5. Round operation

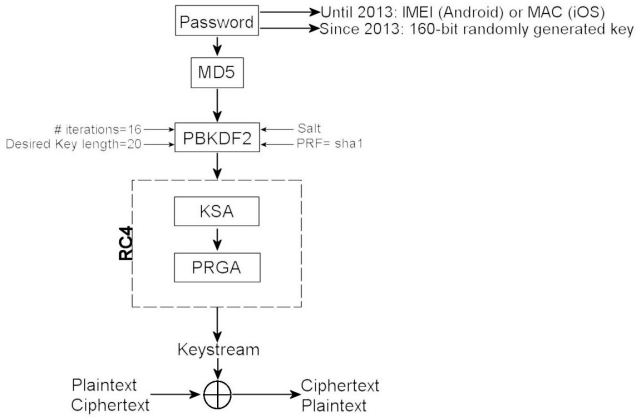


Fig. 6. General view of the Encryption process.

These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. This procedure can be seen in figure 5

3) PASSWORDS USED UNTIL 2013:

IOS: The key used for those devices was the MD5 hash of the MAC address repeated twice and encoded in base64. It seems to be a good encryption, but the problem is: How do you protect/encrypt the ”session token” while getting it from server? We will, the answer is: it was not protected. So, what the attacker probably needed was just to catch the session token while session negotiation and know the Mac address, which can be easily achieved on a WiFi network with Wireshark [5], for example. This session key was the same that was used for authentication.

ANDROID: In Android devices, the password was likely to be an inverse of the phone's IMEI number with an MD5 cryptographic hash thrown on top of it (without salt).

$$md5(strrev(”your - imei”))$$

This is not a good method for key generation as it is also easy to get the IMEI of the device. For example if you have direct access to your victims phone, in which case you dial and call $*\#06\#$ (in most cases) and you have got their IMEI number, or you can also develop an app that silently sends the victims IMEI number to your server in the background (many applications do this already) and phone number. Paradoxically, Apple does not allow third-party applications to access IMEI number, that is the reason why the MAC address was used, but it results that the Android key is more secure than the iPhone key, as the MAC address can be easily sniffed.

C. PASSWORD USED SINCE 2013

Using these passwords WhatsApp guaranteed a very limited confidentiality because it was so easy to know the keys and deciphering the messages.

In order to resolve these confidentiality problems, since 2013 WhatsApp has stopped using IMEI and MAC numbers for confidentiality and authentication on all mobile platforms and has stated that the application is now using a 160-bit randomly generated key. This way, currently WhatsApp is able to ensure the confidentiality of messages.

V. INTEGRITY AND NON-REPUDIATION

Data integrity is the assurance of non-alteration: the data (either in transit or in storage) has not been undetectably altered whether by accident or deliberately malign activity.

WhatsApp does not use any cryptographic techniques to provide integrity. This means that no Hash or MAC are sent together with the message, so integrity is not provided. Although TLS standard establish that integrity should be provided using message authentication codes, we have not found any mechanism that implements that in the WhatsApp API.

Non-repudiation is the security service that guarantees protection against the sender's denial of having written the message and the receiver's denial of having received the message, so provides evidence that entities participating in a communication could not deny having been involved in it.

This service is not provided by WhatsApp because digital signatures or notarization are not used. It could be useful in some occasions, nevertheless the fact that your mobile could be stolen easily would lead to identity problems. Indeed, asking a password to the user every time he/she writes or reads a message would not be practical.

VI. AUTHENTICATION

To provide authentication, the user is periodically asked to login, using some credentials that were negotiated during the registration process. In this section we will discuss how

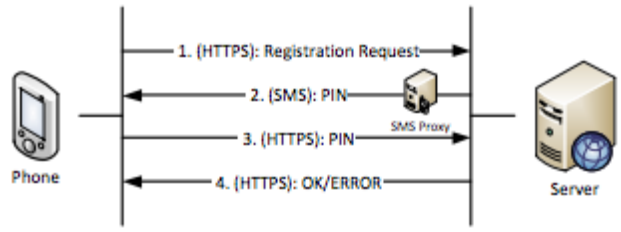


Fig. 7. Authentication process.

the registration and the login are carried out and how they ensure authentication.

The registration is the first contact that server and user have. In this first stage, they exchange credentials that will be used to authenticate the user in the following communication, so it is important to avoid the interception of these initial messages. To do so, an SSL connection is established where messages are securely sent thanks to RSA mechanism. The main structure of this process is that of a challenge-response procedure: in this case, the server sends a code to the client via SMS to verify that he possesses the phone number that is to be registered.
After receiving the code, the client sends it back to the server through the internet and, finally, receives the credentials that will be used during the following connections.
Until recently, as was explained before, this supposedly private credentials were just identifiers of the device like the IMEI number (in the case of Android) or your MAC address (for IOS).

To understand the login procedure that is done in every new connection to the server, we have followed the function that was used for that purpose in whatsAPI, which we have included the url. It consists of two steps:

1) In first place, the client begins the connection sending the main parameters that will be used during the connection. These parameters include the identifier of the mobile phone, which is basically the mobile number, the authentication algorithm that will be used, etc.

2) After that, a typical challenge-response authentication is carried out. The server sends a message which the client will encrypt with a shared key and send back to the server. The encryption algorithm is the same that is used to encrypt the regular messages, that is, RC4 with a key generated through PBKDF2 and MD5.

VII. ATTACKS

A. MIM-ATTACK AGAINST WHATSAPP AUTHENTICATION

To prevent malicious users to impersonate someone else using the victim's number, a verification SMS containing a $4-digit$ PIN is sent to the mobile phone. The user then has to copy that code into the WhatsApp application's GUI. This process binds a WhatsApp user account(represented by the phone number) to a physical device.

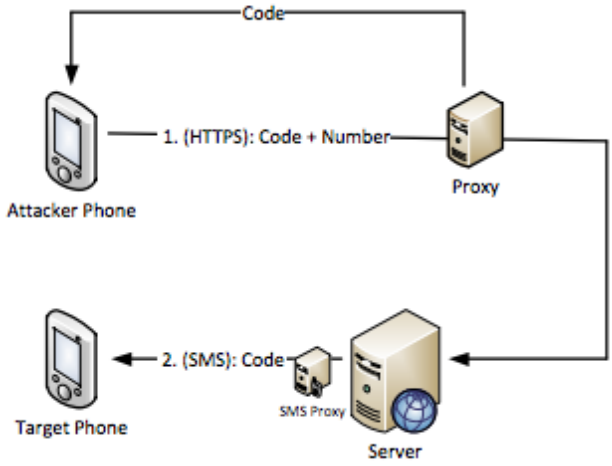


Fig. 8. Authentification hijack.

This verification process of WhatsApp was fatally broken. The PIN for the verification SMS message was generated in the phone and then sent to the server via a HTTPS connection. The server then initiates the SMS message via a SMS proxy to the phone, where the app then checks if the PIN entered by the user matches the previously generated PIN. An attacker could exploit this mechanism to hijack any WhatsApp account. This can be done by typing the victim's phone number during the verification phase and then intercepting the communication between the phone and the server to eavesdrop the PIN.
This communication is SSL-protected; however, the attacker has to intercept only the connection between his own phone and the WhatsApp server. To exploit this vulnerability, it is possible set up a SSL proxy and install the proxy's certificates on the phone in order to get access to the encrypted communication transparent to the application[6].

Once the attacker has entered the PIN into his phone, the victim's WhatsApp account is linked to the attacker's phone. This enables the attacker to send and retrieve messages from the victim's account. This process also unlinks the victim's device, causing it to not receive messages from WhatsApp anymore. This security hole was fixed through the implementation of the authentication method previously explained.

B. DENIAL OF SERVICE

To avoid brute forcing attacks, WhatsApp introduced a mechanism that only one validation request was accepted in a period of 10 minutes. Therefore, someone asking a validation code of the victim's number was able to make a Denial of Service.

During the process of validation, and until the holder of the number revalidate their identity, WhatsApp installation left him in a zombie state. To reset victim's account the

victim needs to clear all the data from the application and wait a minimum time of ten minutes before the application let him ask for a validation code (because of course, the previous validation code that the victims received by SMS was not processed, because was not the victim's WhatsApp who requested it).

And script appeared that was able to portray a deny of service to a phone number or a list of phones numbers. Some people begin to speculate if it was possible to do a deny of service to a whole country, but nobody did it.

Since the last update, this bug has been solved so now it is not possible to perform this attack anymore.

C. CHANGING WHATSAPP STATUS

An additional feature of WhatsApp is the possibility to set a status message, similar to instant messaging clients like Skype, that can be read by the user's contacts.
Changing this status message does not require any authentication some time ago. In fact, everyone could change anyone else's status message by sending an HTTPS request to:

$$https://s.WhatsApp.net/client/iphone/u.php?$$

$$cc =< countrycode > \&me =< phonenumber >$$

$$\&s =< statusmessage > .$$

This failure in the security system of WhatsApp was exploited by a web server *WhatsAppstatus.net*, that let the users change any account status from any phone around the world. The unique thing that the users have to know is the victim's mobile phone number.

To avoid this problem, what WhatsApp did in first time was to reject all the incoming requests from the IP of the web server, meaning that if someone was still using this https request explained before, was still able to change status. Then WhatsApp implemented an IP check. The check entails checking if the update-request is for a WhatsApp account currently signed in, and checks if it is coming from the same IP as the target client is using. This means that still worked for target WhatsApp users behind the same NAT (for example), but since the last update on February, this attack has been avoided.

VIII. PRIVACY

WhatsApp had been under investigation by governmental privacy authorities in Canada [7] and The Netherlands [8] for violations of both nations's privacy acts. The investigation, limited to privacy issues, was initiated on January 2012 and the complaint was notified to the application one month later. From March 2012 through to January 2013 the application cooperated fully with the investigation and responded to the Privacy Commissioner's recommendations.

A. INTEGRATION WITH A USER'S ADDRESS BOOK

An issue regarded in the complaint was the lack of integration with a user's address book and if it was collecting more personal information than necessary for the service provided.

1) DESCRIPTION: The application requires the user consent of an upload of a user's mobile contact list to her servers up to two times daily, to assist in the identification of other WhatsApp users. WhatsApp assures this contact discovery process is limited to mobile phones, not collecting names, emails or any personal information, an affirmation that was confirmed by the investigation. The association between contact names and mobile phones is done only in the user's device.

The transferring of the user's address book to the WhatsApp servers is done using SSL/TLS encryption. There, mobile phone numbers are stored perpetually in the servers divided in two categories: "in-network", which are registered users, and "out-of-network", which are users that don't have the application installed. The fact is that "in-network" numbers are stored in plain-text, otherwise "out-of-network" numbers are irreversibly hashed values. These values are obtained using an MD5 hash function. The phone number and a fixed salt value serve as input to the hash function, and the output is truncated to 53 bits and combined with the country code for the number. The result is a 64-bit value which is stored in data tables on WhatsApp servers. According to WhatsApp, this procedure is designed to render out-of-network numbers anonymous.

To sum up, WhatsApp requires users to upload their entire address book to his server to determine which of their contacts are users of the application. It was not allowed to choose manually which users you want to communicate with and only upload these users contact information.

2) RECOMMENDATIONS .: The Canadian and Dutch recommendation was to allow users to have the ability to manually add and manage contacts, rather than have to consent to provide their entire address book for using the service, which was considered a breach of privacy and an overreach by the company. Furthermore, it was advised to not retain non-users numbers in the servers, since the application does not need them to run. It was found that in reality the true-anonymity claimed by WhatsApp in the storage of non-users numbers was actually not reached. True-anonymity is only achieved where information can never be linked to an individual. Instead, WhatsApp treatment of "out-of-network" numbers could be easily overpassed through a data breach and some computing effort. Related to this weakness, re-submitting the same phone number would result to the storage of the same hash value in the server, so the company could adopt the practice to reprocess these values and find it in his database. WhatsApp stated that could make possible for different numbers to result to the same hash values, making it more difficult to reverse the hash. But the small amount of overlapping values makes this approach

not sufficient to provide anonymity.

3) WHATSAPP RESPONSE: WhatsApp has updated its iOS app to version 2.8.7 which allows iPhone users to manually uploading contacts so avoiding the application's discovery process. It is intended by the application to add this functionality to Android, Blackberry, Symbian and Windows clients as well.

B. BROADCAST STATUS MESSAGES.

WhatsApp automatically shares your status messages to everyone who has your number in their address book, even though you may not know the individual or you would not want to share information with him.

1) DESCRIPTION: WhatsApp allows its users to share a message status, which can be a personalized one or select a default status provided by the application like "Busy" or "Sleeping" and are periodically refreshed during the day. Personalized status are limited to 139 characters, and it is only available for iPhone users to leave it blank. Once the status is saved, it is broadcasted to all the users that have your phone number. As such, a sender may not know the identity of the users who are receiving and maybe monitoring their status.
In an act to prevent that, it is possible to block an individual adding it to the "Blocked contacts" list, so the status message would not be shared to these group. But this group can only be populated with individuals who the user knows.
Regarding the nature of the status message, there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information, that would render the individual identifiable. Even it is publicly available, is still personal information. Although, WhatsApp did not make these vulnerabilities clear in its Terms of Use and Privacy Policy.

2) RECOMMENDATIONS: The Canadian and Dutch requires for WhatsApp were to provide better notice of the potentially indiscriminate nature of status submissions. These broadcasting request knowledge and consent by the users for the collection and use of this personal information. Otherwise, WhatsApp's Terms of Service and Privacy Policy may not be readily available to users on mobile devices so it was recommended to notify the user with a real-time active notification for more meaningful consent of this automatic sharing of status messages.

3) WHATSAPP RESPONSE: During the course of the investigation, WhatsApp actualized its Terms of Service and Privacy Policy to better inform users of the public nature of broadcast messages. Some paragraphs were added that showed the implications of the broadcasting, for example this clarifying sentence: "*A good rule of thumb is if you don't want the whole world to know something or see something, don't submit it as a Status Submission to the Service.*" Although, it remained clear that they do not believe status messages to be personal information: "*Please note that any Status Submissions or other content posted at the direction or discretion of users of the WhatsApp Service becomes published content and is not considered personally identifiable information subject to this Privacy Policy.*"

In addition, WhatsApp has stated to its future implementation plan to add real-time notification, which will be integrated in future releases of the application beginning on September, 2013.

C. OFFLINE STORAGE OF MESSAGES

Governments were concerned whether WhatsApp was doing a properly use of undelivered messages and also if its retention policy of personal information was well communicated to the user.

1) DESCRIPTION: When a WhatsApp message is sent, its first destination is to corporate servers co-located at secured facilities in Washington DC and Virginia. Then the message is routed by WhatsApp to its recipient only if its online. Point in fact, delivered messages are not retained by WhatsApp, neither a record of messages delivered. This message register is only saved in the user's device, in an encrypted way, so it can be deleted or saved at user's will.
Following this further, if the recipient happens to be offline WhatsApp stores the message in its servers, pending delivery. After 30 days the message would be automatically deleted if it has not reached its destination. Messages not delivered are mapped to one of four server partitions. Within each partition, one file is reserved for each user. Nevertheless, WhatsApp collect date and time stamp information associated with successfully delivered messages and the mobile phone numbers the messages were sent from and to.
Files that are sent through the WhatsApp Service will reside on its servers after delivery for a short period of time, but are deleted and stripped of any identifiable information shortly afterwards.
At the beginning of the investigation, WhatsApp did not provide any information about retention policies in its Terms of Service, Privacy Policy or Licensed Application End User License Agreement.

2) RECOMMENDATIONS: The 30 days retention of undelivered messages was considered satisfactory for the purpose of the application. However, it was recommended to make readily available to users its general retention policy for personal information without unreasonable effort.

3) WHATSAPP RESPONSE: WhatsApp updated and expanded its Terms of Service and Privacy Policy in July, 2012. In its words: "*If the recipient is not online, the undelivered message is held in WhatsApp's server until it can be delivered. If the message is undelivered for thirty (30) days, the undelivered message is deleted from our servers. Once a message has been delivered, it no longer resides on our servers.*" However WhatsApp has agreed to provide better notification of those policies to its users.

D. DATA RETENTION AFTER ACCOUNT TERMINATION

Regarding the fact that a user can freely choose to close its WhatsApp account, it was necessary to determine whether the application process of deactivating the account was correctly managed.

1) DESCRIPTION: By the time the governments initiated the investigation, when a user removed WhatsApp from its mobile phone its personal information was retained by the instant message application during 30 days, including billing information. In order to be removed immediately the user had to send an email notifying its request.
According to WhatsApp, this 30-day retention period of payment information is to provide users an easy renewal or registration without going through the long registration process again. But even so, an exception exists to this 30-day period. If a user has a one year free trial of the application and after this year fails to subscribe to the service as a payment user, its personal information may be retained for up to one year. This is done to assure that this trial user would not re-subscribe for the free trial again, so never paying for the service.

2) RECOMMENDATIONS: Privacy Commissioners recommended that WhatsApp should develop guidelines and ensure the implementation of respectful procedures regarding the retention and destruction of personal data. Indeed, it would be satisfactory to have easy access for users to the WhatsApp policy of personal information retention.

3) WHATSAPP RESPONSE: In response to recommendations stated before, *WhatsApp has committed to make its policy publicly available and provide better notification to its users*[7].

E. PRIVACY CONCLUSION

In conclusion, we must admit that WhatsApp cooperated transparently with the investigation and committed to implementing the recommendations received by the Commissioners. Even though its treatment of personal information sometimes was (and maybe still is) poorly managed, as it has been regarded also in the Encryption Section, the fatal mistake regarding the privacy law was that these risks were not well notified to its users, who trusted the application.

IX. CONCLUSION

After this research we can say that WhatsApp's priorities have many times been other than security. In particular, we believe that most decisions taken by the company pursue the objective of enhancing the performance of the system in terms of traffic fluidity. This approach has been proved very effective, as users have preferred WhatsApp in front of other similar applications that provide better security. This is so because traffic fluidity has a direct impact on user experience, whereas security issues tend to be disregarded. There is still the doubt on whether users do not mind about these issues or they simply give them by granted.

In other contexts, such as in online payments, security is provided by default. Because of this, people tend to rely on the applications without really analyzing the privacy conditions or taking any caution in this aspect.

Nevertheless, companies have an obligation to provide this services, taking into account that privacy has been recognized as a human right since the Human Rights Act of 1998, article 8[9] . This was shown in 2012, when a coalition of national governments complained to WhatsApp for its security holes. WhatsApp answered to this investigation with some changes in its methods, but most of the issues were addressed just by introducing new articles to their Terms of Use and Privacy Policy, leaving the decision in hands of the users.

WhatsApp uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information. We cannot, however, ensure or warrant the security of any information you transmit to WhatsApp and you do so at your own risk[10].

Regarding the changes in their methods, WhatsApp can be cryticised for implementing the improvements at a very slow pace, waiting until weaknesses were detected instead of taking the initiative and introducing robust security methods from the beginning.

Moreover, one could criticize that WhatsApp has often relied on a security-through-obscurity police, whereas it has been proved during time that it is not advisable to do so. Instead, the best way to proceed would be to use standard protocols whose security has been verified through time.

X. ACKNOWLEDGEMENTS

This work was partially supported by the Spanish Comisión Interministerial de Ciencia y Tecnología CICYT COPPI (TEC2011-26491), the Spanish Ministerio de Ciencia e Innovación with the CONSOLIDER project ARES (CSD2007-00004), as well as the Generalitat de Catalunya with the Grant 2009 SGR-1362 to consolidated research groups, the funding of which is gratefully acknowledged.

REFERENCES

[1] WhatsApp Api https://github.com/venomous0x/WhatsAPI (seen 13-05-2013).
[2] Explanation of the rc4 algorithm https://en.wikipedia.org/wiki/RC4 (seen 16-05-2013).
[3] Password-Based Cryptography Specification Version 2.0 http://tools.ietf.org/html/rfc2898 (seen 16-05-2013).
[4] *Recommendation for Password-Based Key Derivation*,*National Institute of Standards and Technology*.
[5] Wireshark is a free and open-source packet analyzer http://www.wireshark.org/ (seen 16-05-2013).
[6] Software used to break ssl http://www.thoughtcrime.org/software/sslsniff. (seen 18-05-2013).
[7] Canada Report: http://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp (seen 16-05-2013).
[8] Dutch Report: http://www.dutchdpa.nl/downloads_overig/rap_2013-whatsapp-dutchdpa-final-findings-en.pdf (seen 14-05-2013).
[9] The human rights act http://www.equalityhumanrights.com/human-rights/what-are-human-rights/the-human-rights-act/ (seen 18-05-2013).
[10] Whatsapp Terms of Service http://www.WhatsApp.com/legal/?l=es (seen 21-05-2013).

Impacto de las unidades a pie de carretera en las interferencias en redes vehiculares

Carlos Gañán Sergi Reñé Jorge Mata-Díaz Juanjo Alins
Universitat Politècnica de Catalunya (UPC)
{carlos.ganan,sergi.rene,jmata,juanjo}@entel.upc.edu

***Resumen*—Las redes ad hoc vehiculares (VANETs) han emergido como una tecnología clave que posibilita el despliegue diversas aplicaciones. Proporcionar seguridad a los servicios de información y entretenimiento en estos entornos requiere del uso de unidades a pie de la carretera (RSU) como puertas de acceso a los recursos solicitados. Idealmente, las RSUs deben desplegarse para proporcionar conectividad continua. Si bien esto aumenta la capacidad y cobertura, también acarrea un aumento de la interferencia que puede degradar seriamente el rendimiento de la VANET. En este trabajo se estudia el impacto de la interferencia entre RSUs y sostenemos que la versión actual de la norma IEEE 1609.4 no puede hacer frente a la alta densidad vehicular. Extensas simulaciones apoyan las conclusiones obtenidas en este trabajo.**

***Index Terms*—VANET, interferencia inter-RSU.**

I. Introducción

Las redes vehiculares serán desplegadas a gran escala en una amplia gama de autopistas y entornos urbanos. Cubrir áreas muy densas requiere que miles de unidades en carretera tienen que ser colocadas y configuradas correctamente, sin interferencias. Por lo tanto, un requisito primordial de una VANET eficiente es una cobertura adecuada donde los vehículos pueden acceder a aplicaciones y servicios. El despliegue de la infraestructura debe reducir la interferencia tanto como sea posible a fin de lograr estas funciones mediante un uso rentable y eficientes de los recursos [1].

Lamentablemente, las RSU se desplegarán de manera empírica, colocando manualmente sobre la base de mediciones de la intensidad de señal recibida. Tal enfoque no estructurado del diseño de la infraestructura VANET implica una fuerte interferencia de canales y la utilización deficiente de los recursos. Por ejemplo, más RSUs se pueden usar para mejorar la cobertura en puntos ciegos o lugares remotos. Esto conducirá a una superposición de señal, que a su vez causará interferencia y desperdicio de recursos. En este trabajo se cuantifica el impacto de esta superposición en el rendimiento VANET.

El control de acceso al medio (MAC) para el acceso inalámbrico en entornos vehiculares (WAVE) se describe en el estándar IEEE 1609.4 [2]. No obstante, este acceso al medio es incapaz de hacer frente al fuerte aumento de la interferencia causada por estos despliegues densos. Además, la mayoría de las aplicaciones previstas para este tipo de redes requieren de la difusión periódica de las balizas y anuncio de servicio WAVE (WSA). Esta señales baliza se generan con una frecuencia típica de 1-10 Hz. Consecuentemente, este alto índice de generación no sólo podría causar tan sólo la congestión en el canal de control (CCH), sino también la pérdida de balizas que contienen información crítica. El hecho de no recibir balizas podría dificultar el funcionamiento normal de algunas aplicaciones y poner en peligro la seguridad de los pasajeros. Bajo este criterio, no se reconocen la recepción de balizas, por lo que las transmisiones fallidas no se pueden detectar. Esto podría ser un grave problema para aquellas balizas que necesitan ser recibidas inmediatamente, de lo contrario los datos contenidos podrían ser anticuados e inútiles.

La radiodifusión en redes vehicular ha sido estudiada desde el punto de vista de comunicaciones vehículo a vehículo (V2V) [3], [4], sin embargo, el papel de la RSU se ha ignorado. Autores en [5] han modelado las transmisiones difundidas analíticamente, teniendo en cuenta que un cambio de canal pero sólo desde el punto de vista V2V. En escenarios de alta densidad, los servicios WAVE se anuncian por la infraestructura durante el CCH. A pesar de que estos anuncios no serán tan sensibles al retardo como las aplicaciones de seguridad de pasajeros, es necesario proporcionar un servicio de radiodifusión fiable a través de las RSUs.

En este trabajo se analiza el servicio de transmisión desde la perspectiva de la infraestructura mostrando que está sujeto al problema de terminal oculto. Se demuestra que uno de los principales problemas para los protocolos de transmisión radica en la entrega no-fiable de paquetes. El IEEE 1609.4 define el uso de un mecanismo de intercambio de comunicación RTS/CTS para las transmisiones de unidifusión con tal de aumentar la fiabilidad, sin embargo, las transmisiones de difusión en el CCH tan sólo se basan el puro protocolo CSMA/CA sin RTS/CTS. Por medio de una serie de simulaciones realistas mostramos la incapacidad del mecanismo de radiodifusión para lograr una tasa de recepción de baliza cercana al 100 %. Debido al despliegue empírico de RSUs, varias versiones del problema del terminal oculto aparecerán cuando las RSUs están transmitiendo simultáneamente señales baliza a automóviles sin ser conscientes de la presencia de otras RSUs. Se demuestra que este problema es especialmente crítico en VANETs, donde las señales relativas a mensaje de seguridad de pasajeros chocan y no se reciben a tiempo para evitar accidentes.

II. Limitaciones del Estándar IEEE 1609.4

Las densidades vehiculares variarán desde carreteras con muy pocos vehículos a zonas urbanas densamente pobladas. Por lo tanto, la capa MAC de la VANET tiene que ser escalable. El IEEE 1609.4 [2] se basa en la función de coordinación distribuida (DCF) como técnica MAC. El DCF emplea

CSMA/CA con el algoritmo de backoff exponencial binario. Este mecanismo se ha mejorado mediante el uso de las mismas técnicas de priorización que el IEEE 802.11e [6], es decir, la función de coordinación híbrida (HCF). Básicamente, el HCF permite usar espaciado entre tramas (por ejemplo, AIFS [i]) variable en función de la prioridad (i) del paquete (véase la fig. 1). Además, la longitud de la ventana de contención varía entre las diferentes prioridades.

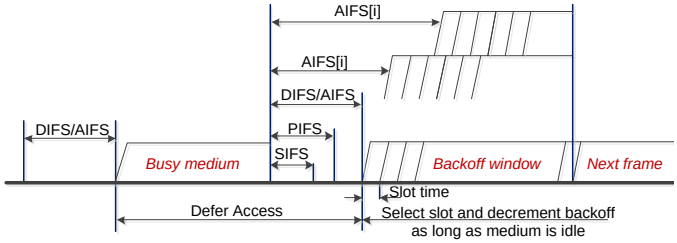


Figura 1. Priorización de acceso EDCA, como se especifica en [6].

Sin embargo, este mecanismo de MAC no es eficiente para redes densas. El CSMA/CA no evita totalmente las colisiones durante la emisión de mensajes de broadcast. Al igual que el tradicional unicast IEEE 802.11, éste presenta caídas drásticas de rendimiento en entornos poblados. Por otra parte, para la comunicación de broadcast, no hay control de errores ya que no hay acuses de recibo y por lo tanto no hay crecimiento del backoff exponencial. En este sentido, como el tamaño de la ventana de contención no se incrementa, la priorización es limitada e incluso aumenta la probabilidad de colisiones de paquetes. Así los mensajes de broadcast sufren de problemas de nodo oculto, debido a la falta de un RTS/CTS. Por otra parte, los mensajes de broadcast relativos a la seguridad vial se envían con la máxima potencia de transmisión, lo que aumenta la cobertura y, en consecuencia, la interferencia inter-RSU. De acuerdo a las diferentes intensidades de señal, se pueden distinguir tres rangos diferentes (ver Figura 2):

- *Rango de comunicación*: es la región en la que tanto umbral de sensibilidad del receptor del vehículo y la SINR se cumplen para la carga útil. Vehículos dentro de esta región de las RSUs son capaces de decodificar los paquetes.
- *Rango de detección*: es la región donde otros vehículos pueden detectar una transmisión en curso.
- *Rango de interferencia*: se inicia desde el punto en que no hay suficiente potencia de señal para decodificar el paquete. La transmisión de otras entidades en este rango interfieren y su SINR local es degradada por esta transmisión.

Vale la pena señalar que, aunque en teoría la región de interferencia es infinita, con el tiempo la potencia de transmisión de las RSUs es menor que el ruido térmico y por lo tanto puede ser ignorado. En cualquier caso, la probabilidad de tener varias RSU que se solapan en términos de alcance de la interferencia es mayor que en términos de alcance de la comunicación.

Por otro lado, el IEEE 1609.4 describe un de un protocolo de división de tiempo, donde el tiempo se divide en intervalos

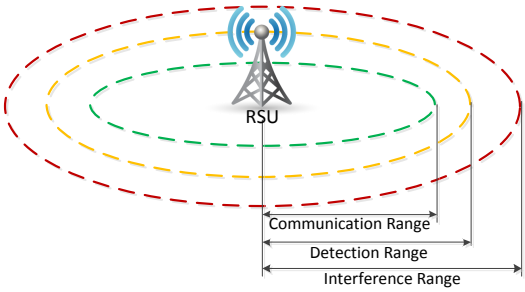


Figura 2. Rangos de transmisión de las RSUs.

entre el canal de control (CCH) y del canal de servicio (SCH) (véase la fig. 3). Por otra parte, los mensaje de broadcast en el CCH no son reconocidos y consecuentemente las colisiones no pueden ser detectadas. Así, el mecanismo único en el estándar IEEE 802.11 que tenía la función de mejorar la escalabilidad en el caso de mensajes de unidifusión (el backoff exponencial binario) no se puede utilizar en el canal de control en las VANETs. El hecho de que, en el caso de mensajes de broadcast, las colisiones no pueden ser reconocidas a partir de las transmisiones fallidas debido a que los errores de canal hacen que este mecanismo sea ineficiente.

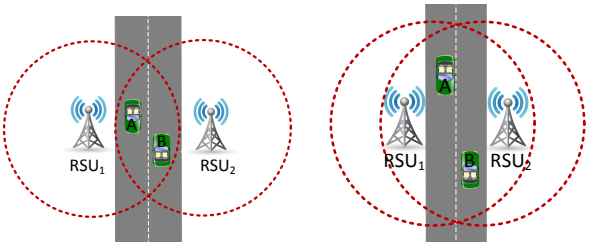
Figura 3. Intervalos multi-canal [2]

Por lo tanto, durante la transmisión el mecanismo MAC que se describe en el estándar IEEE 1609.4 incurrirá en altos retrasos debido a la conmutación de canal y sufrirá el problema de terminal oculto que dará lugar a colisiones en los mensajes de broadcast. Además, como estos mensajes no están autenticados, cualquier entidad con una interfaz 802.11p podría emular una RSU y difundir balizas que condujeran a la denegación de servicio. El IEEE 1609.4 actual no puede hacer frente a estos ataques que podrían conducir a una degradación grave del rendimiento de la red. Por lo tanto, durante el despliegue de RSUs se debe tener en cuenta que existe un equilibrio entre la cobertura y la interferencia entre RSUs. Desplegar un alto número de RSUs incrementará la cobertura pero la potencialmente inevitable superposición de cobertura dará lugar a interferencias.

III. Interferencias Inter-RSU

En esta sección, se analiza la interferencia entre varias RSUs. Diferentes escenarios de interferencia se distinguen de acuerdo a la distancia, D, entre las RSUs. En este trabajo, sólo tenemos en cuenta la interferencia dentro del alcance de las comunicaciones de las RSU. Una RSU se considera que es interferida por otra RSU si los vehículos de su rango de transmisión pueden decodificar transmisiones de la RSU interferente.

La Figura III muestra dos escenarios diferentes de interferencia inter-RSU, es decir, escenarios de tipo A y escenarios de tipo B corresponden a $R < D \leq 2R$ and $D \leq R$,



(a) Tipo-A ($R < D \leq 2R$) (b) Tipo-B ($D \leq R$)

Figura 4. Tipos de interferencia entre RSUs.

respectivamente, donde R es el rango de comunicación. Cabe destacar que para distancias más grandes (es decir, $D > 3R$), no hay interferencia entre ambas RSU. Antes de profundizar más en las características de cada escenario de interferencia, definimos la zona de solapamiento O como nuestra región de interés.

En los escenarios de tipo A, las RSU no están dentro del alcance de comunicación entre ellas y por lo tanto no pueden recibir paquetes de transmisión una de la otra. No obstante, las RSUs pueden recibir paquetes de los vehículos bajo la cobertura de la RSU interferente, de manera que la RSU interferente y los vehículos en su rango de transmisión pueden convertirse en nodos ocultos. Por ejemplo, en referencia a la figura 4(a), cuando la RSU_1 y la RSU_2 están transmitiendo mensajes de broadcast, estos mensajes podrían potencialmente chocar ya que ambas RSUs son nodos ocultos una a la otra. Por lo tanto, los dos vehículos en la región O sufrirán pérdidas de mensajes de broadcast. Así, la transmisión desde la RSU_1 no se recibe en su totalidad en el vehículo A debido a una colisión con los mensajes de broadcast de la RSU_2. Tradicionalmente, este problema se aborda utilizando los mensajess de negociación RTS/CTS/DATA/ACK. Sin embargo, los mensaje de broadcast tales y como están definidos en el estándar IEEE 1609.4 no utilizan ningún tipo de negociación. Por lo tanto, el efecto de RSU oculta será una de las principales razones de la pérdida de paquetes en la comunicación vehicular. En [7], Bianchi construyó un modelo analítico utilizando cadenas de Markov para estimar la colisión de paquetes en 802.11. Usando sus resultados y teniendo en cuenta que en el estándar 1609.4 no hay backoff exponencial, la probabilidad de colisión de n radiodifusión RSUs (ρ) se puede calcular como:

$$\rho = 1 - (1 - \varphi)^{n-1} \tag{1}$$

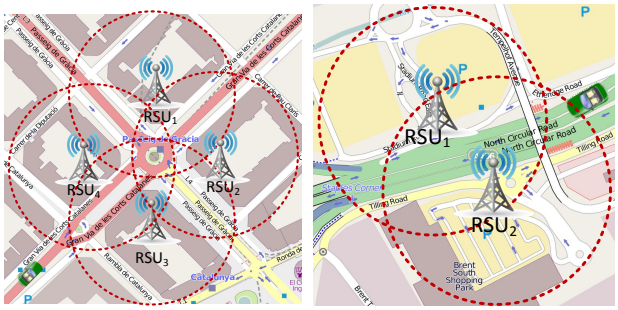
donde φ denota la probabilidad de una RSU envía mensajes de broadcast dentro de la ventana de contención CW sin usar el backoff exponencial. Esta probabilidad se puede calcular como:

$$\varphi = \frac{2}{CW + 1} \tag{2}$$

Para los escenarios Tipo-B (véase la fig. 4(b)), una RSU puede recibir transmisiones directas desde las RSUs interferentes y desde algunos o todos de los vehículos bajo la cobertura de la misma. El problema que enfrenta el escenario de interferencia de tipo-B es que todas las entidades en el rango de transmisión de cualquiera de las RSUs (es decir, vehículos o RSU interferente) pueden convertirse en potenciales nodos ocultos a la transmisión en curso. Como el mecanismo RTS/CTS no se usa para los mensajes de broadcast, los vehículos pueden estar expuestos a una pérdida de paquetes en cola en situaciones de alta densidad de vehículos donde el canal se encuentra ocupado la mayoría del tiempo. Esta pérdida de paquetes se debe a que todas las RSU expuestos a la interferencia llenan su la cola local de mensajes. En el peor de los casos, ni siquiera un sólo mensaje de broadcast llegará a los vehículos. Tal situación se puede describir como la congestión de mensajes local. La pérdida de paquetes se produce en función de la estrategia de descartar un mensaje. En el caso de la información de sensible a retardo, como mensajes sobre el estado de la carretera, sólo el más reciente puede ser de interés para los demás vehículos. La pérdida de paquetes en este caso afectaría a todos los paquetes excepto por el más reciente. Si ahora consideramos diferentes densidades de RSU se pone de manifiesto que, incluso en densidades localmente bajas, las RSU pueden estar expuestos a estos problemas si hay altas densidades en el rango de detección de portadora. En este caso, algunos nodos podrían ser bloqueados sin transmitir innecesariamente. Por lo tanto, en ambos tipos de escenarios de interferencia, es evidente que se producirá un importante número de colisiones de paquetes cuando se envían mensajes de broadcast.

IV. Evaluación

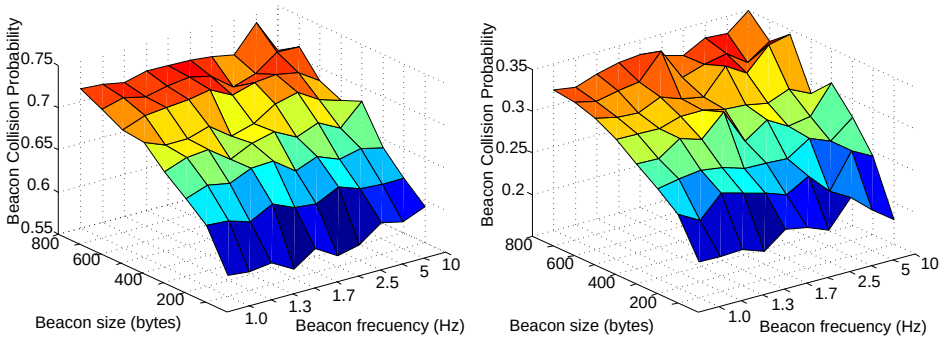
En esta sección, extensas simulaciones a nivel de paquete se llevan a cabo para validar las observaciones formuladas en el apartado anterior. Utilizamos el simulador VeinS [8] para evaluar el impacto de la interferencia entre RSUs. VeinS es un marco de simulación de comunicación inter-vehicular que integra el simulador de red OMNeT++/INET [9] y la herramienta de microsimulación de tráfico SUMO [10]. VeinS implementa un modelo de simulación multi-canal para IEEE 1609.4/802.11p que permite cubrir en su totalidad las características distintivas de esta tecnología.



(a) Intersección Urbana (Tipo-A) (b) Autopista (Tipo-B)

Figura 5. Escenarios de simulación.

Utilizamos dos escenarios reales (cada una representa un tipo diferente interferencia) para evaluar la interferencia entre RSUs (ver fig. IV). En primer lugar, se evalúa un cruce urbano de la ciudad española de Barcelona. De acuerdo con la autoridad de transportes española, cada año, en Barcelona, de 70 a 100 intersecciones se detectan con más de diez accidentes,



(a) Type-A (b) Type-B

Figura 6. Probabilidad de colisión de las señales de baliza P_{col}.

con un total de 1.500 accidentes, cerca del 60 % de los que se producen en toda la ciudad. Por lo general, estos accidentes se concentran en las intersecciones de las carreteras con dos carriles. El segundo escenario es una autopista urbana situada en la ciudad de Londres. Debido a la alta densidad de los coches y las carreteras en esta zona, es previsible que la cobertura de las RSUs se superpongan como en un escenario de interferencia de tipo-B. Los parámetros de configuración de las RSUs/vehículos se muestran en la Tabla II. Tenga en cuenta que un mismo automóvil se coloca en cada escenario moviéndose a través de la intersección en el tipo A y a través de la autopista en el escenario de Tipo-B. Cada balizas emisión RSU en el CCH con la más alta prioridad. SUMO [10] se utiliza para recrear un ambiente de tráfico real.

Parámetro	Valor
Potencia de Transmisión	20 mW
Tasa de bits	18 Mbps
Sensibilidad	-94.0 dBm
Ruido Térmico	-110.0 dBm

Cuadro I
RSU PARÁMETROS DE CONFIGURACIÓN.

El resto de los parámetros PHY/MAC se establecen de acuerdo con los valores por defecto que utiliza el VeinS [8]. Los experimentos de simulación para cada escenario se llevan a cabo con suficientes repeticiones para obtener resultados estadísticos significativos, y todos los intervalos de confianza están por encima del 95 % de la métrica correspondiente.

Parámetro	Valor
Velocidad	20 m/s
Max. Aceleración	5 m/s
Max. Deceleración	3 m/s
Ancho de banda del canal	10 MHz
Sensibilidad del receptor OBU	-94.0dBm

Cuadro II
PERFIL DE LOS VEHÍCULOS.

IV-A. Métricas de rendimiento

Definimos cuatro métricas diferentes para evaluar la interferencia entre RSUs:

- *Probabilidad de colisión de mensajes de broadcast* (P_{col}): probabilidad de que un mensaje de broadcast enviado por la RSU$_j$ colisiones con otro mensaje enviado por la RSU$_i$.
- *Retardo*: tiempo transcurrido desde la creación del mensaje de broadcast en la RSU$_j$ y la recepción en el vehículo$_i$. Este retardo sólo se calcula para los mensajes de broadcast enviados.
- *Caudal por vehículo* (T): tamaño de los mensajes de broadcast recibidos por un vehículo en particular durante un periodo de tiempo.
- *Tiempo entre llegadas*(τ): cantidad de tiempo entre la recepción de dos mensajes de broadcast consecutivos en el vehículo$_i$. Esto es importante desde el punto de vista de las aplicaciones en tiempo real. Idealmente, el tiempo entre llegadas sería equivalente al intervalo de generación de mensajes de broadcast.

IV-B. Resultados de la simulación

IV-B1. Probabilidad de colisión de mensajes de broadcast: La figura 6 muestra P_{col} para diferentes tamaños de los mensajes de broadcast (b_s) variando entre 100 a 800 bytes, y diferentes frecuencias de generación (BGF) de los mismos variando de 1 a 10 Hz. Como era de esperar, la probabilidad de colisión crece tanto con b_s como con BGF. Cabe destacar que P_{col} es mayor en el escenario de Tipo-A dado que todas las RSUs se comportan como nodos ocultos entre ellas. Así, el mecanismo para evitar las colisiones es totalmente ineficiente, y P_{col} alcanza valores superiores al 70 %. En el escenario de Tipo-B, el problema del terminal oculto no es tan frecuente, por lo que la probabilidad de colisión es menor.

El escenario con $b_s = 800$ bytes y BGF = 10Hz se muestra en la figura 7. En este caso, queda patente que cuando un vehículo está bajo la cobertura de 4 RSUs, el número de colisiones incrementa. En la autopista londinense, el mecanismo CSMA/CA evita la mayor parte de las colisiones pero no es capaz de evitar su totalidad.

La probabilidad de recepción necesaria depende del tipo de aplicación que soporte la red vehicular. Sin embargo, para

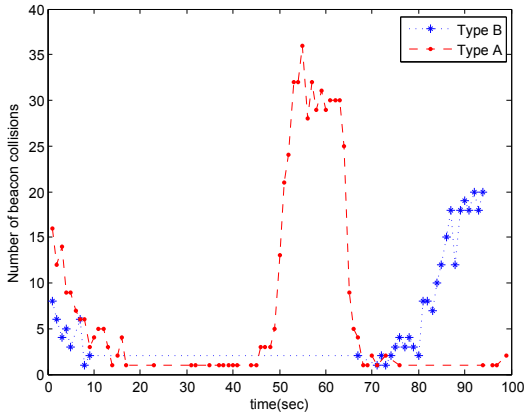
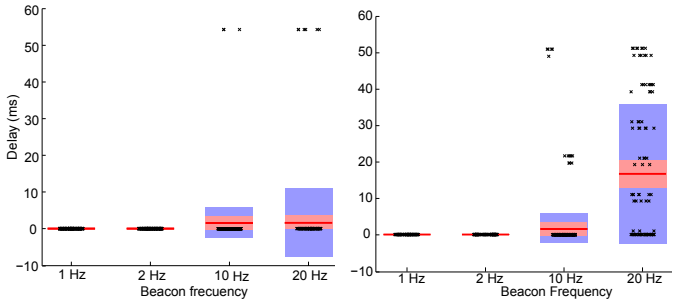


Figura 7. Número de colisiones para b_s= 800 bytes y BGF=10 Hz

aplicaciones de seguridad vial P_{col} no debería superar el 1 %. Como se infiere de los resultados obtenidos, este requisito no se alcanza cuando los vehículos se encuentra bajo la cobertura de dos o más RSUs que no se ven entre ellas. Los resultados muestran que una P_{col} por debajo del 1 % sólo se alcanza en escenarios de Tipo-B donde la BGF se encuentra por debajo de los 10Hz y los mensajes de broadcast son de un tamaño inferior a los 200 bytes.

IV-B2. Análisis del retardo: Adicionalmente, analizamos el retardo en la recepción de mensajes de broadcast variando las BGF, i.e., el tiempo transcurrido desde la generación en la RSU y la recepción en el vehículo. Tal y como se muestra en la figura 9, mientras que para frecuencias bajas (BGF$<$ 10 Hz) las diferencias entre los escenarios Tipo-A y Tipo-B son mínimas, para frecuencias grandes (BGF$>$ 10 Hz) t diferencias significativas aparecen. Esto se debe a la imposibilidad de distribuir todos los mensajes de broadcast durante el intervalo correspondiente del canal de control. Con esta tase de BGF, todos los mensajes de broadcast generados durante el intervalo del canal de servicio tienen que esperar hasta el próximo CCH para poder ser enviados. Por lo tanto, cualquiera de éstos deben esperar como mínimo 53 ms para ser envíaos. Cabe destacar que para BGF$>$ 10 Hz el retardo es mayor en el escenario de Tipo-B. La razón es que para este tipo de escenario cuando una RSU detecta que el canal está ocupado ésta entra en el período de backoff.



(a) Tipo-A (b) Tipo-B

Figura 9. Diagrama de caja del retardo para b_s= 800 bytes.

IV-B3. Caudal por vehículo: La figura 8 muestra el impacto de la BGF en el caudal de un vehículo. Como se esperaba, cuando se generan mensajes de broadcast de manera más frecuente, el caudal incrementa. Sin embargo, este incremento no es directamente proporcional a la BGF ya que existen más colisiones a medida que la BGF incrementa. Cabe reseñar que mientras en el escenario de Tipo-B el caudal se mantiene aproximadamente constante durante el período de simulación, en el escenario Tipo-A el caudal varía con el tiempo.

La figura 11 muestra el caudal para b_s= 800 bytes y BGF=10Hz. En el caso del escenario Tipo-A, cuando el vehículo está bajo la cobertura de las 4 RSUs, el caudal disminuye drásticamente. Esto es debido al gran número de colisiones. Después de 40s, el vehículo se encuentra situado en la intersección y las 4 RSUs están transmitiendo mensajes de broadcast como si el medio estuviera libre. De esta forman, casi todos estos mensajes colisionan (véase fig. 7)y el caudal se reduce a casi 0 KBps.

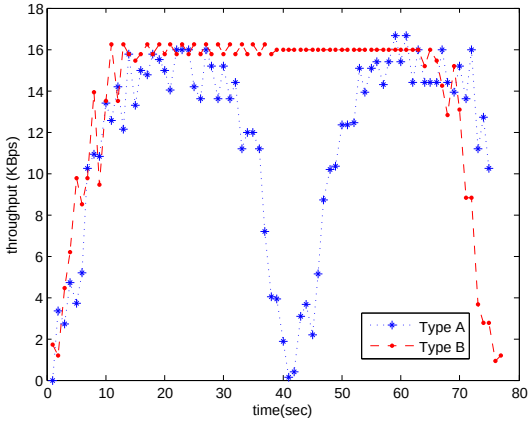
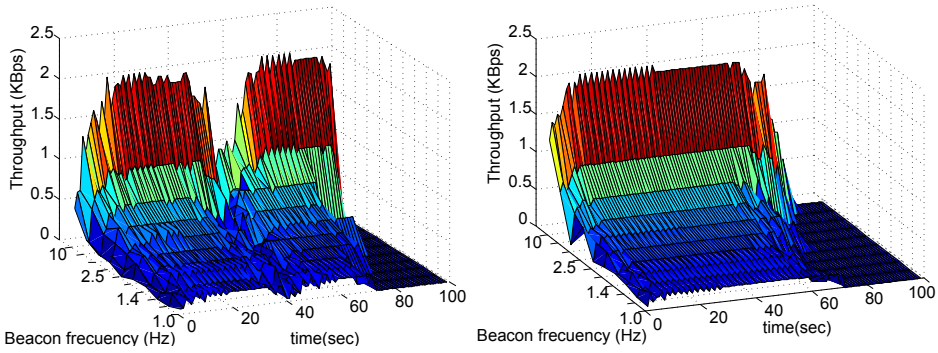


Figura 11. Caudal para b_s= 800 bytes y BGF 10 Hz

IV-B4. Inter-arrival Time: La figura 11 muestra la función de distribución acumulativa empírica (ECDF) de τ para diferentes BGF. A medida que la BGF aumenta la probabilidad de colisión también lo hace, con un efecto perjudicial en el tiempo entre llegadas de los mensajes de broadcast. Por lo tanto, τ aumenta para valores más grandes de BGF. Esta es una consecuencia directa de las colisiones de estos mensajes. Cuando una RSU transmite un mensaje de broadcast y éste se pierde, no es retransmitido. En el siguiente intervalo de transmisión CCH, la RSU transmitirá un nuevo mensaje con información actualizada. Este efecto es más evidente en los escenarios de tipo-A, ya que hay más colisiones. Debido a esta periodicidad, la ECDF de τ adopta una forma de escalera. En el escenario de tipo-B, τ es menor (ya que hay menos colisiones).

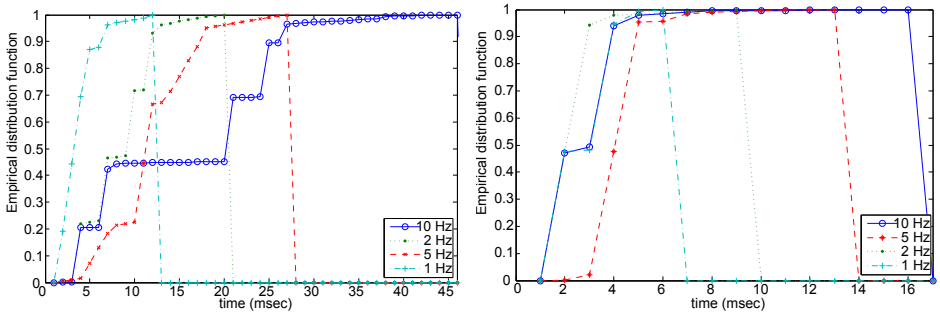
V. Conclusiones

En este trabajo, hemos demostrado el impacto de interferencia entre RSUs en dos escenarios diferentes: una intersección urbana y una autopista Hemos demostrado que la técnica de acceso al medio actual definida en el estándar IEEE 1609.4 no es capaz de hacer frente a la interferencia causada por la superposición de cobertura de RSUs. Hemos llevado a cabo un análisis de los efectos de este solape en el rendimiento del broadcasting en VANETs. Los efectos sobre las colisiones de



(a) Tipo-A (b) Tipo-B

Figura 8. Caudal vs BGF



(a) Tipo-A (b) Tipo-B

Figura 10. ECDF del tiempo entre llegadas para $b_s = 800$ bytes.

los mensajes de broadcast, el caudal por vehículo y tiempo entre llegadas de los mensajes de broadcast se analizan en un estudio de simulación realista. Los resultados muestran que este tipo de interferencia es crítica, y puede causar gran número de colisiones, grandes retrasos, variabilidad en los tiempos entre llegadas de paquetes y caídas en el rendimiento. El análisis de la probabilidad de colisión muestra que el rendimiento de emisión cae por debajo de 30 % cuando un vehículo está bajo la cobertura de cuatro RSUs que no se ven la una a la otra. Por otra parte, debido al esquema de conmutación de canal se define en el estándar IEEE 1609.4, el retardo puede ser superior al 54 ms, lo que hace inviable el despliegue de una aplicación de seguridad vial.

Los resultados obtenidos de este análisis no sólo conducen a una mejor comprensión de los efectos de interferencia entre s en VANETs, sino también se pueden utilizar para mejorar la asignación de asignación de canal, optimizar el balanceo de carga y diseñar nuevas técnicas de control de potencia. Por otra parte, sobre la base de estos resultados, esquemas de despliegue de RSU podrían mejorarse para aumentar la cobertura de la red, mientras se optimiza la interferencia entre RSUs. El trabajo futuro incluye controlar adaptativamente e la potencia de transmisión y la directividad de la antena para conseguir un sistema RSUs que es capaz de operar en áreas densas.

Agradecimientos

Este trabajo ha sido financiado por el Ministerio español de Ciencia y Educación bajo los proyectos CONSOLIDER-ARES (CSD2007-00004) y TEC2011-26452 “SERVET”, y por la Generalitat de Catalunya bajo la ayuda 2009 SGR 1362.

Referencias

[1] *IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments*, May 2008.

[2] “IEEE draft standard for wireless access in vehicular environments (WAVE) - multi-channel operation,” *IEEE 1609.4/D8.0*, pp. 1 –92, June 2010.

[3] A. Vinel, Y. Koucheryavy, S. Andreev, and D. Staehle, “Estimation of a successful beacon reception probability in vehicular ad-hoc networks,” in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, ser. IWCMC ’09, 2009, pp. 416–420.

[4] C. Campolo and A. Molinaro, “On vehicle-to-roadside communications in 802.11p/wave vanets,” in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, march 2011, pp. 1010 –1015.

[5] C. Campolo, Y. Koucheryavy, A. Molinaro, and A. Vinel, “Characterizing broadcast packet losses in ieee 802.11p/wave vehicular networks,” in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, sept. 2011, pp. 735 –739.

[6] “IEEE Standard for Information Technology - Telecommunications and Information Exchange between systems - local and metropolitan area networks - specific requirements,” *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11)*, pp. 1 –189, November 2005.

[7] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[8] C. Sommer, R. German, and F. Dressler, “Bidirectionally coupled network and road traffic simulation for improved ivc analysis,” *Mobile Computing, IEEE Transactions on*, vol. 10, no. 1, pp. 3 –15, jan. 2011.

[9] A. Vargas, “Objective modular network testbed in c++ (omnet++),” version 4.2. Available: www.omnetpp.org.

[10] D. Krajzewicz, G. Hertkorn, C. Rössel, and P. Wagner, “SUMO (simulation of urban mobility); an open-source traffic simulation,” in *4th Middle East Symposium on Simulation and Modelling (MESM2002)*, ser. MESM2002, 2002, pp. 183–187.

Redes neuronales aplicadas al proceso de aprendizaje de un sistema de respuestas a intrusiones automático

Pilar Holgado, Víctor A. Villagra, Verónica Mateos.
Departamento de Ingeniería y Sistemas Telemáticos,
Universidad Politécnica de Madrid
Avenida Complutense, 30, 28040, Madrid
pilarholgado@dit.upm.es, villagra@dit.upm.es, vmateos@dit.upm.es.

***Resumen*- La contribución de este artículo es el uso de métodos de aprendizaje automático en la arquitectura realizada dentro del proyecto RECLAMO en trabajos previos. La arquitectura se basa en un AIRS (sistema de respuestas a intrusiones automático) que infiere la respuesta más apropiada a un ataque, teniendo en cuenta el tipo de ataque, la información de contexto del sistema y la red, y la reputación del IDS que ha reportado la alerta. También, es imprescindible conocer el ratio de éxito y fracaso de las respuestas lanzadas ante un ataque, de tal manera que, además de tener un sistema adaptativo, se consiga la capacidad de autoaprendizaje. En este ámbito es donde las redes neuronales entran en juego, aportando la clasificación de éxito/fracaso de las respuestas.**

***Palabras Clave*- Métodos de aprendizaje automático, Redes Neuronales, Retropropagación, Ontología, OWL, IDMEF, AIRS.**

I. INTRODUCCIÓN

Todos los sistemas que componen una unidad organizativa tienen que estar protegidos contra ataques externos, ya sea para que no decaigan los niveles de disponibilidad de los servicios que ofrecen a sus clientes, como para mantener información confidencial de la empresa y el funcionamiento correcto de sus aplicaciones.

Cada vez es mayor el número de eventos de seguridad, su sofisticación y extensión [1]. Los Sistemas de Detección de Intrusiones (IDS) [2], han evolucionado rápidamente, y en la actualidad, hay herramientas muy sofisticadas basadas en los distintos paradigmas (estadísticas basadas en anomalía [3], basadas en firmas e hibridas [4]) con un alto nivel de confiabilidad. Los IPS (Sistemas de Prevención de Intrusiones) también se han desarrollado por combinación de un IDS con respuestas reactivas básicas, como reestablecer una conexión. Los IRS (Sistemas de Respuestas a Intrusiones) aprovechan el concepto de IPS para logar una respuesta específica de acuerdo a unas reglas predefinidas.

Hoy en día, los IRSs están jugando un papel importante en la arquitectura de seguridad. Estos sistemas mitigan el impacto de ataques que intentan comprometer la integridad, confidencialidad y disponibilidad de los recursos del sistema. Un Sistema de Respuestas Automático (AIRS) proporciona la mejor defensa posible y acorta o cierra la ventana de oportunidades hasta que el administrador del sistema puede tomar un rol activo en defender contra el ataque.

Un AIRS es un sistema de seguridad que elige y ejecuta respuestas automatizadas contra las alertas detectadas por IDSs, con el objetivo de mitigarlas o reducir su impacto [5].

En el proceso de respuestas a intrusiones es necesario definir varias métricas que ofrecen un medio para medir diferentes parámetros útiles para la selección de la respuesta, tales como, confiabilidad del IDS, el nivel de actividad de la red, fiabilidad de los informes de intrusión, la importancia de los componentes de la red y la complejidad, gravedad, coste y eficiencia de las respuestas.

Los AIRS existentes tienen un enfoque fijo para las métricas de respuesta, por lo que las métricas no pueden ser elegidas de manera dinámica. En este artículo se propone una arquitectura de seguridad que es capaz de seleccionar la respuesta más apropiada dinámicamente teniendo en cuenta una serie de factores, como el contexto del sistema, el coste de la respuesta, el valor del recurso atacado y la eficiencia de las respuestas.

En este contexto, el proyecto RECLAMO (Red de sistemas de Engaño virtuales y Colaborativos basados en sistemas Autónomos de respuesta a intrusiones y Modelos de cOnfianza), dentro del proyecto R&D financiado por el Ministerio de Ciencia e Innovación, define un AIRS capaz de interpretar métricas dinámicamente.

El sistema autónomo desarrollado está basado en modelos formales de información definidos con ontologías [7] para combinar la información de las intrusiones, parámetros de autoevaluación del sistema aprendidos en usos anteriores, confianza y reputación de los diferentes componentes, así como la información enviada por otros IDS/IPS colaborativos en el mismo o distinto dominio. Esta información será evaluada con un conjunto de métricas de seguridad representadas en un lenguaje formal de especificación de comportamiento, SWRL (Semantic Web Rule Language) [6], para razonar e inferir la respuesta más apropiada, teniendo en cuenta toda la información de entrada y otros criterios especificados.

Para homogeneizar la información se usan ontologías basadas en IDMEF (Intrusion Detection Message Exchange Format) [8], donde las alertas son representadas como instancias de clases en la ontología [9]. La ontología ha sido definida usando OWL (Web Ontology Language) [10], aprovechando las ventajas de la web semántica, como es la inferencia.

En definitiva, se ha desarrollado un AIRS adaptativo, haciendo un balance del daño que causaría la intrusión con el coste de la respuesta. Además, se realiza el análisis de la eficiencia de la respuesta, para que el AIRS sea totalmente autónomo y aprenda de manera automática.

Para la evaluación de la respuesta que se ha lanzado tras la llegada de un ataque se propone el uso de redes neuronales. Las redes neuronales se encuentran dentro de una rama de inteligencia artificial denominado aprendizaje automático. Dentro de este grupo, hay una gran cantidad de técnicas de aprendizaje [11]. El papel del algoritmo realizado es la clasificación del éxito o no de la respuesta ejecutada, y mediante un ratio de respuesta, el sistema sea capaz de auto-aprender para futuras incidencias del mismo tipo.

A continuación se indica cómo se va a estructurar el artículo. Primero se muestran trabajos previos de sistemas similares al propuesto. Posteriormente se resumirá la arquitectura del AIRS basado en Ontologías, la métrica y el proceso de inferencia llevado a cabo. Tras ello, se introducen las redes neuronales, el algoritmo seleccionado y su proceso de aprendizaje. Después, se detallará el escenario de pruebas. Y finalmente, las conclusiones y el trabajo futuro.

II. TRABAJOS PREVIOS

El uso de sistemas automáticos para la prevención, detección y respuesta de intrusiones es un concepto clave en la investigación de los últimos años. A continuación se muestra algunos de estos proyectos actuales.

Un sistema de respuestas a intrusiones adaptativo basado en inmunidad artificial llamado MAIM [16] implementa un modelo de políticas de respuesta automática de acuerdo con el peligro global de la red y el host en tiempo real, en vez de centrarse en los ataques individuales. Para ello utiliza una estrategia basada también en sistemas biológicos como es el sistema inmunológico. Por otro lado, realizan el aprendizaje del estado de peligro de la red para la detección de falsos positivos y luego realizar una respuesta más o menos estricta a un ataque con políticas predefinidas. En nuestro caso, realizamos el análisis del contexto para la detección de falsos positivos y realizamos una respuesta más o menos exigente en función del coste del ataque y la respuesta con respecto a la importancia del recurso comprometido. Además, el aprendizaje se realiza sobre la efectividad de la respuesta a un ataque dado.

En [17], se aborda las intrusiones a través de varias ejecuciones con ráfagas de respuesta y al final de cada ráfaga, un mecanismo para medir la efectividad de las respuestas. Esto se realiza con una máquina de estados finito. La efectividad de la respuesta se mide en función de las consecuencias sobre el host relativas a la integridad, disponibilidad, confidencialidad y rendimiento del mismo, lo que repercute en el orden en que serán ejecutadas dentro de la ráfaga. Por otro lado, divide en niveles las ráfagas de respuestas, basado en la efectividad de estas en el histórico de respuestas aplicadas, de manera que modifica el orden del conjunto de respuestas a ejecutar. En nuestro caso, la efectividad medida en las respuestas ejecutadas es totalmente adaptativo y cuantitativo, de manera que es más precisa la clasificación de respuestas.

COSIRS [18], se basan en tres factores para la evaluación de las respuestas, el coste del daño causado por la intrusión, el coste de la respuesta automática a la intrusión y el coste operacional. Al contrario que el sistema presentado, sólo se basan en la efectividad de la respuesta anterior por lo que el sistema carece de inteligencia.

En general, las redes neuronales se han utilizado en distintos ámbitos de la seguridad de red. Entre ellos se encuentra el ámbito de detección de intrusiones. Se pueden encontrar tanto el uso de algoritmos supervisados como no supervisados. Por ejemplo en [19] y [20] usan el algoritmo de Retropropagación.

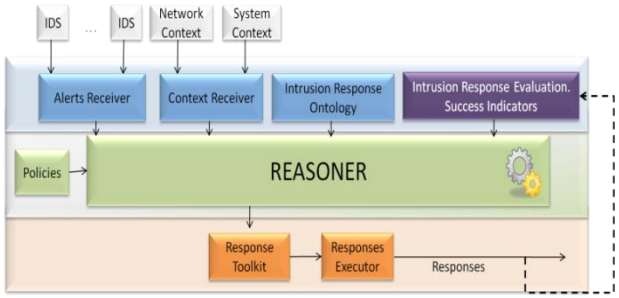


Fig. 1. Arquitectura del AIRS basado en Ontologías

III. ARQUITECTURA

En la Fig. 1. se representa el funcionamiento del AIRS propuesto en [12]. El objetivo de la arquitectura mostrada es elegir la respuesta óptima de un conjunto de respuestas disponibles.

El AIRS recibe un conjunto de entradas, incluyendo, informes de intrusiones, información de contexto, políticas de las métricas de seguridad y la ontología de respuesta a intrusiones. Las políticas especifican diferentes métricas que serán elegidas dependiendo del contexto y tipo de intrusión. A continuación se explica en detalle los módulos principales.

- *Reasoner*: Ejecuta procesos de inferencia para elegir la mejor respuesta basado en los módulos, *Policies*, *Alerts Receiver*, *Context Receiver* e *Intrusion Response Ontology*. Utiliza OWL para definir toda la información del proceso de respuesta. Tras procesar las entradas se infiere un conjunto de respuestas óptimas en Response Toolkit. Por último, el módulo Response Executor es el que lleva a cabo la respuesta inferida.
- *Policies:* Conjunto de reglas SWRL que especifican el comportamiento del AIRS. Estas políticas son definidas por el administrador del sistema. En este módulo se definen las métricas de respuesta de acuerdo con la información de contexto para así realizar un AIRS adaptativo, proactivo y cost-sensitive.
- *Alerts Receiver*: Tratan con alertas de distintos IDSs, por lo que es común que generen la misma alerta pero con distinto formato y sintaxis; por lo que este módulo garantiza que las alertas sean semánticamente iguales y se correspondan con los conceptos definidos en la Ontología.
- *Context Receiver*: Realiza la correspondencia de los datos de los módulos recogidos en *Network Context* y *System Context* con los conceptos definidos en la Ontología.
- *Intrusion Response Ontology:* Define los conceptos y relaciones necesarios para gestionar la seguridad de redes a través de un AIRS (Fig. 2.). La ontología se basa en la estructura IDMEF, que sigue un modelo de clases y propiedades. Hay dos clases directamente relacionadas con el sistema de evaluación, *Response* y

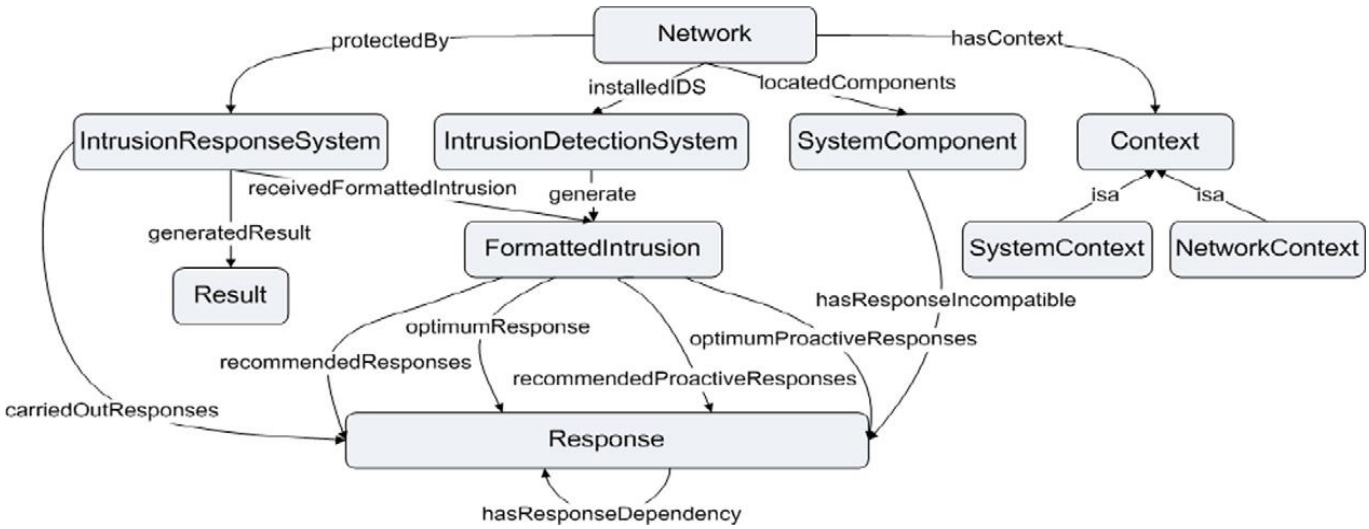


Fig. 2. Ontología de respuestas a intrusiones

Result. Durante la integración del sistema de evaluación en el AIRS, será necesario modificar y añadir propiedades a estas clases. En la clase *Response*, *executionTimes* y *sucessFactor*, número de veces que se lanza una respuesta y ratio de satisfacción de la respuesta, respectivamente. En la clase *Result*, se añade la propiedad *responseEfficiency*, que se corresponde con el cociente entre *executionTimes* y *successFactor*. Se actualizan dichos valores en la respuesta cada vez que es lanzada.

- *Intrusion Response Evaluation:* Se encarga de evaluar las respuestas lanzadas por el AIRS mediante el uso de una red neuronal previamente entrenada con muestras del contexto del sistema y de red.

IV. Métricas de respuesta y proceso de inferencia

Las métricas aplicadas para inferir la respuesta más apropiada han sido definidas y analizadas en [13]. A continuación se muestra un resumen:

- Reducción del daño: Realiza el balance del coste del daño causado por el ataque y el coste de despliegue de la respuesta. Es la primera de las métricas aplicadas.
- Coste mínimo: De todas las respuestas inferidas se lanza la respuesta de menor coste cuando el componente afectado no es muy relevante para la organización.
- Alta severidad y eficiencia: Si el recurso de la organización es muy relevante o crítico se utiliza esta métrica para maximizar la severidad y éxito de la respuesta.

El proceso de inferencia del AIRS se basa en estas métricas para razonar la respuesta más apropiada siguiendo los siguientes pasos:

1. Recolección de información cada vez que llega una intrusión:
    a. Comparación del contexto del sistema y la red en un estado normal, es decir libre de intrusiones y en un entorno seguro, que ha sido almacenado anteriormente con el contexto después de la intrusión
    b. Informes extraídos de los IDSs
2. Inferencia de un conjunto de respuestas recomendadas:
    a. Primero se comprueba si es la primera intrusión que llega al sistema.
    b. En el caso de que sea la primera, se infieren las respuestas recomendadas mediante las políticas SWRL a través de la Métrica de reducción del daño, basada en el tipo de intrusión y los parámetros de contexto.
    c. Si el ataque es similar a uno anterior, se ejecuta la respuesta seleccionada anteriormente si fue satisfactoria.
    d. En otro caso, se infieren las respuestas recomendadas como en b.
3. Se selecciona la respuesta óptima a inferir del conjunto de respuestas recomendadas, de acuerdo con la importancia del recurso comprometido:
    a. Recursos poco relevantes: Se aplica la métrica del coste mínimo
    b. Recursos relevantes: Se aplica la métrica de mayor eficiencia y severidad de menor coste
    c. Recursos críticos: Utiliza la métrica de mayor eficiencia y severidad, aplicando la respuesta más severa sin tener en cuenta el coste de su despliegue.

V. Redes neuronales

Las redes neuronales artificiales son redes interconectadas masivamente en paralelo y con organización jerárquica, las cuales intentan interaccionar con los objetos del mundo real del mismo modo que hace el sistema nervioso [14].

Las neuronas que conforman una red neuronal están interconectadas a través de su sinapsis, que es lo que permite la transmisión de información. No todas las conexiones son iguales, por lo que se le asigna un peso de conexión.

Los pesos obtenidos tras la fase de aprendizaje determinan la salida de la red, por lo que se podría decir que forman la memoria de la red neuronal.

Las redes neuronales son particularmente útiles para solventar problemas que no pueden expresarse como una serie de pasos, tales como reconocimiento de patrones, clasificación, predicción de series y minería de datos. En nuestro caso será utilizado para la clasificación de respuestas a intrusiones.

.

La clasificación es un proceso muy relacionado con el reconocimiento de patrones. Una red neuronal entrenada para clasificación está diseñada para tomar muestras de entradas y clasificarlas en grupos. Estos pueden ser difusos, es decir sin límites claramente definidos; o con fronteras definidas en el caso de seleccionar valores umbrales.

A continuación se van a presentar las ventajas de estas redes:

1. Aprendizaje adaptativo mediante algoritmos de entrenamiento, de acuerdo a experiencias previas
2. Autoorganización: Representación propia de la información.
3. Tolerancia a fallos: Robustez frente a destrucción parcial de la información.
4. Integración modular, por su fácil inserción dentro de la tecnología existente.
5. Son una eficiente herramienta de clasificación que puede ser aplicada a problemas complejos con gran cantidad de parámetros.
6. Es confiable en la predicción de problemas de regresión y clasificación.
7. Proporcionan muy buena clasificación en entornos ruidosos.
8. Robustez frente a destrucción parcial.

Por último, presentamos las desventajas de este tipo de algoritmos:

1. La fiabilidad de las predicciones se degrada con la presencia de múltiples soluciones causadas por muchos mínimos locales.
2. Es difícil determinar y entender su rendimiento.
3. Hay que ajustar cuidadosamente por el usuario un gran número de parámetros para obtener unos buenos resultados.
4. Son muy lentas tanto en fase de entrenamiento como de validación
5. Utilización de validación cruzada para evitar sobreajustes.
6. Sensibles a los conjuntos de datos incompletos
7. La falta de reglas para la definición de la red como por ejemplo la elección del algoritmo de aprendizaje, la arquitectura de la red, el número de neuronas por capas, el número de capas.

A. Algoritmos de entrenamiento de las redes neuronales

Hay muchas maneras de entrenar una red neuronal. Generalmente, las categorías de algoritmos de entrenamiento se encuentran dentro de:

- Supervisado: Se sabe a priori como son las características a clasificar. Al conocer la salida esperada, el entrenamiento se beneficia de la supervisión de un maestro. Por tanto, se necesita un conjunto de entrenamiento con un conjunto de datos de entrada previamente clasificado o con su salida objetivo conocida. La red supervisada realiza una serie épocas, hasta que la salida se corresponde con la esperada con un ratio de error razonablemente bajo o con la condición de parada que se considere más apropiada. Una época se corresponde con la ejecución del algoritmo para todas las muestras del conjunto de entrenamiento. Es el tipo de entrenamiento más habitual. Ejemplos de este tipo de entrenamiento son el Perceptrón Simple, Red Adeline, el Perceptrón Multicapa, red de Retropropagación y Memoria Asociativa bidireccional.
- No supervisado: No se sabe las categorías o características a clasificar, por lo que este aprendizaje se basa en una estadística para determinar el patrón. Se suele utilizar para la clasificación de los patrones en grupos diferenciados que se van descubriendo a medida que progresa el entrenamiento. Al igual que en el aprendizaje supervisado, se ejecuta el algoritmo durante varias épocas hasta llegar a la condición de parada. Ejemplo de este tipo de redes son las Memorias Asociativas, las redes de Hopfield, la Máquina de Boltzmann, la Máquina de Cauchy, las redes de Aprendizaje Competitivo, las redes de Kohoneno, Mapas Autoorganizativos, las Redes de Resonacia Adaptativa (ART).
- Redes híbridas: Tienen un enfoque mixto entre las dos anteriores. Utilizan una función de mejora para facilitar la convergencia. Un ejemplo son las redes de Base Radial.
- Aprendizaje Reforzado: Se sitúa a medio camino entre el entrenamiento supervisado y el autoorganizado. Hay que proporcionar datos de entrada a la red neuronal sin indicar la salida esperada. Sin embargo, para cada salida generada por la red neuronal se dice si es o no correcta para cada una de las entradas, para la realización de la realimentación de la red basada en ensayo-error.

VI. RETROPROPAGACIÓN

En la evaluación de la respuesta seleccionada por el AIRS, se ha optado por el uso de las redes neuronales porque es un problema en el que no se puede determinar si la respuesta ha sido o no satisfactoria de una manera clara para cualquier sistema o intrusión.

Se propone el algoritmo de Retropropagación (backpropagation) o también llamado Perceptrón Multicapa (LMP), ya que se puede disponer de un conjunto de entrenamiento para tener un aprendizaje supervisado. Los beneficios de éste modo de aprendizaje son:

- Redes que convergen más rápido a la clasificación esperada que un algoritmo no supervisado.
- Aprendizaje guiado por observaciones pasadas: Se llevará a cabo a través de un conjunto de ejemplares clasificados que se obtienen durante la experimentación dentro de un sistema de pruebas.

Esta red es capaz de clasificar a partir del contexto si la respuesta ha sido correcta, lo que se representaría con un 1 o incorrecta, con un –1, en la capa de salida de la red. Para darle más detalle al resultado en vez de una función escalón se toma una salida real para así saber en qué factor la respuesta se ha enfrentado a la intrusión, consiguiendo un intervalo comprendido entre -1 y 1 denominándolo SuccessLevel. Tras ello se calcula la eficiencia de la respuesta con las siguientes fórmulas:

$$SuccessFactor = \sum_{i=0}^{j-1} SuccessLevel_i \qquad (1)$$

$$ResponseEfficiency = \frac{SuccessFactor}{ExecutionTimes} \quad (2)$$

Donde j y ExecutionTimes es el número de veces que se ha ejecutado esa respuesta.

A. Parámetros de entrada

Los parámetros se podrían corresponder con los parámetros obtenidos del contexto del sistema y red tras la ejecución de la respuesta. La desventaja radica en que el valor del contexto que podríamos indicar como "normal", es dependiente del dispositivo o sistema de la organización. Por tanto, para que sea totalmente independiente y que el mismo algoritmo se pueda implantar en todos los host, los parámetros elegidos se corresponden con el grado de anomalía del contexto del sistema y la red tras la ejecución de la respuesta lanzada por el AIRS con respecto al contexto normal.

El contexto de red ha sido recogido con un solo parámetro y para el contexto del sistema se han usado siete parámetros obtenidos tras la monitorización del sistema con Nagios Core Tool [15]:

- Estado: Si el sistema está o no activo.
- Latencia: Tiempo en el que los agentes de Nagios tardan en corresponder al servidor de Nagios.
- Uso de CPU: Anomalías debidas a sobrecarga del sistema.
- Espacio de disco: Para comprobar cambios drásticos en el espacio de disco duro.
- Número de procesos activos: La mayoría de las intrusiones contienen procesos que antes no existían.
- Número de usuarios.
- Número de procesos zombies: Algunos virus aumentan el número de procesos zombies para que sufran una degradación del rendimiento.

El contexto de anomalía se encuentra dentro de un rango de [0-10]. Pero, hay que tener en cuenta que la representación de las entradas en una red neuronal debe ser numérica y normalizada, ya que valores muy altos pueden perjudicar la efectividad del algoritmo. Debido a ello, antes de introducir el contexto como entrada de la red, es necesario dividirla por 10, para que quede en un rango de [0-1].

B. Función de transferencia

La función de activación se corresponde con la definición de una función para normalizar la salida de la red neuronal tras el procesamiento de la información. Se clasifican en tres tipos:

- Función identidad: Mantiene el valor de salida procesado
- Umbral: Función escalón binaria o bipolar.
- Sigmoidal: Normaliza teniendo en cuenta un rango real de salida. También puede ser binaria o bipolar.

En este caso se utilizará una función sigmoidal para determinar el grado de satisfacción de la respuesta ante la intrusión. Por otro lado, nos basaremos en funciones bipolares ya que consiguen antes la estabilización del error. Dentro del grupo de funciones sigmoidales probaremos con dos:

- Función Sigmoide logística bipolar:

$$f(x) = \frac{2}{1 + e^{-x}} - 1 \quad (3)$$

- Función Tangencial Hiperbólica:

$$f(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}} \quad (4)$$

C. Condición de parada

Como condición de parada se tiene en cuenta el error cuadrático medio (ECM):

$$ECM = \sum (y_{obj} - y_{en})^2 \quad (5)$$

Donde y_{obj} es la salida deseada y y_{en} es la salida generada por el algoritmo.

Por tanto, el algoritmo intenta encontrar los pesos de las neuronas que minimicen el ECM para dar la clasificación más acertada posible.

D. Validación

Esta última etapa es muy importante porque permite determinar si se requiere de entrenamiento adicional. Para ello se debe tener otro conjunto, denominado conjunto de test, que validará la generalización de la red.

Para evitar sobreajustes, es decir, que haya un sobreaprendizaje de la red debido a demasiada información presentada en el conjunto de entrenamiento, se utiliza el método de validación cruzada. Es decir, que toda la muestra disponible se divide en dos partes, una para el conjunto de entrenamiento y otro para el de test, con ejemplos de todos los tipos de patrones.

E. Número de neuronas y número de capas

La relación entre el número total de parámetros y el número de patrones debe estar entre el 10% o 15% para que haya suficientes patrones para la generalización.

Hay que tener en cuenta la relación entre patrones y parámetros, para la elección del número de neuronas de la capa oculta:

- Muy pocas neuronas en la capa oculta conducirán a un alto error de entrenamiento y un alto error de generalización debido al underfitting.
- Si por el contrario, se tienen muchas neuronas en la capa oculta se podría obtener un bajo error de entrenamiento, pero se tiene un alto error de generalización debido al overfitting (sobreajuste).

Otro tema a tener en cuenta es el número de capas ocultas, ya que al aumentar el número de capas ocultas, se puede disparar el número de parámetros. Además, la mayoría de los problemas se puede resolver de manera óptima en 1 o 2 capas ocultas, debido a que se ha demostrado que aunque el aprendizaje sea más rápido al principio, luego puede estabilizarse antes de encontrar el error mínimo.

Por otro lado, normalmente el número óptimo de neuronas en la capa oculta es de 2/3 la suma de neuronas de la capa de entrada y de salida.

VII. ALGORITMO DE APRENDIZAJE

El algoritmo de Retropropagación se basa en el método de descenso del gradiente para acercarse a al mínimo error cuadrático.

$$w_{ij}(t+1) = w_{ij}(t) + \Delta w_{ij} \quad (6)$$

$$\Delta w_{ij} = \alpha \cdot \delta_j \cdot x_i \quad (7)$$

Donde δ_j es el error propagado, x_i el valor de la entrada y α es el factor de aprendizaje.

Sin embargo, la función de error suele tener muchos mínimos locales, quedando el algoritmo atrapado en un mínimo local no deseado. Para prevenirlo, se puede hacer que los cambios de pesos sinápticos dependan del gradiente medio de los puntos de un entorno, en vez de depender de un solo punto. Pero dicha modificación suele requerir un gran esfuerzo computacional y no resultar eficiente. A continuación se muestran dos mejoras del algoritmo posibles.

A. *Factor de aprendizaje adaptativo*

Esta modificación del algoritmo de aprendizaje, se basa en la modificación del factor de aprendizaje inicial,α, adaptándose según las necesidades del aprendizaje de la siguiente forma:

- Si las pendientes tienen el mismo signo, los pesos cambiarán más rápido.

$$\alpha(t+1) = \alpha(t) + k \quad (8)$$

  Donde k se denomina valor de capa y se le asigna el valor de 0,035.
- Si las pendientes tienen distinto signo, los pesos cambiarán más lentamente.

$$\alpha(t+1) = \alpha(t) \cdot (1-\gamma) \quad (9)$$

  Donde γ tiene el valor de 0,333.

B. *Aprendizaje por momentos*

Rumelhart, Hinton y William (1986) [21] propusieron que se tuviera en cuenta el gradiente de la iteración anterior y realizar un promedio con el gradiente de la iteración actual. Dicho promedio produce una reducción drástica de las fluctuaciones del gradiente en iteraciones consecutivas evitando que el algoritmo sea tan lento y por tanto poco eficiente.

$$\Delta w_{ij} = \alpha \cdot \delta_j \cdot x_i + \mu \cdot \left(w_{ij}(t) - w_{ij}(t-1)\right) \quad (10)$$

Donde μ es el momento, que suele tener el valor de 0,9 como valor óptimo.

La inclusión del Momento en el algoritmo de Retropropagación tiende a acelerar la bajada en direcciones similares al descenso, mientras que si se tiene oscilaciones de signo en iteraciones consecutivas, se ajustará el peso en cantidades pequeñas, actuando como estabilizador.

VIII. PRUEBAS

En el ámbito del proyecto RECLAMO, se ha comenzado la validación de las distintas partes de la arquitectura propuesta. En concreto, se han realizado diversas pruebas de concepto con redes pequeñas para la validación de la eficacia de clasificación obtenida por el algoritmo propuesto en este artículo. Todas ellas han sido satisfactorias, obteniendo clasificaciones correctas.

No obstante, las siguientes fases de validación se están realizando para garantizar la viabilidad del algoritmo con respecto a la clasificación de respuestas dado el contexto.

De manera aproximada, teniendo en cuenta lo mencionado en el apartado VI.E. , para la realización del entrenamiento con una capa oculta, ha sido necesario recoger como mínimo unas 200 muestras compuestas de diferentes contextos recogidos tras introducir en el sistema distintos tipos de ataque y respuestas posibles.

Concretamente se está realizando la batería de pruebas con los tipos de ataques que se han clasificado dentro de la ontología: Backdoors, Buffer Overflow, DoS, Exploits, Mapping, Scanning, Sniffing, Hijacking, Spoofing, Cookie Poisoning, Cross Site Scripting, Parameter Tampering, SQL Injection, Brute Force, Diccionary Attack, Trojan, Virus, Worms.

IX. CONCLUSIONES

En este artículo se propone el uso de aprendizaje automático para entrenar al sistema de respuestas a intrusiones desarrollado. Concretamente, se ha optado por el uso del algoritmo de Retropropagación ya que al ser un algoritmo supervisado el entrenamiento de la red neuronal convergerá más rápidamente.

Por otro lado, el uso de esta tecnología nos permite la clasificación de cualquier respuesta, sea cual sea la intrusión que llego al sistema. Esto quiere decir que se pueden obtener buenos resultados aunque se presenten intrusiones desconocidas para el sistema; ya que este algoritmo se ha desarrollado de manera independiente al tipo de intrusión.

Una vez que tenemos entrenada la red, este algoritmo se puede implantar en cualquier host independientemente de cual sea su uso o importancia como activo de la organización.

Como trabajo futuro inmediato se está realizando la validación del uso de dicho algoritmo para la clasificación de respuestas del AIRS. Para ello, la implementación se ha realizado de manera totalmente parametrizable, de manera que podamos realizar estudios de rendimiento de distintas arquitecturas de red neuronal y así obtener los resultados más óptimos.

Además de esto, como trabajo futuro se propone el uso de otras técnicas de mejora del algoritmo como son:

- La inicialización de pesos aleatoria basada en rango
- Utilización del método SAB que combina momento y aprendizaje adaptativo.

Por último, se estudiarán las posibilidades para desarrollar respuestas proactivas en el sistema propuesto. Con esto, podremos adelantarnos a los pasos del atacante para evitar de manera anticipada posibles intrusiones.

AGRADECIMIENTOS

Este trabajo ha sido financiado parcialmente con el apoyo del MICINN Español (Proyecto RECLAMO, Virtual and Collaborative Honeynets based on Trust Management and Autonomous Systems applied to Intrusion Management, con códigos TIN2011-28287-C02-01 y TIN2011-28287-C02-02).

REFERENCIAS

[1] Symantec Corp., “Internet Security Threat Report, Vol. 17,” Abril 2012.

[2] Anderson, James. "Computer Security Threat Monitoring and Surveillance". Washing, PA, James P. Anderson Co. 1980.
[3] H. J. Mattord. "Principles of Information Security Course Technology". 2008. ISBN 9781423901778: 290-301.
[4] Ali Aydin M, Halim Zaim A, Gökhan Ceylan K. "A hybrid intrusion detection system design for computer network security". Comput Elect Eng, 2009; 35(3):517–26.
[5] Stakhanova N, Basu S, Wong J. "A taxonomy of intrusion response system." Int J Inform Comput Secur. 2007; 1(1/2):169–84
[6] I. Horrocks, P.F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, M. Dean, "SWRL: A semantic web rule language combining OWL and RuleML". W3C Member Submission, 21, 2004.
[7] J. E. López de Vergara, E. Vázquez, A. Martin, S. Dubus, M. N. Lepareux. " Use of ontologies for the definition of alerts and policies in a network security platform", Journal of Networks, Vol. 4, Issue 8 (2009) pp. 720-733
[8] H. Debar, D. Curry, B. Feinstein. "The Intrusion Detection Message Exchange Format (IDMEF)". IETF Request for Comments 4765, Marzo 2007
[9] J.E. López de Vergara, V.A.Villagrá, J.I. Asensio, J. Berrocal. "Ontology-based network management: study cases and lessons learned". J Network Syst Manage 2009; 17(3):234–54.
[10] D. L. McGuinness, F. van Harmelen. "OWL Web Ontology Language Overview. " W3C Recommendation 10 Febrero 2004
[11] Hu, Xunlei Rose, and Eric Atwell. "A survey of machine learning approaches to analysis of large corpora." Proceedings of the Workshop on Shallow Processing of Large Corpora, Lancaster University, UK. 2003.
[12] V. Mateos, V.A. Villagrá, F. Romero. "Ontologies-Based Automated Intrusion Response System. " Computacional Intelligence in Security for information Systems 2010. Volume 85/2010. 2010:99/106
[13] V. Mateos. V. A. Villagrá, F. Romero, J. Berrocal. "Definition of response metrics for an ontology-based Automated Intrusion Response Systems." Computers & Electrical Engineering. 2012
[14] J. Heaton. "Introduction to Neural Networks for Java". 2nd Edition.
[15] Nagios Core Tool : http://www.nagios.org/projects/nagioscore
[16] Ling-xi Peng, Dong-qing Xie, Ying Gao, Wen-bin Chen, Fu-fang Li, Wu Wen. "An Inmune-inspired Adaptative Automated Intrusion Response System. International Journal of Computational Intelligence" Systems, 2012, 5:5, 808-815.
[17] Alireza Shameli-Sendi, Julien Desfossez, Michel Dagenais, Masoume Jabbarifar. "A Retroactive- Burst Framework for Automated Intrusion Response System", Journal of Computer Networks and Communications, Volume 2013.
[18] Justina, Aderonke, and Adesina Simon. "A credible cost-sensitive model for intrusion response selection." In Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on, pp. 222-227. IEEE, 2012.
[19] Z. Mahmood, C. Agrawal, S. S. Hasan, S. Zenab, "Intrusion Detection in Cloud Computing environment using Neural Network". International Journal of Research in Computer Engineering & Electronics, 2012. 1(1), 19-22.
[20] R. S. Naoum, Abid, N. A., Z. N. Al-Sultani, "An Enhanced Resilient Backpropagation Artificial Neural Network for Intrusion Detection System". IJCSNS, 2012. 12(3), 11.
[21] Rumelhart, D.E., Hinton, G.E. y Williams, R.J. (1986). Learning internal representations by error propagation. En: D.E. Rumelhart y J.L. McClelland (Eds.). Parallel distributed processing (pp. 318-362). Cambridge, MA: MIT Press

Aplicación del concepto de SDN a las redes vehiculares

Xavier Ramón, Agustín Zaballos, Guiomar Corral
Departamento de Ingeniería, La Salle
Universitat Ramon Llull
c/ Quatre Camins, 2, 08022-Barcelona
xavir@salle.url.edu, zaballos@salle.url.edu, guiomar@salle.url.edu

***Resumen*- Miles de personas fallecen anualmente en accidentes de tráfico en todo el mundo. Los esfuerzos por mejorar la seguridad de los vehículos, tanto activa como pasiva, están dando sus frutos, reduciendo el número de accidentes así como sus consecuencias. Aunque estas actuaciones están reduciendo el número de heridos y fallecidos en las carreteras, las instituciones de todo el mundo siguen haciendo hincapié en la necesidad de reducir este número aún más. Este documento presenta el estudio de la aplicación del concepto de *Software Defined Networks* a las redes vehiculares con el objetivo de aportar nuevos conceptos que puedan ayudar a la mejora de la seguridad pasiva, a partir del uso de las redes de telecomunicaciones en vehículos. A partir de los servicios que deben ofrecer las redes vehiculares, tanto de seguridad como de información, se definen los requisitos que debe cumplir la red de telecomunicaciones para soportar dichos servicios, con el fin último de aumentar la seguridad de los usuarios. Para la consecución de este objetivo se propone una red que debe ser completamente escalable y debe incorporar nuevos elementos, como son los dispositivos que permiten la comunicación entre vehículos (V2V) y la comunicación vehículo a infraestructura (V2I) que se encargan de analizar y transmitir la información útil generada por diversos sensores en sentido vehículo-red y viceversa. Esta red debe ser completamente configurable y debe adaptarse a los requisitos de transmisión de los datos en cada momento, por lo que se propone el uso de una red definida por software juntamente con la composición de servicios, así como el uso de comunicaciones V2I, cuya combinación permite mejorar la fluidez de la información por toda la infraestructura. Esto permite al conductor de un vehículo conocer la situación de la calzada que va a utilizar mucho antes de llegar, siendo éste capaz de maniobrar y evitar situaciones de peligro que puedan afectar a su integridad y ayudando, por lo tanto, a reducción de accidentes y muertos en las carreteras.**

***Palabras Clave*- SDN, V2I, Service Composition, Redes Vehiculares**

I. Introducción

Los accidentes de tráfico matan anualmente a más de 1300 personas en las carreteras españolas contabilizadas a 24 horas del accidente. Con un descenso medio del 13,8% anual, los accidentes de tráfico han pasado a convertirse en un problema de vital importancia para nuestra sociedad [1]. Algunas de las medidas introducidas en los últimos años, como el carnet por puntos en 2006, ha reducido de forma significativa el número de víctimas mortales de los accidentes de tráfico. Aún así, el número de fallecidos es, todavía, muy elevado. Una de las principales causas de los accidentes mortales es la velocidad, que provoca el 40% de estos accidentes. Siendo conscientes de este elevado porcentaje de accidentes mortales que son causados por el exceso de velocidad, o por la velocidad inadecuada, podemos concluir que una gran causa de la mortalidad en las carreteras se origina por la limitada concepción del entorno por parte del conductor. Por ello, si el conductor es el responsable del vehículo y su percepción es limitada, para mejorar la seguridad en las carreteras deberíamos mejorar la percepción por parte del conductor. Esto contribuiría a aumentar el nivel de conciencia de un conductor sobre las condiciones actuales de la vía por la que circula y reducir el nivel de incertidumbre sobre el entorno que lo rodea, de forma que le ayudaría a adecuar su actitud a las condiciones reales y actuales del tráfico.

Con estas bases nacen las redes vehiculares: mejorar la percepción del entorno del vehículo informando al conductor sobre estos hechos para evitar posibles accidentes. Las fuentes de esta información deben ser, generalmente, otros vehículos que han detectado ese cambio en el entorno antes que el vehículo que será destinatario de esta información. La fuente decide que este cambio en el entorno debe ser comunicado a otros vehículos con el fin de mejorar la seguridad en la zona, de manera que los vehículos que reciben esta nueva información hasta ahora desconocida, mejoran su conocimiento sobre el entorno y son capaces de prever situaciones que hasta ahora no eran posibles de anticipar.

El objetivo de este trabajo es el estudio y desarrollo de una propuesta de implementación de infraestructura para la comunicación entre vehículos usando una red escalable gracias a Software Defined Network (SDN) y Composición de servicios y que sea capaz de proveer de conexión a vehículos separados geográficamente usando una red de transporte transparente para los vehículos. La meta de esta implementación es permitir la mejora de la percepción que tienen los vehículos sobre el escenario en el que se encuentran, usando tanto la comunicación entre vehículos como la comunicación entre vehículo e infraestructura con el objetivo final de mejorar la seguridad en la vía y, en consecuencia, reducir el número de accidentes de tráfico así como sus consecuencias.

El resto del artículo se organiza de la siguiente manera: En la sección II se introduce el estado del arte sobre los trabajos realizados hasta el momento en el campo de redes vehiculares. En la sección III se explica la relación entre redes vehiculares y las redes SDN, mientras que en la sección IV se presenta la composición de servicios y su aplicación a las redes vehiculares. En la sección V se describen los distintos tipos de nodos de las redes vehiculares. En la sección VI se introduce la utilidad de las

redes tolerantes al retardo. La sección VII muestra la propuesta realizada para la mejora de la seguridad en los vehículos y la sección VIII muestra las conclusiones sobre el trabajo realizado. Finalmente, la sección IX propone una serie de trabajos futuros a realizar para la mejora de la seguridad en los vehículos.

II. Trabajos anteriores

Durante los últimos años se han publicado diversos trabajos enfocados a tratar los temas de ITS (*Intelligent Transport System*), mayoritariamente relacionados con las soluciones tecnológicas para mejorar la operación y la seguridad del transporte terrestre, principalmente. El tema ha sido tratado desde diferentes puntos de vista, tanto desde un punto de vista de modelación del canal de transmisión [2, 3], como desde el punto de vista de las ventajas del balizamiento de las infraestructuras [4]. Más centrados en un aspecto en concreto, algunos trabajos se centran en el estudio y simulación de algunas situaciones específicas, como la evasión de colisiones en cruces urbanos [5, 6]. Otros, más generalistas, definen el conjunto de servicios y tecnologías que deberían proveer las redes vehiculares [7, 8, 9, 10].

Los trabajos referenciados proveen de los diferentes servicios que deben ofrecer y los protocolos que deben usar las redes vehiculares. Sin embargo, no hacen una propuesta específica de la tecnología que se debería usar para una posible implementación. Otros artículos ofrecen un entorno de simulación completo sobre el que realizar las experimentaciones necesarias para evaluar el rendimiento de diferentes protocolos, pero no proponen ningún entorno de implementación usando un hardware existente [9, 10].

En este artículo se propone el estudio de las ventajas que puede suponer para las redes vehiculares el uso de dos conceptos emergentes tales como las redes definidas por software y la composición de servicios. La interrelación entre estos conceptos se traduce en un conjunto de tablas que vinculan, para cada servicio útil en una red vehicular, cuales son las características de red relacionadas y, consecuentemente, qué tecnología o protocolo puede dar mejor respuesta a dichas características. Estos resultados se muestran en las Tablas I y II, como se detallará posteriormente. Introducir estos conceptos nos permite testear cualquier protocolo en un entorno real, exigiendo como único requisito disponer del hardware necesario para cumplir con los estándares de transmisión que deseen ser evaluados. Además, este trabajo también presenta una implementación en un escenario de pruebas de los distintos conceptos tratados, con el fin de evaluar la viabilidad del uso de este concepto en las redes del futuro. Tanto el estudio de los conceptos como la experimentación se detallan a continuación.

III. Redes vehiculares y SDN

Las redes vehiculares son redes móviles que suministran información sobre el tráfico vehicular y pueden ser usadas, entre otras cosas, para mejorar la seguridad así como para evitar congestiones. En este tipo de redes sus nodos son vehículos, y debido al movimiento de dichos vehículos, presentan cambios constantes en su topología. Las redes vehiculares también reciben el nombre de VANET (*Vehicular Adhoc Network*).

Las comunicaciones en los vehículos se pueden clasificar en 3 tipos principalmente: V2V, V2I y V2G.

- V2V (*Vehicle to Vehicle*): se refiere a las comunicaciones entre los vehículos para diseminar la nueva información creada por uno de los vehículos.
- V2I (*Vehicle to Infrastructure*): se refiere a cualquiera de las comunicaciones que se pueden establecer entre un vehículo y la infraestructura que está utilizando, por ejemplo, las balizas de una carretera, o RSU (*Road Side Unit*).
- V2G (*Vehicle to Grid*): se refiere a la comunicación que puede establecer un vehículo con la infraestructura eléctrica. Este tipo de comunicaciones puede utilizarse para que el vehículo informe a la red eléctrica del inicio de la recarga de sus baterías, por ejemplo.

A continuación se hace énfasis en las características diferenciadoras y más relevantes de cada una de las redes. En V2V cobran especial importancia las características de *authentication*, *unicast*, *geocast*, *multihop* y *mobility* para permitir validar el origen de la información, y transmitir dicha información al nodo o grupo de nodos que corresponda, teniendo en cuenta que son nodos que se desplazan a alta velocidad y que es posible que el destino se encuentra a varios saltos de distancia. En comunicaciones V2I, las características más destacadas son: *authentication*, *unicast*, *multicast*, *geocast*, *ACL* y *mobility*. La finalidad de estas características es permitir valorar el origen de la información y la correcta transmisión de la información, normalmente a un salto permitiendo la movilidad y filtrando la información que aporte valor añadido de la que no. Finalmente, las características que principalmente se deben cumplir para las comunicaciones V2G son *authentication*, *reliability*, *latency* y *real time*. El objetivo es autenticar a la entidad emisora de la información, así como garantizar que esta información es correctamente transmitida y a baja latencia, debido a los estrictos requisitos de tiempo de la red eléctrica.

Es de gran importancia entender que cada uno de los tipos de comunicaciones en los vehículos tiene unos requisitos de conectividad que son muy diferentes entre ellos. Debemos ser conscientes de que nos encontramos ante un tráfico heterogéneo con unos requisitos de calidad de servicio muy diferentes entre ellos sobre una misma infraestructura.

Tabla I
CARACTERÍSTICAS DE RED QUE PUEDE SOPORTAR CADA PROTOCOLO

	WSN	IEEE 802.11	PLC	MANET	Automotive ethernet	Ethernet	DES	3DES	AES	Homomorfic encryption	GPRS	UMTS	LTE	GPS	GALILEO	DiffServ	IntServ	PAP	CHAP	TRILL	OSPF	IS-IS	RIP	GATA	AODV	OLSR	ZRP
Encryption	3	5	1	1	0	3	1	4	5	5	2	3	4	0	0	0	0	0	3	0	0	0	0	0	0	1	0
Authentication	1	4	0	1	0	2	0	0	0	0	5	5	5	0	0	0	0	2	5	4	4	4	4	0	0	0	0
QoS	2	3	2	1	5	5	0	0	0	0	1	1	3	0	0	5	5	0	0	4	4	4	4	0	0	0	0
Reliability	2	3	3	3	5	5	0	0	0	0	4	4	4	3	4	4	4	0	0	5	5	5	4	4	4	5	4
Latency	2	4	1	1	5	4	0	0	0	0	0	2	5	1	2	5	5	0	0	5	5	5	3	0	0	4	3
Jitter	2	2	1	1	0	5	0	0	0	0	0	0	4	0	0	5	5	0	0	5	5	5	5	0	0	0	0
Unicast	5	5	5	5	5	5	0	0	0	0	5	5	5	0	0	5	5	5	5	5	5	5	5	5	5	5	5
Multicast	0	5	3	3	0	5	0	0	0	0	0	0	3	0	0	5	5	0	0	5	5	5	5	0	0	0	0
Geocast	0	1	0	0	0	0	0	0	0	0	1	1	1	5	5	0	0	0	0	0	0	0	0	0	0	0	0
Need of Positioning System	0	0	0	0	0	0	0	0	0	0	0	0	0	5	5	0	0	0	0	0	0	0	0	0	0	0	0
Tolerance to delay	1	1	3	2	0	5	5	5	5	5	3	2	1	5	4	0	0	2	2	0	0	0	1	5	5	0	3
DoS Defense System	1	0	1	0	0	5	0	0	0	0	0	0	0	0	0	3	3	3	5	3	3	3	2	0	0	0	0
ACL	0	0	1	0	0	3	0	0	0	0	0	0	0	0	0	5	5	0	0	0	0	0	0	0	0	0	0
Multihop	4	2	5	5	5	5	5	5	5	5	5	5	5	0	0	5	5	5	5	5	5	5	5	5	5	5	5
Real time	1	3	2	3	5	5	4	4	3	4	0	4	5	4	5	3	2	0	0	5	5	5	4	0	0	1	0
Bandwidth	1	4	3	3	3	5	0	0	0	0	0	2	5	1	1	0	0	0	0	5	4	4	4	3	3	1	2
Mobility	4	4	0	4	0	0	5	5	5	5	5	5	5	5	5	3	3	5	5	0	1	1	1	5	5	5	5
TOTAL:	29	46	31	33	33	62	20	23	23	24	31	39	55	29	31	48	47	22	30	51	51	51	47	27	27	27	27

Por lo tanto, debemos ser conscientes de las diferentes tecnologías y protocolos existentes actualmente y de las problemáticas que son capaces de solucionar cada una de ellas, como se muestra en la Tabla I. En esta tabla se resume el estudio realizado en este trabajo sobre los protocolos o tecnologías más relevantes respecto a las redes vehiculares en relación con las características que pueden soportar. La selección de las tecnologías se ha basado en los diferentes bloques que debe implementar la red para ser eficiente, escalable, segura y adaptable.

Para ello, en la Tabla I se han clasificado algunas de las tecnologías existentes en la actualidad junto con las características del tráfico de las redes vehiculares y se ha ponderado cada una de las tecnologías con una puntuación de más idoneidad (5) a no aplicable (0). De esta forma, dicha tabla nos muestra de una manera visual las diferentes características que pueden tener una red vehicular y el nivel de afinidad que muestran una serie de protocolos con estas características. Esto nos permite evaluar de manera efectiva, cual es el mejor protocolo existente para solucionar cada una de las necesidades de las redes vehiculares. En la última fila de la tabla se incluye una valoración global de cada uno de los protocolos evaluados, donde una nota más alta implica más afinidad para el uso en redes vehiculares; aunque se debe tener en cuenta que el problema que soluciona cada uno de ellos no es excluyente sobre los demás.

Por otro lado, SDN es una arquitectura de red emergente, donde el control de la red se desacopla de la función de comunicación y permite ser programable. Dicha separación del plano de control permite abstraer las aplicaciones y los servicios de red de la infraestructura base, de forma que estos pueden manejar la red como una entidad lógica. Esta propiedad permite construir redes especialmente escalables y flexibles y que se adapten de forma rápida a las necesidades de cada momento.

Por ello, la utilización de la Tabla I junto con el uso de SDN, permite decidir al sistema cuál de todo el conjunto de protocolos disponible debe usar en cada momento para comunicarse con la infraestructura teniendo en cuenta los diferentes servicios que debe proporcionar la red en cada momento. Como consecuencia, esta tabla nos permitirá decidir el conjunto de protocolos que debemos utilizar en la implementación realizada para conseguir unos resultados óptimos de encriptación, autenticación, movilidad y transmisión de datos en tiempo real entre otros con el fin de que la red sea capaz de proveer los servicios de la Tabla II.

La potencia del uso de SDN en este caso reside en el hecho de poder adaptar diferentes características de la red al tráfico que circula por ella. Por ejemplo, en un funcionamiento normal de la red, en el que no haya incidencias, el protocolo de encaminamiento que se use puede ser reactivo, realizando un cambio a un protocolo de encaminamiento proactivo en el caso de que se produzca una incidencia y sea necesaria la comunicación en tiempo real y sin interrupciones del vehículo con la infraestructura. Al mismo tiempo, un servicio que no se considere importante por la red en ese mismo instante puede ser eliminado o no priorizado en ese momento.

IV. La composición de servicios aplicada a las redes vehiculares

El concepto de composición de servicios se basa en el diseño de los servicios en forma de componentes que puedan ser intercambiados de manera sencilla con el objetivo de disponer del mejor valor agregado.

Es importante destacar que el uso de SDN permite utilizar el concepto de la composición de servicios para optimizar el uso de la red para la transmisión de cada flujo de datos independiente. Para ello, se debe tener en cuenta también el conjunto de actores diferentes que pueden actuar en las redes vehiculares. En cuanto a la composición de servicios, esta característica nos permite formatear la información según las necesidades de transmisión de la red y de la información. Por ejemplo, en el caso de enviar una comunicación entre dos dispositivos sanitarios no será necesario usar encriptación si el canal es seguro, sin embargo, en el caso de usar una red no segura será necesario usar la encriptación para mantener el secreto de las comunicaciones.

Para la correcta implementación de la composición de servicios debemos definir, en primer lugar, las características del flujo de tráfico de cada uno de los servicios que soportará la red vehicular. El estudio y análisis realizado sobre las características de red para los distintos servicios se ha sintetizado en la Tabla II. Esta tabla nos permite relacionar algunos de los servicios que se pueden ofrecer sobre las redes VANET con las características del tráfico que se debe generar para que este servicio pueda funcionar de manera óptima.

La correcta adaptación de la infraestructura de comunicaciones a las características del tráfico nos permitirá una mejor experiencia del usuario, así como una mejora en la seguridad del conjunto de vehículos que participen en el intercambio de información. Usando la composición de servicios, la red es capaz de modificar el formato de la información a transmitir según las características de red, teniendo en cuenta, por ejemplo, añadir redundancia a la

Tabla II
CARACTERÍSTICAS DE RED NECESARIAS SEGÚN SERVICIO

	Encryption	Authentication	QoS	Reliability	Latency	Jitter	Unicast	Multicast	Geocast	Need of Positioning System	Tolerance to delay	DoS Defense System	ACL	Multihop	Real time	Bandwidth	Mobility
Intersection Collision Avoidance	0	1	5	5	5	3	4	1	4	5	0	2	0	0	5	1	5
Safe distance advertisement	0	1	3	5	4	3	4	3	3	5	2	2	0	4	3	1	2
In vehicle signage	0	2	3	3	1	1	1	4	3	4	4	3	0	1	1	1	0
Curve speed/angle warning	0	3	4	4	4	3	1	5	3	1	1	3	1	1	1	2	5
Passing assistance	0	1	5	5	5	3	5	3	0	5	1	2	0	3	5	1	3
Platooning	0	5	5	5	5	5	5	5	3	5	0	5	3	5	5	2	3
Internet access	1	3	1	0	2	2	5	0	0	0	5	3	3	5	1	5	5
Traffic flow management	5	5	3	3	2	2	4	4	4	5	3	2	0	3	2	2	5
Traveler information	3	0	1	3	2	2	5	0	5	4	4	4	0	2	2	3	5
Automatic cruise control	0	3	4	5	5	3	4	4	4	5	1	3	1	4	5	1	3
Vehicle tracking and tracing	4	5	5	5	5	5	4	1	0	5	4	5	2	4	5	3	5
Traffic monitoring	4	5	2	5	4	2	5	5	5	5	4	4	1	4	2	2	2
Station advertisement	0	2	0	5	4	1	2	3	5	3	2	5	3	3	5	1	0
Adaptative speed limit	0	5	3	4	4	3	0	4	5	4	1	4	0	4	4	1	2
Traffic light scheduling	0	3	3	5	4	1	1	2	5	5	0	5	0	5	5	2	5
Emergency vehicle advertisement	0	5	5	5	5	3	0	1	5	5	0	5	0	5	5	3	5
Emergency services	0	2	5	5	5	5	2	4	4	5	0	4	0	4	5	4	5
Parking assistance	0	0	0	5	3	4	5	3	3	3	3	4	0	1	2	2	1
Post crash warning	0	2	5	5	4	2	2	4	5	5	1	2	0	4	2	1	5
Road condition information	3	5	2	4	2	1	1	2	4	3	2	3	3	4	4	3	5
Inter-vehicle applications	5	5	1	3	1	3	5	2	1	0	2	4	3	5	4	5	5
Parking payments	5	5	1	5	3	2	5	3	2	0	0	1	0	0	5	1	1
Repair and maintenance	5	5	1	3	2	0	5	3	0	0	5	1	1	0	0	1	1
Multimedia files	2	5	0	5	0	0	5	3	0	2	5	2	4	1	0	5	1
TOTAL:	37	78	67	102	81	59	80	69	73	84	50	78	25	72	78	53	79

información si ésta se debe enviar por un segmento de la red en la que la confiabilidad de la correcta transmisión de la información es baja debido a efectos del canal de transmisión.

V. Tipos de nodos en una red VANET

Una vez que los diferentes servicios y sus respectivas características están definidos, es necesario diferenciar los diferentes nodos de los que se compone la red. Básicamente se pueden distinguir dos tipos de nodos en una red tipo VANET, los nodos móviles y los nodos estáticos, que se describen a continuación.

A. Nodos móviles

Estos nodos se refieren a los dispositivos instalados en las OBUs (*On Board Unit*) de los diferentes vehículos que pueden circular por una vía y que permiten la transmisión de datos. La principal característica de estos nodos es que no disponen de una localización específica, si no que puede cambiar con el paso del tiempo y a una velocidad elevada. Su función es la de analizar los datos que genera un vehículo, evaluar si se produce algún evento que sea necesario comunicar a otros dispositivos y, en caso afirmativo, decidir el modo en el que hará llegar la información al resto de dispositivos, tanto si son otros vehículos como si es un nodo estático.

B. Nodos estáticos

Un nodo estático es aquel en el que la movilidad es prácticamente nula. Pueden estar instalados como balizas (RSU) en diferentes emplazamientos como, por ejemplo, puntos kilométricos, señales de tráfico o áreas de servicio. La principal función de este tipo de nodos es la de anunciar información que puede ser interesante para los nodos móviles, tales como información referente al estado de la vía o el listado de precios de una estación de servicio. Además, este tipo de nodos también deberá encargarse de la retransmisión de información generada por otros dispositivos móviles que no pueda ser entregada en el momento de su generación.

Es de vital importancia prestar especial atención al hecho de que los dos tipos de nodos son muy diferentes entre sí, principalmente en el aspecto de la movilidad. Sin embargo, será necesario que estos dos tipos de dispositivos sean interoperables de manera transparente con el fin de conseguir que la información fluya de manera correcta, aportando valor añadido a la solución propuesta.

Esto nos obliga a utilizar un direccionamiento y un protocolo de encaminamiento que sea capaz de manejarse con estos tipos de nodos tan diferentes entre sí. El direccionamiento a nivel de enlace dependerá, obviamente, del protocolo que se utilice en cada caso. En el caso del protocolo de encaminamiento, se deberá usar un algoritmo que sea capaz de manejar la movilidad de todos los nodos de la red.

VI. La persistencia de la información: Delay Tolerant Network

Las redes vehiculares y, más concretamente, las comunicaciones V2V, deben ser consideradas como redes tolerantes al retraso o DTN (*Delay Tolerant Network*). Una red DTN debe abordar los problemas técnicos asociados a redes heterogéneas que pueden carecer de conectividad continuada de red. Este tipo de redes se caracterizan por estar en entornos con retardo variable o imprevisto de las comunicaciones, o bien por sufrir tasas de error variables y altas, o bien por la movilidad variable de los equipos, o bien por la comunicación oportunista entre los distintos nodos de la red.

Uno de los problemas principales de las comunicaciones V2V es que los dos dispositivos deben ser capaces de comunicarse uno con el otro. Para ciertos tipos de tráfico esto es estrictamente necesario, debido a que la información que se genera en ese momento tiene un efecto inmediato en la situación del tráfico actual. Sin embargo, para otro tipo de tráficos, la información tiene una validez más duradera y puede darse el caso de que no sea posible transmitir esa información en el momento en que se genera porque no existe un camino posible entre emisor y receptor en una determinada zona geográfica, denominada como ZOR (*Zone Of Relevance*).

En el caso de que se produzca un accidente en una carretera de doble sentido se generarán los dos tipos de tráfico comentados anteriormente: por un lado, a los vehículos que sigan el mismo sentido de la marcha que el vehículo que genera la información, se les debe informar de la situación de inmediato y estos vehículos deberán informar a nuevos vehículos que se acerquen al punto del accidente con el fin de mejorar la seguridad en la zona. Por otro lado, cuando la información sea capaz de llegar a uno de los vehículos situados por delante del punto de accidente, este vehículo deberá avisar a los vehículos que viajan en sentido contrario del accidente, con el fin de aumentar la seguridad en el sentido contrario de circulación.

La incertidumbre que se produce al no poder asegurar el tiempo que este vehículo podrá seguir alertando a los vehículos que vienen en sentido contrario manifiesta la necesidad de transformar esta información en permanente, siendo tolerable al retardo, aunque siendo todavía totalmente válida. Por ello, la información deberá ser transmitida desde el vehículo que disemina la información hacia un nodo capaz de almacenar esta nueva información y retransmitirla cuando sea necesaria a los nuevos vehículos que entren en la zona de influencia de la ZOR. De esta manera, el diseminador de la información libera recursos y se asegura la vigencia y la transmisión de la información aunque dicho vehículo abandone la ZOR.

Esta información se considerará válida hasta que alguno de los nodos móviles dentro de la ZOR informe de un cambio de estado en la situación actual. A partir de entonces, el nodo con tolerancia al retardo dejará de transmitir dicha información al resto de nodos, ya que pasará a ser información no relevante.

VII. Implementación

Con el fin de probar los diferentes conceptos explicados anteriormente se ha creado un escenario de pruebas que incluye dos nodos móviles y un nodo estático. Este escenario permite simular diferentes eventos que pueden producirse en un entorno real y, de esta manera, testear la viabilidad de la solución propuesta para la mejora de la seguridad en una vía.

Para ello se dispone de tres transmisores inalámbricos Zolertia Z1 que cumplen con el estándar IEEE 802.15.4, aplicable en WSN, y dos vehículos capaces de comunicarse con los transmisores por medio de conexión serie, tal y como se muestra en la Figura 1.

Las características de la plataforma Z1 más interesantes para la implementación de la experimentación propuesta son las siguientes: compatibilidad con IEEE 802.15.4 a 2.4 GHz (banda que permite mayores tasas de transferencias de datos del estándar), uso del micro controlador MSP430, orientado a bajo consumo eléctrico, y la radio CC2420 de Texas Instruments, sensores de temperatura y acelerómetro y, además, incorpora un puerto micro USB que permite al dispositivo ser programado, así como comunicarse con otros dispositivos que utilicen el estándar USB. El sistema operativo que utiliza la plataforma Z1 es TinyOS, un sistema Open Source diseñado para la optimización del consumo eléctrico de los dispositivos. El conjunto permite a los dispositivos Z1 alimentarse de dos pilas AA ofreciendo una vida útil de hasta 10 años.

En cuanto a los vehículos, cabe destacar que se utilizan dos robots LSMaker [11]. Éste es una plataforma robótica educativa creada en La Salle – Universitat Ramon Llull y que todos los alumnos de los diferentes grados de ingeniería utilizan desde el primer curso para las prácticas de distintas asignaturas. Es un robot autónomo, programable, modificable y fácilmente ampliable a nivel electrónico y de programación, que crece a medida que los conocimientos de los estudiantes crecen. Para este trabajo, a cada LSMaker se le añade el dispositivo Z1 en sus puertos de expansión I2C, de manera que sea capaz de conectarse a la red VANET. Como se puede ver en la Figura 2, se trata de un robot con forma de automóvil, por lo que permite simular un escenario con redes vehiculares a escala reducida. El LSMaker se puede mover tanto en modo teledirigido y manual utilizando su mando a distancia, como mediante la programación de aplicaciones que interactúan con el procesador integrado en el propio robot.

El objetivo de la experimentación es que todos los dispositivos sean capaces de compartir entre ellos la información de los eventos que detecten y sean capaces de tomar decisiones sobre los vehículos, como por ejemplo disminuir la velocidad, aumentarla o cambiar de dirección, tratando y transmitiendo la información de forma diferente, adaptándola a los requerimientos de cada servicio.

Las pruebas que se han realizado se han soportado para

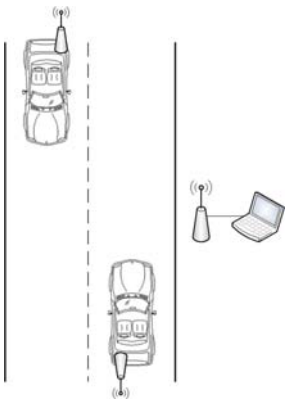


Fig. 1. Representación del escenario de pruebas.

comunicaciones V2I. Los servicios que se han implementado son *Traffic flow management, Station advertisement, Post crash warning* y *Road condition information*, todos ellos incluidos en la Tabla II. En todos los casos la comunicación es bidireccional entre el vehículo y el nodo de control, permitiendo que la comunicación sea iniciada por cualquiera de los dos dispositivos. Además, la información puede ser enviada usando encriptación o sin usarla, según convenga a cada servicio, como se muestra en la Tabla I.

En el primer servicio, *Traffic flow management*, el nodo de control es el que se ocupa de informar al vehículo de que debe realizar un paro inmediato y, posteriormente, le permite reanudar la marcha. Estas dos opciones se ejecutan desde el nodo de control de manera manual. Una vez el dispositivo z1 recibe la información, informa al vehículo de ésta y es el propio vehículo el que ejecuta la orden.

En la implementación del servicio de *Station advertisement*, el mismo nodo de control de la infraestructura anuncia la disponibilidad de diferentes servicios en la zona, como son hospitales o estaciones de servicio. Esta información de balizamiento se transmite en modo broadcast y permite mantener informado al vehículo sobre los servicios que tiene disponible en su zona.

El coche es capaz de utilizar el tercer servicio, el *Post crash warning*, para informar a la infraestructura de la detección de una colisión a partir del uso de los acelerómetros incluidos en el dispositivo Z1. La información es recibida por el nodo de control y éste puede actuar en consecuencia, avisando a los servicios que considere oportunos, así como a los vehículos que se encuentran dentro de su área de cobertura.

La infraestructura también es capaz de avisar de la proximidad de vehículos de emergencias en la zona, usando el servicio de *Road condition information*. Este servicio funciona a modo informativo y no actúa directamente sobre el vehículo, de manera que provee de la información necesaria para que el vehículo extreme la precaución.

Teniendo en cuenta los requisitos de la red que se exigen para el correcto funcionamiento de los servicios, en la Tabla I se pueden evaluar los diferentes protocolos y el grado en el que cumplen con estos requisitos. En este caso, si evaluamos la opción de WSN, vemos como se adapta de manera correcta a los requisitos marcados para V2I, siendo, por lo tanto, capaz de proveer todos estos servicios. Además, la experiencia previa en proyectos anteriores utilizando los dispositivos Z1 con el sistema operativo TinyOS, refuerza la opción del uso del protocolo IEEE 802.15.4 como viable para la experimentación en este escenario.

El entorno de pruebas dispone de, aproximadamente, 1 metro de ancho y 15 metros de largo, de manera que los dispositivos Z1 no sean capaces de comunicarse entre ellos si se encuentran en los extremos y deberán enviar la información al nodo intermedio, situado aproximadamente en la mitad de la vía, y que sea capaz de reenviar la información al nodo destino una vez se encuentre disponible.

Los transmisores Z1 de los vehículos simulan las OBUs de los vehículos, considerados nodos móviles, que tienen capacidades para conectarse con las OBUs de otros vehículos y de informar al sistema de las actualizaciones recibidas de otros dispositivos. Por otro lado, el dispositivo restante se conecta a un ordenador que actúa como un nodo estático, simulando ser una área de servicio. Este nodo estático tiene

capacidades de tolerancia al retardo, almacenando la información que no pueda ser entregada al destinatario inmediatamente. Además, es importante tener en cuenta que este nodo dispone de un equipo conectado que le permite aumentar sus características de velocidad de proceso y de cantidad de memoria, de manera que este nodo puede guardar más información que los integrados en los vehículos, así como procesarla de manera más rápida.

En el escenario, los robots LSmaker son capaces de detectar cambios en el terreno, disminución de la velocidad o fuertes deceleraciones y, a continuación, transmitir dicha información a los vehículos que tiene dentro del alcance de la radio si considera que esta información es importante para otros nodos. En el caso de que el nodo no pueda transmitir la información a ninguno de los vehículos, si la información es tolerante al retardo, tiene la capacidad de guardar la información para enviarla al nodo de la estación de servicio, que puede reenviar el mensaje cuando el nodo destino se encuentre disponible.

También el nodo estático que simula el área de servicio es capaz de diseminar información sobre los diferentes nodos de la VANET si lo cree necesario. De esta forma, por ejemplo, puede declarar un paro obligatorio de todos los vehículos dentro de la ZOR a mismo tiempo que actúa como baliza de señalización de la estación de servicio.

El objetivo final de estas pruebas es presentar el análisis de los distintos servicios y el protocolo implementado en un entorno real de forma que se puedan evaluar los datos obtenidos. De esta manera, estos datos a analizar pueden llegar a representar al máximo posible los datos que se obtendrían en un entorno de producción con vehículos reales, teniendo en cuenta que algunos de los parámetros no van a ser completamente correlativos entre estos dos entornos ni directamente extrapolables, aunque sí puedan servir de guía para realizar determinadas pruebas a mayor escala.

Para la realización de las pruebas V2V, la información se debe originar en uno de los vehículos, siendo el destino el otro de los vehículos. Cuando el origen de la información detecte algún cambio de vital importancia en su entorno debe intentar contactar con el segundo vehículo usando la interfaz radio. En el caso de que éste se encuentre fuera de su alcance, la información a transmitir será almacenada hasta que pueda ser transmitida al dispositivo destino o al nodo estático si se trata de una información tolerante al retardo. El nodo fijo entregará la información cuando el vehículo destinatario esté dentro del alcance de su módulo de radio. Adicionalmente, el nodo estático podrá decidir actuar sobre todos los vehículos que se encuentran dentro de su alcance en un momento determinado. En el caso de que la información a enviar no sea de característica tolerante al retardo y tampoco pueda ser entregada inmediatamente al destinatario, el vehículo la descarta directamente. En la actualidad se ha realizado el diseño de las pruebas V2V, pero todavía no se ha implementado la experimentación.

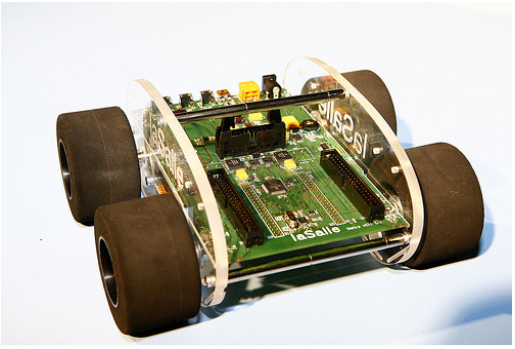


Fig. 2. Robot LSmaker de La Salle

En las pruebas realizadas para los distintos servicios para V2I se ha analizado el comportamiento de los dispositivos para comprobar el correcto envío de los mensajes. Por ello, se ha corroborado que se iluminaban una serie de LEDs dependiendo de la orden lanzada desde el control, de manera que se muestra de manera visual si el dispositivo ha recibido la información y la ha interpretado. En todos los casos, el tiempo de respuesta de los dispositivos ha sido suficientemente rápido.

VIII. Conclusiones

En este trabajo se han analizado los requerimientos de las redes vehiculares, los servicios asociados a dichas redes y se han relacionados estos conceptos con las distintas tecnologías y protocolos existentes. Una vez presentada la implementación propuesta y las pruebas realizadas en la sección VII, pasamos a detallar las conclusiones extraídas del trabajo realizado.

A nivel de enlace, el uso del protocolo IEEE 802.15.4 se ha presentado como una opción discutible para su adopción en redes VANET ya que su alcance es muy limitado y el ancho de banda del que proveen no es suficiente para algunos de los servicios que se deberán ofrecer sobre estas redes. Los servicios propuestos en la experimentación de este trabajo para V2I tienen poco requerimiento de ancho de banda, por lo que IEEE 802.15.4 es una alternativa viable siempre que se consideren estos aspectos de capacidad, limitadores por el propio diseño de la tecnología. En el caso de que se deseen implementar otros servicios como el acceso a Internet, las aplicaciones entre vehículos o los servicios de emergencia, otras tecnologías proporcionan mayor ancho de banda que las WSN. También debemos tener en cuenta que el retardo que ofrecen las redes basadas en este estándar es bastante elevado comparado con otras tecnologías, del orden de 60 ms con un único salto a baja velocidad y sin obstáculos que interfieran en la transmisión, por lo que ciertos servicios sensibles al retardo se podrían ver perjudicados. Cabe añadir también que el retardo no es estable y puede doblarse de la marca de 60 ms hasta el doble sin producirse cambios en el escenario. Por lo tanto, para entornos V2V donde el retardo es crítico será necesario evaluar otras tecnologías.

En cuanto a SDN y la composición de servicios, debemos destacar que la implementación ha sido limitada debido a que los dispositivos usados disponen de restricciones técnicas con la interacción entre el sistema operativo TinyOS y el Linux que utiliza el host de control que limitan bastante la implementación en cuanto a comunicación serie. Para solucionar esta restricción se podría implementar un driver que permita utilizar el dispositivo Z1 como una tarjeta de red que cumple con el estándar 802.15.4, de manera que toda la gestión podría ejecutarse desde el host.

Sobre DTN, será importante ajustar tiempo que esta información se considera válida, ya que se han detectado algunos casos en los que la información aún era retransmitida al vehículo destino y ésta ya no era válida. Del

mismo modo, algún tipo de sistema de autenticación deberá ser implementado para validar el origen de la información que se envía.

No menos importante será validar el sistema a la velocidad del entorno real, ya que en el entorno testeado, a escala reducida, la velocidad es menor en comparación con el entorno de explotación de este tipo de sistemas.

IX. Trabajos futuros

Será necesario estudiar la posible inclusión de algún tipo de sistema de reputación que sea capaz de gestionar la fiabilidad que se le otorga a cada una de las fuentes de datos, con el fin de asegurar que la información que el sistema está tratando sea de confianza. Dicho sistema deberá otorgar una puntuación a todos los generadores de información y debe ser capaz de revisarla con el fin de mantener el sistema de reputación actualizado. El trabajo debería estar en consonancia con el trabajo expuesto en [12].

Con la movilidad que proveen las VANET aparece un nuevo concepto de direccionamiento que se suma a los existentes hasta ahora. Este nuevo tipo de direccionamiento se denomina *geocast* y su misión es la de decidir si un nodo debe recibir un mensaje o no tomando como referencia su posición física. Se debería valorar el uso de este tipo de direccionamiento así como estudiar una implementación viable.

Agradecimientos

Queremos agradecer a La Salle – Universitat Ramon Llull por su apoyo en esta investigación.

Referencias

[1] Área de Formación y Comportamiento de Conductores, "Cuestiones de seguridad vial, conducción eficiente, medio ambiente y contaminación", online http://www.dgt.es , pp. 33-50, 2011.

[2] Cheng-Xiang Wang, Xiang Cheng, David I. Laurenson, "Vehicle-to-Vehicle Channel modeling and Measurements: Recent Advances and Future Challenges", IEEE Communications Magazine November 2009, pp. 96-103, 2009.

[3] Wen-Long Jin, Hong-Jun Wang, "Modeling Connectivity of Inter-Vehicle Communication Systems with Road-Side Stations", The Open Transportation Journal, vol. 2, pp. 2-6, 2008.

[4] Jens-Matthias Bohli, Alban Hessler, Osman Ugus, Dirk Westhoff, "A Secure and Resilient WSN Roadside Architecture for Intelligent Transport Systems", WiSec '08 Proceedings of the first ACM conference on Wireless network security, pp. 161-171, 2008.

[5] Vicente Milanés, Joshué Pérez, Enrique Onieva, Carlos González, "Controller for urban Intersections Based on Wireless Communications and Fuzzy Logic", IEEE Transactions on intelligent transportation systems, vol. 11, n. 1, pp. 243-248, March 2010.

[6] Michael Behrisch, Laura Bieker, Jakob Erdmann, Daniel Krajzewicz, "SUMO – Simulation of Urban MObility", SIMUL 2011, The Third International Conference on Advances in System Simulation, pp. 55-60, October 2011.

[7] Mihail L. Sichitiu, Maria Kihl, "Inter-vehicle Communication Systems: a Survey", IEEE Communications Surveys & Tutorials 2nd quarter 2008, vol. 10, n. 2, pp. 88-105, 2008.

[8] Kashif Dar, Mhamed Bakhouya, Jaafar Gaber, Maxime Wack, Pascal Lorenz, "Wireless Communication Technologies for ITS Applications", IEEE Communications Magazine May 2010, pp. 156-162, 2010.

[9] Timo Kosch, Ilse Kulp, Marc Bechler, markus Strassberger, Benjamin Weyl, Robert Lasowski, "Communication Architecture for Cooperative Systems in Europe", IEEE Communications Magazine May 2009, pp. 116-125, 2009.

[10] Panos Papadimitratos, Arnaud de La Fortelle, Knut Evenssen, Roberto Brignolo, Stefano Cosenza, "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation", IEEE Communications Magazine November 2009, pp. 84-95, 2009.

[11] Jordi Albó, David Vernet, Xavi Canaleta, Xavier Vilasís-Cardona, "LSMaker: A Robotic Platform for Engineering Education", Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS 2013), p.2573-2576, Beijing, 2013.

[12] Sînziana Mazilu, Mihaela Teler, Ciprian Dobre, "Securing Vehicular Networks based on Data-Trust Computation", 2011 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.

SERIA

Aunque de forma breve, no puedo dejar pasar la oportunidad de aprovechar estas líneas que siguen en varios sentidos. En primer lugar, para agradecer a la organización de JITEL la oportunidad que me ha brindado de organizar un evento de carácter específico en el marco general de esta nueva edición de las Jornadas de Ingeniería Telemática. El campo de la seguridad en redes inalámbricas ad hoc constituye sin duda alguna un tópico de alto interés dentro de los nuevos paradigmas de comunicación, interés que va en aumento creciente a lo largo de los años. Como tal, nuestra área de conocimiento resulta clave en el desarrollo y afianzamiento de este nuevo tipo de sistemas y de los servicios que los mismos implican.

En esta línea, mi reconocimiento a todos aquellos de vosotros que habéis contribuido activamente con vuestros trabajos a que SERIA sea finalmente una realidad. Confío en que las sesiones de presentaciones y discusiones que vamos a compartir resultarán útiles para un mejor conocimiento de algunos de los aspectos diferenciadores de este tipo de entornos, al tiempo que una posible semilla para futuras colaboraciones entre los equipos de personas que conformamos nuestra pequeña pero capaz área.

Desde aquí quiero agradecer también la participación general de todos a JITEL, participación que permite conocernos mejor y, como tal, estrechar lazos entre miembros de una comunidad científico-tecnológica y educativa que, precisamente en estos momentos difíciles que nuestra sociedad está atravesando, se hacen más necesarios. Animo así a todos a buscar nuevas y mejores formas de interrelación que permitan poner en valor nuestros conocimientos y capacidades.

No puedo concluir esta presentación sin agradecer y reconocer a mis compañeros del área de Ingeniería Telemática de la Universidad de Granada, el trabajo realizado en la organización de estas jornadas. Estoy seguro de que esta encomiable labor, junto con el marco incomparable que constituye la ciudad de Granada, abierta y cosmopolita donde las haya, hará de estos días de convivencia unos momentos memorables para todos.

Bienvenidos a Granada,

Pedro García Teodoro
Organizador de SERIA

Evaluación de mecanismos de seguridad en entornos de *Smart Grid*

El bachir El achhab, Gregorio López López, José Ignacio Moreno Novella
Departamento de Ingeniería Telemática
Universidad Carlos III de Madrid
Avenida de la Universidad 30, Leganés, Madrid, España
bac.nadir@gmail.com, gregorio.lopez@uc3m.es, joseignacio.moreno@uc3m.es

Resumen - Debido a que la información que se maneja en las denominadas Redes Eléctricas Inteligentes (Smart Grids) es extremadamente sensible, la seguridad representa un requisito clave para su despliegue y aceptación. Sin embargo, la utilización de mecanismos de seguridad puede tener un impacto en el rendimiento de la infraestructura de comunicaciones así como en el coste de operación de la misma. Este artículo analiza varios protocolos comúnmente utilizados para establecer redes privadas virtuales y evalúa el impacto - tanto desde un punto de vista técnico como económico – de emplearlos en una plataforma basada en comunicaciones máquina-máquina inalámbricas, cuyo objetivo es reducir el consumo eléctrico e integrar instalaciones de micro-generación basadas en energías renovables a nivel de distrito.

Palabras Clave - Comunicaciones Inalámbricas; M2M (Machine-to-Machine); Seguridad; Smart Grid; VPN (Virtual Private Networks)

I. INTRODUCCIÓN

El consumo eléctrico en el sector residencial en la UE (Unión Europea) no ha parado de subir durante los últimos años [1], convirtiéndose en un problema importante para gobiernos y operadores eléctricos (*utilities*). Estudios recientes han concluido que dicha tendencia creciente se debe a la alta penetración de dispositivos TIC (Tecnologías de la Información y las Comunicaciones), tales como *routers* u ordenadores de sobremesa, y a los altos consumos en *standby* que presentan [2]. Asimismo, dichos estudios también destacan la importancia de los consumos asociados a los dispositivos conocidos como HVAC (*Heating, Ventilating and Air Conditioning*), así como el hecho de que hay determinados electrodomésticos que son utilizados durante las horas de máximo consumo de electricidad, cuando podrían utilizarse en otro momento sin afectar considerablemente a los usuarios finales [2].

La alta penetración de energías renovables y su integración con el resto de la red eléctrica, requisitos indispensables para alcanzar los objetivos de la UE para 2020 en materia energética (*20-20-20*), también suponen un importante reto para gobiernos y *utilities*. La integración de la generación procedente de fuentes de energía renovables aumenta considerablemente la complejidad de gestionar la red eléctrica, debido a la variabilidad y aleatoriedad que introducen. La complejidad aumenta aún más si dichas fuentes de energía renovable se despliegan de forma altamente distribuida [3]. Sin embargo, los conocidos como programas y eventos de respuesta a la demanda (DR - *Demand Reponse*) representan una solución para este problema, ya que permiten actuar sobre la demanda de energía para acomodar mejor la oferta energética procedente de fuentes renovables [3].

Las comunicaciones M2M (*Machine-to-Machine*) están llamadas a jugar un papel clave en este nuevo paradigma de red eléctrica inteligente (*Smart Grid*) para permitir el intercambio masivo de información en casi tiempo real entre las infraestructuras de consumo y generación a monitorizar y controlar y los sistemas de información donde se toman las decisiones de optimización.

Entre el amplio abanico de tecnologías de comunicación disponibles para infraestructuras M2M para *Smart Grids* destacan las comunicaciones inalámbricas, como ilustra el hecho de que el NIST (*National Institute of Standards and Technologies*) haya lanzado un grupo de trabajo específico dentro del PAP2 (*Priority Action Plan 2*) dedicado exclusivamente a este tema.

El principal objetivo del proyecto europeo ENERsip es precisamente desarrollar una plataforma basada en comunicaciones M2M inalámbricas que permita reducir el consumo residencial, ajustándolo a la micro-generación distribuida dentro de un mismo distrito [5].

La seguridad y la privacidad representan dos requisitos clave para el despliegue y aceptación de este tipo de plataformas [6], [7]. Sin embargo, proporcionar estos servicios no es gratuito, sino que puede suponer un coste tanto desde el punto de vista técnico como económico. El principal objetivo de este artículo es evaluar de manera integral el coste de utilizar mecanismos que incrementen la seguridad de las comunicaciones en la plataforma ENERsip y proponer los más adecuados.

El resto del artículo está organizado de la siguiente manera. La sección II presenta la arquitectura de la plataforma ENERsip y caracteriza el tráfico de la misma en diferentes escenarios. La sección III analiza los protocolos de seguridad considerados desde un punto de vista técnico. La sección IV evalúa el coste de operación que implicaría utilizar dichos protocolos en los diferentes escenarios considerados. Por último, la sección V presenta las principales conclusiones del artículo.

II. ANTECEDENTES

La Fig. 1 muestra la arquitectura de comunicaciones de la plataforma ENERsip, que se describe en detalle en [8]. Como se puede observar, todas las infraestructuras de consumo y

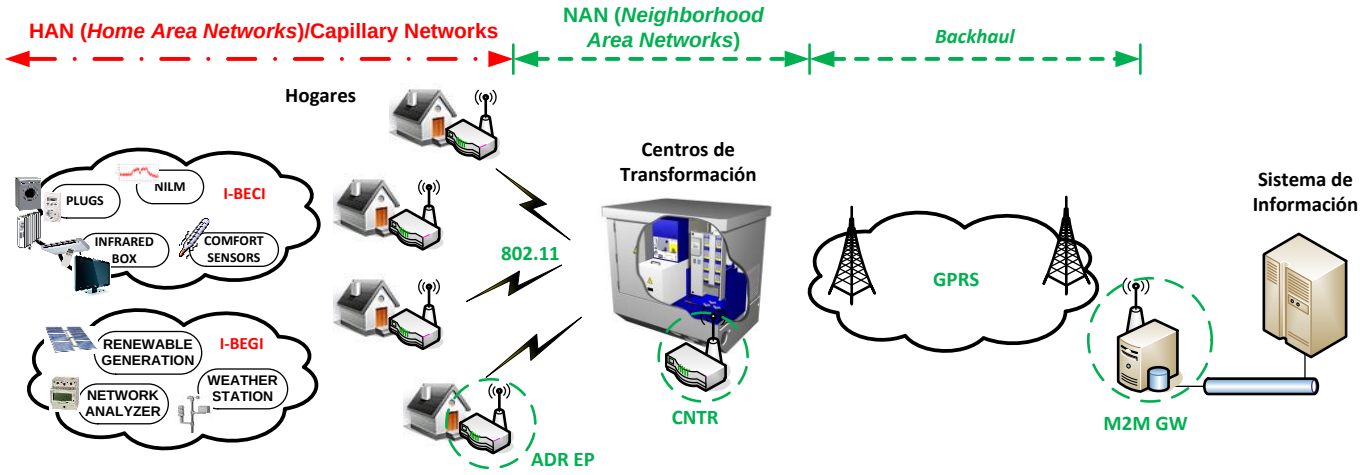


Fig. 1. Arquitectura de ENERsip

generación residenciales (denominadas I-BECI [9] – *In-Building Energy Consumption Infrastructures* – e I-BEGI [10] - *In-Building Energy Generation Infrastructures*) están equipadas con los denominados ADR EP (*Automatic Demand Response End Points*). Los ADR EP funcionan como pasarela de comunicación, agregando y enviando datos de consumo o de generación hacia fuera de la red que comandan y encaminando comandos hacia el dispositivo apropiado de dicha red. Los ADR EP se comunican directamente con su CNTR (*Concentrator*) asociado. Un CNTR gestiona un grupo de ADR EPs, reenviando los datos procedentes de los mismos y encaminando comandos hacia el/los ADR EP/s adecuados. Por último, el M2M GW (*Gateway*) tiene una visión global de la infraestructura de comunicaciones M2M. Así, el M2M GW funciona como OSS (*Operations Support System*), realizando tareas como inventario de red, configuración de equipos, gestión de fallos o aprovisionamiento de servicios, y como pasarela hacia el Sistema de Información donde se ejecutan los algoritmos de optimización y ajuste de consumo y generación. La comunicación entre ADR EP y CNTR se basa en UDP/IP (*User Datagram Protocol*/*Internet Protocol*) sobre IEEE 802.11b, mientras que la comunicación entre CNTR y M2M GW se basa en TCP/IP (*Transport Control Protocol*) sobre GPRS (*General Packet Radio Service*).

La Fig. 1 también muestra el mapeo de la infraestructura de comunicaciones de ENERsip a la infraestructura eléctrica de distribución. Como puede verse, los ADR EP están asociados a los hogares/domicilios, los CNTR están localizados en los CT (Centros de Transformación) y el M2M GW estará localizado típicamente en un CPD (Centro de Proceso de Datos) de la entidad que gestione la plataforma.

Basándose en este mapeo, en datos de infraestructuras eléctricas de distribución reales, y en datos relativos a la implementación de la plataforma ENERsip, en [11] se modela el tráfico de la misma en diferentes escenarios. El principal objetivo de este trabajo es sentar las bases que permitan evaluar el rendimiento de la plataforma de comunicaciones diseñada en escenarios cercanos a la realidad. Por lo tanto, el análisis de seguridad que se realiza en este artículo toma como referencia dicho trabajo centrándose en el núcleo de la arquitectura de comunicaciones (desde el ADR EP hasta el M2M GW), tal y como se ilustra en verde en la Fig.1.

En base a los datos de infraestructuras eléctricas de distribución reales, [11] distingue entre escenarios *Urbanos* y *Rurales*, ya que el número de domicilios/CT y el número de CT/Subestación (es decir, ADR EP/CNTR y CNTR/M2M GW – ***C*** en la Tabla I - respectivamente) difiere considerablemente entre ambos.

Para aportar valor a los resultados obtenidos a partir del modelo presentado en [11] y potenciar que su validez perdure en el tiempo, también se distingue entre escenarios a *Corto plazo* y a *Largo plazo*. Así, mientras los escenarios a *Corto plazo* se basan en datos actuales y previsiones a unos pocos años vista, los escenarios a *Largo plazo* pretenden predecir la evolución de este tipo de sistemas en un período de tiempo considerablemente más amplio (p. ej., 10 años). Básicamente, los escenarios a *Largo plazo* son más exigentes desde el punto de vista de la infraestructura de comunicaciones, ya que el tráfico agregado que cursa es considerablemente mayor. A continuación, se explica detalladamente a qué se debe dicho aumento en el tráfico cursado, analizando los principales parámetros que varían del *Corto* al *Largo plazo*:

- Periodicidad con la que los ADR EP envían datos (***T***) y tamaño de los mismos (***S***), lo que a su vez influye en la tasa de transmisión. Por un lado, *T* será más baja en el largo plazo, lo que representa una situación más cercana al envío de información en casi tiempo real. Por otro lado, *S* será más alto en el largo plazo, ya que se asume un número mayor de dispositivos con capacidades de comunicación tanto en el I-BECI como en el I-BEGI y los ADR EP agregan la información procedente de dichos dispositivos. Además, *S* no es el mismo para las I-BECI (***Sc***) que para las I-BEGI (***Sg***), ya que las redes de sensores y actuadores que componen estas infraestructuras están compuestas por diferentes dispositivos.
- Penetración de la micro-generación. En principio, este parámetro será siempre superior en escenarios rurales que en escenarios urbanos debido al tipo de viviendas (p. ej., casas tipo chalé, en cuyos tejados se pueden instalar paneles solares fotovoltaicos, son más comunes en entornos rurales, mientras que en entornos urbanos son más comunes los bloques de pisos). Este parámetro también será más alto en el largo plazo que en el corto, ya que la penetración de la micro-generación distribuida y el autoconsumo se prevé que aumente durante los próximos años. Llegados a este punto es necesario recalcar que, bajo el enfoque del proyecto ENERsip, cada I-BECI tiene un ADR EP asociado (ADR EP-C) y cada I-BEGI tiene

TABLA I
RESUMEN DE LOS PARÁMETROS MÁS RELEVANTES EN CADA ESCENARIO

Escenarios	Corto plazo	Largo plazo
Urbano	Ac = 360; Ag = 36 Sc = 540B; Sg = 1030B T = 15 min; C = 150	Ac = 360; Ag = 144 Sc = 895B; Sg = 1700B T = 5 min; C = 150
Rural	Ac = 100; Ag = 40 Sc = 540B; Sg = 1030B T = 15 min; C = 220	Ac = 100; Ag = 80 Sc = 895B; Sg = 1700B T = 5 min; C = 220

un ADR EP asociado (ADR EP-G). Así, el número de ADR EP-C (***Ac***) es igual al número de domicilios/CT, mientras que el número de ADR EP-G (***Ag***) se calcula multiplicando *Ac* por un factor que estima la penetración de la micro-generación (dicho factor se asume siempre menor que 1).

La Tabla I resume los valores de dichos parámetros en los 4 escenarios que resultan de combinar escenarios *Urbanos* y *Rurales* en el *Corto* y el *Largo plazo*.

III. ANÁLISIS DE SEGURIDAD

A. Escenarios de seguridad considerados

El objetivo concreto de este artículo es analizar protocolos de seguridad que soporten la gestión de VPN (*Virtual Private Networks*). Lo que se pretende por tanto es establecer túneles de comunicación seguros entre pares de entidades de la arquitectura de comunicaciones.

En este sentido, en principio se considera que se puedan establecer VPN desde los ADR EP hasta el M2M GW o desde el CNTR hasta el M2M GW.

El establecimiento de túneles entre los ADR EP y el M2M GW se descarta debido a que presenta numerosos inconvenientes. En primer lugar, el número de túneles necesario es muy elevado, lo que incrementa la complejidad de gestionar la infraestructura de comunicaciones. Además, el que los ADR EP sean capaces de implementar VPN implica un incremento en su complejidad y, por tanto, en su coste, lo que puede suponer un incremento en los costes de despliegue considerables. Por lo tanto, este segmento en principio se confía a los mecanismos de seguridad proporcionados por IEEE 802.11 (concretamente, se recomienda el uso de WPA2 - *Wi-Fi Protected Access 2*).

En el caso de que se establezcan VPN entre el CNTR y el M2M GW, se distinguen a su vez dos escenarios:

- RI *(Reenvío Inmediato)*: el CNTR reenvía los paquetes que le llegan de sus ADR EP asociados uno a uno en cuanto los recibe utilizando para ello una conexión TCP.
- *Agregación*: el CNTR almacena todos los paquetes que le llegan de sus ADR EP asociados durante un período, los agrupa y los transmite todos juntos utilizando FTP (*File Transfer Protocol*) sobre TCP.

B. Protocolos de seguridad considerados

Existen numerosos mecanismos para proporcionar seguridad a distintos niveles de la torre de protocolos [12], [13]. A nivel de enlace se pueden implementar VPN utilizando L2TP (*Layer 2 Tunneling Protocol*), por ejemplo. IPSec (*Internet Protocol Security*) representa la opción más extendida para hacerlo a nivel de red. TLS/SSL (*Transport Layer Security*/*Secure Socket Layer*) es la opción más utilizada a nivel de transporte. Y SSH (*Secure SHell*) se emplea comúnmente a nivel de aplicación para acceder de forma segura a máquinas remotas.

Este artículo se va a centrar en IPSec y TLS/SSL. A lo largo de esta subsección se resumen brevemente las características más relevantes así como los servicios de seguridad que proporcionan ambos.

1. IPSec

IPsec es una extensión al protocolo IP para proporcionar seguridad a nivel de red. IPSec puede funcionar en modo transporte y en modo túnel. En modo transporte sólo se cifra la carga útil del paquete IP, quedando la cabecera intacta. Por lo tanto, el modo transporte no afecta de ninguna manera al encaminamiento. En el modo túnel, en cambio, se cifra todo el paquete IP. En este modo, para que el encaminamiento sea posible, el paquete cifrado debe ser encapsulado de nuevo en IP, añadiéndosele una cabecera IP adicional. El modo túnel es el que se usa normalmente para establecer VPN, por lo que es el que se va a considerar en este trabajo.

IPSec define dos tipos de cabeceras que proporcionan diferentes servicios de seguridad. Por un lado, AH (*Authentication Header*) proporciona integridad y autenticación del origen. Esta cabecera se calcula sobre los valores del datagrama original utilizando un HMAC (*Hash Message Authentication Code*), es decir, que utiliza un algoritmo de *hash* especial junto con una clave secreta conocida sólo por origen y destino. Por otro lado, ESP (*Encapsuling Security Payload*) proporciona autenticación de origen, integridad y confidencialidad.

El protocolo que se utiliza en IPSec para intercambiar las claves de cifrado es IKE (*Internet Key Exchange*). Los mensajes IKE se transmiten a través del puerto 500 de UDP y se basan en ISAKMP (*Internet Security Association and Key Management Protocol*).

Cuando se establece una conexión IPSec, hay dos fases de negociación. En la primera fase se negocia la SA (*Security Asociation*) de IKE. En este momento todavía no hay datos encriptados ni autenticados. Sin embargo, los dos extremos del túnel deben autenticarse entre ellos, para lo que utilizan el método de intercambio de claves *Diffie-Hellman*. Durante la segunda fase, que está protegida por la SA negociada en la fase anterior, se negocian los parámetros del túnel VPN, incluyendo las claves simétricas, política de seguridad y otros parámetros relevantes de la conexión. A partir de este momento se pueden intercambiar datos de manera segura.

Debido a que las claves tienen un tiempo de caducidad, el proceso de refrescar las claves debe ser ejecutado periódicamente. Para ello, sólo es necesario repetir la segunda fase. Ambas fases sólo se llevan a cabo, por tanto, durante el proceso de establecimiento de la conexión.

2. SSL/TLS

El aplicar un mecanismo de seguridad a nivel de red puede conllevar que ciertos *routers* necesiten ser actualizados para que la solución funcione. Para evitar este tipo de problemas, se puede recurrir a una solución a nivel de transporte. La solución más empleada actualmente a este nivel es el protocolo TLS y su predecesor SSL.

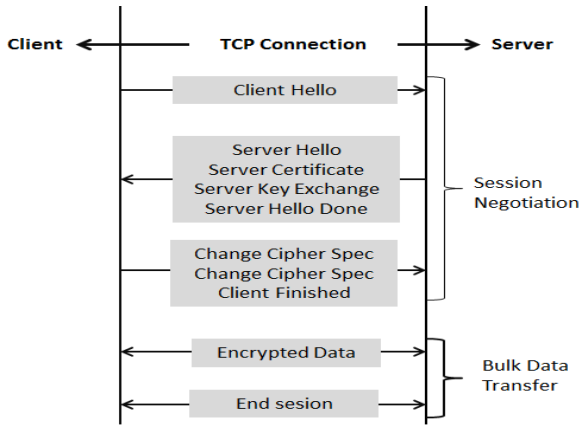


Fig. 2. Intercambio de mensajes en TLS/SSL [14]

TLS utiliza algoritmos de clave asimétrica (típicamente RSA) para proteger el intercambio de claves, algoritmos de clave simétrica para proporcionar confidencialidad y MAC para proporcionar integridad.

Una conexión TLS/SSL empieza con la negociación de la asociación de seguridad, que se usará antes y durante del intercambio de datos. En la Fig. 2 se presentan los mensajes que se intercambian tanto en la fase de negociación como en la fase de envió de datos [14].

C. Comparativa de protocolos de seguridad

Después de ver una breve descripción de los dos protocolos considerados en este trabajo, esta subsección presenta una comparativa de ambos en base a los métodos de autenticación que utilizan, el orden de encriptación que emplean y la sobrecarga (*overhead*) que introducen [15]. Para concluir, se incluye un resumen comparativo de IPSec frente a TLS/SSL.

1. *Métodos de autenticación*

IPsec soporta solo un método de autenticación, mientras TLS/SSL soporta varios. La Tabla II resume los métodos de autenticación que soporta cada protocolo.

Después de que se establezca la conexión, se usa MAC para autenticar los mensajes intercambiados. Tanto IPsec como TLS/SSL implementan HMAC-SHA-1 y HMAC-MD5. HMAC es una función *hash* que requiere una clave secreta para producir el mensaje *digest*. Los mecanismos utilizados en IPSec y TLS/SSL para intercambiar dicha clave son diferentes, tal y como se explica en la sección III.B. La resistencia del algoritmo *hash* depende de la longitud de la salida. En la Tabla III se muestra la longitud del mensaje de salida dependiendo del protocolo y del algoritmo utilizado.

2. *Orden de encriptación*

En IPsec primero se encriptan los datos y luego se crea el MAC sobre los datos encriptados. Esto tiene la ventaja de que si ocurre cualquier modificación durante el intercambio de un mensaje, IPsec puede detectarlo verificando el MAC sin desencriptar los datos. TLS/SSL, en cambio, aplica MAC sobre los datos y luego encripta el resultado. Por lo tanto, si ocurre cualquier modificación a mitad de la transacción, se detecta al verificar el MAC después de desencriptar los datos, lo que implica una pérdida de tiempo y recursos.

3. *Sobrecarga (Overhead)*

El *overhead* que introducen estos protocolos de seguridad representa uno de los parámetros más relevantes para el presente estudio, ya que puede aumentar el volumen de datos que circula a través de la red GPRS y, en consecuencia, los costes de operación de la plataforma.

En este sentido, una de las desventajas de IPsec frente a TLS/SSL es que introduce un *overhead* mayor. La Tabla IV resume el *overhead* que introduce cada protocolo. El modo túnel de IPsec requiere 20 bytes adicionales ya que añade una nueva cabecera IP al paquete original.

4. *Resumen*

La Tabla V presenta un resumen comparativo entre IPsec y SSL. Puede observarse que ambos mecanismos soportan los servicios de seguridad básicos requeridos por aplicaciones como la aplicación objetivo de este estudio (autenticación, integridad y confidencialidad). Las principales desventajas de IPSec son su complejidad de configuración y su incompatibilidad con NAT (*Network Address Resolution*), mientras que uno de los principales inconvenientes potenciales de TLS/SSL es la complejidad que implica utilizar PKI (*Public Key Infrastructure*). En cuanto al hecho de que TLS/SSL sólo proporciona soporte a ciertas aplicaciones de TCP, no supone un problema para el presente trabajo puesto que FTP es uno de los protocolos que soporta. Por lo tanto, desde un punto de vista técnico, no hay ningún motivo por el que descartar el uso de ninguno de estos dos protocolos.

TABLA II
MÉTODOS DE AUTENTICACIÓN EN IPSEC Y TLS/SSL [15]

Protocolo	Método de Autenticación	Algoritmo
IPSec	Autenticación mutua	PSK
		Firma digital RSA/DSA
		Clave pública RSA
		KINK
TLS/SSL	Autenticación del servidor	RSA (Desafío/Respuesta)
		Firma digital DSA
	Autenticación del cliente	Firma digital RSA/DSA
	Anónimo	Ninguno

TABLA III
LONGITUD DE LA SALIDA DEL MAC DEPENDIENDO DEL PROTOCOLO Y EL ALGORITMO UTILIZADO [15]

Protocolo	Algoritmo MAC	Longitud (Bytes)
IPSec	HMAC-SHA-1-96	12
	HMAC-MD5-96	12
TLS/SSL	HMAC-SHA-1	20
	HMAC-MD5-96	16

TABLA IV
OVERHEAD INTRODUCIDO POR IPSEC Y TLS/SSL [15]

Protocolo	Modo	Tamaño (Bytes)
IPSec modo túnel	ESP	32
	ESP y AH	44
IPSec modo transporte	ESP	36
	ESP y AH	48
TLS/SSL	HMAC-MD5	21
	HMAC-SHA-1	25

TABLA V
RESUMEN DE LA COMPARATIVA ENTRE IPSEC Y TLS/SSL

Función	IPsec	TLS/SSL
Autenticación	Sí	Sí
Integridad	Sí	Sí (Más segura, ya que HMAC más largo)
Confidencialidad	Sí (Con ESP)	Sí
Configuración	Compleja	Sencilla
Problemas de interoperabilidad	Sí (Problemas con NAT convencionales)	No
Soporte de aplicaciones TCP	Todas	Algunas
Soporte de UDP	Sí	No
Emplea PKI	No	Sí (No todos los clientes lo soportan)
Soporte de compresión	Sí	Sólo OpenSSL
Software específico para el cliente	Sí	No
Soporte de múltiples entornos	A veces (Se implementa a nivel de red)	Sí
Dispositivos móviles	No (Porque hay que cambiar la torre de protocolos)	La mayoría lo soportan
Filtro de aplicaciones	No	Sí (Se puede proporcionar VPN a aplicaciones concretas)

IV. EVALUACIÓN DE PROTOCOLOS DE SEGURIDAD

Esta sección analiza el impacto que tendría utilizar los protocolos de seguridad presentados en la sección III en los costes de operación de la plataforma ENERsip para cada uno de los escenarios considerados.

Para ello, en primer lugar es necesario decidir el MSS (*Maximum Segment Size*) de TCP, que influirá en el número de paquetes enviados y en el ratio de información útil frente a cabeceras de control de dichos paquetes. Existen numerosos estudios en la literatura sobre el uso de TCP en GPRS. Inicialmente, se tendía a utilizar MSS bajos (512 B [16] y 431 B [17]). Si bien es cierto que el uso de MSS bajos puede ser adecuado para aplicaciones interactivas, en [18] se demuestra que la utilización de MSS altos (1400-1600 B) maximiza el rendimiento de la infraestructura de comunicaciones cuando se trata de aplicaciones de envío masivo de datos como la que nos ocupa.

Partiendo de ese rango de MSS de TCP deseables, el MSS de TCP que se utiliza en este trabajo se calcula restándole a los 1482 B indicados en [19] como la MTU (*Maximum Transfer Unit*) óptima del nivel SNDCP (*Sub Network Dependent Convergence Protocol*) de GPRS, el tamaño de las cabeceras de nivel superior hasta llegar al nivel de aplicación (es decir, a los datos). Respecto al *overhead* introducido por los protocolos de seguridad (Tabla IV), se considera siempre el peor caso, es decir, la cabecera de mayor tamaño (44 B más 20 B de la cabecera IP adicional, para IPSec en modo túnel, y 25 B, para TLS/SSL). La Fig. 3 muestra la arquitectura de protocolos que implementan los CNTR y el M2M GW (especificando el tamaño de las cabeceras) en cada caso.

Para traducir el volumen de tráfico cursado por GPRS en coste, se asumen dos tarifas comerciales de M2M. Una permite el envío de 100 MB por 10 € al mes y la otra permite el envío de 20 MB por 3 € al mes. Para cubrir el volumen total de tráfico cursado por la red GPRS en un mes en cada

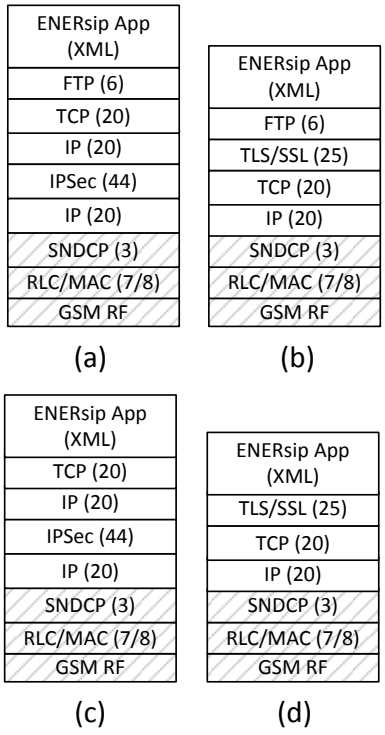


Fig. 3. Arquitectura de protocolos de CNTR y M2M GW para: (a) IPSec & Agregación; (b) TLS/SSL & Agregación; (c) IPSec & RI; (d) TLS/SSL & RI

escenario, se combinarán un número determinado de cada una de estas tarifas hasta alcanzar el volumen de tráfico más próximo al necesario por encima del mismo.

La Tabla VI detalla los resultados de este análisis para cada uno de los escenarios considerados. ***Vss*** representa el volumen de tráfico (en MB), sin utilizar ningún protocolo de seguridad, que cursa la red GPRS (lo que implica datos y cabeceras hasta el nivel SNDCP) en un mes. ***Vcs*** representa el volumen de tráfico (en MB), empleando el protocolo de seguridad oportuno, que cursa la red GPRS en un mes. ***Rss*** representa el ratio entre el volumen de datos de nivel de aplicación y *Vss* (en %). ***Rcs*** representa el ratio entre el volumen de datos de nivel de aplicación y *Vcs* (en %). ***Os*** se calcula como la diferencia entre *Rss* y *Rcs*, por lo que representa el *overhead* introducido por el protocolo de seguridad (en %). ***Css*** representa el coste mensual de cursar *Vss* (en €). ***Ccs*** representa el coste mensual de cursar *Vcs* (en €). Por último, ***Dc*** se calcula como la diferencia entre *Ccs* y *Css*, por lo que representa el coste mensual de aplicar el mecanismo de seguridad en cuestión en el escenario considerado (en €).

La Tabla VII muestra la diferencia entre el coste anual de utilizar *Reenvío Inmediato* y el coste anual de utilizar *Agregación* ($C_{cs}|_{RI} - C_{cs}|_{Agr}$) en cada escenario para un solo CNTR. La Tabla VII también muestra esta diferencia en cada escenario para un distrito entero, para lo que es necesario multiplicar el coste anual por CNTR por el número de CNTR/M2M GW (ver parámetro *C* en Tabla I)[1]. Para facilitar la visualización de cómo influye utilizar *Reenvío*

[1]Se considera como distrito toda la infraestructura eléctrica a la que da servicio una misma Subestación, donde se llevarían a cabo los procesos de optimización y ajuste de consumo y generación.

TABLA VI
EVALUACIÓN DE LOS PROTOCOLOS DE SEGURIDAD CONSIDERADOS EN CADA ESCENARIO

		Corto plazo		**Largo plazo**	
		IPSec	**SSL/TLS**	**IPSec**	**SSL/TLS**
Urbano	**Agr.**	Vss =656,25 Vcs=686,74 Rss =96.88 % Rcs =92.58 % Os = 4.3 % Css = 69 Ccs = 70 Dc = 1	Vss = 656,25 Vcs = 667,96 Rss =96.88 % Rcs =95.18 % Os =1.7% Css = 69 Ccs = 70 Dc = 1	Vss =4821,65 Vcs =5047,17 Rss =96.895 % Rcs =92.56 % Os =4.335 % Css = 486 Ccs =509 Dc = 23	Vss = 4821,65 Vcs =4907,11 Rss = 96.895 % Rcs = 95.207% Os = 1.688 % Css = 486 Ccs =493 Dc = 7
	RI	Vss =679,28 Vcs =748,89 Rss =93.6 % Rcs =84.89 % Os =8.71 % Css = 70 Ccs =79 Dc = 9	Vss =679,28 Vcs =706,48 Rss =93.6 % Rcs =90 % Os =3.6% Css = 70 Ccs =73 Dc = 3	Vss =4885,51 Vcs =5227,23 Rss =95.628 % Rcs =89.38 % Os =6.248 % Css = 490 Ccs =526 Dc = 36	Vss =4885,51 Vcs =5018,99 Rss = 95.628 % Rcs =93.085 % Os =2.543 % Css = 490 Ccs =500 Dc = 10
Rural	**Agr.**	Vss =269,94 Vcs=282,62 Rss =96,86% Rcs =92.5 % Os =4.36 % Css = 30 Ccs = 30 Dc = 0	Vss =269,94 Vcs =274,74 Rss =96,86% Rcs =95,17 % Os =1.69 % Css = 30 Ccs = 30 Dc = 0	Vss =1917,95 Vcs =2007,61 Rss =96.877 % Rcs =92.55 % Os =4.327 % Css = 193 Ccs = 203 Dc = 10	Vss =1917,95 Vcs =1951,67 Rss =96.877 % Rcs =95.2 % Os =1.67 % Css = 193 Ccs = 199 Dc = 6
	RI	Vss =276,86 Vcs =301,46 Rss =94.4 % Rcs =86.7 % Os =7.7 % Css = 30 Ccs = 33 Dc = 3	Vss =276,86 Vcs =286,47 Rss =94.4 % Rcs =91.27 % Os =3.6 % Css = 30 Ccs = 30 Dc = 0	Vss =1943,76 Vcs =2080,87 Rss =95.59 % Rcs =89.29% Os =6.3 % Css = 199 Ccs = 210 Dc = 11	Vss =1943,76 Vcs =2021,04 Rss =95.59 % Rcs =91.9 % Os =3.69 % Css = 199 Ccs = 206 Dc = 7

Inmediato o *Agregación* en los costes de operación de la plataforma, la Fig. 4 representa dicha diferencia en cada escenario para un distrito. Se observa que la diferencia de costes a nivel de distrito puede llegar a ser considerable, especialmente en escenarios *Urbanos* a *Largo plazo*, así como que la diferencia es siempre más notable en el caso de que se utilice IPsec, ya que el *overhead* que introduce este protocolo es mayor.

La Fig. 4 ilustra por tanto el ahorro que se puede alcanzar utilizando *Agregación*. No obstante, cabe destacar que la reducción de costes que supone la *Agregación* es tanto más alta cuanto mayor sea el número de períodos sobre el que se agregue la información, por lo que los resultados obtenidos en el presente análisis representan una cota inferior del ahorro que podría alcanzarse utilizando *Agregación.*

La Tabla VIII muestra la diferencia entre el coste anual de utilizar IPSec y el coste anual de utilizar TLS/SSL ($C_{cs}|_{IPSec} - C_{cs}|_{TLS/SSL}$) en cada escenario tanto por CNTR como para todo el distrito. Para facilitar la interpretación de cómo influye utilizar IPSec o TLS/SSL en los costes de operación de la plataforma, la Fig. 5 representa dicha diferencia en cada escenario para un distrito. Se observa que la diferencia de costes es especialmente relevante en el *Largo plazo*.

Combinando este análisis con el análisis técnico realizado en la sección III, se puede concluir que, para minimizar los costes de operación de la plataforma, se recomienda utilizar *Agregación* y TLS/SSL como protocolo para establecer VPN.

Sin embargo, cabe señalar que el coste de emplear IPSec podría reducirse si se implementasen mecanismos de compresión, pudiendo ocurrir lo mismo si se utilizase OpenSSL como solución TLS/SSL.

TABLA VII
DIFERENCIA DE COSTE (EN €) POR CNTR Y POR DISTRITO EN 1 AÑO ENTRE USAR REENVÍO INMEDIATO Y AGREGACIÓN EN CADA ESCENARIO

	Corto plazo		**Largo plazo**	
	IPSec	**TLS/SSL**	**IPSec**	**TLS/SSL**
Urbano	9*12=**108** 108*150= **16200**	3*12=**36** 36*150= **5400**	17*12=**204** 204*150= **30600**	7*12=**84** 84*150= **12600**
Rural	3*12=**36** 36*220= **7920**	0	7*12 = **84** 84*220= **18480**	7*12=**84** 84*220= **18480**

TABLA VIII
DIFERENCIA DE COSTE (EN €) POR CNTR Y POR DISTRITO EN 1 AÑO ENTRE USAR IPSEC Y TLS/SSL EN CADA ESCENARIO

		Corto plazo	**Largo plazo**
Urbano	**Agr.**	0	16*12 = **192** 192*150= **28800**
	RI	6*12 = **72** 72*150=**10800**	26*12 = **312** 312*150=**46800**
Rural	**Agr.**	0	4*12 = **48** 48*220=**10560**
	RI	3* 12=**36** 36*220=**7920**	4*12 = **48** 48*220=**10560**

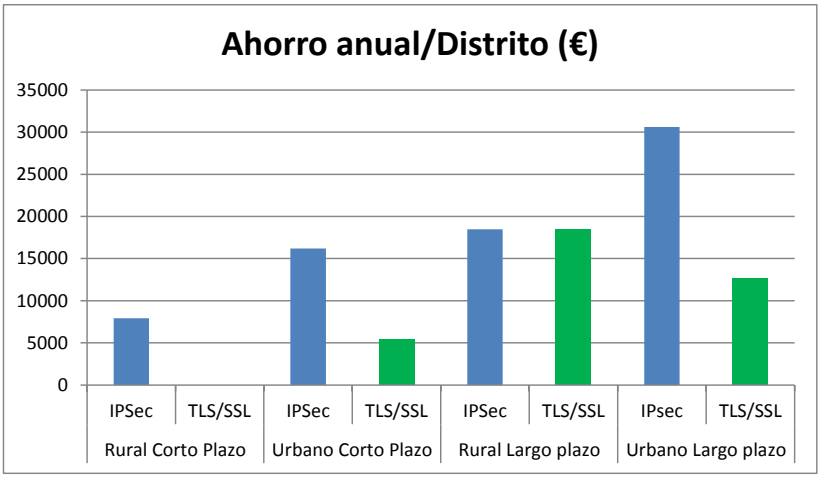


Fig. 4. Diferencia de coste por distrito en 1 año entre realizar RI (*Reenvío Inmediato*) y *Agregación* para cada protocolo de seguridad en cada escenario

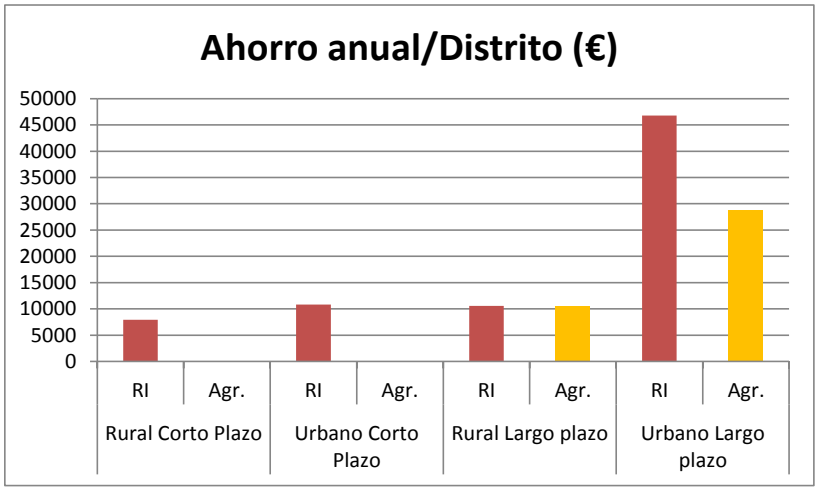


Fig. 5. Diferencia de coste por distrito en 1 año entre usar IPSec y TLS/SSL en cada escenario dependiendo de si se realiza *RI* o *Agregación*

V. Conclusiones

Este artículo analiza y compara IPSec y TLS/SSL y evalúa el impacto - tanto desde un punto de vista técnico como económico – de emplearlos como soluciones para establecer VPN en una plataforma orientada a reducir el consumo eléctrico e integrar la micro-generación distribuida a nivel de distrito.

Las principales conclusiones de este trabajo son que, aunque ambos protocolos cumplen con los requisitos básicos de este tipo de aplicaciones, la utilización de TLS/SSL minimiza los costes de operación de la plataforma, especialmente en escenarios a *Largo plazo*.

La agregación de información en el CNTR también permite reducir considerablemente el coste de operación de la plataforma a nivel de distrito.

Agradecimientos

Este trabajo ha sido financiado parcialmente por el Ministerio de Economía y Competitividad español a través del programa INNPACTO dentro del proyecto PRICE-GEN (IPT-2011-1507-920000), y por la Comisión Europea a través del Séptimo Programa Marco FP7 2007-2013 dentro del proyecto ENERsip (247624).

Referencias

[1] Eurostat Energy Statistics: http://epp.eurostat.ec.europa.eu/portal/page/portal/energy

[2] A. de Almeida, P. Fonseca, B. Schlomann, N. Feilberg, "Characterization of the Household Electricity Consumption in the EU, Potential Energy Savings and Specific Policy Recommendations", *Energy and Buildings*, Vol. 43, No. 8, pp. 1884-1894, 2011.

[3] L. Hernández *et al*, "A multi-agent system architecture for smart grid management and forecasting of energy demand in virtual power plants", IEEE Communications Magazine, Vol. 51, No 1, pp 106 - 113, 2013.

[4] P. Moura, A. de Almeida A, "The Role of Demand-Side Management in the Grid Integration of Wind Power", *Applied Energy*, Vol. 87, No. 8, pp. 2581-2588, 2010.

[5] G. López, P. Moura, B. Kantsepolsky, M. Sikora, J. I. Moreno, A. de Almeida, "European FP7 project ENERsip: Bringing ICT and Energy Together", *IEEE Global Communications Newsletter*, Vol. 15, No. 11, pp. 2-4, 2012.

[6] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. Chen, "Cyber Security and Privacy Issues in Smart Grids", IEEE Communications Surveys & Tutorials, Vol. 14, No.4, pp. 981-997, 2012.

[7] P. McDaniel, S. McLaughlin, "Security and Privacy Challenges in the Smart Grid", IEEE Security and Privacy, vol. 7, no.3, pp.75-77, May/June 2009.

[8] G. López, P. Moura, J. I. Moreno1, A. de Almeida "ENERsip: M2M-based platform to enable energy efficiency within energy-positive neighbourhoods" IEEE INFOCOM 2011 Workshop, Shanghai, China, 2011.

[9] A. M. Carreiro, G. López, P. Moura, J. I. Moreno, A. T. de Almeída, J. L. Malaquias, "In-House Monitoring and Control Network for the

Smart Grid of the Future", IEEE PES Innovative Smart Grid Technologies Europe 2011, Manchester, UK, 5-6th December 2011.

[10] G. Lopez, J. Moreno, P. Moura, A. de Almeida, M. Perez, L. Blanco "Monitoring System for the Local Distributed Generation Infrastructures of the Smart Grid," *22nd European Conference and Exhibition on Electricity Distribution CIRED 2013*, Stockholm, Sweden, 2013.

[11] G. López, P. Moura, V. Custodio, J. I. Moreno, "Modeling the Neighborhood Area Networks of the Smart Grid", IEEE ICC, Ottawa, Canada, 2012.

[12] S. Khanvilkar, A. Khokhar, "Virtual Private Networks: An Overview with Performance Evaluation", IEEE Communications Magazine, Vol. 42, No10, pp. 146-154, 2004.

[13] T. Berger, "Analysis of current VPN technologies", IEEE ARES 2006, 2006.

[14] L. Zhao, R. Iyer, S. Makineni, L. Bhuyan, "Anatomy and Performance of SSL Processing", IEEE ISPASS 2005, Austin, USA, 2005.

[15] A. Alshamsi, T. Saito, "A Technical Comparison of IPsec and SSL", IEEE AINA 2005, 2005.

[16] M. Meyer, "TCP Performance over GPRS", IEEE WCNC 1999, New Orleans, USA, 1999.

[17] J. Rendón, F. Casadevall, D. Serarols, "Snoop TCP Performance over GPRS", IEEE VTC Spring 2001, Rhodes, Greece, 2001.

[18] P. Benko, G. Malicsko, A. Veres, "A Large-scale, Passive Analysis of End-to-End TCP Performance over GPRS", IEEE INFOCOM 2004, Hong-Kong, 2004.

[19] N. Aschenbruck, M. Frank, W. Hansmann, P. Martini, C. Scholz, J. Tölle, "Integration of 3G Protocols into the Linux Kernel to Enable the Use of Generic Bearers", *High Speed Networks and Multimedia Communications*, pp. 533-544. Springer Berlin Heidelberg, 2004.

A Security Response Approach Based on the Deployment of Mobile Agents: Limitations and Improvements

Roberto Magán-Carrión, José Camacho-Páez, Pedro García-Teodoro
Department of Signal Theory, Telematics and Communications,
Faculty of Computer Science and Telecommunications - CITIC,
University of Granada
Periodista Daniel Saucedo Aranda, s/n, E-18071 GRANADA (Spain)
rmagan@ugr.es, josecamacho@ugr.es, pgteodor@ugr.es

***Abstract*—This paper introduces a response mechanism to improve the tolerance against security threats in MANET environments. The mechanism is launched after detecting the existence of nodes with malicious behavior, and is based on the use of one or more mobile agents to improve the connectivity of the network. This way, in the event of the detection of a malicious node (e.g. a *selfish* node or a *dropper* node), a set of agents are deployed to recover and maximize the overall connectivity of the network. Every agent acts as a relaying node within the MANET and is automatically positioned according to a particle swarm optimization (PSO) process. Also, the paper introduces some improvements in the use of PSO to maximize the connectivity in comparison to previous works. The experimental results show the suitability of the approach to improve the survivability of the network from a security perspective.**

***Keywords*—Agent, PSO, detection mechanism, malicious behavior, MANET, response, survivability, tolerance.**

I. INTRODUCTION

In the context of ad hoc networks, mobile ad hoc networks (MANETs) have several special characteristics: lack of a fixed infrastructure, dynamic changing topology, resource constraints and restricted physical security, among others [1]. In this kind of networks, the communication between nodes is limited by their coverage range. Therefore, not all the nodes are directly connected, and thus a multi-hop relay-based scheme is needed for end-to-end transmissions. Some possible applications of MANETs include military scenarios (e.g. soldier communications in the battlefield), emergency rescue (e.g. earthquakes) or fire disasters management when the fixed communication infrastructures are no longer available.

Compared with traditional wired networks, MANETs are much more vulnerable to attacks due to the limited energy of nodes, which avoids the use of complex security solutions; the wireless transmission medium, which makes eavesdropping easier; the lack of management and control unit; and the implicit mobility of these environments. Attacks like *black-hole*, *sinkhole*, *dropping* or malicious behaviors as *selfish*, are specific for MANETs [2]. These inherent threats have a high impact over the network performance, since nodes need to send information through intermediate neighbors that could be attackers. Thus, security mechanisms to strengthen the services provided are needed. Deploying efficient security systems to reduce risks and threats by providing proper mechanisms to maximize the network performance is also required. This will raise the network survivability, which is defined as *"the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures or accidents"* [3].

In this context, the present work proposes a multiagent-based system aimed at enhancing the connectivity between nodes in the network in the presence of nodes with malicious behavior. Hence, a tolerant and resilient network is obtained. The response mechanism presented here is based on the work of *Dengiz et al*. [4], where the authors improve the network performance by maximizing the connectivity and the data flow transmitted. They make use of the particle swarm optimization (PSO) algorithm and model prediction control (MPC) for future user node locations (by using kinematic based techniques), to locate the agent nodes in optimal positions to maximize the overall connectivity.

The principal contribution of this paper is the use of mobile agents as a response mechanism for improving security in MANETs. This way, in the event of detecting malicious nodes in the environment, the corresponding worsening of the network performance is mitigated by deploying some agents in charge of relaying packets and thus recovering and improving overall coverage and connectivity. Although the solution introduced by *Dengiz et al.* in [4] exhibits good performance in general, it does not provide the best results. This work introduces some modifications of the original approach which improve the overall connectivity of the network, as it will be shown along the paper.

The rest of the paper is organized as follows. Section II presents some relevant works about multiagent systems in general, and security related ones in particular. Section III introduces a discussion about the reference work by *Dengiz et al.* [4] and the novel system proposed here. Some simulation-based experimental results to corroborate and validate the application of the original approach in the security domain are described in Section IV. Despite the good performance exhibited in the desired direction, some flaws for the technique are discussed in Section V, so that it is improved by introducing some alternative metrics to lead the deployment of the agents. Finally, Section VI summarizes the principal conclusions and remarks of this work while future research directions are highlighted.

II. RELATED WORK

There are several proposals in the literature centered on the use of mobile agents in ad hoc wireless networks addressing different challenges: network connectivity and node optimization positioning, improvement of network quality of service (QoS) parameters, energy optimization and security issues. In [5] the locations of agent nodes are optimized by means of a PSO algorithm to maximize the connectivity between user nodes and a control node. A PSO algorithm is also used in [4] enhanced with a model predictive control (MPC) by using kinematic techniques, with the aim of maximizing the connectivity and flow transmission (throughput) in MANETs. Furthermore, in military scenarios, a mobile agent trajectory is optimized according to the deployed positions of the user nodes, thus maximizing the connectivity between the control node and the arranged user nodes [6].

Another group of contributions have been proposed to improve QoS parameters and for energy optimization using ant colony optimization (ACO) and bee colony optimization (BCO) algorithms. Packet delivery ratio and end-to-end delay are the focus in [7]. In that reference, an ACO scheme is used to find out the shortest path both in routing discovery and maintenance phases. Similarly, the authors in [8] improve the network bandwidth by using an ACO algorithm. There, a number of ants are in charge of discovering the best routes according to the destination distance, the available bandwidth and the queue of the nodes. An efficient routing algorithm is proposed in [9], where the routes are selected by employing bees to select the path with least energy consumption requirements.

Deploying attack detection (recognition) and event response (recovery) mechanisms constitute key issues for network survivability [3]. Non-legitimate event detection in networks is an aspect that has been recurrently studied in the specialized literature. On the other hand, response mechanisms try to solve the non-legitimate events detected in order to guarantee the continuity of the network and the affected services. Nevertheless, in the multiagent system field just a few works have been developed to address security detection and response issues, and these are limited to the use of software agents. In [10] an agent node is created and sent from the sender to the destination crossing the suspected node. If the agent never comes back, the suspected node is concluded to be a *grayhole* or a *blackhole* node. Unlike the previous work, in [11] the agent records the amount of packets received and forwarded by each node along the path. If the agent detects that the forwarded and received packets ratio is under a fixed threshold, the node is labeled as malicious. Then, a report is sent to the sender. A scheme imitating the human immune system is proposed in [12]. There exists an immune agent (IA) that is distributed along the network. The IA is in charge of detecting, classifying, isolating, and recovering if needed. A node that exceeds a certain number of attacks launched will be isolated. Reference [13] introduces a similar scheme, where the nodes are monitored and, if necessary, isolated by using two types of mobile agents: detection agent and counterattack agents. The first ones are in charge of detecting malicious behaviors, while the second ones will surround and isolate the invaders. In [14] the dynamic source routing protocol (DSR) for MANETs is modified by attaching two agents to each network node: a monitoring agent (MOA) and a routing agent (ROA). The first one monitors the node behavior to assign a trust value. The trust values are spread throughout the network into the route request packets. Afterwards, the ROA agent selects the trustworthiness route discarding others with less trust level. Thus, the nodes with low trust value are isolated.

In what follows we propose the use of physical and mobile agents as a response mechanism. Based on the pre-existence of a detection module for malicious behaviors, our approach consists of the deployment of one or more agents to solve the loss of "coverage" due to malicious nodes. The agents, acting as relaying nodes, will allow to recover and improve the overall connectivity of the network.

III. MARS: MOBILE AGENT-BASED RESPONSE SYSTEM

As mentioned above, the proposed system is inspired by the work of *Dengiz et al*. work [4], in which the connectivity of a MANET is improved by using mobile agent nodes. In this section, a brief explanation of that approach is first presented. A description of the specific response system proposed here, named MARS, is afterwards provided.

A. Connectivity maximization using PSO and MPC

Two types of nodes are involved in [4]: user nodes and agent nodes. User nodes are final nodes demanding some given network service, while agent nodes try to guarantee that user nodes are receiving the best network service as possible by maximizing the overall connectivity. The connectivity is related to the coverage range. Two nodes are accessible or connected (that is, there is a link between them) if the Euclidean distance between them is less or equal to R, where R is the coverage range of a radio node.

Basically, the authors in [4] suggest two objectives: to maximize the overall connectivity of the network, and to maximize the throughput. This optimization process is achieved by using the PSO algorithm [15] and several optimization functions. Two important and particular entries of the PSO algorithm are: (a) the future motion predictions of user nodes for a specific prediction time horizon $(t + H)$, and (b) the best solution obtained in the previous time step. Afterwards, a comparison among several possible problem solutions (*particles*) is made. The different particles in the same PSO execution are specific network distributions where the user node locations at $t + H$ are the same and the agent nodes positions are modified by increasing or decreasing its velocity and direction values. When the PSO optimization process is finished, the algorithm returns the best locations of each agent node to maximize the overall connectivity and flow transmission of the network at a given time instant.

There are three optimization or objective functions involved. With the first, O_{1t}, the global network connectivity is evaluated. This function follows:

$$O_{1t} = \frac{2 \times \sum_{i,j \in UN_t : j > i} Z_{ijt}}{UN \times (UN - 1)} \quad (1)$$

where UN is the number of user nodes and $Z_{ijt} = 1$ if there exists an available (either single or multi-hop) path connecting the i-th and j-th user nodes at time t. Otherwise, $Z_{ijt} = 0$.

A second function, O_{2t}, maximizes the data flow transmission by improving the weakest link, in terms of throughput, of the network. This is supposed to enhance the overall network performance. O_{2t} is only evaluated when several possible solutions of the optimization (several particles under evaluation) represent completely connected networks, that is if $O_{1t} = 1$ in all of them. O_{2t} is computed through the following expression:

$$O_{2t} = \min_{i,j \in UN_t : j>i} \{U(G_t, i, j) : U(G_t, i, j) > 0\} \quad (2)$$

where $U(G_t, i, j)$ is the throughput between the node i-th and j-th throughout the network G_t at time t.

For disconnected networks, a third function O_{3t} is considered. O_{3t} measures the distance from each agent to the imaginary middle point (*attraction points*) among partitions of the network. O_{3t} minimizes these distances to locate the agent nodes closer to the attraction points. O_{3t} is obtained as:

$$O_{3t} = \min_{i \in AN_t, j \in A_t} \left\{ \sqrt{(x_{it} - x_{jt})^2 + (y_{it} - y_{jt})^2} \right\} \quad (3)$$

where AN_{it} is the i-th agent node and the A_{jt} is the j-th attraction point at time t.

In summary, the solution with a higher value for O_{1t} ($\max\{O_{1t}\}$) is the best solution. If there are several completely connected networks in the solution of the optimization, the one with higher O_{2t} value ($\max\{O_{2t}\}$) is selected. However, if there are disconnected networks with equal values for O_{1t}, the one with lower O_{3t} value ($\min\{O_{3t}\}$) is chosen.

The optimization algorithm is iteratively repeated over time, the agents being dynamically positioned at their best locations step by step. More details about the entire process can be found in the reference paper [4].

B. System description

As commented in Section II, there are few research proposals about response security solutions in MANET networks, specially involving multiagent systems. Also, most of them are merely related to the detection of malicious behaviors.

In this context, our proposal MARS is intended to establish a response mechanism against malicious behaviors in MANETs by using mobile agents. MARS is conceived to be a tolerant mechanism against attacks such as *selfish*, where a node has an egoistic behavior not forwarding packets to preserve its own resources (e.g. battery life); or *dropping*, where a node drops the received packets instead of forwarding them.

Both types of attacks, *selfish* and *dropping*, among others, have similar consequences on network performance. These kinds of malicious nodes will prevent other nodes to communicate with each other.

MARS is conceptually composed of two modules: a detection module and a response module. The first one is in charge of detecting the malicious behaviors triggering the corresponding alarm to activate the response module. Then, the response module dynamically launches a set of mobile agents around the area. These agent nodes have two main features. First, they act as mere relaying nodes to solve the network connectivity decreased due to the appearance of malicious nodes. Second, the base optimization algorithm proposed in [4] is executed to determine the best positions of the agents to maximize the overall connectivity at each time. The functional architecture for MARS is shown in Figure 1. The detection module design is out of the scope of this work, an example of which can be found [16].

To illustrate how MARS works, Figure 2 depicts different network situations. Initially, several user nodes (solid circles) are randomly distributed throughout a given network area, where there is also one malicious node (inverted triangle) and one agent node (solid square). At the beginning, in Figure 2(a), the malicious node works as a normal node. Afterwards, in Figure 2(b) the attack is in progress, so that the overall connectivity is broken and two separated networks are obtained. Figures 2(c) and 2(d) show the coverage recovery process. The agent, A1, is approaching to its optimal position (according to PSO), thus making possible the connection among the previously disconnected user nodes. In this case, the use of one single agent cannot provide full connectivity between user nodes due to their motion and the coverage range. Nevertheless, the position of A1 is optimally computed in order to connect the maximum number of nodes, as shown in Figures 2(e) and 2(f). Obviously, is a very difficult task that only one agent makes the network totally connected, so more agents should be deployed.

IV. EXPERIMENTAL RESULTS

This section is devoted to study the performance of our security response/tolerance system, MARS. For that, a set of experiments in a simulation scenario with Matlab are carried out. The main features of the scenario are:

1) The network area is 5m $\times$ 5m.
2) The coverage range R=1m, thus assuring disconnection among nodes.
3) The prediction horizon H=4, because it is an optimal value that offers better connectivity values in accordance with [4].

In order to evaluate the evolution of the connectivity of the network under various situations with respect to the number of final user nodes (UNs), number of malicious nodes (MNs), and number of agent nodes (ANs), five different combinations are proposed. We consider a first scenario with only 20 UNs, a second one with 20 UNs and 5 MNs and three additional scenarios with 20 UNs, 5 MNs and 1, 3 and 5 ANs. From these scenarios, we will show how the connectivity decreases due to the operation of the malicious nodes (a), and how it is recovered and improved after deploying the agent nodes.

Each connectivity analysis involves 25 repetitions for each experiment, where different initial random distributions of UNs and ANs in the network area are considered. Figure 3 shows the results obtained from our experimentation. The negative effect of the MNs in the network connectivity is illustrated. In this case the connectivity is decreased in comparison to the case where only UNs exist. The deployment of ANs in the environment, once the the existence of MNs is determined, contributes to the recovery of the connectivity of the overall

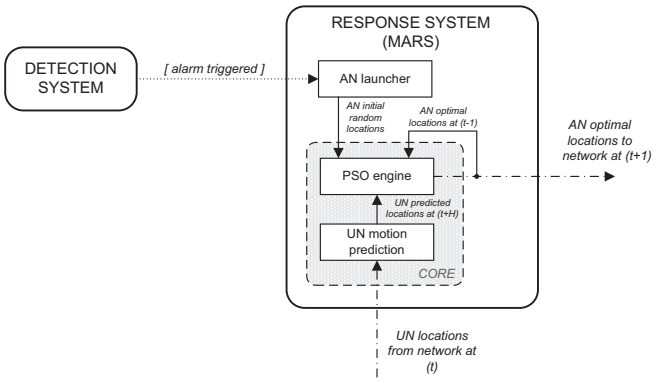
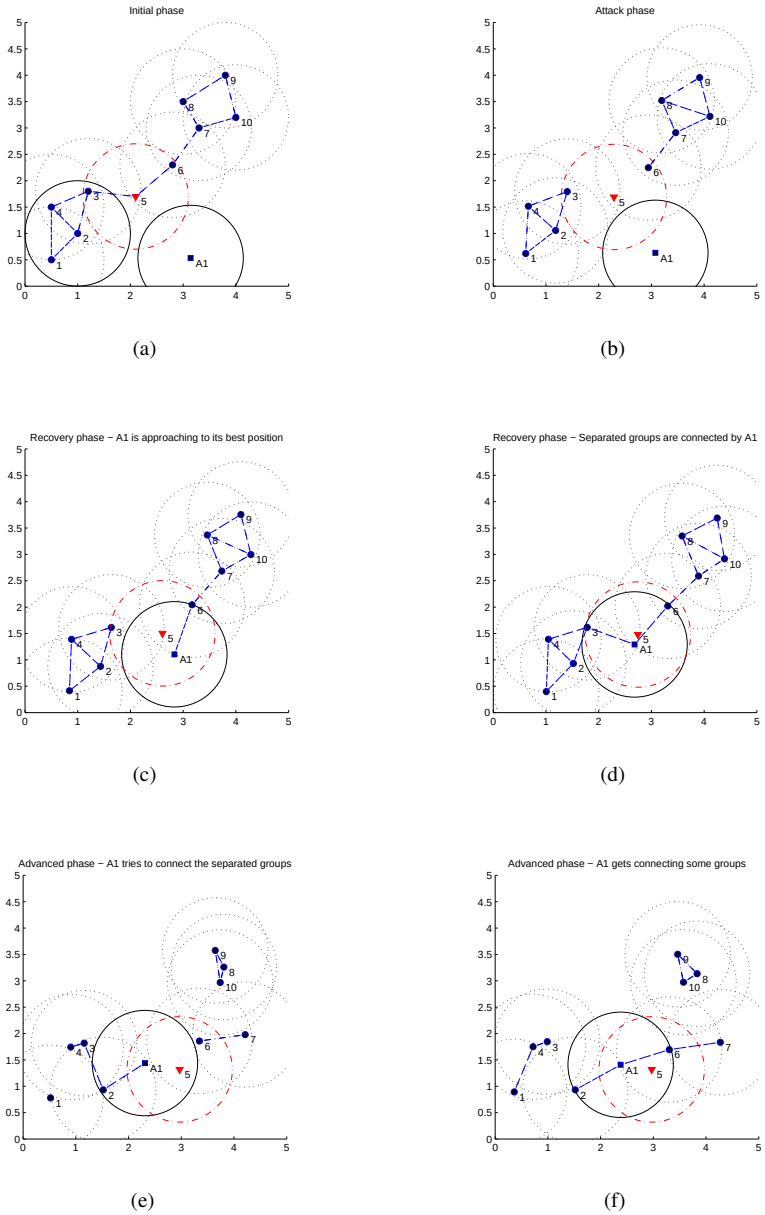


Fig. 1. Functional architecture for MARS



(a) (b) (c) (d) (e) (f)

Fig. 2. Connectivity maximization and recovery process. Initial phase where a malicious node (inverted triangle) is performing the forwarding process together with the user nodes (solid circles) (a). Two separated groups of nodes result when the attack is carried out (b). Motion of the agent A1 when approaching to its optimal location recovers connectivity and thus communications (c) (d). The agent is finally positioned to connect the maximum number of nodes (e) and (f), but full connectivity is not attained.

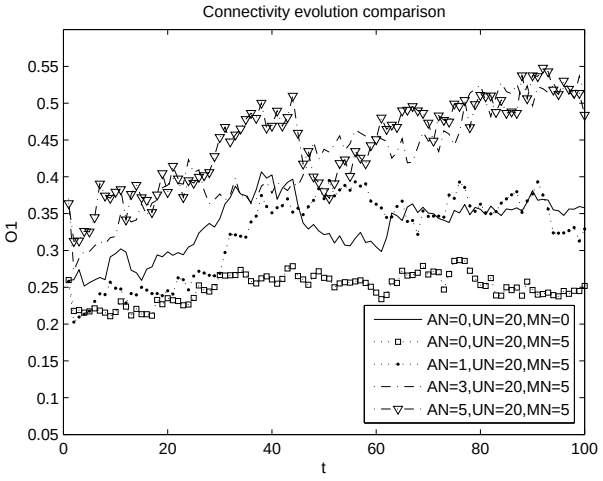


Fig. 3. Connectivity evolution along 100 time instants under influence of both malicious and agent nodes. The agents contribute to recover and improve the connectivity, so the latter is increased with the number of ANs.

network. On the one hand, the connectivity increases with the number of ANs. On the other hand, the connectivity with 5 ANs and 5 MNs is even higher than when there is no MNs in the MANET. Also, the scenario with no MNs presents an steady connectivity, as expected, while the connectivity with ANs is increased with the time evolution. This shows the effectiveness of the approach, and it is the result of the optimization of the position for ANs. Therefore, the deployment of ANs in the environment contributes to recover and improve the lost connectivity of the overall network.

V. LIMITATIONS OF THE APPROACH AND IMPROVEMENTS

In this section we introduce some flaws encountered in the reference work [4] the current proposal is based on. To fix them some improvements are introduced.

A. Limitations of the system

The response module of MARS is composed by two subsystems: the MPC (for UN motion prediction) and the PSO engine. Both are derived from the reference work [4], where PSO is intended to determine the best positions for the agents to mitigate the effects of the malicious nodes by maximizing the overall network connectivity. As described in Section III-A, through O_{3t} we try to minimize the distances between the agent nodes and the attraction points when disconnected networks appear due to the malicious nodes operation (see Eq. (3)). We can see a flaw in O_{3t} regarding the distance minimization procedure itself. Although it is aimed at attracting the agents to the attraction points to recover the overall connectivity, it does not work correctly when more than one agent is considered.

To corroborate this undesirable behavior in a visual way, we present a static scenario in which there are 3 ANs for recovering and maximizing the connectivity; 14 UNs distributed around the area, and 2 MNs to interrupt the normal network operation. Initially the network is totally connected (see Figure 4(a)). Then, when the attack occurs, the network is partitioned, so three partitions appear with the corresponding attraction points between each one.

The inadequate behavior of the original O_{3t} function is illustrated in Figure 4(b). The expected logical behavior is to locate each agent node just in the attraction point (inverted empty triangles in Figure 4) position or in a close area. From Eq. (3), we can see that by minimizing the minimum distance between agent nodes and attraction points only one agent node is correctly positioned. It demonstrates that O_{3t} function is ill-defined.

B. System improvements by varying O_{3t} function

To improve the behavior of the O_{3t} and thus the connectivity of the network we propose here three alternative O_{3t} functions. For each one we compare the connectivity evolution obtained with the original O_{3t} in a mobile scenario with 5 ANs, 20 UNs and 5 MNs.

The first one, O_{31t}, corresponds to the sum of the minimum distances obtained from each agent node to each attraction point, as expressed in the following equation:

$$O_{31t} = \sum_{i=1}^{AN_t} \min_{j \in A_t} \{d_{ij}\} \tag{4}$$

where d_{ij} is the Euclidean distance between the i-th agent node and the j-th attraction point. Through this slight conceptual modification we move all the agent nodes to all the attraction points making the agents nodes more intelligent. In fact, an improvement on the connectivity is obtained and illustrated in Figure 5(a) when a mobility scenario is used. Nevertheless, this approach produces an inadequate behavior when the agents nodes are close to the same attraction point at the same time. All of them reach this attraction point and remains there over the time. Figure 4(c) shows this limitation.

The second alternative function, O_{32t}, is a slight modification of the previous one. This new function is the sum of the minimum distances obtained from each attraction point to each agent node. The corresponding definition is presented below:

$$O_{32t} = \sum_{j=1}^{A_t} \min_{i \in AN_t} \{d_{ji}\} \tag{5}$$

where d_{ji} is the Euclidean distance between the j-th attraction point and i-th agent node. Now the attraction points are in charge of attracting each agent node just to their locations. By replacing O_{3t} with O_{32t}, the connectivity is improved, as shown in Figure 5(b). Although the connectivity is improved again, this function is also ill-defined. As O_{32t} attracts the closest agent to all the attraction points, this agent is positioned in the "center of mass" of the area represented by the attraction points. This behavior is depicted in Figure 4(d).

The previous alternative O_{3t} functions improve the network connectivity obtained by the original O_{3t} function in [4]. Nevertheless, they still present limitations. To solve this limitation we introduce a third variant of O_{3t}, O_{33t} function. This function subtracts the total sum of the distances among the agent nodes and the attraction points with the total sum of the distance among agents. These two components of the function are introduced in the following equation:

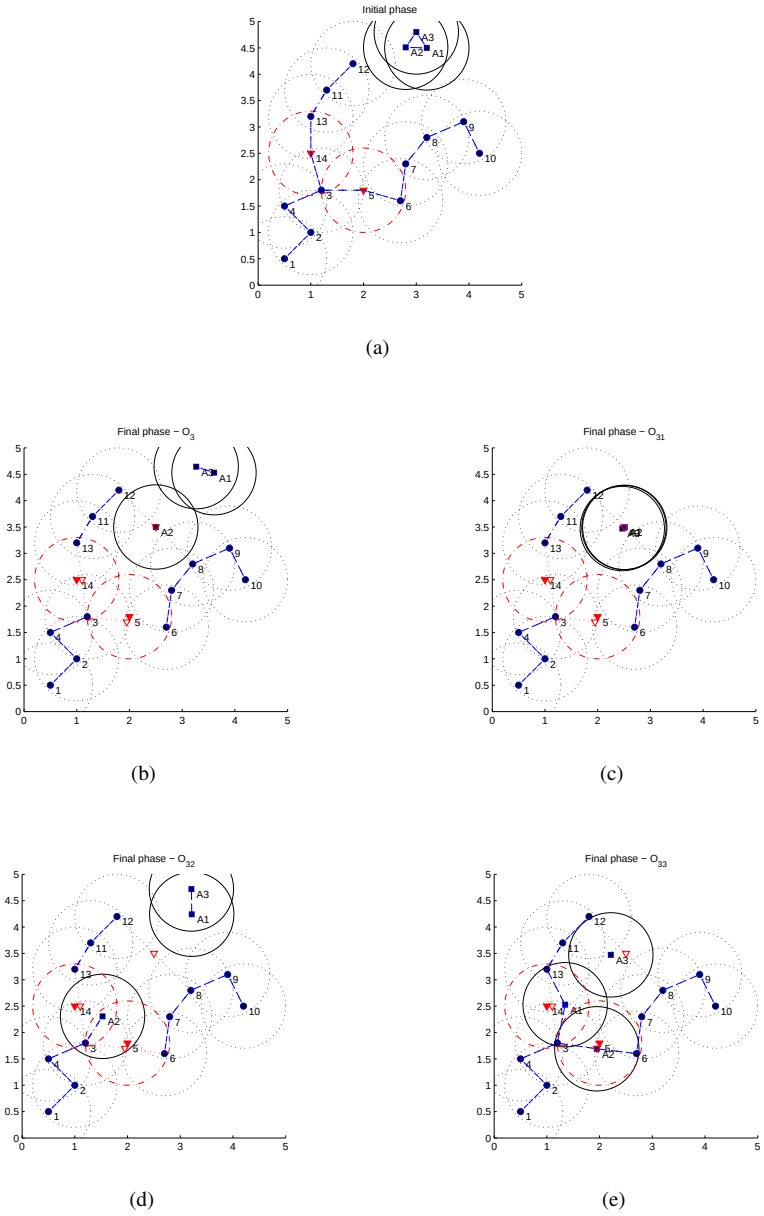


Fig. 4. Agent node movements and final positions over time: (a) Initial positions of the user nodes and the agent nodes, just before the attack; (b) final locations of the agents by using the original O_{3t} function in [4]; (c) final locations of the agents by using O_{31t} function; (d) final locations of the agents by using O_{32t} function; (e) final locations of the agents by using O_{33t} function.

$$O_{33t} = \sum_{i=1}^{AN_t} \sum_{j=1}^{A_t} d_{ij} - \sum_{i,j \in AN_t : j>i} da_{ij} \qquad (6)$$

where da_{ij} is the Euclidean distance between i-th and j-th agents. The first part of Eq. (6) represents the total distance among the agent nodes and the attractions points. We want to minimize this value to attract the agent nodes. The second term of the equation measures the total distance among each pair of agent nodes. This part is introduced to separate as much as possible the agents among them. The bigger this value, the lower O_{33t} value. This reasoning seems logical and, in fact, solve the problems encountered with the previous O_{3t} variants.

As expected, the connectivity obtained by O_{33t} is better than that provided by the previous two variants. We can see the connectivity evolution in Figure 5(c) and the final agent positioning in Figure 4(e). In this case the agents are located just over each attraction point thus recovering the lost connectivity.

VI. CONCLUSIONS AND FUTURE WORK

In this paper a novel response/tolerance approach for security threats in MANETs is proposed, MARS. It is based on the use of mobile agent nodes, which are launched in case of detecting the existence of malicious nodes in the environment that decrease the connectivity of the network. A positioning optimization procedure is carried out to determine the best positions of agents at a given instant and repeated over time.

The experimental results obtained show the improvement in connectivity and thus the tolerance and survivability exhibited by the network operation when confronted to security attacks, when our approach is considered. However, there are situations where the approach does not work properly. To fix such

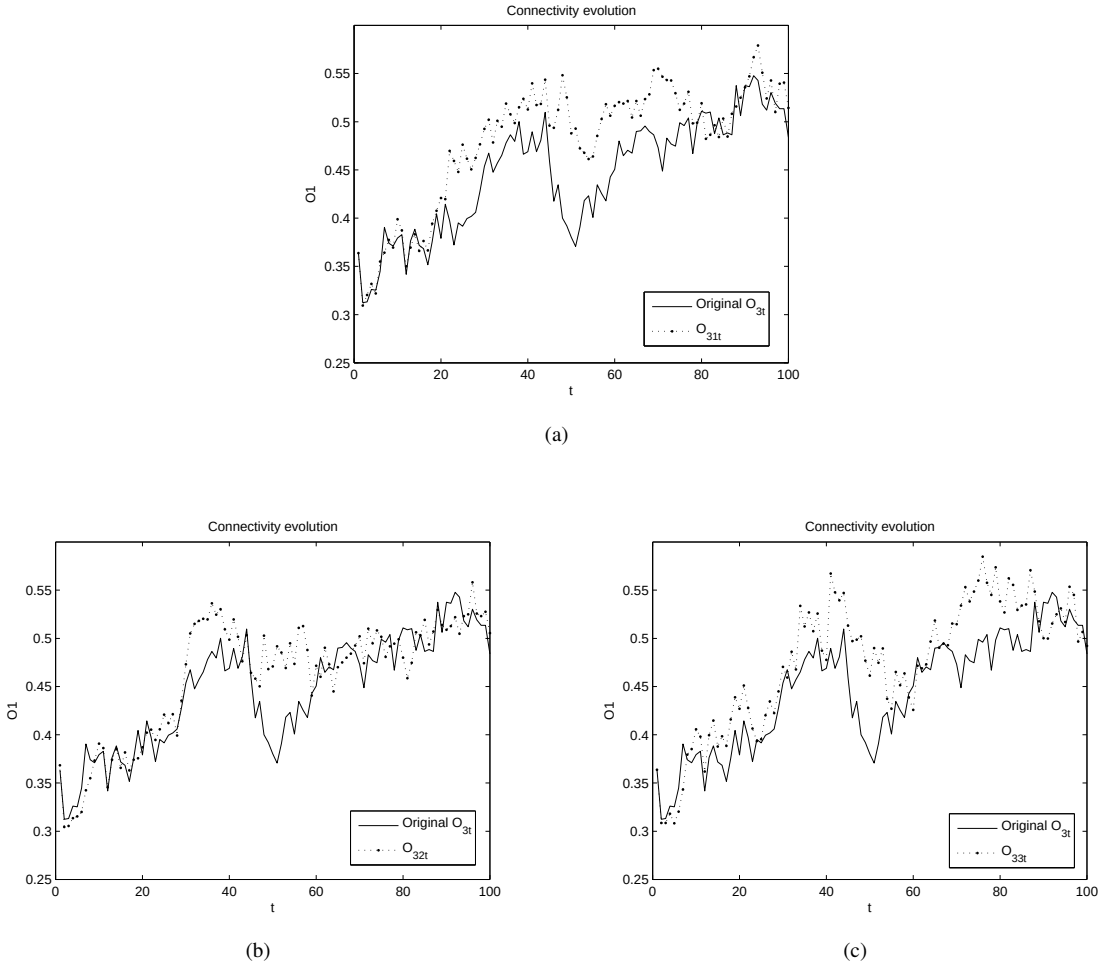


Fig. 5. Connectivity evolution provided by each of the alternative O_{3t} functions proposed with AN=5, UN=20, MN=5 considering mobility. All of them are compared to the original O_{3t} solution. (a) O_{31t} case; (b) O_{32t} case; (c) O_{33t} case. As shown, the last one provides the best results.

undesirable limitations, new alternative objective functions are studied to position the agent in a more intelligent way. In fact, the new experimental results obtained evidence the goodness of the ulterior improvements proposed.

Nevertheless, further work should be performed to strengthen the current proposal. First, more complete, multi-level related objective functions may be studied to lead deploying the agents over the network. Second, positioning the agent nodes might depend on the particular type of attack detected. Third, the response/tolerance scheme can used as a feedback element to strengthen the security design of the network.

ACKNOWLEDGMENT

This work has been partially supported by Spanish MICINN through project TEC2011-22579 and by the FPU P6A grants program of the University of Granada.

REFERENCES

[1] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, ser. Signals and Communication Technology, Y. Xiao, X. S. Shen, and D.-Z. Du, Eds. Springer US, Jan. 2007, pp. 103–135.

[2] H. Ehsan and F. Khan, "Malicious AODV: implementation and analysis of routing attacks in MANETs," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2012, pp. 1181–1187.

[3] M. Lima, A. dos Santos, and G. Pujolle, "A survey of survivability in mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 11, pp. 66–77, 2009.

[4] O. Dengiz, A. Konak, and A. E. Smith, "Connectivity management in mobile ad hoc networks using particle swarm optimization," *Ad Hoc Networks*, vol. 9, no. 7, pp. 1312–1326, Sep. 2011.

[5] Y. Cho, J. Smith, and A. Smith, "Optimizing tactical military MANETs with a specialized PSO," in *2010 IEEE Congress on Evolutionary Computation (CEC)*, Jul. 2010, pp. 1–6.

[6] J. Miles, G. Kamath, S. Muknahallipatna, M. Stefanovic, and R. Kubichek, "Optimal trajectory determination of a single moving beacon for efficient localization in a mobile ad-hoc network," *Ad Hoc Networks*, 2012.

[7] S. Asadinia, M. Rafsanjani, and A. Saeid, "A novel routing algorithm based-on ant colony in mobile ad hoc networks," in *2010 3rd IEEE International Conference on Ubi-media Computing (U-Media)*, Jul. 2010, pp. 77–82.

[8] A. Daniel and R. Singh, "Swarm intelligence based multicast routing and bandwidth management protocol for ad-hoc wireless network using backpressure restoration," in *2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, vol. 5, Jul. 2010, pp. 516–520.

[9] I. Fahmy, H. Hefny, and L. Nassef, "PEEBR: predictive energy efficient bee routing algorithm for ad-hoc wireless mobile networks," in *2012 8th International Conference on Informatics and Systems (INFOS)*, May 2012, pp. NW–18–NW–24.

[10] A. Taggu and A. Taggu, "TraceGray: an application-layer scheme for

intrusion detection in MANET using mobile agents," in *2011 Third International Conference on Communication Systems and Networks (COMSNETS)*, Jan. 2011, pp. 1–4.

[11] D. B. Roy and R. Chaki, "Detection of denial of service attack due to selfish node in MANET by mobile agent," in *Recent Trends in Wireless and Mobile Networks*, A. zcan, J. Zizka, and D. Nagamalai, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, vol. 162, pp. 14–23.

[12] Y. Mohamed and A. Abdullah, "Immune-inspired framework for securing hybrid MANET," in *IEEE Symposium on Industrial Electronics Applications, 2009. ISIEA 2009*, vol. 1, Oct. 2009, pp. 301–306.

[13] X. Ye and J. Li, "A security architecture based on immune agents for MANET," in *International Conference on Wireless Communication and Sensor Computing, 2010. ICWCSC 2010*, Jan. 2010, pp. 1–5.

[14] I. Halim, H. Fahmy, A. Bahaa El-Din, and M. El-Shafey, "Agent-based trusted on-demand routing protocol for mobile ad hoc networks," in *2010 4th International Conference on Network and System Security (NSS)*, Sep. 2010, pp. 255–262.

[15] R. Eberhart and J. Kennedy, "A new optimizer using particle swarm theory," in , *Proceedings of the Sixth International Symposium on Micro Machine and Human Science, 1995. MHS '95*, Oct. 1995, pp. 39–43.

[16] L. Sánchez-Casado, G. Maciá-Fernández, and P. García-Teodoro, "An efficient cross-layer approach for malicious packet dropping detection in MANETs," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Jun. 2012, pp. 231–238.

Método seguro y ligero para la detección y selección de canales en redes cognitivas de sensores

Olga León, Juan Hernández-Serrano, Juan Vera-del-Campo
Departamento de Telemática
Universitat Politècnica de Catalunya
Barcelona, Spain
{olga|jserrano|juanvi}@entel.upc.edu

Carles Garrigues, Helena Rifà-Pous
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Barcelona, Spain
{hrifa|cgarrigueso}@uoc.edu

***Resumen*—La inclusión de funciones cognitivas en redes inalámbricas de sensores permite maximizar la disponibilidad de los servicios ofrecidos por las mismas. De forma general, estas propiedades cognitivas permiten que los nodos de la red puedan escoger en cada momento el canal frecuencial de mayor calidad para la transmisión; hecho que evita la denegación del servicio debido a interferencias o ataques de jamming. Para dificultar estos ataques se debe dotar de seguridad todo el proceso de intercambio de datos de canales. Sin embargo, las propuestas en el estado del arte no son adecuadas para nodos de muy bajo perfil, como es el caso de los sensores colocados en pacientes en el entorno de la eSalud. En este artículo se presenta un mecanismo ligero que permite el intercambio y selección de canales con este tipo de nodos proporcionando unos niveles adecuados de seguridad.**

***Palabras Clave*—sensores, redes de radio cognitiva, seguridad, autenticación, eSalud**

I. Introducción

En las aplicaciones que tienen unos requisitos de disponibilidad muy estrictos cualquier fallo puede causar grandes pérdidas económicas, ambientales, o incluso humanas. Es el caso de aplicaciones como las de seguimiento y vigilancia de objetivos militares, las operaciones de atención en situaciones de desastres naturales, o el control en entornos industriales. En estos escenarios las redes inalámbricas de sensores (*Wireless Sensor Networks* - WSN) [1] son una buena solución para facilitar el control de la situación a través de la toma distribuida de medidas en una amplia zona geográfica. Estas redes se componen de nodos de sensores inteligentes, es decir, dispositivos de baja potencia, capaces de detectar, medir y recopilar información del entorno y, a partir de un proceso local de decisión, transmitir los datos detectados. Debido a que en muchos casos los datos detectados pueden ser críticos, es de suma importancia maximizar la disponibilidad de este tipo de comunicaciones.

Las redes de radio cognitiva (*Cognitive Radio Networks* - CRN) pueden maximizar los servicios de disponibilidad sacando el máximo provecho de las bandas de espectro disponibles. Estas redes utilizan las bandas del espectro libres (tanto bandas sin licencia como bandas con licencia pero muy poco utilizadas) y las ocupan de forma oportunista, actuando de esta manera como usuarios secundarios de dicho espectro. Como consecuencia, los nodos de CRN hacen una detección y selección periódica de los canales disponibles para detectar las bandas en desuso y evitar interferencias a los usuarios primarios que tienen los derechos principales de uso de estas bandas.

La implementación de mecanismos de detección y selección de canales que eviten las interferencias con los usuarios primarios es uno de los principales retos de las CRN. Puesto que evitar interferencias es de máxima prioridad, las CRN habitualmente realizan el proceso de detección y selección de canales de una forma cooperativa [2], lo que permite obtener unos resultados mucho más precisos y robustos que los que pudiera obtener un nodo sólo. Así, por ejemplo, el hecho que un nodo no detecte la señal de un usuario primario debido a problemas de desvanecimientos de la señal no da lugar a posibles interferencias ya que la detección y decisión final es tomada de forma conjunta por diversos nodos. Por lo tanto, si una mayoría de nodos han detectado el canal como ocupado, la CRN descarta el uso de este canal inmediatamente.

Las redes de sensores inalámbricas y cognitivas (*Cognitive Wireless Sensor Networks* - CWSNs) [3], [4], son un nuevo paradigma de redes de sensores que ha aparecido recientemente de la combinación de redes CRN y WSN. La inclusión de capacidades cognitivas en las redes de sensores de una WSN puede tener numerosas ventajas: el comportamiento cognitivo incrementa significativamente la disponibilidad de servicios basados en WSN, incrementando su fiabilidad y aplicabilidad general.

Los mecanismos cooperativos de detección y selección de canales en las CWSN son vulnerables a ataques de denegación de servicio. El envío de datos falsos en la detección de canales podría llevar a la red a intentar operar en bandas no disponibles. De la misma forma, la escucha de los mensajes de control que intercambian los sensores podría permitir a un atacante adivinar y ocupar el que debiera ser el siguiente canal de operación, impidiendo de esta forma el correcto funcionamiento de la CWSN. Es por ello que hasta la fecha se han presentado varios métodos de detección que proponen el uso de mecanismos de seguridad para garantizar que los resultados de la detección son correctos [5], [6], es decir que no han sido manipulados por terceras entidades.

Sin embargo, estos mecanismos son difícilmente implementables cuando los nodos de red están muy limitados en cuanto a potencia de transmisión y recepción, memoria, capacidad de cómputo y batería, que es a menudo el caso de las WSN y las CWSN.

Hoy en día, uno de los ejemplos con mayor proyección

dónde es posible la aplicación de las CWSN son las redes de adquisición de datos médicas [7]. Este tipo de redes, entre otras aplicaciones, permite la monitorización constante de pacientes y requiere por tanto una garantía de disponibilidad del servicio.

Dentro del marco de desarrollo del proyecto CICYT TAMESIS (Tecnologías de Apoyo para la Monitorización del Estado de Salud e Intercambio Seguro de registros médicos) se hacía necesaria una solución de CWSN que mejorase la disponibilidad del servicio de transmisión de los datos de los pacientes. Sin embargo, los nodos sensores que se utilizan, a menudo integrados en el propio paciente, suelen ser nodos de un perfil muy bajo y no soportan, que sepamos, ninguno de los protocolos seguros de intercambio de datos de canales disponibles propuestos hasta la fecha.

En este trabajo proponemos un método para asegurar el intercambio de datos de detección en CWSN. El método minimiza los bits adicionales necesarios para garantizar la confidencialidad y la autenticación de los datos detectados. Por otra parte, el uso de un esquema ligero de cifrado y autenticación reduce al mínimo el consumo energético con respecto a los enfoques estándar al mismo tiempo que logra un nivel adecuado de seguridad.

El resto del artículo se estructura como sigue. En la sección II definimos nuestra propuesta ligera para cifrar, autenticar y descifrar los datos de detección de canales. A continuación, en la sección III analizamos la seguridad de la propuesta. La sección IV presenta un estudio tanto de la trasmisión como del coste computacional comparado con otras posibles soluciones. Y finalmente, la sección V concluye el trabajo.

II. Dotar de seguridad a la detección y selección de canales

Como hemos comentado, la presente propuesta tiene como objetivo garantizar la seguridad de la detección y selección en CWSN del siguiente canal operativo para dispositivos de sensores con capacidades de cómputo y de transmisión limitadas. Como veremos, nuestra propuesta logra niveles adecuados de confidencialidad y autenticación evitando el uso de mecanismos criptográficos costosos y permite reducir al mínimo la cantidad de información que tiene que ser transmitida a través de la red.

II-A. Requisitos y objetivos de diseño

El protocolo está diseñado para ser utilizado con dispositivos muy limitados tales como nodos sensores, pero deben ser capaces al menos de:

- Realizar una función de hash con un tamaño de salida predefinido de m bits.
- Almacenar temporalmente en su memoria RAM (memoria de acceso aleatorio) como mínimo $m \cdot (N+3)$ bits, con N el número de nodos en la red.

El estado actual de la tecnología permite asegurar que se cumple el primer requisito incluso en dispositivos muy limitados. Como se muestra en [8], hay varias funciones hash ligeras que se pueden integrar en motas inalámbricas.

El segundo requisito no es más difícil de conseguir que el primero. Como se detalla en las sección II-C, durante cada período de detección cada nodo guarda un secreto

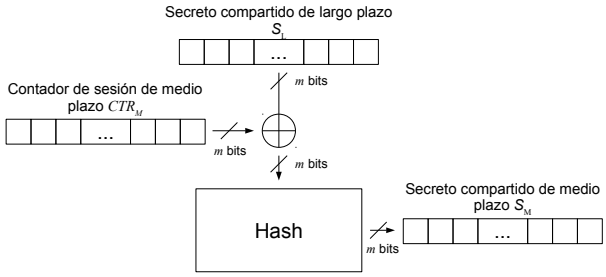


Figura 1. Generación del secreto compartido de medio plazo S_M

por cada miembro de la red, un secreto compartido global y dinámico, y dos contadores. Cada uno de estos datos tiene la misma longitud que la salida de la función de hash. Asumiendo una función de hash típica con una longitud de 128 ó 256 bits y redes de centenares de nodos, los requisitos de la memoria RAM están limitados como máximo a unas pocas decenas de kilobytes.

II-B. Inicialización

Antes de desplegar una CWSN, se tiene que precargar cada sensor con la siguiente información:

1. conjunto de canales que el sensor tendrá que escuchar en cada proceso de detección y selección de canales cooperativo.
2. un secreto compartido global y de largo plazo S_L de m bits (los mismos que el tamaño de salida de la función de hash).

Tras el despliegue, cada nodo obtiene un secreto compartido global de medio plazo S_M aplicando una función hash a la suma XOR del secreto precargado de largo plazo S_L y un contador. El proceso de generación de S_M se muestra en detalle en la figura 1. Este proceso se repite periódicamente, con los datos actualizados del contador de medio plazo, con el fin de proteger el secreto contra atacantes. Los detalles de cuándo se debe llevar a cabo este proceso están detallados en la sección III.

II-C. Funcionamiento del protocolo

Tal y como se muestra en la figura 2, en una primera fase, cada nodo genera diferentes secuencias aleatorias de m bits para sí mismo y sus vecinos. Estas secuencias aleatorias, S^u, con u el identificador del nodo, son obtenidas haciendo un hash de la suma XOR del identificador a nivel de enlace del nodo ID^u, el secreto compartido de medio plazo S_M, y el contador de sesión de corto plazo CTR_S. A su vez, cada secuencia S^u se divide en diversos fragmentos de r bits, que denominaremos keystreams K_i^u, y cada una de estos keystreams se usa como una clave de un sólo uso para cifrar y autenticar los datos en diferentes rondas de detección de canales. De esta manera no hay necesidad de generar un nuevo secreto compartido a medio plazo para cada periodo de detección y selección de canales.

Cuando un nodo realiza el proceso de detección y selección de canales, genera una secuencia binaria D_i^u de l bits que indica la disponibilidad de los canales. La longitud de dicha secuencia l dependerá del número de bits utilizados para codificar el estado de cada canal. Por ejemplo, la forma más sencilla sería utilizar un único bit para cada

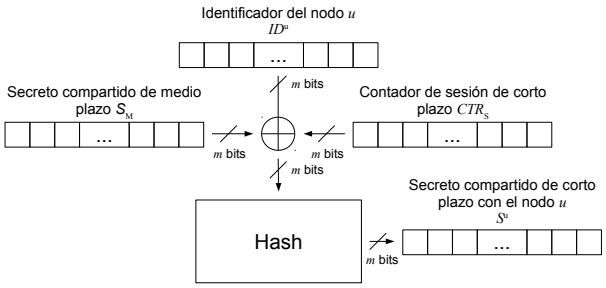


Figure 2. Generación del secreto compartido de corto plazo para el nodo u

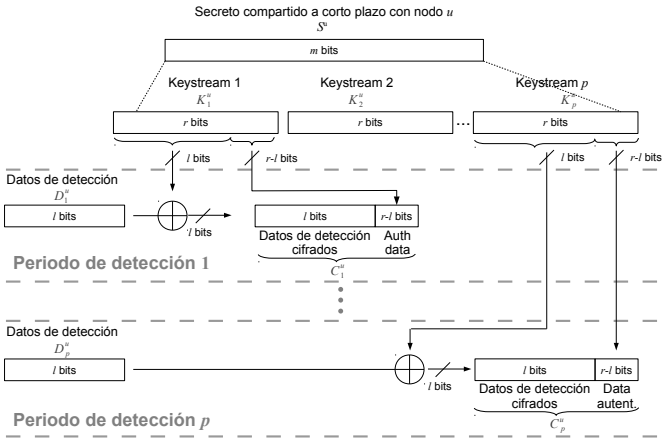


Figure 3. Cifrado y autenticación de los datos de detección de canales

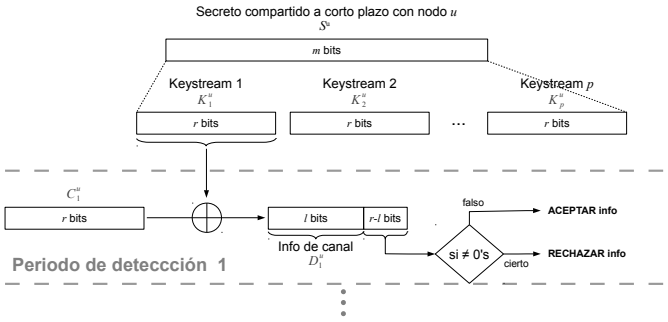


Figura 4. Descifrado de los datos de detección de canales

canal, con el valor "0" si el canal está ocupado y "1" en caso contrario. Si se necesita información más precisa sobre la calidad de los canales (i.e., alta, media, baja, muy baja), se podrían utilizar más bits para codificar el estado del canal.

Durante una ronda de detección y selección de canales i, cada nodo debe enviar a sus vecinos su propia información de detección; pero al mismo tiempo también debe procesar la información que recibe de sus vecinos con el objetivo de alcanzar una decisión conjunta. Para enviar su propia información de detección de canales, el nodo u hará uso del correspondiente keystream K_i^u: los primeros l bits del flujo de claves se utilizan para cifrar la información del canal D_i^u mediante una suma XOR; los restantes $r-l$ bits no se modifican, y se utilizarán para proporcionar autenticación al mensaje tal y como se ilustra en la figura 3. La secuencia resultante C_i^u se enviará a todos los nodos vecinos.

Para verificar la autenticidad de los paquetes recibidos de sus vecinos y descifrar su contenido, un nodo hace uso de los keystreams precalculados K_i^u asociados a sus vecinos haciendo una suma XOR de la secuencia C_i^u del paquete recibido con el keystream K_i^u como se muestra en la figura 4. Si los últimos $r-l$ bits de la secuencia resultante no son todo 0, la autenticación ha fallado y por lo tanto el paquete entero es descartado. En caso contrario, la información de canal se puede recuperar de los primeros l bits resultantes de la adición XOR.

El proceso que acabamos de describir se repite para cada nodo vecino u. Entonces, el canal seleccionado por un mayor número de vecinos es el seleccionado para el funcionamiento de la red. Obsérvese que debido a que varios canales pueden ser seleccionados por el mismo número de nodos, necesitamos definir un mecanismo de desempate que nos permita garantizar que el proceso concluye con los mismos resultados en cada nodo. Una aproximación muy sencilla sería seleccionar el canal con el identificador más alto pero, obviamente, este planteamiento llevaría a un menor uso de los canales con identificadores bajos y por lo tanto, un atacante tendría información estadística muy valiosa sobre la utilización del espectro. Como consecuencia, el proceso de desempate debería basarse en gran medida en el formato elegido para D_i^u.

Vale la pena remarcar que una característica fundamental de este protocolo es que no hay ninguna entidad central que deba ser conocida y de confianza para todos los sensores. Esto hace que el protocolo sea adecuado para escenarios desatendidos, y también lo hace muy eficiente en términos de datos transmitidos a través de la red ya que no se envía información sobre qué canales se tienen que detectar o que canal se selecciona finalmente. En lugar de esto, los sensores se despliegan con toda la información necesaria para realizar la detección y selección de canales de forma distribuida y para poder tomar de forma autónoma una decisión conjunta.

III. Análisis de seguridad

III-A. Periodo de validez de los secretos compartidos

En el contexto de esta propuesta, el periodo de validez de cada uno de los secretos compartidos es el intervalo en el que estos secretos son considerados computacionalmente seguros contra un ataque de criptoanálisis.

Para este análisis se asume que el atacante no puede acceder al material de claves almacenado en un nodo sensor. Este reto podría resolverse almacenando las claves en una memoria volátil, como la RAM estática del sensor, y utilizando una carcasa sin accesos a los pines de configuración que no pudiese abrirse sin desconectar la pila (lo que borra la RAM) y machacar los accesos. No es ésta una solución perfecta (un atacante con medios podría congelar el sensor para evitar el borrado de la RAM y extraer el material de claves en un laboratorio especializado) pero sí suficiente en una gran cantidad de escenarios.

En general, el periodo de validez de los secretos está relacionado con un criptoperiodo. Como la naturaleza de los protocolos criptográficos es muy diferente, se debe

tener en cuenta diferentes limitaciones para adecuar los criptoperiodos a cada aplicación dada; a veces los criptoperiodos se definen por un periodo de tiempo arbitrario, y otras veces se definen por la cantidad máxima de datos protegidos por la clave.

En nuestra propuesta, los secretos a partir de los cuales se construyen las claves se pueden clasificar en tres tipos de secretos compartidos:

- **Secretos compartidos a corto plazo asociados a nodos individuales.** Para cada nodo, se genera un secreto S^u que se utiliza para cifrar de forma ligera, descifrar y autenticar los datos de detección y selección de canales.
- **Secretos compartidos a medio plazo de ámbito global.** Son secretos compartidos S_M que se utilizan para generar los secretos compartidos a corto plazo asociados a nodos individuales.
- **Secreto compartido a largo plazo global.** Este es el secreto S_L precargado inicialmente que se utiliza para generar los secretos compartidos a medio plazo S_M cuando el criptoperiodo de estos últimos está a punto de expirar.

Como puede verse claramente en la figura 3, nuestra propuesta, de alguna forma, opera como un cifrador de flujo aditivo. Asumiendo que la salida de la función de hash es impredecible si se desconocen las entradas, cada secreto asociado a un nodo individual S^u es aleatorio. Por tanto, como los cifrados de flujo aditivos cumplen la propiedad *One-Time Pad*, podemos considerar que los datos cifrados de detección y selección de canales son seguros siempre y cuando S^u no se repita. Esto significa que S^u debe ser actualizado cada $p = \frac{m}{r}$ periodos de detección y selección.

Evidentemente, la elección de la función de hash tiene un fuerte impacto en la aleatoriedad de S^u. Una función de hash con una salida de m bits puede ofrecer un nivel de seguridad de 2^m operaciones a ataques preimagen y $2^{m/2}$ a ataques de colisiones. En general, se requiere una salida de como mínimo 128 bits para proporcionar un nivel alto de seguridad para aplicaciones de ámbito general, pero se aceptan longitudes más cortas en algunas circunstancias. Como se muestra en la Sección IV, nosotros proponemos funciones de hash de 128 bits, lo que significa que podemos asumir que es computacionalmente imposible para un atacante predecir el contenido de un nuevo S^u durante el tiempo de validez de este secreto.

En cuanto a la figura 2, para obtener el secreto compartido a medio plazo global S_M, un atacante debe disponer de S^u, el identificador de u y el contador de sesión a corto plazo CTR_S, y luego invertir la función de hash que da como resultado S^u. La seguridad de estas claves radica en este último paso, lo cual está fuertemente relacionado con la función de hash escogida. En este caso, S_M debe ser actualizado antes de que pueda ser recuperado mediante la inversión de la función de hash, lo cual protegerá los valores de S^u que se generen posteriormente.

El secreto compartido a largo plazo global S_L se utiliza sólo para actualizar el secreto compartido a medio plazo S_M actual. Para obtener S_L a partir de S_M, un atacante tendría que invertir la función de hash. Por lo tanto, podemos asumir que el criptoperiodo de S_L es suficientemente largo como para no tener que actualizarlo durante la vida útil de un nodo.

III-B. Autenticación

Un criptograma C_i^u de datos de detección y selección de canales contiene un campo de autenticación de 16 bits que se comprueba al ser recibido por cualquier nodo (ver figura 4). Por tanto, un atacante tiene una probabilidad entre 2^{16} de adivinar el próximo campo de autenticación, lo cual le permitiría generar un criptograma válido.

Si el ataque intenta enviar criptogramas válidos de manera repetida, tendrá éxito después de una media de 2^{15} intentos. Es importante tener en cuenta aquí que: i) los datos de detección y selección de canales que enviaría el atacante serían para él aleatorios, porqué el atacante no conoce el secreto S^u actual; y ii) el atacante no puede determinar off-line si un criptograma concreto ha sido aceptado o rechazado como inválido, puesto que el receptor no notifica la aceptación/denegación de los criptogramas. Como resultado, esto implica que el atacante debe enviar 2^{15} mensajes para conseguir hacer pasar por válido un único paquete de datos de detección y selección de canales.

En redes convencionales, 2^{15} puede parecer un número extremadamente bajo de paquetes; sin embargo, provee de un nivel de seguridad adecuado en CWSN. En estas redes, el atacante sólo puede inundar el canal con criptogramas falsos durante el periodo de detección y selección de canales, que suele tener una duración de unos pocos milisegundos en la mayoría de escenarios de redes cognitivas [9]. Además, el canal tiene probablemente una tasa de transferencia baja que permite transmitir unas pocas decenas de kilobits por segundo. Por ejemplo, asumiendo una cota superior de 1Mbps por canal, un periodo de detección y selección de 10ms, y un tamaño de paquete de sólo 10 bytes, el atacante sólo tendrá tiempo de enviar un máximo de 125 paquetes.

IV. Evaluación de costes y comparación con otras posibles soluciones

La propuesta presentada está diseñada para CWSN en las que los dispositivos están limitados en cuanto a energía, memoria y otras capacidades. Aunque la confidencialidad y la autenticación se pueden proporcionar por medio de criptografía simétrica tradicional, nuestra propuesta proporciona mejor rendimiento en cuanto a ahorro de energía. En esta sección, evaluamos los costes del mecanismo propuesto en términos de consumo de energía debido al incremento de datos transmitidos y de coste computacional, y lo comparamos con otras posibles soluciones que usan criptografía simétrica. En particular, hemos considerado una implementación ligera de AES, puesto que esta es la solución adoptada en redes de sensores típicas [10].

IV-A. Incremento en la transmisión de bits

El cifrado AES requiere una clave de 128 bits y, normalmente, se obtiene un fragmento del criptograma de 128

Tabla I
Número de bits transmitidos/recibidos y consumo de energía para AES

N	Tx bits	Rx bits	Energía total (μJ)
5	128	512	43,104
10	128	1152	84,544
20	128	2432	167,424

Tabla II
Número de bits transmitidos/recibidos y energía consumida para el método propuesto

N	l	Tx bits	Rx bits	Energía total (μJ)
5	16	32	128	10,776
5	32	48	192	16,164
5	64	80	320	26,94
10	16	32	288	21,136
10	32	48	432	31,704
10	64	80	720	52,84
20	16	32	608	41,856
20	32	48	912	62,784
20	64	80	1520	104,64

Tabla III
Costes de potencia y energía para la Dust Network LTP5901/LTP5902-IPM [11].

Campos	Valor
Corriente para Rx	5 mA
Corriente para Tx	6 mA
Corriente para la CPU	2.4 mA
Voltaje	3.6 V
Tasa de transferencia	250 Kbit/s
Tiempo para Rx y Tx 1 Byte	32 uS
Ciclos para Comparar	5 Ciclos/Byte
Frecuencia CPU (Activa)	7 MHz
Energía para Rx	0.576 uJ/Byte
Energía para Tx	0.691 uJ/Byte
Energía para comparar	24.68 nJ/Byte

Tabla IV
Coste del cifrado/descifrado AES y las funciones de hash

Algoritmo	Tamaño de salida	Ciclos	Consumo de energía (nJ)
AES	128	1032	5093.952
MAME	256	96	473.856
H-PRESENT	128	32	157.952
H-PRESENT	196	108	533.088

bits por cada bloque de entrada. Como consecuencia, la mínima cantidad de datos transmitidos que se requieren para transmitir de forma segura será igual al tamaño del bloque de salida de AES: 128 bits.

En nuestra propuesta, en cambio, la mínima cantidad de datos a transmitir dependerá del número de canales sobre los que esté informando un determinado nodo, el número de bits utilizados para codificar el estado de cada canal, y la longitud del código de autenticación. Como se explica en la sección III-B, una longitud de 16 bits es suficiente para proporcionar seguridad a la mayoría de aplicaciones en WSNs y, por tanto, hemos fijado este valor para este parámetro. Esto da lugar a una cantidad total de bits transmitidos de $Bits_{tx} = l+16$, donde l representa el número total de bits utilizados para codificar todos los posibles canales y el número de bits recibidos es $Bits_{rx} = (n-1)Bits_{tx}$

Durante cada periodo de detección y selección, cada nodo debe transmitir un paquete con información sobre la disponibilidad de los canales, pero también debe procesar los paquetes recibidos de sus vecinos. Las tablas I y II muestran el consumo de energía debido a la transmisión/recepción de información de detección y selección de canales para un sensor típico de una red 802.15.4 [11], mediante el uso de AES y el mecanismo propuesto respectivamente. Los valores se muestran en función del número de nodos vecinos N y, para el método propuesto, del número de bits l utilizados para codificar el estado del canal. El estándar 802.15.4 identifica 27 canales distribuidos a lo largo de diferentes bandas de frecuencia (1 canal para 868.3 MHz, 10 canales para 902-928 MHz y 16 canales para 2.4-2.4835GHz), con tasas de transferencia de 20, 40 y 250 Kbps respectivamente. Para este análisis, hemos asumido que los nodos de la red operan en el rango de los 2,4 GHz sobre 16 canales posibles, y los valores de consumo de energía se han extraído de las especificaciones mostradas en la tabla III.

Como puede verse, con el método propuesto el consumo de energía se reduce considerablemente hasta un 75 % con respecto a AES, a la vez que se mantiene un nivel de seguridad adecuado.

IV-B. Costes operacionales

En esta sección, proporcionamos una comparativa de la energía consumida debido a la implementación de las funciones criptográficas. En el mecanismo propuesto, un nodo debe computar N hashes y realizar N XOR para enviar la información de disponibilidad de los canales y procesar la información recibida de sus vecinos. Si se utiliza AES, el coste criptográfico total es igual al coste de 1 cifrado y $N-1$ descifrados. La tabla IV muestra el número de ciclos de CPU necesarios para cada bloque [12] y la memoria requerida para el cifrado/descifrado AES, así como también el número de ciclos de CPU necesarios para el cómputo de dos funciones de hash ligeras diseñadas específicamente para entornos restringidos (como es el caso de las CWSNs): MAME [13] y PRESENT [14]. El consumo de energía se ha calculado teniendo en cuenta las especificaciones mostradas en la tabla III.

Como puede verse, la energía consumida por las funciones de hash ligeras es claramente inferior a la consumida por AES. Cabe notar, sin embargo, que con el mecanismo propuesto, el consumo de energía tiene 3 componentes: el cómputo de las diferentes secuencias S_i^u con la función de hash antes de que se inicie el periodo de detección y selección de canales, la XOR de K_i^u con D_i^u que indica la disponibilidad de canales, y la XOR de las secuencias recibidas de los vecinos C_i^u con el S_i^u precomputado. Según la tabla III, cada operación XOR consume 24,68 nJ por byte, lo que significa que, en cada periodo de detección

y selección de canales, el consumo energético para cada nodo se incrementa ligeramente en función del número de vecinos y la longitud de la clave. Sin embargo, esto no representa un problema para el método propuesto, puesto que este coste es dos órdenes de magnitud inferior que la energía consumida durante la transmisión/recepción. Consideremos un escenario desfavorable formado por una red con 20 nodos y secuencias C_i^u de 80 bits: la energía consumida debido a las operaciones XOR sería de 5,923 μJ, mientras que la transmisión y recepción de la información de disponibilidad del canal supondría un consumo de 104,64 μJ.

V. Conclusiones

Las redes inalámbricas de sensores (WSN) están siendo ampliamente utilizadas para monitorizar condiciones físicas o ambientales como la temperatura, la presión, la presencia, etc.

Una de las aplicaciones más prometedoras de las WSN es el ámbito de la e-Salud, donde las redes de sensores se utilizan para monitorizar el estado de los pacientes con mejoras patentes en términos de calidad de la monitorización y reacción ante alertas médicas. Sin embargo, la transmisión de los datos de los pacientes se realiza por un medio inalámbrico que es especialmente sensible a denegaciones de servicio, ya sea por interferencias no premeditadas o por jamming intencionado; lo que afecta de manera muy significativa e inaceptable a la disponibilidad de dichos datos.

En este contexto, las CWSN aparecen como una solución para mejorar dicha disponibilidad, permitiendo que los datos puedan enviarse por diferentes canales de frecuencia, siempre buscando las mejores oportunidades. Sin embargo, un atacante puede perturbar el proceso de búsqueda y selección de canales impidiendo el funcionamiento cognitivo de la red. Por este motivo, dotar de seguridad a este proceso es también de vital importancia.

Existen diversas propuestas en el estado del arte que dotan de seguridad al proceso de búsqueda y selección de canales de frecuencia. A pesar de ello, ninguna es, hasta donde sabemos, adecuada para CWSN con nodos sensores de bajo perfil, como es el caso de las que potencialmente se usarían en el entorno de la eSalud.

En este artículo se ha presentado un método ligero específico para dotar de seguridad a los datos de detección y selección de canales en CWSN. El método propuesto ha sido descrito y analizado, y se ha probado que es más eficiente en términos de consumo de energía que otras soluciones tradicionales; reduce los costes de cifrado a menos de una operación de hash por paquete de detección y selección transmitido, y proporciona un nivel adecuado autenticación de paquetes con tan sólo 16 bits de overhead.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el Gobierno español a través de los proyectos TSI2007-65406-C03-03 “E-AEGIS”, TIN2011-27076-C03-02 “CO-PRIVACY”, CONSOLIDER INGENIO 2010 CSD2007-0004 “ARES”, TEC2011-22746 “TAMESIS”, TSI-020400-2011-55 ITEA2 “DiCoMa”, así como por la Generalitat de Catalunya con la concesión 2009 SGR-1362 a grupos de investigación consolidados.

Referencias

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, “Cooperative spectrum sensing in cognitive radio networks: A survey,” *Physical Communication*, pp. 40–62, 2011.

[3] K. Shenai and S. Mukhopadhyay, “Cognitive sensor networks,” in *Microelectronics, 2008. MIEL 2008. 26th International Conference on*. IEEE, 2008, pp. 315–320.

[4] O. Akan, O. Karli, and O. Ergul, “Cognitive radio sensor networks,” *Network, IEEE*, vol. 23, no. 4, pp. 34–40, 2009.

[5] G. Jakimoski and K. P. Subbalakshmi, “Towards secure spectrum decision,” in *IEEE International Conference on Communications*. Piscataway, NJ, USA: IEEE Press, 2009, pp. 2759–2763. [Online]. Available: http://portal.acm.org/citation.cfm?id=1817770.1817783

[6] H. Rifà-Pous and C. Garrigues, “A secure and anonymous cooperative sensing protocol for cognitive radio networks,” in *Proceedings of the 4th International Conference on Security of Information and Networks. Pags. 127-132*. The Association for Computing Machinery, 2005, pp. 127–132.

[7] R. E. Glasgow, “ehealth evaluation and dissemination research,” *American Journal of Preventive Medicine*, vol. 32, no. 5, Supplement, pp. 119–126, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0749379707000529

[8] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, and Y. Seurin, “Hash functions and rfid tags: Mind the gap,” in *Proceeding sof the 10th international workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES ’08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 283–299. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-85053-3_18

[9] C. Cordeiro, K. Challapali, D. Birru, and N. Sai Shankar, “Ieee 802.22: the first worldwide wireless standard based on cognitive radios,” in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*. IEEE, 2005, pp. 328–337.

[10] N. Sastry and D. Wagner, “Security considerations for ieee 802.15. 4 networks,” in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 32–42.

[11] Dust networks, *SmartMesh IP LTP5901/LTP5902-IPM products*, Jul. 2012. [Online]. Available: http://www.linear.com/product/LTP5901-IPR

[12] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. Robshaw, and Y. Seurin, “Hash functions and rfid tags: Mind the gap,” *Cryptographic Hardware and Embedded Systems–CHES 2008*, pp. 283–299, 2008.

[13] H. Yoshida, D. Watanabe, K. Okeya, J. Kitahara, H. Wu, Ö. Küçük, and B. Preneel, “Mame: A compression function with reduced hardware requirements,” *Cryptographic Hardware and Embedded Systems-CHES 2007*, pp. 148–165, 2007.

[14] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, “Present: An ultra-lightweight block cipher,” *Cryptographic Hardware and Embedded Systems-CHES 2007*, pp. 450–466, 2007.

Analysis and improvement of a game theoretic malicious node revocation process for vehicular networks

Fernando Pascual Blanco, Bernardo Alarcos Alcázar, Iván Marsá Maestre, Enrique de la Hoz de la Hoz.
Departamento de Automática
Universidad de Alcalá.
Edificio Politécnico. Campus Universitario. 28871 Alcalá de Henares.
fer.pasc@gmail.com, {bernardo.alarcos, ivan.marsa, enrique.delahoz}@uah.es

Vehicular ad-hoc network (VANET) is an emerging technology that will contribute with great benefits to society. A trust relationship is needed and malicious nodes (vehicles) suppose an important risk for the safety applications based on VANET infrastructure. Therefore, a reliable revocation procedure is a key issue in vehicular networks. This paper will focus the study of node revocation processes.

There have been significant recent works on node revocation in ad-hoc networks. In particular, game theory approaches seem to be specially suited for ephemeral environments like VANETs. However, these approaches have some performance limitations which difficult their implantation in real environments. This paper proposes a set of improvement mechanisms, which effectively reduce the process times for game-theoretic malicious node revocation.

Keywords- vehicular network, ad-hoc network, VANET, security, revocation, game theory

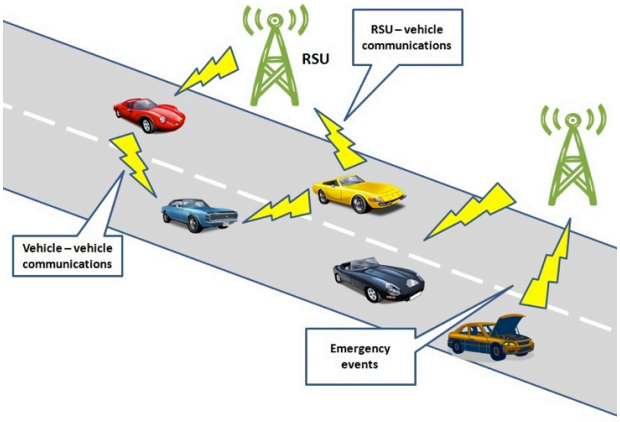


Fig. 1 Typical VANET scenario

I. INTRODUCTION

Vehicular ad-hoc networks (VANET) [1] are ad-hoc networks [2] wherein mobile nodes are vehicles provided with an OBU (On-Board Unit) to send and receive messages. VANET networks can be dynamically created anywhere with the presence of at least two vehicles. As shown in Fig. 1, VANET can have RSUs (Road-Side Unit), which are fixed stations near the roads able to provide connection between vehicles and fixed infrastructure network (e.g. to the Internet or to a government private network). Nevertheless, there may be areas without RSU coverage (e.g. remote roads).

VANET communications let governmental organizations to offer value-added services like safer roads, traffic management or driving aids. Being an ephemeral infrastructure these offering becomes a challenge. For example, node authentication in this context becomes much harder because we cannot rely on some of the assumptions used by classical schemes because of the ephemeral nature of VANETs. The detection of malicious nodes in VANETs is also a more difficult task because a node can be part of a different VANET at the time. This paper proposes a solution to deal with the malicious node revocation issues on VANETs.

In order to focus the problem that this work deals with, we introduce details about the security architecture in VANETs. Among other messages, VANET nodes exchange periodically beacon [3] messages with their neighbour nodes, containing position and time marks. It is mandatory to maintain a trust relationship under this message exchange because of the critical value of the exchanged information. If a malicious node intercepts and modifies or broadcasts fake information in the VANET network, vehicles will figure out unreal geographical situations of other vehicles, which could lead to accidents. Many authors [4, 5] propose the utilization of PKI and asymmetric cryptography to protect the information exchange in VANETs. VANET nodes typically have several key pairs (private keys and public keys) available and they can switch the key pair in use to avoid undesired third-party tracking. This way, nodes can maintain network anonymity [6, 7]. Under the PKI approach, the CA (Certification Authority) needs to maintain and distribute an updated CRL (Certificate Revocation List) [4]. The CRLs are made up of revoked certificates identified by a fraud service use. When a node uses a public key to verify the digital signature of a message, it must check whether that public key is contained in the CRL, and messages signed with revoked private keys should be ignored. VANET nodes will have sporadic connections to fixed infrastructure networks (only when driving near a RSU) and consequently a sporadic access to the updated CRL, so nodes will typically have an out of date CRL. Therefore, VANET network security cannot relay only on this approach and it makes necessary a local identification and revocation of malicious nodes method adapted to VANET networks paradigm.

There are different proposals [9-18] to enable revocation mechanisms in ad-hoc networks. To identify and revoke a malicious node in an efficient way, a VANET node should

consider both its own opinion and its neighbours' opinion. The revocation mechanism should also be strong enough to resist confabulation attacks, where a group of malicious nodes try to force the revocation of the certificate of a non-malicious node (assuming a scenario with a majority of well-behaved nodes). Some authors [9, 10] propose the utilization game theory based proposals [11-15], which seem to outperform classical approaches. Game theory models situations where actors must choose specific actions (strategies) with mutual, and potentially conflictive, consequences. Game theory requires actors to be rational, and that means to maximize benefits or, alternatively, minimize costs. Another important definition is the complete information game concept, which means a game where players have a full knowledge of all game aspects: who are the other players, their strategies, the profit obtained by each node… To predict the result of the game, Nash equilibrium (NE) concept [16] can be applied. A NE means a common strategy, composed by every individual strategy of every player in which a player cannot increase his benefit by only modifying his own strategy. Game theoretic solutions will be contained between the existing possible NEs.

In this paper a new malicious node revocation process in VANET networks based on [9] is proposed. We present three main contributions among others. First, we build a non-degenerative system, letting nodes to be out of RSUs range for a long time and participating in revocation processes. Second, we improve the system performance by reducing the number of analysed strategies, which results in a lower processing time and consequently in a faster revocation process. Third, we give to the nodes the possibility to participate in the process against the revocation of the accused node, supporting that way the accused node if others think it is a well-behaved one.

The paper is organized as follows. After discussing the related work in Section II, we briefly describe the approach by Bilogrevic et al. [9] in Section III. In Section IV we propose the new revocation process explaining its benefits. In Section V we evaluate the performance of the proposed mechanism. The last section summarizes our conclusions.

II. Related work

The main problem to revoke malicious nodes is to define a mechanism for trust establishment between neighbour nodes. Different strategies have been proposed in the state of art.

Trust establishment in VANETs is still an open and challenging field. Trust in wired networks is commonly established using indirect trust mechanisms, including trusted certification agencies and authentication servers. In VANETs, the absence of fixed trust infrastructure, limited resources, ephemeral connectivity, and the shared nature of the wireless medium makes it much harder to use that scheme and additional schemes have to be considered. Pirzada and McDonald [11] propose to include a trust agent in the nodes to collect network information passively, which will be used to build a distributed trust model where trust in nodes is classified into levels. Nevertheless, this model requires a neighbour's behaviour learning process not feasible in huge ephemeral ad-hoc networks like VANETs.

Moore et al. [12] propose a voting scheme for node revocation. Under this scheme, good nodes reelect each other as good nodes once in each time period. When a node joins the network, and periodically thereafter, must demonstrate that it is still authorized to be on the network. Revocation becomes preventing a bad node from renewing its membership. This model can be implemented either by a classical voting scheme or by a lightweight process based on the periodical distribution of trust neighbours lists by nodes. The authors also introduce a mechanism to allow a single node to force the revocation of another node. Should a node believe another node is misbehaving, it can commit suicide to force the revocation of the malicious node. Suicide of the accusing is required in avoid false accusations, making it costly. From that moment on, both nodes (accusing and accused) are considered invalid in the network. Although the self-sacrifice concept will be reused in other mechanisms explained ahead, none of these proposed mechanisms are suitable for VANETs because of the need to maintain huge lists of neighbours updated and the need of knowing all of them.

Raya et al. [14] introduce the LEAVE protocol to identify and revoke malicious nodes in an environment without CA connectivity. Vehicles that detect a malicious node will broadcast signed warning messages. For a given vehicle, if the number of warnings against it exceed a defined threshold, warning messages are transformed into disregard messages, that instruct all the neighbour of the malicious node to ignore it. Taking into account other nodes opinion is quite interesting but, on the other hand, confabulation attacks could arise quite easily under this protocol. Another way of evaluating other node´s reputation is needed because a node cannot trust in the disregard messages from an unknown node, which could be a malicious one.

Chinni et al. [13] propose a distributed model where trust relationships evolve through iterations. Trust in a node does not depend solely in its potential maliciousness, but also in terms of the quality of service it provides (availability, forwarded messages rate…). Although the quality of service of a node is not interesting when we talk about revocation processes, when a node has no or little interaction with other node, it has no opinion about it and the trust in that node is determined only by recommendations from other nodes. Trust relationships require node interaction and that will not be the typical scenario in a huge network with ephemeral iterations like VANETs are. This mechanism is not scalable enough for VANETs.

Samara [15] states that the CRL mechanism needs a frequent warning broadcasting due to the adversary discovery process, which produces a heavy channel load from all the vehicles in the road. A mechanism is proposed to replace the CRL: the Local Revocation List (LRL), a list with the faulty vehicles present in a particular road, and when a vehicle enters the road is provided by the RSU with the road´s LRL. When a faulty vehicle is identified is added to the LRL and the LRL is broadcasted every 0,3 seconds. When a faulty vehicle leaves the road it is removed from the LRL. The problem here is that vehicles only have one certificate, and therefore others can track them.

Raya et al. [10] consider game theory as an efficient tool to improve local revocation processes in ephemeral networks and defined a game-theoretic model to analyse different local revocation strategies. The authors suggest a game where nodes participate sequentially and they are able to see each other strategy. There are three strategies: 1) abstention, which means not to contribute in the revocation (hoping others to do so), 2) vote, which means to contribute to the revocation with a vote (supposing that the revocation is

successful with n votes, a threshold is statically defined) and finally 3) self-sacrifice. Nodes have to consider two types of costs: the attack-induced cost (the cost of not revoking the malicious node and assume the potential attack of that node within the network) and the selected strategy cost (every strategy has an associated cost trying to avoid the abuse of the revocation by malicious nodes, also known as confabulation attack). These costs are quantified in public certificates because periodical ciphering key changes are required in order to avoid undesired third-party tracking (public certificates are a limited network resource). Finally, to revoke a malicious node, the number of votes must be over a given threshold or a node must perform sacrifice. They found the problem that having fixed costs, and being a sequential revocation process, the only objective of the players is to revoke the attacker, but they do not care in which stage of the revocation process. So, the result was that the decision of the revocation was left to the last players, either by voting or by self-sacrifice. Nevertheless, they solved that by proposing a new scheme having variable costs, increasing the attack-induced in each stage of the revocation process where the attacker is not revoked. Thus, players were more concerned about quickly revoke the malicious node because its cost was increased with time.

Finally, Bilogrevic et al. [9] described the Optimal Revocations in Ephemeral Networks (OREN) revocation scheme. They proposed a very innovative approach based on game theory for incentivizing nodes to participate in the revocation processes. The revocation procedure will take into account the reputation of nodes, which is dynamically adapted according to their behaviour. The main differences with [10] are that the game is concurrent in the time and each node will be provided with a secure tamper resistant hardware inside itself, where OREN is executed and store a counter representing its reputation and avoiding its malicious manipulation. Only the CA can update the information stored in the secure hardware module. For a node, its selected strategy depends on the OREN algorithm and on its trust counter. Provided that every node knows every trust counter, nodes do not need to broadcast their selected strategies, avoiding unnecessary communication and performing the revocation process faster. There is a distributed revocation process that computes the revocation strategy that minimizes the global cost. As long as it is a distributed procedure, there is no need of delivery messages at the end of the revocation process. All that they need to make a decision about one node revocation, it is the reputation of the rest of participant nodes.

Nevertheless, we have found some limitations in [9]. Each node is equipped with a numerical counter that represents its reputation and they need to own certificates to be able to communicate within the VANET. This counter can only be modified either by the CA or using the secure hardware device embedded within the node. The most reliable a node is, the greatest the weight that its power to revoke nodes will be. At the same time the counter will represent the power to revoke potentially malicious nodes. For the nodes to increase their counters and to acquire new certificates, they have to connect to the CA. Because of that, nodes out of RSUs coverage for a long time, and therefore without communication with the CA, will not be able to increase their counter or to obtain new certificates. As a result of that, the proposed procedure could result into a time-degenerative system, because. Those nodes will not be able to participate in any revocation process (or have little influence) as long as they are not able to communicate with the CA. Another limitation of the proposed procedure is that, when performing the revocation process, the only option for the participating nodes is to vote against the accused node; they cannot support the accused node even if they think it is a non-malicious node. It would be helpful to enable the possibility of supporting the accused node, as a way to circumvent confabulation attacks, where malicious nodes are trying to revoke a well-behaved one. Also, this would add fairness to the revocation processes.

III. Game theoretic certificate revocation in VANETs

A. Scenario

Based in [9], we assume that each node has a reserve containing all valid certificates, a counter, which measures the number of valid certificates within the reserve that can be used for revocations, and a tamper-resistant device, where the revocation protocols are executed. This device will be employed to sign sent *beacon* messages within the VANET. We will consider devices powerful enough to perform public key cryptography. The counter and the pool of certificates can be modified by the secure hardware module or by the CA, but not by the device itself. The counter value intends to reflect the trust level that can be granted to the device, its reputation: a high reputation will be reflected in a high counter value and a low reputation will be reflected with a low counter value (revocation protocols stored within the secure hardware will update the counter accordingly). On the other hand, the counter should move within a range, to avoid very high trust levels that will let a device to act with maliciousness during a period of time without reaching a low counter value. By definition, the counter value cannot be bigger than the credential pool size.

Nodes can thus obtain new valid certificates by either buying them from the CA or by revoking malicious nodes, as an incentive for its participation in the revocation process. While when purchasing new credentials, the counter remains unchanged, if the node obtains new certificate by participating in a revocation process, the counter can be increased. At least during the deployment phase, connections between vehicles and RSUs will be sporadic, and therefore the connections between the vehicles and the CA will be sporadic too. These sporadic communications will be employed by the CA and vehicles to deal with the credentials issues. Vehicles will send revocation processes reports to the CA to verify them and share out rewards properly. Note that the CA will receive several reports from nodes (vehicles) for each revocation process and they can be taken in to account with the level of trust of the sending node. These reports will contain a unique identification and the actions taken by each participating node in the revocation process, and these actions will define the level of trust that can be granted to them.

To sum up, vehicles participating in revocation processes and revoking malicious nodes will renew its public/private keys (certificates or credentials) and will tend to have a bigger counter (always when verifying towards the CA) because this behaviour is considered good. On the other hand, vehicles not participating in revocation processes or participating with a bad behaviour (trying to revoke a well-behaved vehicle and failing) will not renew its public/private keys or will tend to have a smaller counter respectively.

An important point to make that revocation process viable is that it is supposed that the number of well-behaved nodes is greater than the number of malicious nodes. That supposition is very common in game theoretic procedures and it will be the typical situation and a key point of the hypothesis.

B. OREN: Optimal Revocations in Ephemeral Networks

This section will briefly explain OREN, the process proposed by Bilogrevic et al. in [9] to define the revocation of malicious nodes in the VANET.

First of all, some basic definitions will be introduced to understand how the revocation process works. It is important to highlight that if a node decides to participate in the revocation process, it means that she wants the revocation of the accused node because the revocation procedure does not include any way to support the node against the accusation. Once a node has decided to participate in the revocation process, it has to choose a ***strategy***, either to *abstain*, to *vote* or to *self-sacrifice*. The accused node will be revoked if the sum of the counters of players that decided to vote is greater than the counter of the accused node, or if one of the accusing nodes sacrifices itself. The ***cost*** is defined as the damage quantified in number of certificates obtained by a node. Under this settings, we define are several types of costs. First, the *attack-induced cost* quantifies the damage produced by the accused node if it is not revoked. Second, the *strategy cost* is related with the attitude of the node towards the revocation procedure. The vote has a fixed cost associated, while the sacrifice has variable cost associated and the abstention has no cost. Finally, the *retaliation attack cost* quantifies the potential risk of revenge (e.g. by a confabulation attack) from other malicious nodes when revoking the accused node: the more malicious nodes are present in a given area, the more costly it becomes for benign nodes to revoke one of them assuming that, potentially, they will be targeted by a retaliation attack. The ***benefit*** is defined as the reward quantified in number of certificates obtained by a node when taking a determined strategy and revoking the accused node. The main point of that mechanism is the incentive provided to the participant nodes. There is a fixed benefit for contributing to the revocation with a vote and a different one for contributing with a sacrifice. The ***payoff*** is the difference between benefits and costs expressed in public certificates, and finally will be added or taken away from the node counter. As ***game solutions***, only *Nash Equilibriums* (NE´s) where the malicious node is revoked will be selected. A NE is a set of strategies (one per participant node) where no node has any incentive to change unilaterally its own strategy to obtain a benefit.

Every node will participate in a single revocation process at the same time and the decision about to participate or not in a revocation process will be based on an Intrusion Detection System (IDS) [17] placed in every node. The revocation process starts when a node (initiator) detects a malicious node and decides to accuse it by broadcasting a message containing the following information: the identity of the accused node, its own signed counter value, the attack-induced cost in case the malicious node is not revoked and the estimated number of malicious nodes in the communication range. That estimation is given in order to let participating nodes to calculate the risk of be targeted by a retaliation attack from other malicious nodes. When a node receives this message and both nodes, initiator and accused, are in its communication range, it must decide, by using the report from its IDS, whether to revoke the accused node or not. Once decided, only nodes that want to revoke the accused node and the accused node itself must reply to the initiator node with its signed counter value. Therefore, at this point, every node has all the information to start the revocation process (the network is capable enough to deliver every participating node the information transmitted by the initiator node and the counters of the participating nodes) and there is no need to transmit any more information over the air (the process can be performed off-line). The off-line revocation protocol works as follows:

1. Every participant node must process every possible NE and must discard every NE that does not revoke the accused node and every NE that does not fit with the most beneficial response for a node.
2. If more than one NE exists the optimal one will be selected. The criteria will be to maximize the utilitarian function (which means to maximize the sum of every node´s payoff) and if there is only one NE that NE will be selected. If not, the criteria will be to maximize the egalitarian function (which means to maximize the minimum node´s payoff).
3. If there are several optimal NE´s in this step, one of them will be randomly selected and broadcast to the participant nodes by the initiator node.

Once executed, every node will be conscious of every node´s strategy.

C. Objections

Although [9] offers a lot of advantages when dealing with malicious nodes, several objections have been found. First of all, in order to limit the abuse of revocations to obtain more and more certificates, the sum of costs is always bigger than the benefits of selecting vote or sacrifice strategy so the payoff is negative, but always bigger than the attack-induced cost (the cost of not revoking the malicious node and assume the potential attack of that node within the network). That means that while to revoke a malicious node is more interesting that to look the other way, a node will only have the incentive to contribute to the revocation when necessary. This way, node´s counters will be always equal or lower, but will never grow by itself. Nevertheless, when contacting with the CA and send the revocation reports, the node will obtain the reward: more certificates and a bigger counter. But, what if contacting with the CA takes more time than expected? This mechanism could cause problems when nodes are not able to reach the CA for a long time, for instance during the RSUs deployment phase or in geographically remote zones.

On the other hand, the retaliation attack cost, which quantifies the risk of revenge from other malicious nodes during the revocation process, is fixed, regardless of the number of participant nodes. However, this cost should be higher if there are a small number of voters because retaliation could be focused in a small group of nodes, and they will have more probability to be targeted by the retaliation attack. Nevertheless, if there are a lot of voters, the retaliation risk will be lower because the revenge will target a larger number of potential victims, and they will have a lower probability to be targeted.

Finally, only are involved in the revocation process the nodes that receive alert about the accused node from their

own IDS. Thus, the opinions of nodes that do not want to revoke the accused node because they think that it is a well-behaved one are not taken into account. For example, if a group of malicious nodes are trying to revoke a well-behaved one, using [9] only malicious nodes will participate in the revocation process and will revoke the well-behaved node. The evaluation of those opinions in the revocation process could be quite interesting because it will add fairness to the revocation process and could be very useful when dealing against confabulation attacks.

IV. PROPOSED MODIFICATIONS

After the study of [9], several aspects have been found that could improve the performance of the proposed revocation process. In addition, some modifications will be proposed with the aim of improve the security of the process against confabulation attacks. Performing this type of attacks, malicious nodes could try to revoke well-behaved ones by using the proposed mechanism.

A. Vote cost modification

In the revocation process proposed in the last section, the cost assumed by a vehicle when voting to revoke a malicious node was constant. This way, the cost was the same when the vehicle had a good reputation and when the vehicle had a bad reputation. We think that a modification in the cost per vote introducing the vehicle´s counter into the cost function could provide benefits in the vehicles behaviour. This modification could be oriented as follows.

We propose a cost per vote function to model a situation in which vehicles with a lower reputation has a lower cost per vote. That option could be taken to the extreme and nodes with a very low counter could obtain a positive payoff per vote (always assuming that the revocation process was successful and the malicious node was revoked), while nodes with higher counter values remains in the former negative pay-off per vote because its benefit keeps lower than its cost. This way, as the proposed protocol try to maximize benefits, those nodes with lower counter (bad reputation) would be forced to vote if they decide to participate in the revocation process because their cost per vote is lower or even could be a benefit.

B. Retaliation attack cost modification

In [9], the proposed retaliation attack cost is defined by *f(M/N)* as the risk of retaliation by the possible M malicious vehicles in a VANET composed by N vehicles. On one hand, if a vehicle uses the sacrifice strategy, it is considered that all the retaliation power is focused on him. On the other hand, if vote strategy is used, it is considered that the retaliation risk is $z{:}f(M/N)$, being z a constant factor such as $0<z<<1$, and this is independent of the number of voters.

We think that is more realistic to consider that the retaliation risk (when selecting the vote strategy) depends on the numbers of voters: for example, if one node is the responsible of the revocation of a malicious node, other malicious nodes will redirect their retaliation against it, but if there are a hundred of nodes responsible of the revocation, the retaliation attack could be distributed or random. So, we propose that the retaliation attack risk should be equal to the total retaliation power divided by the number of voters, instead of multiplying it by a constant and very low factor z. Therefore, we propose a retaliation by vote risk of $f(M/N)/n_v$, being n_v the number of votes in the revocation process.

C. Social benefit modification

In [9], the social benefit proposed functions are the utilitarian and the egalitarian. By maximizing the social benefit the best group result is obtained. On one hand, by maximizing the utilitarian function the strategy selected by each vehicle is the one that maximizes the sum of the individual benefit of every vehicle participating in the revocation process. On the other hand, by maximizing the egalitarian function the strategy selected by each vehicle is the one that maximizes the benefit of the vehicle less beneficiated in the revocation process (trying to help the poorest vehicles).

It is very interesting to find a function to maximize the social benefit in the most uniquely possible way, trying to avoid to find several strategies providing the same maximum social benefit, because in the proposed revocation process in [9] that situation requires to broadcast another message in the VANET to randomly select the strategy to be followed by every vehicle. In this section, in order to find a function which maximize the social benefit in the most uniquely possible way, two alternatives will be proposed:

a) Egalitarian social benefit function modification: A modification in the egalitarian social benefit function is proposed to choose a strategy to maximize the minimum accumulated counter value after the revocation of a vehicle participating in the present revocation process.
b) Nash product social benefit function: A new social benefit function is introduced, *the Nash product*. This way, the function to maximize will be the product of the obtained benefit of every vehicle participating:

$$\omega(s) = \prod_{i=0}^{n} u_i(s) \tag{1}$$

In Ec. 1 $\omega(s)$ is the social benefit function, u_i is the benefit for the vehicle I, n is the total number of participating vehicles and s is the selected strategy.

D. Game rules change

In [9], when a vehicle (initiator) is alarmed because of the presence of a malicious vehicle by its own IDS, it broadcasts a message accusing it and proposing a revocation game against that accused vehicle. The message includes its own counter value, the identity of the accused vehicle, the induced attack cost and the estimated number of the existing malicious vehicles. Vehicles that want to revoke the accused vehicle and the accused node itself answer to this message with their signed counter value.

Meanwhile, no action is allowed to vehicles that do not want to revoke the accused vehicle because they think that it is not a malicious one. Not taking into account that opinion could reflect an unreal scenario and could help the arising of confabulation attacks. Imagine the situation where several vehicles with high counter value think that a vehicle should not be revoked, and it is being accused by a malicious node: that node may be revoked. Even if there are more malicious nodes associated with the accusation, there is the situation

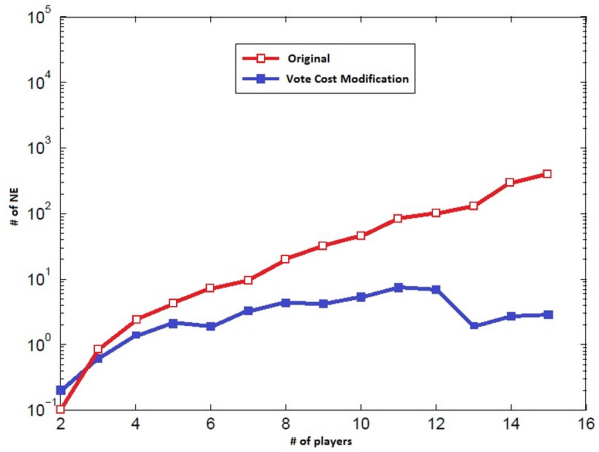


Fig. 2 Performance improvement

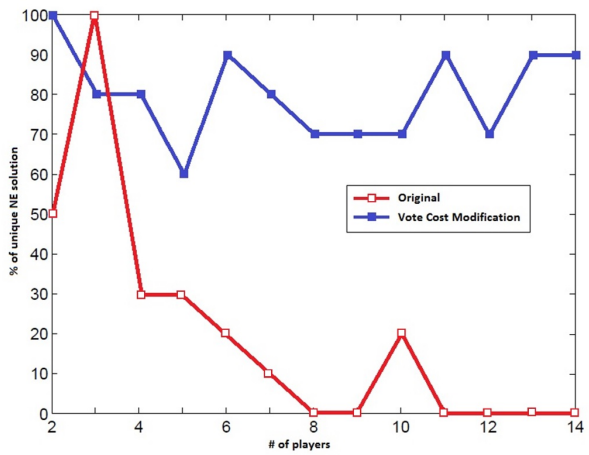


Fig. 3 Unique NE solution improvement

where only malicious nodes are participating in the revocation process to revoke a well-behaved one.

Giving vehicles the option to say no to the revocation, the VANET is protected against this kind of attacks.

The revocation process could be modified as follows:

1. There is a revocation *initiator* node that broadcasts a request for revocation message including the following information: the accused node identity, its own signed counter value, the attack induced cost and the estimated number of malicious nodes.
2. Every participant node in the accused and initiator´s range must respond to the request for revocation message with a broadcast message. This response message contains its own-signed counter value and the desired result for the revocation process (whether to revoke or not the accused node). Every participant node will typically consult its IDS before making this decision, and will have the choice to support the accused node if decided.
3. Modified off-line revocation process: the accused node will be revoked if the sum of the counters of players that want to revoke the accused node is greater than the sum of the counters of players that do not want to revoke the accused node (and here will be typically included the accused node's counter).

Sacrifice strategy will not be considered because revocation would be reached very easily, and that could be very dangerous in confabulation environments.

With this modification we intend to give the possibility to vote against a revocation proposal, so that in the cases where there is disagreement about the malicious nature of a node more votes will be needed to revoke it, thus protecting the network against confabulation attacks. On the other hand, since more votes are needed to revoke nodes, there will be a reduction in the number of possible NE, leading to lower processing power requirements (that effect will be reflected in the next section).

V. Performance Evaluation

To validate the modifications proposed in the last section, an evaluation of the performance obtained is needed. For this purpose the environment has been created and evaluated using Matlab. Every modification result will be compared with the original algorithm raising the benefits obtained.

We consider an ephemeral network with short-duration (1–10 s), short-range (10–100 m) contacts, composed of vehicles with permanent communication needs because vehicles must broadcast signed *beacon* messages to neighbour vehicles. Neighbour vehicles verify the signature of the broadcast messages. The public/private key pair used to authenticate the broadcast messages should be changed frequently to maintain privacy against tracking attacks [6, 7].

The results presented in the present section have been achieved running 10 iterations for each number of players between 2 and 15 and the confidence interval is 95%.

A. Vote cost modification

This modification improves the performance, because the number of possible strategies to analyse has decreased (low-counter nodes are forced to vote if they want to revoke the accused node). Comparing the original proposal [9] with the vote cost modification, for 15 players, the number of strategies to analyse has been decreased from 350 NEs to no more than 10 NEs. That means that with the same hardware, processing time is reduced by 97%. The Fig. 2 reflects the number of NEs to analyse per number of players.

On the other hand, the probability of obtaining a unique NE solution when performing the offline revocation protocol proposed in [9] has increased, so in most cases the broadcast of the selected strategy as last step will not be necessary. This improvement will be reflected as an important power saving source, because a broadcast message will be potentially avoided as the last step of every revocation. The Fig. 3 depicts the percentage of unique NE solution per number of players when the utilitarian social benefit function is used and the accused node has a counter value of 14. It is compared the original proposal versus the vote cost modification. As it is shown, in about 80% of cases the solution is unique.

In addition to that, vote cost modification has a benefit when considering counter evolution over the time. That effect is presented later, in the fifth point of this section.

B. Retaliation attack cost modification

This modification presented in section IV.2, under our point of view, is a better approximation to a real scenario because the retaliation attack risk has a better parameterization. The retaliation attack risk will be distributed among the targets, so the more nodes to be targeted by the retaliation attack the less probability of

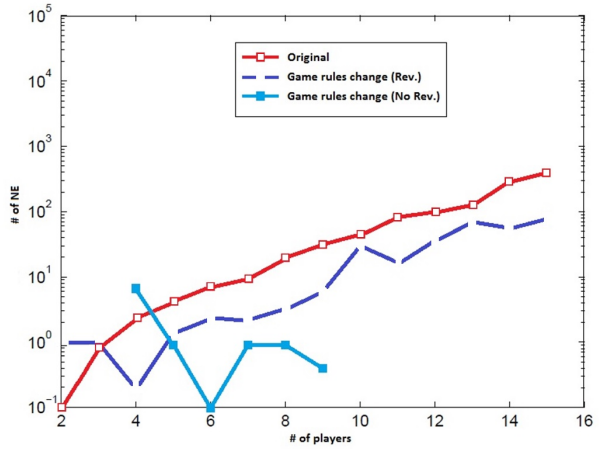


Fig. 4 Game rules change performance improvement

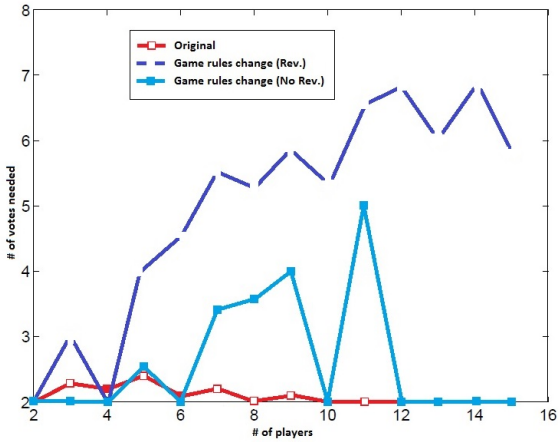


Fig. 5 Votes needed for revocation

receiving the damage. So, taking into account the number of participating nodes in the revocation process we have improved the definition of the retaliation attack cost. Nevertheless, it has not relevant performance implications.

C. *Social benefit modification*

Remember that it was interesting to find a function to maximize the social benefit in the most uniquely possible way, to avoid the broadcast messages proposed in [9], when the solution was not unique. Alternative social benefit functions proposed in section IV.3 have been implemented and compared with the original ones. Nevertheless we have not found any relevant difference, so we can conclude that these alternative functions do not reduce significantly the number of cases with more than one solution.

D. *Game rules change*

When introducing the modifications in the game rules presented in section IV.4 (we have simulated a 70% of players voting for the revocation and a 30% against it) we have observed improvement in the performance because the number of NE strategies to analyze has been reduced, so in Fig. 4 we can observe that for 15 players, the number of NEs has been reduced from 350 to around 80 (77 %). That means that with the same hardware, processing time is almost reduced in the same percentage.

Note that in Fig. 4 and Fig. 5 it is also represented the cases where the nodes against the revocation win the voting procedure (No Rev.), while in the original proposal nodes against the revocation did not participate in the process.

In addition to that, to reach a successful revocation a major number of votes are needed. That makes sense because the possibility of vote against the revocation has been introduced, and that protect nodes against confabulation attacks. In Fig. 5 is reflected the mean number of votes needed for revocation per number of players.

E. *Modifications working together*

It has been stated that vote cost and game rules change modifications have direct effects on the system performance. Working together, that modifications, comparing the original proposal [9], for 15 players, the number of strategies to analyse has decreased from 350 NEs to around 35, this is ten times less strategies to analyse. Regarding the votes needed for revocation and the probability of obtaining a unique NE solution, the results are more or less similar to the ones obtained on Fig. 5 and Fig. 3 respectively, they improve the original proposal.

F. *Temporal analysis*

One of the premises of [9] is that the best benefit must be negative (but less negative than not revoking the malicious node because, if not, nodes could decide to assume the damage not revoking the malicious node) in order to prevent the system from the node´s abuse. If the benefit were positive, the most interesting strategy would be always revoking other nodes, even the good ones. The produced effect is a negative evolution in counter values, as shown in Fig. 6, where the evolution of 10 counter values is represented with a revocation process per iteration.

It can be observed that in the highest counter´s nodes are first decreased (because fewer votes are needed to revoke malicious nodes). In addition to that, after 180 iterations the 10 counters fall dramatically, forcing nodes to contact with the CA before that in order to increase their counters to revoke future malicious nodes. This is a time-degenerative model in case of coverage shortage with a low RSU density.

Nevertheless, with the proposed vote cost modification (section IV.1) the model is not degenerative over the time anymore, because nodes with low counters are forced to vote or sacrifice (if necessary) if they decide to participate in the revocation process. That can be seen as if having a low counter they are willing to revoke a malicious node, they need to be sure enough because if not, their reliability will be dramatically damaged. Otherwise, if they have a low counter and they are willing to increase it to be more reliable, they can do it by participating in revocation processes with a good behaviour. This modification provides a positive pay-off to those nodes if their behaviour is good enough, and now it is not necessary to contact with the CA to increase the node´s counters to be able of revoke future malicious nodes. Nevertheless, although this would be useful for low coverage areas, nodes should contact as soon as possible with the CA in order to update the CRL.

An example of counters evolution with the proposed change is reflected in Fig. 7. It is shown that counters of nodes with low value evolve towards 5. In that case the value 5 has been selected as the threshold to define a counter with a low value, and those nodes are forced to vote.

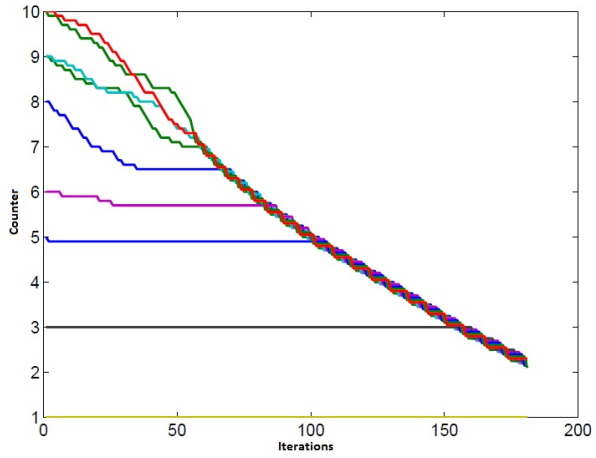


Fig. 6 Counter´s negative evolution in original proposal

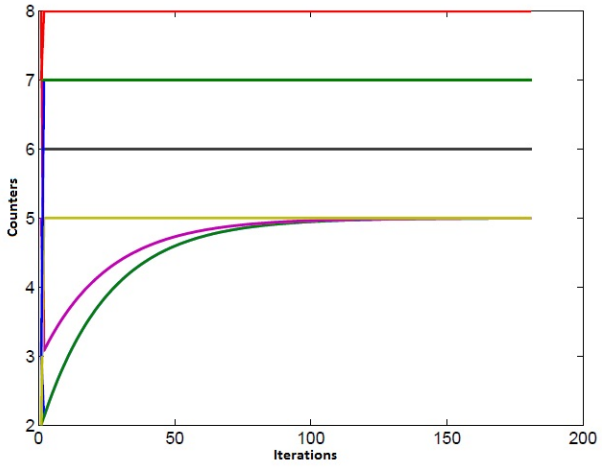


Fig. 7 Counters evolution with vote cost modification

VI. Conclusion

A reliable method to revoke malicious nodes in VANETs is needed, and we believe that [9] and game theory are a very good approach to solve the problem because analysing every possible strategy maximizes the pay-off obtained by the participating nodes. Nevertheless, we have found several problems and we have proposed modifications to [9] to solve the mentioned issues.

Vote cost modification involves a significant change over the original procedure, because introducing a variable cost for voting in function of the counter value means that vehicles with a low counter are forced to vote if they decide to participate in the revocation process, and that results in fewer strategies to analyse, with the consequent resource savings (processing, battery and time). In addition, with variable cost for voting it is more likely to obtain a unique optimal strategy, avoiding broadcasting the selected strategy in case of several optimal strategies. Finally, vote cost modification turns the model conservative over the time because nodes do not need to contact with the CA in order to increase its counter (but they do need to update their CRL).

Retaliation attack cost modification introduces a conceptual improvement over the original procedure bringing the model nearer to a real case scenario. That has been possible because we believe that the retaliation attack risk will be distributed among the targets, so the more nodes to be targeted by the retaliation attack the less probability of receiving the damage. So, we have improved the definition of the retaliation attack cost taking into account the number of participating nodes in the revocation process.

Game rules change modification introduces the possibility of voting against the revocation of the accused node and also suppresses the sacrifice strategy. Both modifications protect the method in environments with a high percentage of malicious nodes because we introduce tools to defend the procedure against confabulation attacks. This modification also provides a performance improvement.

As possible future work, we observe the necessity to simulate the proposed procedure into a test environment reflecting real conditions regarding vehicle distribution or the random presence of malicious nodes. This would be also an opportunity to observe new situations and scenarios not considered.

Referencias

[1] Stephan Olariu and Michele Aylene Clark Weigle, *"Vehicular Networks: From Theory to Practice"*, CRC Press, 2009

[2] Charles E. Perkins, *"Ad Hoc Networking"*, Addison-Wesley Professional, 2008.

[3] Yousefi Saleh, Fathy Mahmood and Benslimane Adberrahim, *"Performance of beacon safety message dissemination in Vehicular Ad hoc NETworks (VANETs)"*, Journal of Zhejiang University - Science A, vol. 8, 2007, pp. 1990-2004

[4] IETF RFC 5280, *"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*, IETF, May 2008

[5] Mohsen Toorani and Ali Asghar Beheshti Shirazi, *"LPKI - a Lightweight Public Key Infrastructure for the mobile environments"*, Proceedings of the 11th IEEE International Conference on Communication Systems, 2008, pp. 162-166

[6] Marco Gruteser and Dirk Grunwald, *"Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis"*, Mobile Networks and Applications, vol. 10 (3), 2005, pp. 315-325

[7] Alastair R. Beresford and Frank Stajano, *"Location privacy in pervasive computing"*, IEEE Pervasive Computing, vol. 2, 2003, pp. 46-55

[8] Drew Fudenberg and Jean Tirole, *"Game Theory"*, MIT Press, 1993

[9] Igor Bilogrevic, Mohammad Hossein Manshaei, Maxim Raya and Jean-Pierre Hubaux, *"OREN: Optimal revocations in ephemeral networks"*, Computer Networks, vol. 55, 2011, pp. 1168-1180

[10] Maxim Raya, Mohammad Hossein Manshaei, Márk Félegyházi and Jean-Pierre Hubaux, *"Revocation games in ephemeral networks"*, Proceedings of the 15th ACM conference on Computer and communications security, 2008

[11] Asad Amir Pirzada, Chris McDonald, *"Establishing trust in pure adhoc networks"*, Proceedings of the 27th Australasian conference on Computer science, 2004

[12] Tyler Moore, Jolyon Clulow, Ross Anderson and Shishir Nagaraja, *"New strategies for revocation in ad-hoc networks"*, Proceedings of the 4th European conference on Security and privacy in Ad-Hoc and sensor networks, 2007

[13] Sudha Chinni, Johnson Thomas, Gheorghita Ghinea and Zhengming Shen, *"Trust model for certificate revocation in ad-hoc networks"*, Journal Ad-Hoc Networks, vol. 6 (3), 2008, pp. 441-457

[14] Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels and Jean-Pierre Hubaux, *"Eviction of misbehaving and faulty nodes in vehicular networks"*, IEEE Journal on Selected Areas in Communications, vol. 25, num. 8, 2007, pp. 1557-1568

[15] Ghassan Samara, *"Certificate Revocation Management in VANET"*, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(2): 115-121, 2012

[16] John Nash, *"Equilibrium points in n-person games"*, Proceedings of the National Academy of Sciences, 36(1): 48-49, 1950

[17] Karen Scarfone and Peter Mell, *"Guide to Intrusion Detection and Prevention Systems (IDPS)"*, Computer Security Resource Center (National Institute of Standards and Technology) (800-94). Retrieved 1 January 2010

Sistema automatizado para detección de anomalías en redes de sensores inalámbricas

André Rodrigues[1], Jorge Sá Silva[2], Fernando Boavida[2]
[1]ISCAC – Coimbra Business School
[2]Departamento de Ingeniería Informática
Universidad de Coimbra
3030-290 Coimbra, Portugal
{arod, sasilva, boavida}@dei.uc.pt

***Resumen*- A medida que las redes de sensores inalámbricas (*Wireless Sensor Networks*, WSN) cobran impulso, la monitorización de este tipo de redes se está convirtiendo en un aspecto crucial, a fin de garantizar que las anomalías sean rápidamente detectadas. Las actuales soluciones de monitorización de WSN tienen varias limitaciones entre las que destacan el ser diseñadas para aplicaciones específicas, requerir *hardware* dedicado o específico, consumir demasiada energía y/o recursos de procesamiento o depender de la intervención manual o fuera de línea. En este trabajo se propone un método para la detección de anomalías en redes de sensores inalámbricas que se ocupa de estas limitaciones. El método se basa en dos indicadores muy simples: una herramienta de registro (*logging*), y un algoritmo de minería de datos. Gracias a este método, se logra un consumo de recursos muy bajo, independencia de las aplicaciones, muy buena potencial para el control y la monitorización de múltiples WSN y simplificación del proceso de detección. El sistema propuesto ha sido validado mediante una implementación donde se ha demostrado las capacidades que ofrece el método para la detección de varias anomalías típicas.**

***Palabras Clave*- redes de sensores inalámbricas, detección de anomalías, monitorización**

I. INTRODUCCIÓN

La detección y el diagnóstico de problemas en redes de sensores inalámbricas (WSN) se considera ahora esencial, debido al hecho de que el despliegue de este tipo de redes está creciendo a un ritmo rápido. Existen numerosas implementaciones, ya sean experimentales o de naturaleza comercial.

Un ejemplo de ello, dentro del área de investigación, es la implantación reciente de Intel, que equipó unos pocos cientos de hogares con dispositivos que permitieron la recogida de un conjunto de valores de parámetros (ambientales, fisiológicos y de comportamiento), con el objetivo de evaluar el potencial de la tecnología WSN en el estudio del envejecimiento y las enfermedades crónicas [1]. Una de las conclusiones del estudio es la necesidad de disponer de herramientas para gestionar este tipo de infraestructuras, que se caracterizan por un gran número de instalaciones geográficamente dispersas, en donde sus usuarios directos (en este caso los ancianos) no tienen suficiente experiencia tecnológica para ayudar en el diagnóstico y solución de problemas que se producen inevitablemente en los sistemas instalados.

En lo que se refiere a implementaciones comerciales, se espera que la tecnología WSN sea ampliamente utilizada para dar soporte a la monitorización en tiempo real de múltiples instalaciones pertenecientes a las mismas o diferentes entidades. Por ejemplo, es fácil prever su uso en granjas para apoyar la monitorización de las condiciones de salud de los animales. Como ejemplo, un sistema basado en WSN podría apoyar la recogida de diversos parámetros y, basándose en sus valores y en un conjunto de reglas, generar alarmas si algo anormal ocurre. Tal sistema se podría desplegar fácilmente en varias instalaciones y, por supuesto, requeriría una supervisión adecuada para asegurar su correcto funcionamiento. Esto es claramente un ejemplo de un escenario en el que la entidad que comercializa o mantiene el sistema también debe tener la capacidad de monitorizar en tiempo real las instalaciones en funcionamiento en los distintos clientes.

Aunque los escenarios de múltiples instalaciones WSN y/o de instalaciones de gran escala estén emergiendo rápidamente, las herramientas existentes para su monitorización aún no cumplen los requisitos de detección de anomalías: simplicidad, eficacia, automatización, operación distribuida y generalidad. Típicamente, los instrumentos de monitorización están específicamente desarrollados para las aplicaciones, consumen recursos considerables, exigen una configuración compleja y su utilización se limita a una única WSN.

El trabajo presentado en este artículo tiene por objetivo demostrar que es posible desarrollar sistemas de detección de anomalías que cumplan con los requisitos antes mencionados, utilizando dos indicadores simples: una herramienta de registro ya existente y un algoritmo de minería de datos.

El artículo se organiza de la siguiente manera. La sección II define el conjunto de requisitos que deben cumplir los instrumentos de monitorización de WSN. La sección III está dedicada a la presentación detallada de la propuesta, es decir, en lo que se refiere a su *hardware* y plataformas de *software*, indicadores utilizados, la recogida y el análisis de registros (*logs*), transformación de datos, y la detección y el diagnóstico. La implementación de prueba de concepto fue objeto de una evaluación en dos escenarios simples que comprenden varias condiciones anómalas. Los resultados de la evaluación se analizan en la sección IV. La sección V identifica el trabajo relacionado, con una breve presentación y discusión de un conjunto representativo de las herramientas de supervisión de WSN. La sección VI presenta las conclusiones y orientaciones para trabajo futuro.

II. Requisitos

En esta sección se presentan y discuten brevemente los requisitos que una herramienta de monitorización de WSN debería cumplir. Estos requisitos se dividen en dos categorías: requisitos relacionados con el escenario y requisitos de prestación/utilización.

A. Requisitos relacionados con el escenario

Escalabilidad – la herramienta debe ser capaz de escalar, tanto en términos del número de nodos por WSN como en el número de redes de sensores inalámbricas soportadas. Como se mencionó antes, los escenarios que comprenden la monitorización simultánea de distintas WSN van a ser frecuentes.

Homogeneidad inter-WSN y heterogeneidad intra-WSN – en cualquier WSN a menudo existe cierta heterogeneidad a nivel de *hardware* y *firmware*. Sin embargo, cuando se da el caso de múltiples WSN bajo la responsabilidad de una cierta organización, es frecuente que tengan las mismas aplicaciones en las mismas plataformas. Por lo tanto, las herramientas de monitorización deberían permitir explorar las ventajas de esta homogeneidad inter-WSN, y también lidiar con la heterogeneidad intra-WSN.

Soporte de WSN geográficamente dispersas – la existencia de redes de sensores inalámbricas situadas en varios lugares es un factor que debe ser tenido en cuenta en el diseño de una herramienta de monitorización, que debe apoyarse en mecanismos adecuados de comunicación.

Soporte de nodos móviles en WSN – es bastante común tener nodos móviles en WSN. Este tipo de nodos no tienen un impacto insignificante en las estrategias de recogida de datos y en las comunicaciones. Por este motivo, las herramientas de monitorización deben ser capaces de lidiar con este tipo de nodos.

B. Requisitos de prestación/utilización

Soporte de todos los paradigmas de aplicación – a fin de no verse limitada por el paradigma de la aplicación (es decir, *schedule-driven*, *query-driven*, o *event-driven*), la herramienta no debe depender de la existencia de patrones específicos de operación.

Soporte de distintas plataformas de *hardware* y sistemas operativos (SO) – la tecnología WSN está cambiando rápidamente, por lo que es importante asegurarse de que la herramienta se puede utilizar con varios sistemas operativos y plataformas, con el fin de hacer frente tanto a las necesidades actuales como las futuras.

Minimizar el uso de recursos de las WSN – por lo general, los nodos WSN tienen recursos limitados, por lo que las herramientas de monitorización deben reducir al mínimo el consumo de recursos, como la energía, el procesamiento y la memoria.

Fácil de instalar y de usar – el esfuerzo necesario para la integración de una herramienta de monitorización en una WSN o un conjunto de WSN debe ser minimizado. Lo mismo se aplica al esfuerzo requerido para utilizar la herramienta.

Flexibilidad y Extensibilidad – es importante que la herramienta incluya los mecanismos que permiten que el gestor adapte la herramienta a sus necesidades (en el despliegue y en tiempo de ejecución) a fin de permitir una aplicación más amplia.

III. Sistema propuesto

Teniendo en cuenta los requisitos identificados en el apartado anterior, nos propusimos demostrar que es posible la construcción de una herramienta de detección de anomalías simple, eficaz y automatizada, e independiente de la aplicación.

Cabe señalar que el objetivo del trabajo presentado no fue la construcción de la herramienta en sí, sino la demostración de que una herramienta basada en indicadores simples, con una funcionalidad de monitorización ligera, y algunos algoritmos de minería de datos puede satisfacer un gran porcentaje de los requisitos identificados.

Con este propósito, hemos desarrollado una implementación de prueba de concepto. En esta sección se ofrece información detallada sobre esa implementación, es decir, el *hardware* utilizado, plataformas de *software*, y en el diseño general, incluyendo indicadores, recogida y análisis de registros, transformación de datos, detección de eventos anómalos y su diagnóstico.

A. Sistema operativo y plataforma seleccionados

El prototipo de herramienta se implementó usando TinyOS [2] en una nueva plataforma de *hardware* llamada Hermes [3]. Esta plataforma incluye un reciente MSP430, una interfaz radio de 868 MHz, un lector de tarjetas SD, un acelerómetro, un giroscopio, un termómetro, un receptor de ritmo cardíaco, y un sistema de gestión de energía.

Como se empleó un sistema operativo basado en eventos, los indicadores que se utilizarán como base para la detección de anomalías se recogerán en el curso de *event procedure instances*. Es preciso aclarar que se utiliza aquí la terminología ya utilizada en [4], según la cual un *event procedure instance* es la secuencia que comienza con una interrupción de *hardware* y termina con la ejecución del último código asociado con el evento inicial.

También hay que señalar que, a pesar de que son esenciales, los indicadores recogidos deben ser complementados con información adicional, con el fin de identificar eficazmente las razones de comportamiento anómalo. En el caso de esta implementación de prueba de concepto, se decidió recoger adicionalmente rastreos de llamadas para el código de la aplicación, y también registrar todas las tareas ejecutadas.

Como observación final, cabe señalar que a pesar de la elección específica de la plataforma de *hardware*, sistema operativo y la implementación, los principios que guiaron la construcción de la herramienta (es decir, los indicadores simples, la independencia de la aplicación, el registro de operaciones y la minería de datos) son de carácter general y se pueden implementar fácilmente utilizando otros sistemas operativos y plataformas.

B. Cálculo de los indicadores

Al considerar la cuestión de qué indicadores utilizar para caracterizar el comportamiento como normal o anormal, se debe tener en cuenta aspectos como el impacto en los recursos del nodo, la aplicabilidad a diversos paradigmas de aplicación, el poder descriptivo, y la especificidad de plataformas de *hardware* y sistemas operativos. Indicadores con las siguientes características deben evitarse: 1) dependientes de la aplicación, por ejemplo, utilizando estadísticas sobre eventos específicos de la aplicación; 2) que requieran registros detallados, por ejemplo, rastreos

completos de llamadas, o vectores de contadores de instrucciones como en [4]; 3) dependientes del paradigma de la aplicación, por ejemplo, contadores de tráfico; 4) que exijan *hardware* dedicado o soporte del sistema operativo, por ejemplo, dispositivos dedicados de medición de energía, mecanismos de registro integrados en el sistema operativo.

De lo anterior, se puede concluir que el tiempo transcurrido, el procesamiento, y la energía son buenos candidatos para caracterizar lo que ocurre entre dos eventos consecutivos de nivel de aplicación. Estas medidas son de carácter general, fáciles de calcular, y no requieren sofisticados mecanismos de apoyo.

En el caso de la implementación de prueba de concepto, los indicadores seleccionados fueron el procesamiento y la energía. La principal razón para la exclusión del tiempo transcurrido fue que, para aplicaciones WSN típicas, no proporciona mucha información acerca de los recursos de procesamiento utilizados, pues la mayoría de tiempo entre dos eventos de nivel de aplicación es periodo inactivo (*sleep time*). Esto también significa que, por ejemplo, una anomalía que resultara en un aumento del periodo activo podría ser fácilmente "ocultada" por una ligera variación en el período inactivo, sin mucho impacto en el valor del indicador de tiempo transcurrido.

Cada indicador se calcula de la siguiente manera. Al arrancar, el contador se pone a cero. Cuando ocurre el siguiente evento de aplicación, el valor del contador se registra y se asocia al evento anterior. Finalmente, el contador se pone de nuevo a cero.

El primer método para calcular el indicador de procesamiento fue contar las instrucciones de la MCU (o ciclos de la MCU) ejecutados entre dos eventos de nivel de aplicación consecutivos. Lamentablemente, la plataforma Hermes no admite este método directamente.

El método seguido fue contar los ciclos del *sub-main clock* (SMCLK) de la MCU (es decir, MSP430F2618) entre eventos consecutivos de nivel de aplicación. El SMCLK en Hermes se define basándose en el *master clock* (MCLK) dividido por 4. El temporizador *TimerA* de la MCU se configuró para utilizar el SMCLK, dando como resultado que cuando la MCU no está durmiendo el SMCLK está funcionando y *TimerA* se incrementa.

Para hacer frente a plazos de ejecución largos durante los cuales *TimerA* podría desbordarse, el contador utiliza una variable de 32 bits que se acumula el valor de *TimerA* cada vez que se desborda o que se lee el contador. Este es un indicador muy ligero, ya que el proceso sólo requiere leer o actualizar la variable asociada al contador. Por razones de simplicidad, a partir de este punto a este indicador se llamará ciclos de MCU.

En lo que se refiere al indicador de energía, en iCount [5] los autores explicaron cómo un regulador de conmutación cuidadosamente seleccionado, utilizado para proporcionar energía regulada a un nodo sensor, se puede usar para obtener mediciones de consumo de energía, casi de forma gratuita. Debido a que el regulador seleccionado utiliza modulación de frecuencia de pulso, la frecuencia de conmutación está casi directamente relacionada con la corriente de carga. Su idea fue conectar la salida del inductor del regulador a la línea MCU INCLK que se puede utilizar para el *TimerA*. De esta manera, cada vez que el voltaje en el inductor cruza el cero en la dirección ascendente, *TimerA* se incrementa pues un nuevo ciclo de conmutación se detectó.

Hermes utiliza un sistema de gestión de energía (*Power Management System*, PMS) que incluye dos reguladores de conmutación basados en la técnica de modulación de ancho de pulso (*Pulse Width Modulation*, PWM), lo que no permite utilizar directamente el método iCount. Sin embargo, con cargas ligeras, el PMS soporta un modo de ráfaga (*burst mode*) en donde la energía se proporciona en una ráfaga de pulsos para reducir al mínimo las pérdidas de conmutación. Durante este modo de operación es posible contar los impulsos (usando un método similar al iCount) para obtener una estimación de la energía consumida.

Este método tiene dos limitaciones. La primera es que cuando el nodo sensor requiere más energía (por ejemplo, cuando se utiliza el canal radio) el regulador cambia automáticamente a modo PWM. La segunda es que, cuando el nodo está conectado a través de USB, está siempre en el modo PWM (aunque esto no sea un problema en escenarios reales pues Hermes utiliza baterías Li-Poly).

A pesar de estas limitaciones, se tomó la decisión de probar la utilidad de un sistema de medición basado en este mecanismo. Cabe señalar que una estimación precisa de la energía consumida no es necesaria. En su lugar, lo que es importante es obtener mediciones que permitan diferenciar entre funcionamiento normal y anómalo. De ahora en adelante, por razones de simplicidad, a este indicador se llamará consumo de energía.

C. Recogida y análisis de registros

Los mecanismos de registro son necesarios para recoger los indicadores y la información sobre los eventos de aplicación (por ejemplo: llamadas, tareas) de los nodos sensores, y remitirlos al sistema de gestión con el fin de apoyar la funcionalidad de detección y diagnóstico.

El mecanismo de registro debe ser flexible y ampliable, no exigir modificaciones al código fuente de la aplicación, ser fácil de instalar y usar, aprovechar las capacidades de comunicación de las aplicaciones, introducir latencia pequeña, ser leve en términos de uso de los recursos, ser fácilmente portable a otras plataformas y/o sistemas operativos, y permitir heterogeneidad de los nodos.

Habiendo que decidir entre el desarrollo de un sistema de registro de acuerdo con los requisitos anteriores o utilizar uno ya disponible, la decisión fue utilizar LIS [6], ya que soporta la mayoría de los requisitos. Sus aspectos negativos son su flexibilidad limitada (ya que no permite configuración pos-despliegue) y soporte limitado de nodos heterogéneos. Sin embargo, ya que estos aspectos no eran esenciales para la implementación de prueba de concepto, no se consideraron un obstáculo para su utilización.

En LIS, los desarrolladores tienen que producir un guión (LIS *script*) utilizando un lenguaje declarativo, que describe los mecanismos de registro y su ubicación en el código fuente de las aplicaciones. Entonces, un motor de instrumentación operando en un PC modifica el código fuente de acuerdo con el guión LIS, con el fin de incluir declaraciones de registro. También se añade al código una biblioteca de tiempo de ejecución que soporta el registro de llamadas a funciones del nodo sensor, y un módulo de código de funcionalidad de almacenamiento y recuperación de datos.

Durante la ejecución, los rastros de ejecución y el estado se guardan en la memoria local y se pueden enviar al nodo

sumidero (*sink node*) utilizando comunicación por cable (es decir, SerialActiveMessages), o la comunicación inalámbrica (es decir, TinyOS CTP para *multi-hop*, o ActiveMessages para un solo salto). Cuando los paquetes llegan al *sink node* se descodifican usando un analizador genérico de LIS y el guión LIS, a fin de extraer la información significativa.

El lenguaje LIS se puede utilizar directamente o como un lenguaje intermedio permitiendo definiciones de tareas reutilizables y de alto nivel. Una de esas tareas de alto nivel es la monitorización de llamadas en una región de interés (*Region of Interest*, ROI), donde el desarrollador especifica una ROI (por ejemplo, un cierto subsistema) y el sistema genera el LIS *script* correspondiente, que permitirá crear un registro de las llamadas de función dentro ese subsistema. Esta funcionalidad es muy útil, ya que permite evitar la necesidad de crear manualmente los guiones LIS.

En el caso de la implementación de prueba de concepto actual, fue necesario modificar los scripts de Python asociados con la funcionalidad de análisis de ROI, a fin de permitir a LIS la generación automática del código fuente modificado de la aplicación, con el objetivo de generar rastreos de llamadas y registros de indicadores.

La primera modificación fue la introducción de una etapa inicial en la que se modifica el código de las componentes de eventos de aplicación para incluir, al comienzo de cada evento, una declaración relacionada con el indicador de interés, como en el ejemplo siguiente:

```
energy = call EnergyMeter.read();
```

Esta instrucción asigna a la variable "`energy`" la energía consumida entre el inicio del evento de nivel de aplicación presente y el comienzo del anterior. El segundo paso fue modificar el *script* de Python utilizado por la ROI para generar el *script* de LIS, para que este pueda generar automáticamente las declaraciones "`watch`" asociadas a la variable "`energy`", con el fin de que sea registrada.

Con estas dos actualizaciones del mecanismo ROI, los guiones LIS resultantes tienen todos los comandos requeridos por el motor de instrumentación del código fuente de la aplicación, con el fin de recoger los rastreos de llamadas y los registros de consumo de energía. Para desplegar esta funcionalidad en los nodos sensores, todo lo que el desarrollador tiene que hacer ahora es programar los nodos de Hermes, como de costumbre, y toda la funcionalidad de registro será incluida automáticamente.

Por último, la recogida de los registros se realiza mediante el comando de consola "`timestampedlisten`", proporcionado por TinyOS, que recoge los paquetes enviados por los nodos de sensores en cuyos el mecanismo de registro está en marcha. Los paquetes recogidos se someten al analizador de LIS, que hace uso de la información de los scripts de LIS para emitir una lista fácil de leer conteniendo los rastreos de llamadas y los indicadores recogidos.

D. Transformación de datos

El fichero de datos producido por el analizador de LIS se filtra para eliminar registros incompletos de eventos de aplicación, que hayan resultado de pérdidas de paquetes. Esto es necesario porque si algunos paquetes se pierden eso puede comprometer el análisis de las entradas de registro siguientes. LIS incluye un mecanismo para descartar entradas de registro incompletas. Sin embargo, fue necesario mejorar este mecanismo, pues se detectó información incorrecta de eventos de aplicación en los registros analizados.

Después de esta fase, los registros son procesados con el fin de generar un fichero conteniendo una lista de eventos de nivel de aplicación con el formato de datos deseado. Este nuevo fichero también contiene la información adicional necesaria para permitir el diagnóstico de los eventos anómalos. Para apoyar todas estas transformaciones, fue desarrollado un conjunto de scripts en Python.

Cada línea del fichero generado tiene el siguiente formato:

<class> <m1>:<v1> <m2>:<v2> # <event> <begin> <end>

En este formato, <class> designa la clase del evento, <m1>:<v1> designa un par indicador/valor, <event> es el nombre del evento de nivel de aplicación, y <begin> y <end> identifican, respectivamente, la línea del fichero donde comienzan las entradas del registro relacionadas con este evento, y la línea donde terminan.

Los datos antes de la "#" son utilizados por el algoritmo de clasificación para identificar eventos anómalos. Los datos después del "#" son ignorados por el algoritmo de clasificación, pero se utilizan para localizar, en el fichero, la información de registro asociada con los eventos anómalos detectados.

E. Detección y diagnóstico de eventos anómalos

El algoritmo de clasificación seleccionado se basa en una técnica de aprendizaje automático (*machine learning*), llamada *Support Vector Machines* (SVM) [7], que genera un modelo que se puede utilizar para predecir la clase de una instancia. En este caso, una 'instancia' representa una instancia de un evento de nivel de aplicación, que tiene valores de indicadores como atributos, y puede ser clasificada como normal o anómala.

En SVM, se crea un modelo durante una fase de entrenamiento basada en un conjunto de instancias de datos etiquetados. En esta fase, se hace un mapeo de las instancias de datos, de su espacio de entrada a un espacio de dimensión superior, para encontrar un hiper-plano que divide las instancias de datos en dos regiones. En la fase de prueba, una instancia de datos se asigna a un mismo espacio superior y se clasifica de acuerdo con el lado del hiper-plano en el que se encuentra.

En el escenario presente, la aplicación de la técnica SVM presenta dos limitaciones. En primer lugar, no está disponible un conjunto de entrenamiento etiquetado. En segundo lugar, se espera que los eventos anómalos representen una pequeña fracción de todos los eventos (ya que el objetivo es detectar problemas esporádicos).

Teniendo en cuenta este escenario, la solución utilizada (también seguida de [4]) fue recurrir a una variante llamada SVM de una sola clase (*one-class* SVM), y admitir que el conjunto de entrenamiento contiene únicamente los eventos normales, a sabiendas de que un pequeño porcentaje de ellos pueden haber sido mal clasificados como tal. Al definir el porcentaje de eventos clasificados erróneamente en el conjunto de entrenamiento, el método *one-class* SVM creará un modelo que pone la mayoría de los eventos en el lado de la clase normal del hiper-plano, mientras que los restantes se colocan en el lado de clase anómala. Este modelo se usa entonces para predecir la clase de los futuros eventos recibidos. El modelo puede ser actualizado periódicamente,

en caso de que se requiera que el mecanismo de detección de evento anómalo tenga cierta flexibilidad para adaptarse a los cambios del entorno/sistema.

Las razones para elegir esta técnica fueron las siguientes: no se requieren datos previamente etiquetados, se puede trabajar con conjuntos de datos no balanceados (es decir, conjuntos de clases desigualmente representadas), y la existencia de una biblioteca de códigos bien documentada y fácil de usar (LIBSVM [8]). Esta biblioteca incluye secuencias de comandos de Python para simplificar su uso, a saber, para la ampliación de los conjuntos de datos, la selección de parámetros optimizados, el entrenamiento del modelo y la prueba de los datos.

La salida de LIBSVM es una clasificación para cada evento de nivel de aplicación. Se desarrolló un script que utiliza esta información para localizar, en el fichero LIS analizado, la información registrada en relación con los eventos de nivel de aplicación clasificados como anómalos. Esto permite a la persona responsable su análisis, con el fin de identificar las posibles razones de su clasificación.

En la Fig. 1 se resumen las actividades involucradas en la funcionalidad de detección y diagnóstico de eventos anómalos presentada en esta sección.

IV. Evaluación

La presente implementación de prueba de concepto fue sometida a varias pruebas, para evaluar la eficacia y la eficiencia de los conceptos subyacentes. Esta sección comienza por describir y presentar los resultados de un conjunto de experimentos realizados para evaluar las capacidades de detección y diagnóstico de la herramienta. A continuación, la herramienta fue evaluada a la luz de los requisitos iniciales.

A. Resultados experimentales

Se llevaron a cabo dos conjuntos de pruebas. En el primer grupo de experimentos, el objetivo fue evaluar la capacidad del indicador 'ciclos de MCU' para detectar comportamientos anómalos.

La aplicación seleccionada fue RadioCountToLeds, una aplicación estándar de TinyOS en la que dos nodos difunden periódicamente paquetes que contienen un contador, y cada vez que un nodo recibe un paquete se muestran los últimos 3 bits del contador en el mostrador LED. Se eligió esta aplicación debido a que tiene un comportamiento simple y está disponible al público, lo que permite a la comunidad validar los resultados presentados en este artículo.

El código de la aplicación incluye los eventos MilliTimer.fired, Receive.receive y AMSend.sendDone. Estos se activan periódicamente durante la ejecución normal.

La aplicación se ha desplegado en ambos nodos presentados en la Fig. 2. Uno de ellos (llamado nodo local, *local node*) se conecta por USB a un PC para enviar los paquetes con los rastreos de llamadas y los indicadores, utilizando la UART del nodo sensor. En este caso, se seleccionó la capa de enlace de SerialActiveMessages. Otras opciones son CTP y ActiveMessages para transmisiones inalámbricas multi-salto o de un solo salto).

El código fuente de la aplicación se modificó automáticamente para incluir los mecanismos de registro necesarios para generar los rastreos de llamadas y los indicadores de ciclos de MCU para los eventos de nivel de aplicación, y para generar los rastreos de llamadas para las

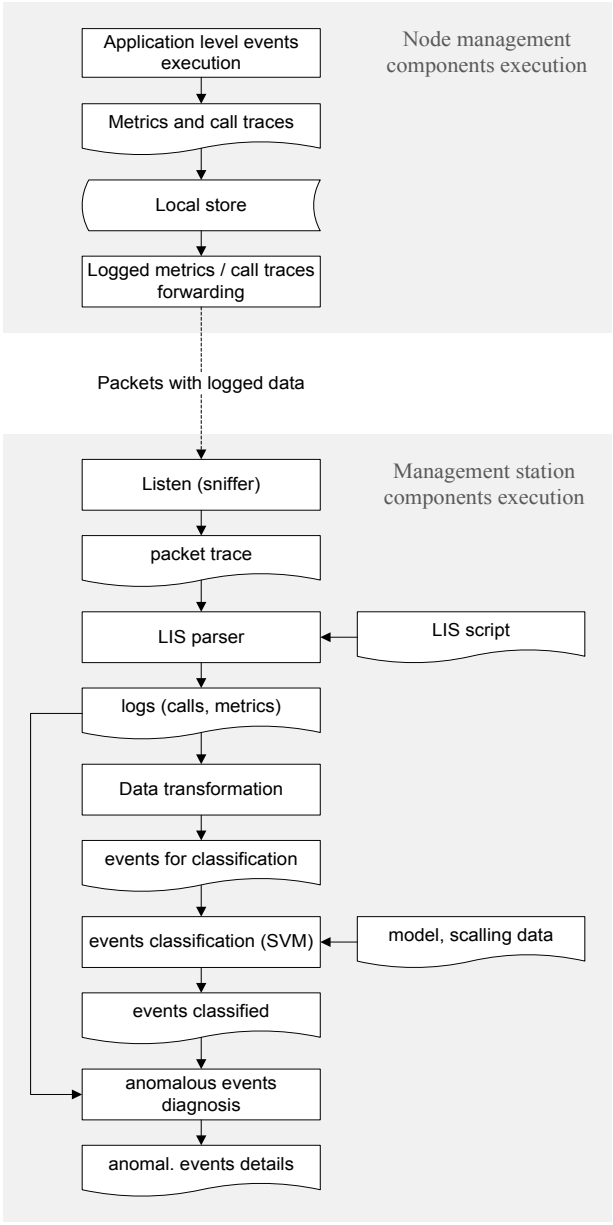


Fig. 1. Diagrama de flujo de detección y diagnóstico.

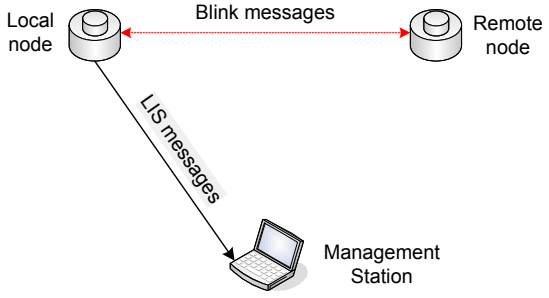


Fig. 2. Escenario de evaluación para el indicador 'ciclos de MCU'.

tareas ejecutadas. Los componentes que tienen sus funciones registradas fueron especificados en tiempo de compilación, evitando la modificación manual del código fuente de la aplicación.

Para la obtención del conjunto de entrenamiento, la aplicación RadioCountToLeds fue ejecutada durante 15 minutos en condiciones normales. En seguida el rastreo de

paquetes fue analizado por LIS, transformado para eliminar eventos de nivel de aplicación incompletos y para contruir la lista de eventos en el formato LIBSVM, y finalmente se sometió a la secuencia de comandos LIBSVM para construcción del modelo. El porcentaje de eventos clasificados erróneamente en el conjunto de entrenamiento se fijó en 1%. El conjunto utilizado para entrenar el clasificador contenía 1486 instancias de eventos.

Todos los experimentos tuvieron 5 minutos de duración y los resultados se presentan en la Tabla I. Antes de proceder al análisis de los resultados, dos aspectos deben ser destacados. En primer lugar, hay que señalar que, en la ausencia de problemas, el porcentaje de eventos clasificados como normales debe ser alrededor de 99% (ya que el umbral definido para los eventos clasificados erróneamente en la fase de entrenamiento fue de 1%). En segundo lugar, en la Tabla I, columna «Observaciones», se presentan los datos que aparecen en los registros de sucesos anómalos y que proporcionan pistas para la clasificación de los acontecimientos.

El experimento #1 fue diseñado para evaluar cómo la funcionalidad de detección de anomalías reacciona ante un fallo permanente (por ejemplo el nodo remoto bloquea y deja de transmitir sus mensajes). El bajo porcentaje de eventos normales (más de 40% de los eventos fueron clasificados como anómalos) apunta claramente a algún tipo de error. Este fallo fue diagnosticado fácilmente mediante la observación de la ausencia de eventos Receive.receive en los registros.

El objetivo de los experimentos #2 y #3 fue determinar si un error lógico (que resultó en la ejecución de código adicional) podría ser detectado. El código del evento MilliTimer.fired fue cambiado para que contuviese un ciclo que incrementaba un contador de 1 a 100 (o a 1000 en el caso del experimento #3). Este ciclo fue ejecutado en 10% de las ejecuciones de eventos MilliTimer.fired. En ambos casos, los eventos anómalos (un exceso de eventos MilliTimer.fired con un alto valor de ciclos MCU) fueron detectados, como se indica por un porcentaje de eventos normales por debajo de 99%.

El objetivo del experimento #4 fue ligeramente más ambicioso: determinar si otro tipo de error lógico podría ser detectado. Específicamente, en este caso, el contador fue incorrectamente incrementado dos veces en 10% de los casos. Esto se hizo mediante la modificación del código del evento MilliTimer.fired. El impacto en la aplicación que se ejecuta en el nodo local fue mínimo y, por lo tanto, no se detectó.

Otro conjunto de experimentos pretendió evaluar la eficacia del indicador 'consumo de energía' en la detección de comportamientos anómalos. En estos experimentos la topología era una estrella con dos nodos que ejecutaban la aplicación RadioCountToLeds, y otro nodo cuya función era recoger los paquetes con los registros y enviarlos, a través de USB, a la estación de gestión (Fig. 3). La aplicación RadioCountToLeds fue modificada para escuchar la red en modo de bajo consumo (*Low Power Listening*) y el temporizador utilizado para enviar los mensajes se incrementó de 1,9 segundos a 5 segundos. La duración de los experimentos se aumentó a 10 minutos. La Tabla II presenta los resultados de los experimentos.

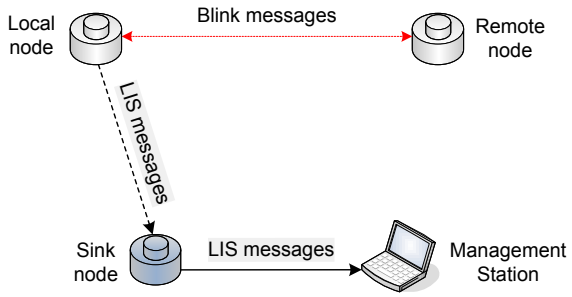


Fig. 3. Escenario de evaluación para el indicador 'consumo de energía'.

En el experimento #5 se reinicia un nodo 5 veces. Mediante el análisis de los registros del otro nodo, fue posible detectar la existencia de un comportamiento anómalo (como se indica por un porcentaje de eventos normales por debajo de 99%), y posteriormente identificar eventos anómalos AMSend.sendDone con valores de alta energía. Esto parecía indicar que algunos mensajes no fueron enviados por el nodo reiniciado o que se perdieron.

En el experimento #6 el porcentaje significativamente menor de eventos normales da una pista sobre alguna anomalía. Después de inspeccionar los registros para los eventos anómalos, se detectó un reinicio del nodo local (específicamente, uno de los eventos anómalos era un Boot.booted).

En el experimento #7, un nodo se movió lejos del otro, a un piso más arriba. El porcentaje relativamente bajo de eventos normales, junto con un menor número de eventos en el conjunto de datos del nodo que no se movía, era un indicio de problemas. Mediante la inspección de los registros de sucesos anómalos fue posible identificar varios eventos anómalos AMSend.sendDone con valores de alta energía. Esto sugirió que se habían producido pérdidas de paquetes, pero fue necesario un análisis de los registros del otro nodo para llegar a una conclusión.

El experimento #8 se diseñó para determinar si un estado

Tabla I
RESUMEN DE CLASIFICACIÓN (INDICADOR 'CICLOS DE MCU')

#	Condición	% eventos normales	Eventos (norm/total)	Observaciones
1	Nodo remoto apagado	58.21%	163/280	Ausencia de registros Receive.receive
2	100 i++	98.66%	443/449	Solo MilliTimer.fired > 21750
3	1000 i++	95.53%	406/425	Solo MilliTimer.fired > 23600
4	Extra op	99.04%	416/420	No detectado

Tabla II
RESUMEN DE CLASIFICACIÓN (INDICADOR 'CONSUMO DE ENERGÍA')

#	Condición	% eventos normales	Eventos (norm/total)	Observaciones
5	5 reinicios remotos	98.77%	322/326	AMSend = 6.213.697
6	1 reinicio local	96.93%	347/358	Boot.booted
7	Un piso arriba	91.97%	229/249	AMSend > 6.000.000
8	Giroscopio encendido	75.36%	260/345	AMSend ~3.200.000

erróneo de energía en un dispositivo sería detectable. Específicamente, no se apagó el giroscopio en el momento de arranque con el fin de crear una anomalía. El porcentaje considerablemente bajo de eventos normales indica claramente que algo andaba mal. Además, la existencia en los registros de varios eventos AMSend.sendDone anómalos con los valores de energía mayor que 3.000.000 lo confirmó. Sin embargo, ya que este tipo de problema no afecta a la ejecución del programa, no hubo información de los registros que permitiera a su diagnóstico.

A la luz de los resultados obtenidos, es evidente que la utilización de indicadores simples combinados con el análisis de registros y la minería de datos permite la detección de condiciones más anómalas. Debe tenerse en cuenta que los objetivos de esta implementación de prueba de concepto y de los experimentos asociados fueron la evaluación de la eficacia de la detección automática de anomalías, no el diagnóstico en sí.

B. Análisis de requisitos

El objetivo de desarrollar y evaluar la implementación presentada era, por un lado, validar los conceptos en los que se basa – a saber, el uso de indicadores simples, el uso de una herramienta de registro ligera, y la minería de datos – y, por otra parte, para evaluar su capacidad para satisfacer las necesidades identificadas. En el apartado anterior, la herramienta se evaluó con respecto a la primera. En el actual sub-sección, se presenta un análisis para esta última.

Escalabilidad – En la implementación actual, el análisis, transformación de datos y las tareas de clasificación requeridas para procesar un registro de 10 minutos tardó menos de 1,5 s (1.295 s, 0,172 s, y s 0,023, respectivamente) por nodo sensor, en un ordenador Intel Core 2 Duo 2,4 GHz con 3 MBytes de memoria RAM. Este es un tiempo de procesamiento bajo. Para mantener bajos tiempos de análisis con un número elevado de nodos y con más componentes cuyas llamadas de funciones sean registradas, una implementación optimizada sólo debe enviar los indicadores en tiempo de detección, guardando localmente los registros de seguimiento de llamadas, para una inspección posterior a pedido.

Soporte de nodos sensores heterogéneos – la herramienta permite trabajar con dispositivos WSN con distinto *hardware* y *software*. Esto se realiza por agrupamiento de los registros, en el sistema de gestión, de acuerdo con su configuración de *software* y *hardware*. De esta manera, cada grupo de información de registro contiene datos de eventos de nodos sensores con el mismo tipo de *hardware*/*software*. Cada grupo se analiza entonces individualmente según el diagrama de flujo presentado en la Fig. 1.

Soporte de WSNs geográficamente dispersas – las herramientas implementadas de acuerdo con los principios presentados pueden trabajar de forma transparente con los datos de registro procedentes de múltiples redes de sensores inalámbricas, siempre que cada WSN esté conectada a Internet a través de una pasarela que se comunique con el sistema de gestión.

Soporte de nodos móviles – Las comunicaciones LIS pueden utilizar mensajes de TinyOS activas o CTP. Para aplicaciones WSN utilizando estos protocolos, la herramienta soportará el mismo patrón de movilidad que la aplicación. La inclusión de otros protocolos no es difícil, ya que el componente de recogida de registros es un componente separado, con interfaces bien definidas. En los experimentos que se llevaron a cabo no se evaluó el rendimiento de la herramienta en situaciones de movilidad de los nodos. Esto se dejó para trabajo futuro.

Independencia de los paradigmas de aplicación – la funcionalidad de detección se basa en la ocurrencia de eventos de nivel de aplicación en los nodos sensores monitorizados y utiliza indicadores generales. De esta manera, es compatible con todo tipo de paradigmas de aplicación. Sin embargo, para aplicaciones de redes de sensores inalámbricas donde los nodos de sensores están inactivos durante largos periodos de tiempo y sólo se activan raramente, este método no funcionará. Este es un problema común, no específico del método presentado, y la solución habitual es utilizar los mecanismos, ya sea iniciados por los nodos sensores o por el nodo *sink*, que permiten saber si un nodo sensor está activo o no. Si este tipo de mecanismo es soportado por la aplicación, la herramienta se beneficiará de él. La otra opción sería que el agente de gestión del nodo sensor forzara una recogida de indicadores si ningún evento se produce durante un período de tiempo predefinido.

Soporte de diversas plataformas de *hardware* y sistemas operativos – la mayor parte de la funcionalidad de detección de los nodos sensores se basa en LIS, siendo la excepción el cálculo de indicadores. En la actualidad, LIS es compatible con Mica2 / Z, TelosB y Hermes. Su uso con otros sistemas operativos, como Contiki, no aparenta ser complejo, dado que LIS opera mediante la modificación de las aplicaciones basadas en el lenguaje C.

Minimizar el uso de recursos – la MCU, RAM, ROM y el consumo se minimizan porque LIS es una herramienta de registro muy eficiente y porque el cálculo de indicadores es muy ligero. El impacto sobre la energía y ancho de banda depende del número de componentes que tienen sus llamadas a funciones registradas. Sólo el envío de registros de llamadas a pedido permitirá un mayor ahorro.

Ser fácil de instalar y de usar – en el caso de esta implementación de prueba de concepto, la implementación de la herramienta en un nodo sensor sólo necesita compilar la aplicación WSN con una opción que indica qué componentes deben tener su actividad registrada (en los experimentos de evaluación presentados, se trataba de la aplicación y del planificador). La facilidad de uso solamente puede ser evaluada con una plataforma integrada y no con una aplicación prototipo de prueba de concepto. Sin embargo, los experimentos no exigieron mucho trabajo de análisis.

Flexibilidad y extensibilidad – la implementación actual no permite la configuración posterior al despliegue de la funcionalidad de registro en los nodos sensores. La funcionalidad implementada se basa en una versión mejorada del mecanismo ROI existente en LIS. Este trabajo se puede extender fácilmente usando el lenguaje de script LIS, más indicadores y algoritmos adicionales de clasificación. Para eso sería necesario modificar el programa de análisis para lidiar con los nuevos indicadores, y en el desarrollo de scripts de Python para soportar los formatos de datos requeridos por los nuevos algoritmos de clasificación.

V. TRABAJOS RELACIONADOS

Varios trabajos han abordado el problema de la monitorización de WSN. Se mencionan brevemente los

principales en esta sección, con un enfoque en los que tuvieron un mayor impacto en la presente implementación de prueba de concepto.

MANNA [9] fue uno de los primeros sistemas de gestión de redes de sensores inalámbricas. A pesar de utilizar una arquitectura muy flexible y general, no incluye mecanismos de detección y diagnóstico para la gestión conjunta de múltiples redes de sensores inalámbricas.

SWARMS [10] se destina a la gestión de redes de sensores inalámbricas de área extensa, en distintas localidades, proporcionando funcionalidades de diagnóstico y programación. Fue diseñado para ser escalable, flexible y extensible. La mayor preocupación con esta arquitectura es el hecho de que se requiere que cada nodo sensor esté directamente conectado a un ordenador que ejecuta un proceso dedicado a ese nodo. Por otra parte, no comporta funcionalidad para permitir la detección y diagnóstico automáticos.

MARWIS [11] se dirige a la gestión de una WSN heterogénea dividiéndola en redes WSN homogéneas conectadas por una red de malla. Fue diseñado para ser escalable, flexible y extensible. El principal problema de esta arquitectura es que soportar heterogeneidad de nodos sensores dividiendo una WSN en un conjunto de redes de sensores inalámbricas homogéneas no encaja bien cuando hay necesidad de administrar varias redes de sensores inalámbricas heterogéneas pertenecientes a diversas organizaciones. Por otra parte, MARWIS asume que los nodos sensores están ejecutando aplicaciones basadas en Contiki y no existen disposiciones para soportar la detección y diagnóstico automáticos.

Sentomist [4] es una herramienta para la identificación de los posibles errores transitorios en aplicaciones WSN, que también utiliza SVM para identificar eventos anómalos. Sin embargo, el hecho de que se apoya en una métrica basada en la información de las instrucciones de procesador ejecutadas en cada evento, requiere el uso del emulador Avrora, lo que lo restringe a uso de laboratorio.

Por último, hay varias herramientas desarrolladas para ayudar a diagnosticar redes de sensores inalámbricas que operan en el campo. Hemos realizado un amplio estudio [12] que describe, analiza y compara un conjunto representativo de dichas herramientas. Ese trabajo nos ha guiado en el desarrollo del sistema actual para la detección de anomalías en redes WSN, y en la elección de LIS como herramienta base de esta implementación.

VI. Conclusiones

Este artículo propone un método simple para la detección de anomalías en las redes de sensores inalámbricas, basado en el uso de dos indicadores generales, una estrategia de registro sencilla, y una técnica de aprendizaje automático. La tesis es que estos conceptos y soluciones son suficientes para desarrollar un sistema automatizado, independiente de la aplicación, ligero, capaz de monitorizar múltiples redes de sensores inalámbricas. Para evaluar esto, una implementación de prueba de concepto fue desarrollada y sometida a prueba. Los resultados han demostrado que el método propuesto tiene muy buen potencial y características, y es capaz de detectar anomalías de *hardware* y *software* de una manera muy eficaz, sin comprometer los requisitos identificados, tales como escalabilidad, heterogeneidad, generalidad y facilidad de uso.

El trabajo presentado en este artículo abre muchas líneas de trabajo futuro. En primer lugar, debe hacerse una evaluación más amplia y más general. Además, otros indicadores generales deben ser identificados y explorados. El desarrollo de una aplicación completa para uso en redes de sensores inalámbricas existentes también será muy interesante, así como el soporte para IPv6 (6LoWPAN) con el fin de aumentar la aplicabilidad de la herramienta.

Agradecimientos

Trabajo parcialmente financiado por el proyecto CENTRO-07-ST24-FEDER-002003. Nos gustaría dar las gracias al Prof. Roy Shea, de UCLA, por aclarar varios aspectos de la operación de LIS, y a la Prof. Alicia Triviño-Cabrera, de la Universidad de Málaga, por sus comentarios, sugestiones y revisión del texto.

Referencias

[1] T. Hayes, M. Pavel, and J. Kaye, “Gathering the Evidence: Supporting Large-Scale Research Deployments,” Intel Technology Journal, 13(3), 2009.

[2] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, “Tinyos: An operating system for wireless sensor networks,” In W. Weber, J. Rabaey, and E. Aarts, editors, Ambient Intelligence. Springer-verlag, 2004.

[3] A. Rodrigues, M. Silva, T. Camilo, N. Blanco, J. Pedro, J. Martins, J. S. Silva, and F. Boavida, “Hermes: A versatile platform for wireless embedded systems,” Proceedings of the IEEE WoWMoM 2012, IEEE, San Francisco, CA, USA.

[4] Y. Zhou, X. Chen, M. Lyu, and J. Liu, “Sentomist: Unveiling Transient Sensor Network Bugs via Symptom Mining,” Proceedings of the IEEE ICDCS, pp. 784-794, 2010.

[5] P. Dutta, M. Feldmeier, J. Paradiso, and D. Culler, “Energy Metering for Free: Augmenting Switching Regulators for Real-Time Monitoring,” Proceedings of the IPSN 2008, IEEE, pp. 283-294, 2008.

[6] R. Shea, Y. Cho, and M. Srivastava, “LIS is More: Improved Diagnostic Logging in Sensor Networks with Log Instrumentation Specifications,” TR-UCLA-NESL-200906-01, 2009.

[7] C.-W. Hsu, C.-C. Chang, and C.-J. Lin, “A Practical Guide to Support Vector Classification,” Technical Report, Department of Computer Science, National Taiwan University, (2010). [Online]. Available: http://www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf

[8] C.-C. Chang, and C.-J.Lin, “LIBSVM: A library for support vector machines,” ACM Transactions on Intelligent Systems and Technology 2(3), article no. 27, 2011.

[9] B. Ruiz, J. Nogueira, and A. Loureiro, “MANNA: a management architecture for wireless sensor networks,” IEEE Communications Magazine 41(2), pp. 116-125, 2003.

[10] C. Gruenwald, A. Hustvedt, A. Beach, and R. Han, “SWARMS: a sensornet wide area remote management system,” Proceedings of the TridentCom, 2007.

[11] G. Wagenknecht, M. Anwander, T. Braun, T. Staub, J. Matheka, S. Morgenthaler, “MARWIS: a management architecture for heterogeneous wireless sensor networks,” Proceedings of the WWIC, pp. 177-188, 2008.

[12] A. Rodrigues, T. Camilo, J. S. Silva, and F. Boavida, “Diagnostic Tools for Wireless Sensor Networks: A Comparative Survey,” Springer JNSM, Springer New York, 2012. doi: 10.1007/s10922-012-9240-6.

Indicadores de Ataques *Sinkhole* en MANETs

Leovigildo Sánchez-Casado, Gabriel Maciá-Fernández, Pedro García-Teodoro
Departamento de Teoría de la Señal, Telemática y Comunicaciones,
E.T.S. de Ingenierías Informática y de Telecomunicación - CITIC, Universidad de Granada
C/Periodista Daniel Saucedo Aranda s/n, E-18071, Granada
{sancale, gmacia, pgteodor}@ugr.es

***Resumen*—Este trabajo estudia y propone una serie de indicadores destinados a reconocer comportamientos maliciosos en los protocolos de enrutamiento empleados en redes MANET. El estudio planteado se centra en el ataque *sinkhole*, especialmente representativo de un conjunto de ataques dedicados a alterar las rutas origen-destino y comúnmente conocidos como ataques de *route poisoning*. Dicho ataque pretende, a través del falseo de las rutas, atraer hacia sí mismo todo el tráfico existente a su alrededor, degradando cuando menos el rendimiento de la red. Nuestra propuesta para luchar contra este tipo de ataques se basa en la recopilación de la información de las rutas de los distintos nodos, la cual es analizada heurísticamente para extraer indicadores de la existencia de nodos maliciosos *sinkhole* en la red. Los resultados experimentales obtenidos a través de simulaciones muestran unas capacidades prometedoras, no sólo en términos de detección, sino también desde el punto de vista de la simplicidad del sistema.**

Palabras Clave*—AODV; Ataques de *poisoning*; Detección de intrusiones; MANETs; *Sinkhole

I. INTRODUCCIÓN

Entre las muchas posibilidades que ofrecen las TIC (Tecnologías de la Información y las Comunicaciones), las redes inalámbricas ganan interés día a día, y en particular, las denominadas redes ad hoc móviles (*Mobile Ad Hoc Networks*, o MANETs) [1]. Una MANET es un tipo de red sin infraestructura fija ni administración centralizada, compuesta por dispositivos móviles auto-configurables, de despliegue sencillo y económico. Los nodos forman topologías dinámicas, comunicándose mediante una estrategia multi-salto, es decir, los nodos se comunican con aquellos que están fuera de su rango de cobertura haciendo uso de otros nodos intermedios que retransmiten sus mensajes hasta el destino. Todas estas características hacen de este tipo de redes un candidato óptimo en multitud de áreas, tales como aplicaciones militares o medioambientales, gestión de desastres, etc. Sin embargo, también presentan una multitud de problemas de seguridad asociados, que deben ser convenientemente tratados.

Existen diferentes aspectos que deben tenerse en cuenta a la hora de diseñar e implementar soluciones de seguridad para MANETs, como son sus limitados recursos, la existencia de colisiones, la movilidad, etc. Debido a esta complejidad, la mayoría de las técnicas y procedimientos desarrollados para redes tradicionales no son directamente aplicables para las MANETs [2].

Entre otros muchos, los ataques de *poisoning* [3] son una de las amenazas potencialmente más perjudiciales en MANETs. Este tipo de ataques consiste en la modificación, creación o eliminación de paquetes de *routing* con la intención de alterar el correcto funcionamiento del protocolo de enrutamiento y, en consecuencia, de la red y sus servicios. Este trabajo se centra en el estudio del ataque *sinkhole*, uno de los más representativos de los ataques de *route poisoning*. Los nodos que exhiben este comportamiento malicioso intentan falsear las rutas origen-destino y así atraer hacia ellos el tráfico circundante. Para ello, modifican los paquetes de control del protocolo de enrutamiento, publicando información de *routing* falsa que los haga más atractivos, con un menor número de saltos hacia el destino o una mejor ruta. De esta manera consiguen que otros nodos legítimos los elijan como siguiente salto en el proceso de retransmisión de la información.

Hay distintas motivaciones por las que llevar a cabo un ataque *sinkhole*: realizar escuchas de los datos recopilados, descartar o modificar paquetes para degradar el rendimiento de la red o incluso como paso previo para la realización de ataques más complejos, como por ejemplo ataques *wormhole* o *blackhole*. Si el *sinkhole* no realiza ninguna de las acciones subsiguientes mencionadas, como la modificación o el descarte, su detección (y posible solución) resulta más compleja.

Centrado en este objetivo, el presente trabajo propone una serie de indicadores del ataque obtenidos mediante una heurística sencilla que recopila y analiza información y estadísticas relativas a las tablas de rutas de todos los nodos de la red. Este indicador podría ser introducido posteriormente en un sistema de detección de intrusiones (*Intrusion Detection System*, o IDS) para determinar si un nodo dado está actuando o no como *sinkhole*.

La contribución principal de este trabajo es la sencillez y bajo coste computacional de la heurística planteada, lo que permite su viabilidad de uso en entornos reales. Los prometedores resultados obtenidos confirman las bondades del esquema propuesto.

El resto del artículo se organiza de la siguiente forma. En la Sección II se describe la implementación y funcionamiento de un ataque *sinkhole* en un protocolo de *routing* específico, AODV. La Sección III proporciona un análisis del estado del arte, describiéndose las principales soluciones de detección frente a ataques *sinkhole*. La heurística propuesta para obtener el indicador de ocurrencia de ataque *sinkhole* se presenta en la Sección IV, mientras que la Sección V detalla el entorno de experimentación y los resultados concretos

obtenidos. Finalmente, la Sección VI expone las conclusiones y líneas de trabajo futuro.

II. ATAQUES *SINKHOLE* EN AODV

AODV (*Ad hoc On-Demand Distance Vector*) [4] es un protocolo de *routing* para MANETs de tipo reactivo, es decir, obtiene las rutas bajo demanda; minimizando así el número de paquetes de control necesarios para establecerlas y mantenerlas, y en consecuencia, también el *overhead* introducido. Así, si un nodo origen, *S*, desea comunicarse con un nodo destino, *D*, y no posee una ruta válida hacia éste, *S* inicia un proceso de descubrimiento de ruta difundiendo en modo *broadcast* un mensaje de solicitud de ruta (*Route Request*, o RREQ). Asimismo, los vecinos de *S* que reciben el paquete RREQ lo retransmiten a sus propios vecinos, repitiéndose el proceso hasta que el RREQ alcanza el destino pretendido. Una vez que *D* recibe el primer RREQ, envía de vuelta un mensaje de respuesta de ruta (*Route Reply*, o RREP) hacia el origen a través de la ruta inversa por la que se recibió el RREQ. Los mensajes RREQ recibidos con posterioridad son ignorados por el destino. Además de este procedimiento de descubrimiento, AODV permite que los nodos intermedios que conozcan una ruta válida hacia el destino generen y respondan mensajes RREP hacia el origen. Por tanto, los nodos origen e intermedios son los encargados de almacenar la información relativa al siguiente salto para cada flujo de comunicación.

Para mantener la coherencia de las rutas y evitar bucles, AODV emplea *números de secuencia*, esto es, unos identificadores que sirven como *marcas temporales*, permitiendo a los nodos comprobar cómo de "reciente" es la información que poseen. Cada vez que un nodo envía un paquete de control, incrementa su número de secuencia. Además, los nodos almacenan el número de secuencia de todos los otros nodos con los que mantienen comunicación. De este modo, un nodo sólo actualizará su información de ruta si el número de secuencia del mensaje RREP recibido es mayor que el último número de secuencia almacenado o igual a éste pero con un menor número de saltos, lo cual indicará una ruta más reciente o mejor.

De este modo, las tablas de rutas de los nodos en AODV estarán constituidas por los siguientes campos: destino, siguiente salto (*NextHop*), distancia al destino medida en número de saltos (*HopCount*), estado (VAL -válida- o INV -caducada-) y número de secuencia (*NumSeq*), además de otros campos usados por AODV, como el tiempo de vida de la ruta, una serie de banderas o *flags*, la interfaz de salida, etc. La Figura 1 muestra un ejemplo simplificado de una tabla de rutas de un nodo, mostrando la información de interés en este trabajo.

Dest	NextHop	HopCount	Estado	NumSeq
2	12	2	VAL	1
3	3	1	VAL	3
6	10	2	INV	4
9	12	2	INV	4
10	10	1	VAL	3
12	12	1	VAL	5
15	12	3	VAL	6

Fig. 1: Ejemplo de tabla de rutas en AODV para un nodo dado.

Una vez que se conocen los conceptos básicos de AODV, es sencillo comprender cómo un nodo malicioso puede tomar ventaja del funcionamiento del protocolo para realizar el ataque *sinkhole*. En AODV, un nodo malicioso podría publicar una ruta hacia un destino dado indicando una métrica óptima, es decir, un mínimo número de saltos hacia el destino, así como un número de secuencia mayor que los previamente recibidos. Si el número de secuencia es suficientemente grande, se invalidarán las posibles rutas alternativas que publiquen otros nodos con rutas válidas hacia el destino. Como consecuencia de esto, el nodo origen aprenderá que la mejor ruta para alcanzar el citado destino es a través del nodo *sinkhole*. Si éste responde con mensajes RREP falsos a cualquier petición de rutas RREQ que reciba, terminará convirtiéndose en un sumidero, pues gran parte del tráfico de la red será enrutado a través de él. Una vez hecho esto, el nodo malicioso podrá realizar distintas acciones sobre los paquetes recopilados, como extraer información sensible de los mismos, modificarlos, descartarlos o llevar a cabo ataques más complejos.

La Figura 2 muestra un ejemplo del ataque *sinkhole*. En este caso, el nodo origen *S* envía una solicitud RREQ hacia el destino *D*. Cuando ésta alcanza a *D*, éste responde con un RREP con los valores *HopCount* y *NumSeq* legítimos (3 y 12, respectivamente). Al mismo tiempo, un nodo malicioso de tipo *M* responde con un falso RREP hacia el origen *S* proclamando que posee la ruta más corta hacia *D* (*HopCount* = 1) e indicando además un número de secuencia mayor que el de otros nodos (*NumSeq* = 37). Así, a pesar de recibir otras respuestas legítimas, el origen *S* elegirá la ruta a través de *M*, al ser considerada como la más reciente y la que posee una métrica de distancia óptima, aún cuando el nodo *M* no conoce realmente la ruta hacia el destino.

III. TRABAJO RELACIONADO

En la literatura especializada se puede encontrar gran cantidad de soluciones que intentan dar solución al ataque *sinkhole* en redes MANETs, bien sea mediante prevención o mediante detección. Algunas de las principales soluciones destinadas a detectar ataques *sinkhole* se estudian a continuación.

El empleo de técnicas de *machine learning* para realizar la detección se han aplicado en numerosas ocasiones. Por ejemplo, Zhang *et al.* [5] introducen un esquema local y cooperativo en el que cada nodo incorpora un agente IDS basado en SVM que monitoriza las trazas locales y es responsable de detectar, de forma local e independiente, señales de posibles ataques. Asimismo, si la evidencia no es concluyente, los agentes IDS vecinos investigan de forma

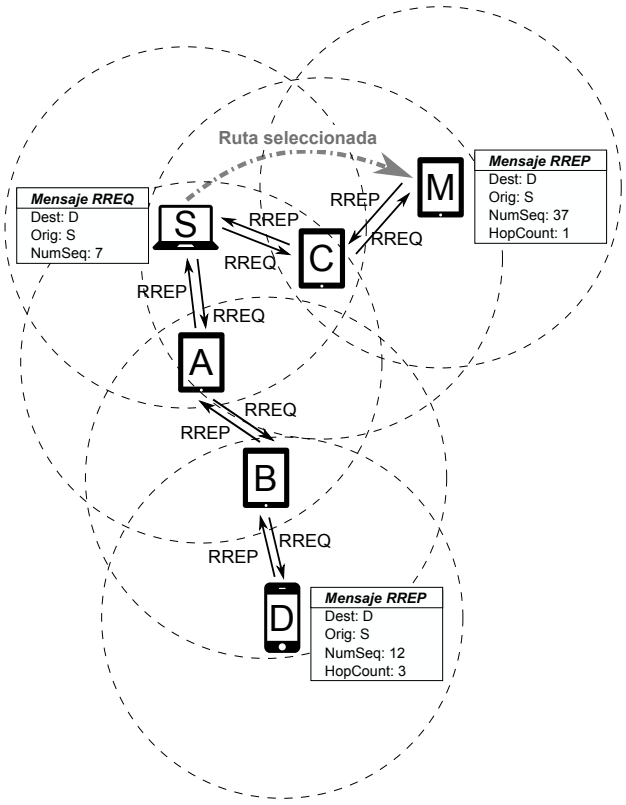


Fig. 2: Ejemplo de nodo *sinkhole* respondiendo con un falso RREP.

colaborativa, participando en un proceso de detección global y cooperativo.

Un método denominado *cross-feature* se describe en [6], en el que se definen un total de 141 características topológicas y relacionadas con el tráfico de red. Este método ejecuta un análisis de minería de datos para extraer correlaciones e intercorrelaciones entre éstas, reduciendo así el espacio de características. Para realizar el procedimiento de detección se utiliza un clasificador, como pueda ser C4.5, RIPPER o Naïve-Bayes.

Los autores en [7] adoptan el concepto de *consistencia* dentro del *círculo íntimo* para identificar respuestas falsificadas y prevenir ataques *sinkhole*. La idea consiste en permitir que cada nodo descubra su vecindario a k saltos de distancia. Todos estos nodos formarán su *círculo íntimo*, responsable de votar y filtrar paquetes falsos procedentes del nodo. En particular, los RREP tienen que ser aprobados por el círculo, que verifica la validez del mensaje. Si una respuesta contiene información de *routing* falsa para atraer paquetes, el ataque será detectado y prevenido por la votación realizada por el círculo.

Kurosawa *et al.* [8] tratan con ataques *sinkhole* introduciendo un esquema de detección de anomalías que emplea un método de entrenamiento dinámico. Los autores consideran para expresar el estado de la red el número de paquetes RREQ enviados y de paquetes RREP recibidos, así como la diferencia media entre el número de secuencia enviado en los paquetes RREQ y el recibido en los RREP. Así, se emplea un conjunto de entrenamiento de dichas características para calcular un umbral de detección basado en el estado normal de la red, que se actualiza dinámicamente a intervalos regulares para mejorar la precisión en la detección. En el proceso de detección, se compara cada muestra con el umbral calculado y se detectan posibles desviaciones respecto del comportamiento normal de la red.

En [9] los autores proponen una solución denominada DPRAODV, en la que los nodos que reciben mensajes RREP desde nodos intermedios comprueban que el número de secuencia no exceda un determinado umbral. Además, para evitar falsas alarmas, dicho umbral se actualiza dinámicamente. En caso de que el número de secuencia sea superior al límite impuesto, el nodo intermedio se convierte en sospechoso y es añadido a una lista negra.

Otra aproximación basada en técnicas de *matching* es IDAD (*Intrusion Detection based on Anomaly Detection*) [10], un IDS basado en *host* que compara la actividad del nodo con un conjunto previamente recolectado de actividades anómalas y maliciosas, denominado *de auditoría*. Los parámetros se obtienen de cada mensaje RREP anómalo, y son: número de secuencia destino, número de saltos, tiempo de vida de la ruta, dirección IP destino y marca de tiempo. De este modo, IDAD es capaz de diferenciar paquetes RREP anómalos sin más que comprobar si son similares a los del conjunto *de auditoría*, en cuyo caso el nodo que envía el paquete RREP es considerado malicioso.

IV. INDICADORES PARA LA DETECCIÓN DE ATAQUES *SINKHOLE*

En esta sección se presenta un esquema que permite obtener un valor indicador de la existencia de ataques *sinkhole* en base a una heurística que emplea características de la capa de red, principalmente información relativa a las tablas de rutas de los nodos. Dicha heurística se apoya en las siguientes **hipótesis**:

I Los nodos *sinkhole* atraen gran parte del tráfico circundante, por lo que los nodos legítimos poseerán una gran cantidad de rutas en las que el nodo malicioso se presentará como siguiente salto. Así, aquellos nodos que aparezcan más veces como siguiente salto en las rutas del resto de nodos serán susceptibles de ser considerados maliciosos, y por tanto este número de rutas que atraviesan el nodo monitorizado debería ser un indicativo del ataque.

II Con el fin de calcular el número de rutas citado en el punto anterior deben tenerse en cuenta únicamente aquellas con un *HopCount* mayor que 1. Las rutas con *HopCount* igual a 1 indican nodos vecinos con los que el nodo monitorizado se comunica directamente. Estas rutas se aprenden de forma automática, y no tienen por qué ser publicadas, por lo que no proporcionarán información útil acerca de si un nodo está publicando rutas falsas hacia otros destinos.

III Sin embargo, estas últimas rutas (*HopCount igual a 1*) sí pueden ser utilizadas para calcular el número de vecinos con los que se comunica directamente el nodo en cuestión, es decir, proporcionan información sobre la densidad de nodos en el área en la que se encuentra éste. Si un nodo se encuentra en un área con una alta densidad, es probable que lo atraviesen gran cantidad de rutas legítimas. Sin embargo, un nodo que se encuentre en una zona geográfica poco densa pero por el que pasen muchas rutas podría referirse a un *sinkhole*.

IV Los nodos *sinkhole* intentan ser seleccionados publicando que poseen la ruta más reciente. Para asegurarse de que son elegidos por el resto de nodos emplean números de secuencia bastante más elevados que los recibidos en las peticiones, evitando que se prioricen otras posibles respuestas legítimas. Así, el parámetro *NumSeq* de las rutas que atraviesen un nodo *sinkhole* presumiblemente será alto. Por tanto, éste número de secuencia deberá pesar positivamente en el cálculo del indicador.

V Del mismo modo, los nodos *sinkhole* también suelen indicar que poseen una ruta óptima hacia el destino, es decir, indican que pueden alcanzar cualquier destino en solo un salto. En consecuencia, el valor del *HopCount* en aquellas rutas que pasen por los nodos maliciosos será en la mayoría de las ocasiones igual a 2. Valores pequeños de *HopCount* indicarán una mayor probabilidad de tratarse de un nodo malicioso.

En consecuencia con lo anterior, las características básicas involucradas en la obtención del indicador para un nodo dado, *i*, serán las siguientes:

- $\#Rt_i$: número de rutas existentes en las tablas de rutas del resto de nodos que emplean al nodo *i* como el siguiente salto. Sólo se tienen en cuenta aquellas entradas cuyo estado sea válido y con un valor de *HopCount* superior a 1.
- $\#RtV_i$: número de entradas en la tabla de rutas del nodo *i* con *HopCount* igual a 1, es decir, el número de rutas hacia nodos vecinos. Sólo se tienen en cuenta aquellas entradas cuyo estado sea válido.
- $HC_{Rt,i}$: distancia, medida en número de saltos, a la que se encuentra el nodo destino si se emplea la ruta *Rt* que atraviesa el nodo *i*.
- $NS_{Rt,i}$: número de secuencia obtenido para la ruta *Rt* que atraviesa el nodo *i*.

La extracción de estos parámetros sigue un procedimiento temporal, es decir, cada uno de ellos se obtiene en ventanas temporales no solapadas, *w*, de T segundos de duración para cada nodo *i* en la red.

Teniendo en cuenta las hipótesis previas y las características básicas previamente indicadas ($\#Rt$, $\#RtV$, HC_{Rt} y NS_{Rt}) se puede aplicar una heurística que permitirá la obtención del indicador pretendido acerca del comportamiento de un nodo dado como posible nodo malicioso *sinkhole* o no. Dicha heurística es como sigue:

Heurística:
El indicador para un nodo *i* como nodo *sinkhole* dado se obtiene como la suma de todas las rutas Rt_i de más de un salto que atraviesan el nodo *i*. Cada ruta Rt_i es ponderada positivamente por su número de secuencia, $NS_{Rt,i}$ y negativamente por el cuadrado del número de saltos hacia el destino, $HC_{Rt,i}$. De forma matemática se expresa como:

$$Ind_i = \sum_{n=1}^{\#Rt_i} \frac{NS_{n,i}}{(HC_{n,i})^2} \quad (1)$$

A su vez, dicho valor será normalizado por el número de vecinos del nodo *i*, que se calcula de la siguiente forma:

$$N_{vec,i} = \#RtV_i \quad (2)$$

De esta forma, el valor indicador final acerca del comportamiento de un nodo *i* se obtiene como:

$$Ind_{comp,i} = \frac{Ind_i}{N_{vec,i}} \quad (3)$$

La descripción detallada del proceso de cálculo del indicador se muestra en el Algoritmo siguiente:

Algoritmo 1 Pseudo código para la obtención de Ind_{comp}.

```
for w=1 hasta el nº de ventanas do
    for i=1 hasta el nº de nodos en la red do
        Obtener #Rt_i(w), #RtV_i(w), HC_{Rt,i}(w) y NS_{Rt,i}(w)
        Estimar Ind_i(w) con (1).
        Calcular el nº de vecinos N_{vec,i}(w) usando (2).
        Obtener el indicador Ind_{norm,i}(w) con (3).
    end for
end for
```

Como puede observarse, el cómputo del indicador del comportamiento para cada nodo es un proceso sencillo y de bajo costo una vez que se ha recopilado toda la información relativa a las rutas de los nodos.

V. RESULTADOS EXPERIMENTALES

En esta sección se presenta primero el entorno experimental utilizado para evaluar el esquema propuesto. Además, se han realizado algunos tests con el objetivo de verificar el correcto funcionamiento del mismo, discutiéndose los resultados experimentales obtenidos.

A. Entorno de Experimentación

En este trabajo se ha utilizado el simulador de redes OMNeT++ [11] para analizar una serie de entornos MANET. Los parámetros comunes a todos los escenarios son los explicados a continuación.

Para simular los nodos maliciosos se ha utilizado el *framework* NETA [12], construido sobre OMNeT++, y que permite la simulación de ataques de forma rápida y sencilla, pudiendo aplicarse distintos parámetros de configuración sobre éstos.

El área de simulación se restringe a un cuadrado de 1000 x 1000 metros. Cada nodo tiene una cobertura de 250 metros. El tiempo de simulación se fija a 50 segundos.

Como protocolos MAC (*Medium Access Control*) y de *routing* se han elegido 802.11g y AODV, respectivamente, así como el mecanismo RTS/CTS para el envío de paquetes. Esta última asunción es coherente, pues el no emplear la detección por portadora virtual en escenarios de movilidad podría implicar un gran número de colisiones debido al problema de la estación oculta (*hidden station*).

El número total de nodos es de 25, siendo uno de ellos un nodo atacante de tipo *sinkhole*. El ataque *sinkhole* es ejecutado durante todo el tiempo de la simulación, y su correspondiente *tasa de ataque* está fijada al 100%, refiriéndose esta tasa a la probabilidad de que un nodo atacante realice el ataque. En este caso el nodo *sinkhole* siempre responde con mensajes RREP falsos a las solictudes RREQ, incluso aunque no conozca una ruta válida. Asimismo, los paquetes RREP falsos enviados por el atacante tienen fijado el *HopCount* a 1, indicando que el nodo malicioso siempre alcanza el destino de la comunicación en un único salto. Los nodos atacantes también generan un falso número de secuencia siguiendo una distribución uniforme entre 20 y 30. Dicho valor se suma al número de secuencia observado en la solicitud RREQ, dando como resultado un valor más elevado que el que pueda encontrarse en otras respuestas legítimas.

El número de flujos con tráfico a nivel de aplicación está fijado a 21. Cada flujo consiste en una conexión CBR (*Constant BitRate*) con una tasa de envío de 4 paquetes/segundo, teniendo cada paquete un *payload* de 512 *bytes*. Para cada flujo, la dirección destino es elegida aleatoriamente entre todos los nodos legítimos, manteniéndose el mismo destino durante todo el tiempo de la simulación. Los flujos comienzan de forma aleatoria entre 0,5 y 1,5 segundos y terminan entre 47 y 48 segundos.

Se utiliza el modelo RWP (*Random WayPoint*) para simular el movimiento de los nodos. La velocidad mínima es fija a 1 m/s y la velocidad máxima a 10 m/s, con un tiempo de pausa de 10 segundos, es decir, cuando el nodo alcanza el destino deseado, espera durante el tiempo de pausa antes de elegir un nuevo destino y repetir el proceso.

La duración de la ventana temporal w usada para la recopilación de las características es de T=1 segundo.

B. Indicadores del Ataque Sinkhole

Es necesario recordar que en el presente trabajo no presenta un sistema de detección como tal, sino que se discute un valor indicador a refinar con el fin de poder ser empleado por un IDS real. La principal diferencia reside en cómo se debe realizar la recopilación de la información por parte del IDS en un entorno real. Así, en esta subsección se intenta demostrar de forma gráfica la efectividad del indicador propuesto mediante una serie de pruebas experimentales basadas en simulaciones.

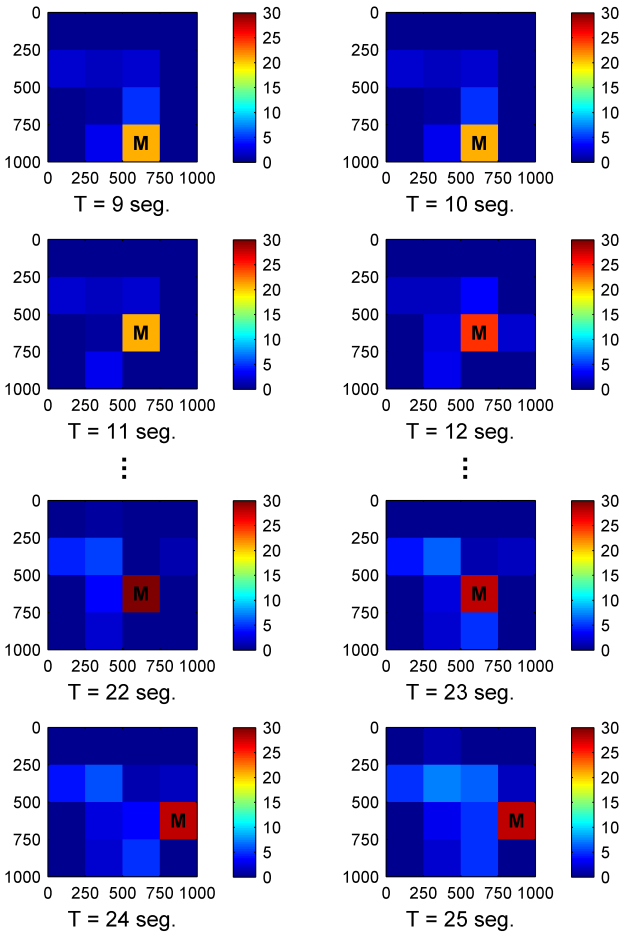


Fig. 3: Indicador del ataque *sinkhole* por cada celda e instante temporal.

Para ello, se podría suponer la existencia de una red *backbone* de nodos monitores confiables y con mayores capacidades, que recopilan la información de los nodos de su vecindad [13]. Estos nodos monitores se encuentran geográficamente distribuidos de forma uniforme en forma de malla, cubriéndose entre ellos todo el área de interés. Así, es posible mediante esta red *backbone* obtener el indicador propuesto para cada nodo, asi como su pertenencia a una determinada celda de cobertura.

Para visualizar de forma grafica cómo el indicador puede ayudar en el proceso de detección de un nodo *sinkhole*, se determina para cada celda *Cell* el indicador de cada uno de los nodos pertenecientes a la misma. De entre estos indicadores, el valor representativo para la celda en cuestión será el máximo de los obtenidos. Matemáticamente se puede expresar cómo:

$$Ind_{Cell} = \max_{i \in Cell} (Ind_{comp,i}) \quad (4)$$

La Figura 3 muestra de forma gráfica el valor obtenido para las todas las celdas en distintos instantes temporales en un escenario aleatorio. La celda en la que se encuentra el nodo *sinkhole* dichos instantes está marcada con la letra **M**.

De esta forma se puede comprobar que, incluso cuando el nodo malicioso se traslada de una celda a otra, el indicador propuesto destaca por su elevado valor frente a los valores obtenidos en otras celdas. Así, con un rápido vistazo a la gráfica se podría determinar que en una celda dada se están dando valores inusualmente altos del indicador de comportamiento, lo que podría ser un paso previo a una detección en mayor profundidad.

Como se ha visto, es posible verificar que las hipótesis propuestas en la Sección IV sobre las que se basa la obtención del indicador son coherentes y correctas, pues éstas se ven avaladas por los resultados obtenidos.

VI. CONCLUSIONES Y TRABAJO FUTURO

En este trabajo se ha propuesto una nueva metodología para la obtención de indicadores de ataques *sinkhole* en redes MANETs, considerando para ello algunas características de la capa de red, principalmente de las rutas. El esquema desarrollado se basa en una heurística sencilla para estimar un indicador de comportamiento, que podrá ser utilizado como entrada en un posterior sistema IDS para detectar eficientemente aquellos nodos que falsifican los paquetes RREP con la intención de atraer hacia sí el tráfico circundante. Debe indicarse que el empleo de una heurística sencilla reduce la carga computacional presente en otros esquemas más sofisticados basado en técnicas de *data mining*.

Se ha verificado el correcto funcionamiento de nuestro sistema mediante simulación, considerando escenarios de aplicación realistas y analizando una serie de despliegues MANET. Como puede comprobarse, los resultados experimentales obtenidos corroboran las bondades de la métrica propuesta.

Sin embargo, este primer estudio sufre algunas limitaciones que deberán ser tenidas en consideración en trabajos futuros para su mejora. Entre los puntos susceptibles de ser modificados destacan:

- La incorporación de otras características relevantes que proporcionen información más precisa y detallada, lo que presumiblemente mejorará las capacidades del sistema. En esta línea, seria interesante la posible consideración de métricas multi-nivel.
- El desarrollo de un sistema IDS que utilice los indicadores propuestos para realizar un proceso de detección fiable.
- No menos relevante resulta el estudio de la posible confabulación de nodos para la comisión de los ataques, cuestión esta de alta relevancia en los entornos actuales.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el MICINN (Ministerio de Ciencia e Innovación) mediante el proyecto TEC2011-22579.

REFERENCIAS

[1] T. S. Rappaport, A. Annamalai, R. M. Buehrer, and W. H. Tranter, "Wireless Communications: Past Events and a Future Perspective," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 148–161, May 2002.

[2] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad-Hoc Networks," in *Proc. of the Symposium on Applications and the Internet Workshops (SAINT)*, Jan. 2003, pp. 368–373.

[3] P. García-Teodoro, L. Sánchez-Casado, and G. Maciá-Fernández, *Taxonomy and Holistic Detection of Security Attacks in MANETs*. Taylor & Francis Group, 2013, pp. 1–12.

[4] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," *IETF, RFC 3561*, Jul. 2003. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3561.txt

[5] Y. Zhang, W. Lee, and Y. A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *Wireless Networks*, vol. 9, no. 5, pp. 545–556, Sep. 2003.

[6] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies," in *Proc. of 23rd IEEE International Conference on Distributed Computing Systems (ICDCS)*, May 2003, pp. 478–487.

[7] C. Basile, Z. Kalbarczyk, and R. K. Iyer, "Inner-Circle Consistency for Wireless Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 39–55, Jan. 2007.

[8] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," *International Journal of Network Security*, vol. 5, no. 3, pp. 338–346, Nov. 2007.

[9] P. N. Raj and P. B. Swadas, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET," *International Journal of Computer Science Issues*, vol. 2, pp. 54–59, Aug. 2009.

[10] Y. F. Alem and Z. C. Xuan, "Preventing Black Hole Attack in Mobile Ad-Hoc Networks using Anomaly Detection," in *Proc. of 2nd International Conference on Future Computer and Communication (ICFCC)*, vol. 3, May 2010, pp. 672–676.

[11] A. Varga, "OMNeT++ simulator." [Online]. Available: http://www.omnetpp.org/

[12] Network Engineering Security Group (NESG), "NETA: NETwork Attacks Framework for OMNeT++." [Online]. Available: http://nesg.ugr.es/index.php/en/neta

[13] P. Agrawal, R. K. Ghosh, and S. K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks," in *Proc. of the 2nd International Conference on Ubiquitous Information Management and Communication (ICUIMC)*, Jan. 2008, pp. 310–314.

Ocultación de la estación base en redes inalámbricas de sensores

Ruben Rios
Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: ruben@lcc.uma.es

Jorge Cuellar
Siemens Corporate Technology
Múnich, Alemania
Email: jorge.cuellar@siemens.com

Javier Lopez
Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: jlm@lcc.uma.es

***Resumen*—La estación base es el elemento más importante en un red de sensores y, por tanto, es necesario evitar que un atacante pueda hacerse con el control de este valioso dispositivo. Para ello, el atacante puede valerse tanto de técnicas de análisis de tráfico como de la captura de nodos. En este trabajo presentamos un esquema que consta de dos fases, la primera está dedicada a homogeneizar los patrones de tráfico y la segunda encargada de perturbar las tablas de rutas de los nodos. Ambas fases permiten mantener a la estación base fuera del alcance del atacante con un coste computacional insignificante y un consumo energético moderado. La validez de nuestro esquema ha sido validada analíticamente y a través de numerosas simulaciones.**

***Palabras Clave*—Redes de sensores, análisis de tráfico, captura de nodos, seguridad, privacidad de localización.**

I. Introducción

Las redes inalámbricas de sensores (WSNs) [1] son redes ad-hoc compuestas por cientos de pequeños dispositivos inalámbricos (nodos sensores o sensores) alimentados con baterías y capaces de medir ciertas propiedades físicas en su entorno como temperatura, humedad o radiación. Estas mediciones son luego enviadas a un dispositivo, llamado estación base, que se encarga de procesar y analizar los datos recolectados.

Dado que las WSNs se encuentran limitadas en términos de consumo energético, los sensores se valen de sus vecinos para hacer llegar sus mediciones a la estación base. Asimismo, para prolongar aún más el tiempo de vida de la red, los paquetes suelen enviarse utilizando el menor número de intermediarios posible, lo que da lugar a marcados patrones de tráfico (véase Fig. 1). Esto hace que un atacante que se limite a observar el número de paquetes enviados y recibidos en su entorno puede determinar información sensible sobre la red a pesar de que el contenido de los paquetes se encuentre debidamente protegido mediante técnicas criptográficas. En particular, el atacante puede distinguir entre los nodos que generan tráfico, los nodos a los que está destinado y los nodos que sirven de meros intermediarios.

El origen del problema es inherente a las redes de sensores y radica en su particular modelo de comunicación. Supongamos, por ejemplo, que un grupo de biólogos decide desplegar una red de sensores acuáticos para monitorizar el comportamiento y paso de cetáceos por las aguas de un determinado país. La información recopilada por la red es enviada a la estación base que se encuentra abordo de un barco donde los investigadores estudian los datos. En este escenario, existen dos tipos de atacantes que podrían estar interesados en identificar bien el origen o bien el destino de los mensajes. Los atacantes interesados en localizar los nodos origen podrían ser

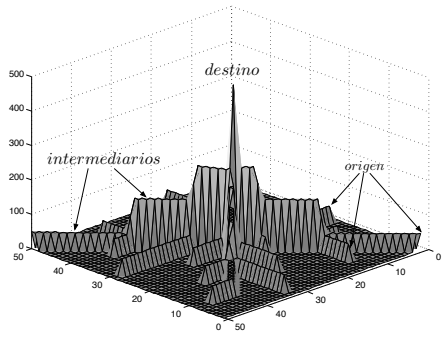


Fig. 1. Tasa de envío en una WSN con 15 emisores

pescadores furtivos porque este tipo de sensor les conduce directamente al cetáceo. Por otra parte, para un grupo de piratas sería atractivo determinar la localización de la estación base ya que esto supondría encontrar el barco. El primer tipo de atacante utilizaría el ángulo de llegada de los paquetes para avanzar hacia el nodo que envía un paquete. Repitiendo este proceso a cada salto, el atacante sería capaz de alcanzar el origen de la comunicación. El segundo tipo de atacante puede valerse de técnicas de monitorización de la tasa de envío y tiempo de envío de paquetes entre vecinos ya que esta información le indica la dirección en la que se encuentra la estación base.

Hasta la fecha los esfuerzos de investigación se han centrado en contrarrestar al primer tipo de atacante [2], [3], [4] mientras que el segundo tipo de atacante ha recibido menos atención [5], [6]. Además, la mayoría de soluciones propuestas para proteger a la estación base son demasiado costosas desde un punto de vista energético o son incapaces de proporcionar un nivel de protección suficiente. Por último es interesante resaltar que un atacante capaz de capturar nodos y obtener sus tablas de rutas daría al traste con los mecanismos de protección propuestos por estas soluciones ya que las tablas de rutas contienen información acerca de la dirección hacia la estación base.

En este trabajo proponemos un protocolo capaz de proteger la localización a la estación base frente a atacantes que realizan análisis de tráfico así como de atacantes capaces de capturar nodos. El protocolo consta de dos esquemas complementarios, uno dedicado a la homogeneización de los patrones de tráfico y el otro a la perturbación de las tablas de rutas de los nodos de manera que estas sean lo suficientemente correctas como para que los paquetes lleguen

al destino y al mismo tiempo oculten la dirección hacia la estación base. A nuestro entender este protocolo es el primero en proporcionar una solución unificada capaz de hacer frente a ambas amenazas.

La organización del trabajo es la siguiente. En la Sec. II hacemos un repaso de las soluciones existentes en la literatura que abordan el problema de la ocultación de la estación base. La Sec. III está dedicada a presentar de manera detallada las características de la red de sensores así como las habilidades de los distintos modelos de atacante considerados en este trabajo. Seguidamente, en la Sec. IV, presentamos una visión general de la solución y los pormenores de los esquemas que la integran. La Sec. V está dedicada a la evaluación de la solución tanto desde el punto de vista de la sobrecarga que introduce en la red como desde el punto de vista del nivel de protección que proporciona. Finalmente, en la Sec. VI se presentan las conclusiones y se esbozan posibles lineas de trabajo futuro.

II. Trabajos relacionados

En [7], [5] se proponen varias técnicas de balanceo del tráfico para solventar el problema de localización de la estación base. En concreto, se presenta un protocolo de encaminamiento en el que a cada salto los nodos envían los paquetes a un nodo arbitrario de entre los más cercanos a la estación base. De esta forma se evita que siempre sean los mismos nodos los que reciben los paquetes, pero el nivel de protección proporcionado es insuficiente. Para tratar de mejorar la solución se propone el envío de paquetes falsos[1] en rutas aleatorias de manera ocasional.

La creación de zonas que reciben un alto volumen de tráfico falso [5], [6] es otra de las técnicas utilizadas para distraer a posibles atacantes. Sin embargo, este tipo de soluciones no sólo requiere una elevada tasa de mensajes sino que además es sólo una medida temporal ya que una vez que el atacante alcanza la zona, la puede descartar. También en [8] se utiliza una gran cantidad de paquetes falsos para hacer que todos los nodos de la red envíen siempre el mismo número de paquetes independientemente de su distancia a la estación base. Esta estrategia es muy costosa ya que implica que todos los nodos de la red estén constantemente generando tráfico falso. Otros trabajos [9] utilizan un enfoque distinto y se basan en que la estación base se comporte como un nodo ordinario o la mueven a otra posición aparentemente más segura. Sin embargo, no siempre es posible mover a la estación base ni sencillo determinar si la nueva posición será realmente segura.

Jian et al. [10] proponen un esquema parecido al nuestro en cuanto a las técnicas de prevención de análisis de tráfico. Su solución se basa, al igual que la nuestra, en enviar los paquetes de datos usando un *biased random walk* (camino aleatorio sesgado) que tratan de ocultar con el envío de paquetes falsos en el sentido contrario con cierta probabilidad. Sin embargo, en ocasiones el atacante puede determinar cuando un paquete es falso y, por tanto, es capaz de obtener la dirección hacia la estación base.

En una versión preliminar de este trabajo [11] conseguimos solucionar algunos de los problemas presentes en trabajos anteriores. Esta nueva versión introduce además un mecanismo de protección capaz de soportar ataques de captura de nodos. Ninguno de los trabajos anteriores había considerado esta amenaza como un problema para la ocultación de la estación base.

[1]Distinguimos entre paquetes (reales) de datos y paquetes (falsos) que contienen basura y cuyo único cometido es despistar al atacante.

III. Descripción del problema

En esta sección presentamos de manera detallada las características de la red así como los modelos de atacante considerados en el resto del artículo.

A. Modelo de red

En este trabajo consideramos WSNs compuestas por un gran número de sensores y una única estación base. Se trata de una red dedicada a la monitorización de eventos y, por tanto, tan pronto como se detecta un fenómeno de interés se envía un mensaje a la estación base.

Asumimos que la conectividad de la red es elevada y que cada nodo conoce a todos sus vecinos gracias a un protocolo de descubrimiento de rutas. Esto permite a los nodos construir sus tablas de rutas de forma que los vecinos que se encuentran más arriba en la tabla son los nodos más próximos a la estación base. En concreto cada nodo puede tener tres tipos de vecinos según su distancia a la estación base: más cercanos, a la misma distancia, o más alejados. Nos referiremos a cada uno de estos grupos como $L^{\mathcal{C}}$, $L^{\mathcal{E}}$ y $L^{\mathcal{F}}$ respectivamente.

Además, supondremos que los nodos comparten claves criptográficas con sus vecinos que les permiten ocultar el contenido de los paquetes. Por tanto, los mensajes con datos reales serán indistinguibles de mensajes falsos.

Finalmente, supondremos que la distancia entre nodos es lo suficientemente amplia como para evitar que el atacante puede observar todas las comunicaciones de manera simultánea. A continuación se dan más detalles sobre las capacidades y estrategias del atacante.

B. Modelo de atacante

El modelo de atacante considerado es capaz de realizar tanto ataques pasivos (análisis de tráfico) como activos (captura de nodos). En ambos casos se trata de un atacante con un ámbito de actuación local y capaz de desplazarse de una lugar a otro de la red.

El rango de acción del atacante *pasivo* viene determinado por el número de nodos que puede observar de manera simultánea. De esta forma, podemos definir $\mathcal{ADV}_n$ como aquel capaz de observar las transmisiones de todos los nodos a distancia menor o igual que n. En general, en la literatura se considera un atacante $\mathcal{ADV}_1$, que tiene un alcance similar al de un nodo ordinario. Tras observar las comunicaciones en su entorno el atacante decide moverse hacia otro nodo que le permita reducir su distancia hasta el destino. Esta decisión depende de si el atacante opta por un ataque por correlación de tiempos o un ataque por volumen de tráfico.

En el ataque por correlación de tiempos (time-correlation) se observa el tiempo de envío de paquetes de un nodo y sus vecinos. Dado que un nodo reenvía un paquete inmediatamente después de recibirlo, el atacante puede deducir la dirección hacia la estación base. El ataque por volumen de tráfico (rate-monitoring) se basa en que la tasa de envío de los nodos más cercanos a la estación base es mayor. El atacante se mueve hacia aquellos nodos con mayor tasa de envío. Es un atacante

menos eficiente ya que requiere hacer varias observaciones antes de tomar la decisión de moverse.

El modelo de atacante *activo* considerado está interesado únicamente en capturar nodos con el fin de obtener sus tablas de rutas ya que con ellas puede determinar qué vecinos del nodo se encuentran más cercanos a la estación base. Tras realizar varias capturas el atacante obtiene información fiel sobre la dirección a seguir para encontrar su objetivo. En la literatura no existe una estrategia de captura claramente definida para la protección de la estación base. Sin embargo, es posible encontrar varios trabajos [12], [13] dedicados al modelado y mitigación de estos ataques durante la distribución de claves. Algunos autores consideran la captura aleatoria de nodos mientras que otros optan por la captura de (algunos o todos) los nodos en una región. En este trabajo consideramos que el atacante es más exitoso si centra su esfuerzo en una región y avanza según la información obtenida. Nótese, que dado el esfuerzo que supone un ataque de este tipo, el atacante sólo podrá comprometer un número reducido de nodos.

IV. Esquema de ocultación

Nuestro esquema de ocultación consta básicamente de dos elementos complementarios que tienen como objetivo alterar los patrones de tráfico y las tablas de rutas de los nodos.

A. Visión general

El protocolo de transmisión consiste básicamente en un *biased random walk* que es ocultado con cantidades controladas de tráfico falso. Ante la recepción de un paquete de datos, el nodo reenvía este paquete hacia la estación base con cierta probabilidad sesgada. Por cada paquete de datos se genera un paquete falso que oculta la dirección del flujo de paquetes reales y la tasa de paquetes reales enviados por cada vecino. De esta forma se homogeneiza localmente el tráfico sin introducir un retraso excesivo en la llegada de paquetes a la estación base.

El algoritmo de perturbación consiste en reordenar la tabla de rutas de cada nodo para que si un atacante tiene acceso a ésta no sea capaz de alcanzar fácilmente la estación base al tener la certeza de que los nodos más próximos se encuentran más altos en la tabla. El nivel de perturbación de la tabla introduce incertidumbre en el atacante pero al mismo tiempo repercute negativamente en el tiempo de llegada de los paquetes.

B. Protocolo de transmisión

El protocolo de transmisión debe cumplir una una serie de propiedades para garantizar la seguridad y usabilidad del sistema. Debemos asegurar que los paquetes de datos alcanzan su destino (Prop. 1) al mismo tiempo que la tasa de envío de paquetes se distribuye uniformemente entre los vecinos (Prop. 2). Finalmente, dado que nuestro protocolo envía parejas de mensajes, la Prop. 3 garantiza que cada uno de estos se envía a un nodo diferente.

Propiedad 1 (Convergencia)**.** *Sea x un nodo arbitrario y BS la estación base. Sea también $neigh(n)$ el conjunto de vecinos de un nodo n. Entonces se dice que el camino es convergente si x elige al siguiente nodo $x' \in neigh(x)$ tal que:*

$$E(dist(x', BS)) < E(dist(x, BS))$$

Algorithm 1 Protocolo de transmisión

Input: $packet \leftarrow receive()$
Input: $combs \leftarrow combinations(sort(neighs), 2)$
Input: $FAKE\_TTL$
1: $\{neigh1, neigh2\} \leftarrow select\_random(combs)$
2: **if** $isreal(packet)$ **then**
3: $send\_random(neigh1, packet, neigh2, fake(FAKE\_TTL))$
4: **else**
5: $TTL \leftarrow get\_time\_to\_live(packet) - 1$
6: **if** $TTL > 0$ **then**
7: $send\_random(neigh1, fake(TTL), neigh2, fake(TTL))$
8: **end if**
9: **end if**

donde E representa el valor esperado y $dist$ es una función de la distancia entre dos nodos.

Propiedad 2 (Homogeneidad)**.** *Sea x un nodo arbitrario y $neigh(n)$ el conjunto de vecinos de un nodo n. Se dice que una transmisión del nodo x mantiene la propiedad de homogeneidad si:*

$$\forall y, z \in neigh(x) \quad Frec_m(x, y) \simeq Frec_m(x, z)$$

donde $Frec_m(x, y)$ representa el total de mensajes enviados por x a y.

Propiedad 3 (Exclusión)**.** *Sean m y m' un par de mensajes y t un tiempo de transmisión determinado. Denotemos $send(m, x, y, t)$ al hecho de transmitir el mensaje m de x a y en el instante t. La propiedad de exclusión establece:*

$$\forall m, m', x, y, t \; send(m, x, y, t) \; \wedge \; m \neq m' \Rightarrow \neg send(m', x, y, t)$$

Dado que cada transmisión consta de dos paquetes, las combinaciones sin repetición de dos elementos de la tabla de rutas es un mecanismo ligero capaz de conseguir una pareja de destinatarios de manera consistente con lo establecido por la Prop. 3. Además, si las tablas están ordenadas (i.e., $[L^{\mathcal{C}}, L^{\mathcal{E}}, L^{\mathcal{F}}]$) se consigue que, con alta probabilidad, el primer elemento de la combinación sea un nodo más próximo a la estación base. Por tanto, si el paquete real lo mandamos al primer vecino y el falso al segundo, estaremos satisfaciendo la propiedad Prop. 1. Finalmente, la Prop. 2 se mantiene si, de entre todas las combinaciones generadas, cada vez se elige una de manera aleatoria.

En Alg. 1 se muestra de manera programática el comportamiento de nuestro protocolo de transmisión. Los argumentos de entrada al algoritmo son el paquete a reenviar, las combinaciones sin repetición de la tabla de rutas ordenada y el parámetro $FAKE\_TTL$, que controla el tiempo de vida de los mensajes falsos en la red y que depende del rango de escucha del adversario. Cuando un nodo recibe un paquete real, se elige una combinación aleatoria de dos vecinos que recibirán el mensaje real y uno falso (líneas 1 a 3). El mensaje falso se reenviará durante $FAKE\_TTL$ saltos. Si el paquete recibido es un paquete falso aún vigente, se reduce su tiempo de vida y se envían dos mensajes falsos (líneas 5 a 7). Además, las parejas de paquetes se envían en un orden aleatorio para evitar que el atacante puede determinar de forma trivial cuál de los paquetes es el real.

C. Perturbación de tablas

Mantener el orden de las tablas de rutas es fundamental para el correcto funcionamiento de nuestro protocolo de transmisión. Sin embargo, esto puede permitir a un atacante determinar qué vecinos se encuentran más próximos a la estación base con solo capturar el nodo y obtener su tabla de rutas. Por ello, es fundamental crear cierta incertidumbre aunque esto conlleve un aumento en el tiempo de entrega de los paquetes.

Definición 1 (Tabla de rutas)**.** *Sea $L^* = L^{\mathcal{C}} \cup L^{\mathcal{E}} \cup L^{\mathcal{F}}$ la lista de todos los vecinos de un nodo n, donde*
$L^{\mathcal{C}} = \{c_1, c_2, c_3, \ldots\}$ son los vecinos más cercanos,
$L^{\mathcal{E}} = \{e_1, e_2, e_3, \ldots\}$ son los vecinos a igual distancia, y
$L^{\mathcal{F}} = \{f_1, f_2, f_3, \ldots\}$ son los vecinos más alejados.

Una tabla de rutas es una biyección $r : \{N-1, \ldots, 1, 0\} \rightarrow L^*$, donde N es el número total de vecinos.

Es decir, una tabla de rutas es una ordenación concreta de los vecinos de un nodo. De manera similar, podemos definir $pos : L^* \rightarrow \{N-1, \ldots, 1, 0\}$ como la inversa de r, de manera que, dado un vecino particular, pos devuelve la posición que éste ocupa en la tabla.

En este punto podemos estudiar bajo qué circunstancias una tabla de rutas está correctamente sesgada (*biased*), esto es, qué ordenaciones permiten la llegada de los paquetes de datos a la estación base.

Teorema 1. *Una tabla de rutas está correctamente sesgada sii* $\sum_{n \in L^{\mathcal{C}}} pos(n) > \sum_{n \in L^{\mathcal{F}}} pos(n)$

En otras palabras, la tabla cumple la propiedad si y sólo si $\mathbb{P}(n_1 \in L^{\mathcal{C}}) > \mathbb{P}(n_1 \in L^{\mathcal{F}})$. Es decir, si al elegir una combinación, la probabilidad de mandar el paquete real a un nodo más próximo a la estación base es mayor que la probabilidad de mandarlo a un nodo más alejado estamos ante una tabla correctamente sesgada.

Demostración:

Asumamos que elegimos aleatoriamente una dupla (n_1, n_2) de vecinos tal que $pos(n_1) > pos(n_2)$. La probabilidad de que n_1 pertenezca al subconjunto $L \subseteq L^*$ viene dada por:

$$\mathbb{P}(n_1 \in L) = \frac{1}{C} \sum_{n \in L} pos(n) \qquad (1)$$

donde $C = N * (N-1)/2$ es el total de combinaciones sin repetición de dos elementos de L^*.

Ahora, si escribimos como una lista de duplas todas las combinaciones como una lista de duplas ordenada lexicográficamente, tenemos:

(r(N-1), r(N-2)),	(r(N-1), r(N-3)),	(r(N-1), r(N-4)),	...,	(r(N-1), r(0))
	(r(N-2), r(N-3)),	(r(N-2), r(N-4)),	...,	(r(N-2), r(0))
		(r(N-3), r(N-4)),	...,	(r(N-3), r(0))
				...
				(r(1), r(0))

Observamos que el primer vecino, $r(N-1)$, aparece como primer elemento en $N-1$ duplas, el segundo, $r(N-2)$, en $N-2$, y así sucesivamente. En concreto, el número de veces que un nodo aparece como primer elemento es exactamente la posición que ocupa en la tabla. Con lo que tenemos $(N-1) + (N-2) + (N-3) + \ldots + 1 = C$ duplas.

Algorithm 2 Algoritmo de perturbación

Input: $br \leftarrow \{L^{\mathcal{C}}, L^{\mathcal{E}}, L^{\mathcal{F}}\}$
Input: $bias$, MAX_ITER
1: $E \leftarrow energy(bias, br)$
2: $i \leftarrow 0$
3: **while** $(i < MAX\_ITER) \wedge (E \neq 0)$ **do**
4: $\quad br' \leftarrow swap(br)$
5: $\quad E' \leftarrow energy(bias, br')$
6: $\quad$ **if** $(E' < E)$ **then**
7: $\quad\quad br \leftarrow br'$
8: $\quad\quad E \leftarrow E'$
9: $\quad$ **end if**
10: $\quad i \leftarrow i + 1$
11: **end while**
12: **return** br

Si elegimos cualquier dupla (n_1, n_2) tal que $pos(n_1) > pos(n_2)$, esto equivale a elegir cualquier dupla de la lista anterior. Por tanto, la probabilidad de que un nodo n_1 aparezca como primer elemento de la dupla equivale al número total de elementos en r que se encuentran por debajo de n_1 dividido por el total de combinaciones. Esto es exactamente $pos(n_1)/C$, de donde la Ec. 1 se deduce directamente. ■

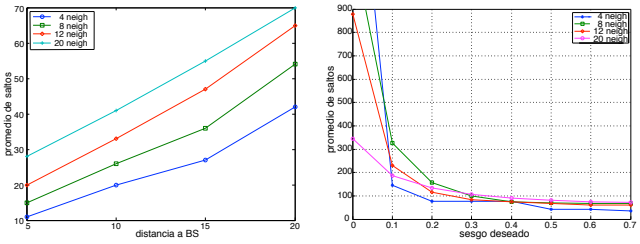
Finalmente, es necesario cuantificar el sesgo de una tabla de rutas, $bias(r) \in [-1, 1]$, ya que es un indicador del tiempo de llegada de los paquetes a la estación base. Cuanto más próximo a 1 más probable es que el siguiente nodo de la ruta se encuentre más próximo a la estación base, mientras que valores próximos a -1 indican que el siguiente nodo se encontrará más alejado. Formalmente puede calcularse como:

$$bias(r) = \frac{1}{C}\left(\sum_{n \in L^{\mathcal{C}}} pos(n) - \sum_{n \in L^{\mathcal{F}}} pos(n)\right) \qquad (2)$$

Es sencillo comprobar que si $L^* \equiv L^{\mathcal{F}}$, entonces $bias(r) = -1$ ya que $\sum_{n \in L^{\mathcal{F}}} pos(n) = C$. Del mismo modo, si $L^* \equiv L^{\mathcal{C}}$, entonces $bias(r) = 1$.

Nuestro algoritmo de perturbación recibirá como parámetros un valor de sesgo deseado y una tabla de rutas, y devolverá la tabla reordenada conforme al sesgo dado. En Alg. 2 puede observarse que hemos modelado este algoritmo como un problema de optimización donde la función objetivo (línea 1) depende del valor de sesgo deseado y la ordenación actual de la tabla. En concreto, el algoritmo se inspira en estrategias evolutivas donde intercambiamos dos elementos de la tabla de rutas (línea 4) y comprobamos si así se reduce la distancia al sesgo deseado (línea 6). El proceso se repite por un número máximo de iteraciones o bien hasta que se genere una ordenación acorde al sesgo.

La principal ventaja de utilizar este tipo de estrategia frente a un algoritmo de búsqueda determinista se encuentra en el tiempo necesario para encontrar una solución (seudo-) óptima al problema, que dependiendo del tamaño del espacio de búsqueda puede diferir varios órdenes de magnitud. Sin embargo, su principal desventaja es que, al contrario de los algoritmos deterministas, este tipo de algoritmos puede no encontrar la solución óptima al problema, aunque converge a ella. Nótese, que la perturbación introducida es difícilmente reversible si el valor de sesgo no es conocido, más aún cuando el algoritmo es no determinista.



(a) Numero esperado de saltos (b) Impacto del sesgo

Fig. 2. Tiempo de entrega de paquetes

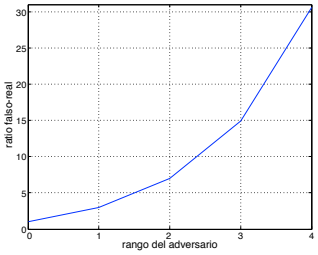
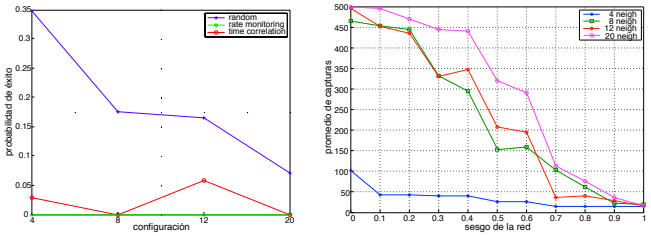


Fig. 3. Ratio de tráfico falso



(a) Ataques de análisis de tráfico (b) Ataques de captura de nodos

Fig. 4. Tasa de éxito de diferentes adversarios

V. Evaluación

En esta sección se evalúa la viabilidad de nuestra solución en relación a la sobrecarga que introduce y al nivel de protección que proporciona frente a distintos modelos de atacante. Las simulaciones se han realizado con MatLab sobre cuatro configuraciones de red en la que variamos el radio de transmisión para conseguir un número promedio de vecinos (4, 8, 12 y 20) diferente por cada nodo.

A. Impacto sobre el tiempo de llegada

La naturaleza probabilística de nuestro protocolo de transmisión influye sobre el tiempo de llegada de los datos a la estación base. En particular, nuestro protocolo puede modelarse como un *biased random walk* donde las probabilidades de enviar hacia la estación base depende del número de vecinos de cada tipo que tenga el nodo.

En la Fig. 2 mostramos el número esperado de saltos para las cuatro configuraciones. En concreto, la Fig. 2a presenta los resultados para nodos origen situados a diferentes distancias (5, 10, 15 y 20 saltos) de la estación base. Como era de esperar, a mayor distancia y mayor conectividad de los nodos, mayor es el número esperado de saltos. Sin embargo, es interesante observar que la velocidad de entrega de los paquetes disminuye cuando los paquetes se acercan a su destino. Esto se debe a que en las proximidades de la estación base hay un mayor número de vecinos $L^{\mathcal{F}}$.

En la Fig. 2b se muestra el impacto que tiene el algoritmo de perturbación sobre el tiempo de entrega. En este experimento todos los nodos están situados a distancia 20. Observamos que a medida que el sesgo se aproxima a cero el tiempo de entrega aumenta siendo este aumento considerablemente mayor para configuraciones con un menor número de vecinos. Esto se debe a que las configuraciones con menos vecinos tienen menos formas de modificar las tablas de rutas. En concreto, cuando el sesgo deseado es cero, el sesgo promedio de la red para la configuración de cuatro vecinos es ligeramente inferior a cero, mientras que para la configuración de veinte vecinos el sesgo promedio está próximo a 0.1. En general, para un sesgo superior a 0.2 la longitud media de los caminos es inferior a 100 saltos.

B. Sobrecarga de tráfico falso

Nuestro protocolo de transmisión se basa en el envío de paquetes falsos para ocultar el flujo de tráfico real. Sin embargo, es necesario controlar la propagación de estos paquetes para evitar el consumo excesivo de energía. Para ello definimos un parámetro, $FAKE\_TTL$, cuyo valor depende del rango de escucha del atacante y que limita el número de paquetes falsos generados.

En la Fig. 3 mostramos el ratio de mensaje falsos frente al tráfico real dependiendo del rango de escucha del atacante. Cuando el adversario sólo escucha los paquetes en su entorno inmediato, $\mathcal{ADV}_0$, el ratio es 1 porque cada mensaje real va acompañado de un mensaje falso que no vuelve a propagarse. A medida que el rango de escucha del adversario (n) aumenta, el ratio lo hace en el orden de $\mathcal{O}(2^{n+1})$.

Nótese que el modelo de atacante más usual en la literatura es $\mathcal{ADV}_1$, es decir, aquel con un rango de escucha similar al de un nodo ordinario.

C. Proteccion frente atacantes

Con el fin de validar la robustez de nuestra solución hemos lanzado simulaciones con atacantes que realizan análisis de tráfico o captura de nodos. En la Fig. 4a se muestra como un modelo de atacante que se mueve de manera aleatoria, sin tener en cuenta las comunicaciones, tiene más probabilidades de llegar a la estación base que aquellos que recurren a técnicas de monitorización del tiempo y tasa de envío de paquetes. Además, como era de esperar, su tasa de éxito es mayor en configuraciones con un promedio de vecinos más bajo. Obsérvese que del total de simulaciones lanzadas, el atacante que realiza monitorización de la tasa de envío nunca llega a la estación base mientras que el que realiza correlación de tiempos lo consigue en limitadas ocasiones. Las ocasiones en las que éste localiza a la estación base se debe a que inicialmente se encuentra a distancia 5 y a la naturaleza de nuestro simulador, que es incapaz de determinar exactamente qué paquete es enviado antes. Por tanto, este atacante elige el siguiente salto de forma aleatoria entre los vecinos que envían mensajes.

En la Fig. 4b, el adversario comienza en un punto del extremo de la red y puede capturar hasta 500 nodos para llegar a la estación base. Además, asumimos que el atacante puede moverse al siguiente vecino tras obtener su identificador

aunque en un escenario real puede necesitar capturar a los vecinos del nodo para saber a cuál de ellos corresponde el identificador encontrado. La estrategia del atacante es moverse al primer nodo de la tabla de rutas que ha visitado un menor número de veces para evitar quedar atrapado en bucles. Los resultados muestran que, a medida que el sesgo de la red se acerca a cero, el adversario necesita capturar un mayor número de nodos para llegar a su destino. Sin embargo, un sesgo bajo influye negativamente en el tiempo de llegada de los paquetes a la estación base (ver Sec. V-A). En general, si consideramos que un atacante podría capturar hasta una décima parte de los nodos de la red, sería seguro utilizar un valor de sesgo menor o igual a 0.5. Nótese que el número de nodos de la red es respectivamente de 400, 1600, 1600 y 3600 para las configuraciones de 4, 8, 12 y 20 vecinos, respectivamente.

VI. Conclusiones

En este trabajo hemos presentado un esquema que permite ocultar la localización de la estación base para protegerla así de posibles ataques. Nuestra solución consta de dos esquemas complementarios capaces de hacer frente a atacantes que realizan tanto análisis de tráfico como capturas de nodos de la red. El primer esquema es un protocolo de transmisión que utiliza cantidades moderadas de mensajes falsos para ocultar el flujo de datos. En concreto, el protocolo preserva tres propiedades (convergencia, homogeneidad y exclusión) lo cual garantiza la llegada de paquetes a la estación base al mismo tiempo que interfiere con los ataques de correlación de tiempos y de volumen de tráfico. El segundo esquema se trata de un algoritmo evolutivo que tiene como objetivo perturbar las tablas de rutas de los nodos para evitar que si un atacante es capaz de obtener estas tablas pueda determinar con facilidad en qué sentido avanzar para encontrar la estación base. Este algoritmo de perturbación está regido por un valor de sesgo, que determina la cantidad de perturbación introducida en las tablas. Este valor introduce un compromiso entre el nivel de protección obtenido y el tiempo medio de espera para recibir los paquetes en la estación base.

La viabilidad de nuestra solución has sido validada analíticamente y a través de simulaciones. En concreto, hemos estudiado el impacto que tiene la conectividad de la red sobre la convergencia paquetes y el nivel de protección de la estación base. Además, hemos analizado el tiempo medio de llegada de los paquetes de datos a su destino y la sobrecarga que supone la inyección de mensajes falsos. Finalmente, hemos evaluado el nivel de protección obtenido frente a atacantes capaces de realizar ataques activos y pasivos.

Como trabajo futuro tenemos como objetivo investigar mecanismos para reducir el número de mensajes falsos requerido para proteger a la estación base de atacantes con un amplio rango de escucha. Además, queremos explorar la robustez de nuestro esquema frente a atacantes más inteligentes. Para ello, en primer lugar será necesario definir una serie de estrategias basadas en el conocimiento del adversario acerca de la red y el esquema de protección utilizado. Este tipo de adversario podría modificar su estrategia de ataque dependiendo del contexto. Para hacer frente a este tipo de atacantes puede ser necesario desarrollar nuevos mecanismos de protección más sofisticados que los considerados hasta la fecha. Finalmente, entre nuestros objetivos se encuentra el desarrollar un sistema de protección integral, que al mismo tiempo sea capaz de hacer frente a atacantes interesados en determinar la localización de la estación base y atacantes cuyo objetivo sea obtener la localización de los nodos origen de eventos.

Agradecimientos

Este trabajo ha sido parcialmente financiado por la Comisión Europea a través del proyecto NESSoS (FP7 256890) y el Ministerio de Innovación y Ciencia a través de los proyectos SPRINT (TIN2009-09237) e IOT-SEC (ACI2009-0949). SPRINT está co-financiado con fondos FEDER. El primer autor es becario FPU del Ministerio de Educación.

Referencias

[1] C. Gómez, J. Paradells, and J. E. Caballero, *Sensors Everywhere: Wireless Network Technologies and Solutions*, Fundación Vodafone España, Ed. Fundación Vodafone España, 2010, iSBN 978-84-934740-5-8. [Online]. Available: http://fundacion.vodafone.es/static/fichero/pre_ucm_mgmt_002618.pdf

[2] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy-Constrained Sensor Network Routing," in *2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04)*, 2004, pp. 88–93.

[3] R. Rios and J. Lopez, "Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks," *The Computer Journal*, vol. 54, no. 10, pp. 1603–1615, 2011.

[4] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Statistical Framework for Source Anonymity in Sensor Networks," in *IEEE Global Telecommunications Conference (GLOBECOM 2010)*, 2010, pp. 1 –6.

[5] J. Deng, R. Han, and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Pervasive and Mobile Computing*, vol. 2, no. 2, pp. 159–186, 2006.

[6] S. Chang, Y. Qi, H. Zhu, M. Dong, and K. Ota, "Maelstrom: Receiver-Location Preserving in Wireless Sensor Networks," in *Wireless Algorithms, Systems, and Applications*, ser. LNCS. Springer, 2011, vol. 6843, pp. 190–201.

[7] J. Deng, R. Han, and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," in *1st International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM '05)*, 2005, pp. 113–126.

[8] B. Ying, J. R. Gallardo, D. Makrakis, and H. T. Mouftah, "Concealing of the Sink Location in WSNs by Artificially Homogenizing Traffic Intensity," in *1st International Workshop on Security in Computers, Networking and Communications*, 2011, pp. 1005–1010.

[9] U. Acharya and M. Younis, "Increasing base-station anonymity in wireless sensor networks," *Ad Hoc Networks*, vol. 8, no. 8, pp. 791–809, 2010.

[10] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in *26th IEEE International Conference on Computer Communications (INFOCOM 2007)*, 2007, pp. 1955–1963.

[11] R. Rios, J. Cuellar, and J. Lopez, "Robust Probabilistic Fake Packet Injection for Receiver-Location Privacy in WSN," in *17th European Symposium on Research in Computer Security (ESORICS 2012)*, ser. LNCS, M. Y. S. Foresti and F. Martinelli, Eds., vol. 7459, Springer. Pisa, Italy: Springer, Sept. 2012, pp. 163–180.

[12] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Node Compromise Modeling and its Applications in Sensor Networks," in *12th IEEE Symposium on Computers and Communications (ISCC 2007).*, july 2007, pp. 575 –582.

[13] T. M. Vu, R. Safavi-Naini, and C. Williamson, "Securing wireless sensor networks against large-scale node capture attacks," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 112–123.

NETA: un *Framework* para Simular y Evaluar Ataques en Redes Heterogéneas. MANETs como Caso de Estudio

Leovigildo Sánchez-Casado, Rafael A. Rodríguez-Gómez, Roberto Magán-Carrión, Gabriel Maciá-Fernández
CITIC - Departamento de Teoría de la Señal, Telemática y Comunicaciones,
E.T.S. de Ingeniería Informática y de Telecomunicación, Universidad de Granada
C/Periodista Daniel Saucedo Aranda s/n, E-18071, Granada
{sancale, rodgom, rmagan, gmacia}@ugr.es

***Resumen*—En este trabajo se presenta NETA, un *framework* para la simulación de ataques en redes de comunicación. Se ha desarrollado basándose en el *framework* INET y el simulador OMNeT++, con implementaciones de diferentes protocolos, así como modelos para la movilidad, consumo de batería, errores en el canal, etc. NETA pretende convertirse en una herramienta útil la comunidad investigadora centrada en el campo de la seguridad en redes. Su diseño flexible es apropiado para la implementación y evaluación de multitud de ataques, permitiendo comparar de forma precisa y bajo las mismas condiciones distintas defensas, así como el desarrollo de nuevas técnicas de detección. Como prueba de concepto se han implementado tres ataques diferentes: *dropping*, *delay* y *sinkhole*. Las capacidades de NETA son puestas de manifiesto mediante la evaluación del funcionamiento estos tres ataques frente a distintos despliegues MANET.**

***Palabras Clave*—Simulación de redes; ataques en redes**

I. INTRODUCCIÓN

La seguridad se está convirtiendo en uno de los principales problemas a la hora de desarrollar nuevas tecnologías y servicios en redes de telecomunicaciones. Las técnicas utilizadas por los *hackers* evolucionan constantemente y a gran velocidad hacia nuevas técnicas de ataque y nuevos objetivos [1] [2], dificultando enormemente el desarrollo de mecanismos de defensa.

En este contexto, se han llevado a cabo numerosos esfuerzos por parte de la comunidad investigadora para desarrollar nuevas técnicas de defensa destinadas a frustrar los ataques a la seguridad en redes. El ciclo es casi siempre el mismo: cada vez que se descubre una nueva vulnerabilidad o técnica de ataque, se implementa una prueba de concepto específica, se evalúan las capacidades de dicha técnica y se proponen nuevas técnicas de defensa.

Sin embargo, como resultado de esta metodología de investigación, aunque numerosos investigadores contribuyen con el código fuente de sus ataques, no existen implementaciones de ataques aceptadas por la mayoría de la comunidad investigadora que permitan la comparación de las soluciones propuestas frente a dichos ataques en las mismas condiciones.

Por tanto, sería deseable la existencia de un *framework* común que posibilitase el desarrollo de implementaciones de ataques y de sus respectivas defensas. Así, este *framework* permite combinar la ejecución de todos los ataques implementados, de forma similar a cómo lo haría un *hacker*, así como analizar su impacto en múltiples tecnologías, protocolos y escenarios.

La contribución principal de este trabajo es NETA (*NETwork Attacks*), un *framework* de ataques basado en OMNeT++ que pretende proporcionar un marco base de referencia con el que unificar el desarrollo y simulación de ataques. NETA es extensible y ofrece un alto grado de versatilidad para el desarrollo de nuevos ataques. Su objetivo es minimizar los esfuerzos en el proceso de creación de ataques con el propósito de probar y evaluar distintas soluciones de seguridad, ofreciendo así una herramienta útil para la comunidad investigadora en el campo de la seguridad en redes. NETA está disponible al público para su descarga en `http://nesg.ugr.es/index.php/en/neta`.

El resto del artículo se organiza de la siguiente forma. La Sección II proporciona un análisis del estado del arte, describiéndose distintos simuladores, así como otras propuestas similares a la presentada en este trabajo. La arquitectura general del *framework* se presenta en la Sección III, donde se explican los principales componentes y las reglas de diseño. En la Sección IV se describen los ataques implementados en esta primera versión. La sección V detalla los escenarios de estudio, así como el entorno de experimentación y los resultados obtenidos. Finalmente, la Sección VI expone las conclusiones y líneas de trabajo futuro.

II. TRABAJOS RELACIONADOS

La simulación se usa generalmente con la intención de analizar protocolos y sistemas complejos, ofreciendo de esta forma un buen compromiso entre coste y complejidad [3]. Sin embargo, la elección del mejor simulador no es una tarea sencilla, pues requiere de un estudio previo que considere las distintas ventajas y desventajas de los mismos.

Según [4] y [5], los simuladores más utilizados en el campo de las comunicaciones son: (*i*) OPNET, (*Optimized Network Engineering Tools*), (*ii*) NS-2, (*Network Simulator 2*) y (*iii*) OMNeT++, (*Optical Micro-Networks*). Todos

ellos son simuladores de eventos discretos para redes de comunicaciones heterogéneas con una gran potencia de cómputo. Es destacable la capacidad de OPNET de ejecutar y gestionar de forma concurrente distintos escenarios, así como la gran variedad de protocolos que ofrece NS-2. Sin embargo, OMNeT++ se está convirtiendo en la actualidad en uno de los simuladores más empleados, principalmente debido a la amplia variedad de *frameworks* (INET, MIXIM, etc.) que ofrece, a su gran flexibilidad y a la inclusión de una interfaz gráfica fácil de usar, entre otras muchas ventajas.

En cuanto al diseño y simulación de ataques, los autores generalmente implementan ataques específicos, con el propósito de usarlos para probar propuestas de seguridad, rendimiento de protocolos, etc [6]. Estas implementaciones suelen ser privadas y, por tanto, distintas propuestas de defensa no pueden compararse con la misma implementación del ataque, haciendo que dichas comparativas sean poco precisas y poco fiables.

Los autores de [7] proporcionan un *framework* basado en OMNeT++ para simular patrones de tráfico y ataques de Denegación de Servicio (DoS) sobre redes IP. Sin embargo, sólo implementan un tipo específico de ataque y su propuesta no es extensible a otros tipos de ataques. Otro *framework* de simulación de ataques aplicado a redes de sensores (WSNs) se propone en [8]. Los autores presentan un procedimiento para simular ataques basado en un lenguaje de ataques particular que describe el comportamiento de los mismos. El *framework* parece ser extensible, pero no se encuentra disponible públicamente y no es aplicable a otros entornos distintos de las redes de sensores. Por estas razones, es necesario un *framework* de ataques general, extensible y versátil, que aborde los inconvenientes citados. Como solución, en este trabajo se propone NETA.

III. NETA: UN *FRAMEWORK* PARA LA SIMULACIÓN DE ATAQUES

NETA se ha desarrollado como un *framework* de OMNeT++ construido sobre el *framework* INET. De esta forma, se pretende extender su uso entre la comunidad investigadora siendo OMNeT++ una de las herramientas de simulación más usadas en el ámbito de la simulación de redes de comunicación. Asimismo, NETA se basa en la misma idea que OMNeT++, *i.e.*, módulos que se comunican entre sí mediante el paso de mensajes.

La idea general es desarrollar, en OMNeT++, nuevos nodos que puedan ejecutar ataques, *nodos atacantes*. Para llevar ésto a cabo los ataques se controlan mediante los denominados *controladores de ataque*. Dichos controladores gestionan uno o varios módulos de NETA mediante el envío de *mensajes de control*. Esto mensajes viajan desde los controladores de ataque hacia módulos específicos que previamente han sido modificados para implementar el comportamiento del ataque. Estos módulos se denominan *módulos hackeados*. Para implementar el citado comportamiento, los módulos hackeados heredan o replican el código de módulos de INET que, posteriormente, modifican conveniente para obedecer

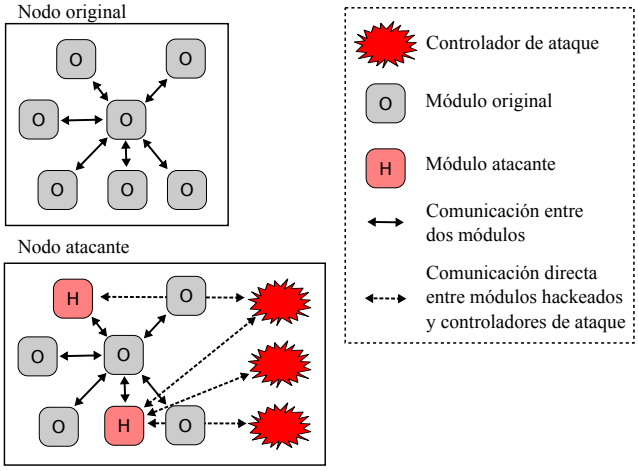


Fig. 1: Esquema comparativo entre un nodo original y el correspondiente nodo atacante en NETA.

las órdenes indicadas por los controladores.

Los principios de diseño del presente *framework* siguen dos reglas principales:

Regla 1: Cualquier framework *base que sea utilizado no debe ser modificado en modo alguno,* e.g.*, cuando se utilizan módulos de INET, éstos deben permanecer como los originales.*

Esta regla pretende facilitar la compatibilidad con futuras versiones de INET y otras implementaciones. Para lograr este objetivo, simplemente se importa la versión más reciente de INET y no se lleva a cabo ninguna modificación sobre ella.

Regla 2: Modificar lo mínimo posible el código original de los módulos hackeados.

Obviamente, para implementar los ataques deseados es necesario realizar modificaciones en el comportamiento de los módulos que se convertirán en módulos *hackeados*. Sin embargo, esta regla pretende minimizar estas modificaciones tanto como sea posible.

Así, la creación de un nodo atacante puede resumirse en los siguientes pasos: (*i*) añadir al archivo `.ned` asociado los controladores relacionados con los ataques a ejecutar, (*ii*) crear los mensajes de control asociados y, (*iii*) sustituir los módulos necesarios por parte de los controladores de ataque por los módulos *hackeados* correspondientes.

La Fig. 1 muestra las diferencias entre un nodo normal y un nodo atacante. El nodo normal se compone de módulos simples y compuestos comunicándose entre sí. El nodo atacante se compone del mismo número de módulos, a los que se añaden los correspondientes controladores. Además, algunos de los módulos originales son reemplazados por los módulos *hackeados* para permitir la ejecución del ataque cuando éste sea iniciado por los controladores de ataque.

A. Arquitectura de NETA

A continuación, se describen los componentes principales de un ataque en nuestro *framework*: (*i*) *controladores de*

ataque, (*ii*) *mensajes de control*, y (*iii*) *módulos hackeados*.

1) Controladores de Ataque: módulos que controlan la ejecución de los ataques. Poseen las siguientes propiedades:

- `attackType`: nombre proporcionado para diferenciar un ataque del resto.
- `active`: indica si el ataque se encuentra o no activo durante la simulación.
- `startTime`: tiempo en el que el ataque comienza en la simulación.
- `endTime`: tiempo en el que cesa el ataque.
- `parámetros específicos de ataque`: diferentes parámetros de configuración que dependen de las funcionalidades específicas del ataque.

El proceso llevado a cabo por un controlador de ataque para un ataque A_i en un nodo atacante puede resumirse en:

1) Obtener los diferentes módulos *hackeados* involucrados en la ejecución del ataque A_i.
2) Activar aquellos módulos *hackeados* en el nodo atacante enviando mensajes de activación que también pueden contener información de configuración.
3) Desactivar los módulos *hackeados* en el nodo atacante enviando un mensaje de desactivación.

2) Mensajes de Control: enviados desde los controladores de ataque a los módulos *hackeados* involucrados en la ejecución del ataque. Éstos transmiten la información necesaria para la activación y desactivación de los ataques. Además, estos mensajes pueden contener la información de configuración necesaria para la ejecución de los ataques.

Es importante remarcar que los mensajes de control se envían directamente a los módulos *hackeados*. Esta es la mejor opción encontrada para cumplir con la segunda regla de nuestros principios de diseño: "Minimizar la modificación en el código original de los módulos *hackeados*".

3) Módulos Hackeados: módulos cuyo comportamiento ha sido modificado para ejecutar un determinado ataque. Por ejemplo, un ataque que descarte paquetes (*dropping*) usualmente requiere la modificación del módulo encargado del reenvío a nivel IP. Por tanto, la implementación de dicho ataque implica la modificación del módulo IPv4 en NETA, que se comportará como un módulo *hackeado*.

Es importante resaltar que sólo existe un único módulo *hackeado* por módulo modificado, en lugar de un módulo *hackeado* por cada implementación de un ataque. Si dos ataques diferentes necesitan modificar el mismo módulo, sólo existirá un único módulo *hackeado*. Por ejemplo, como se mostrará en la sección siguiente, tanto el ataque de *dropping* como el de *delay* están relacionados con el módulo IPv4. Sin embargo, sólo se necesita un módulo IPv4 *hackeado* para la implementación de ambos ataques. Este diseño tiene como objetivo mejorar la flexibilidad del *framework*, permitiendo así la ejecución de más de un ataque simultáneamente, *e.g.*, los ataques de *dropping* y *delay* pueden lanzarse en un mismo nodo sin más que incluir sus correspondientes controladores de ataque.

IV. ATAQUES IMPLEMENTADOS

En esta sección se exponen los ataques implementados como prueba de concepto para el *framework* NETA. En las subsecciones siguientes se describirá, para cada ataque: (*i*) el comportamiento del mismo y (*ii*) los parámetros que pueden modificarse para configurar dicho ataque.

A. Ataque de Dropping en IP

En este ataque, los nodos que exhiben dicho comportamiento descartan, de forma intencionada y con un cierta probabilidad, los paquetes de datos recibidos, en vez de retransmitirlos. De este modo se ve interrumpido el funcionamiento normal de la red. Según la aplicación afectada, el resultado puede ser una ralentización de la red debido a numerosas retransmisiones, un excesivo consumo de energía en los nodos, etc. Los principales parámetros disponibles en la implementación del ataque son:

- `droppingAttackProbability`: la probabilidad de descartar un paquete de datos, definida entre 0 y 1. Por defecto está fijada a 0, lo que indica que el nodo atacante se comporta de forma normal, *i.e.*, sin descartar paquetes.

B. Ataque de Delay en IP

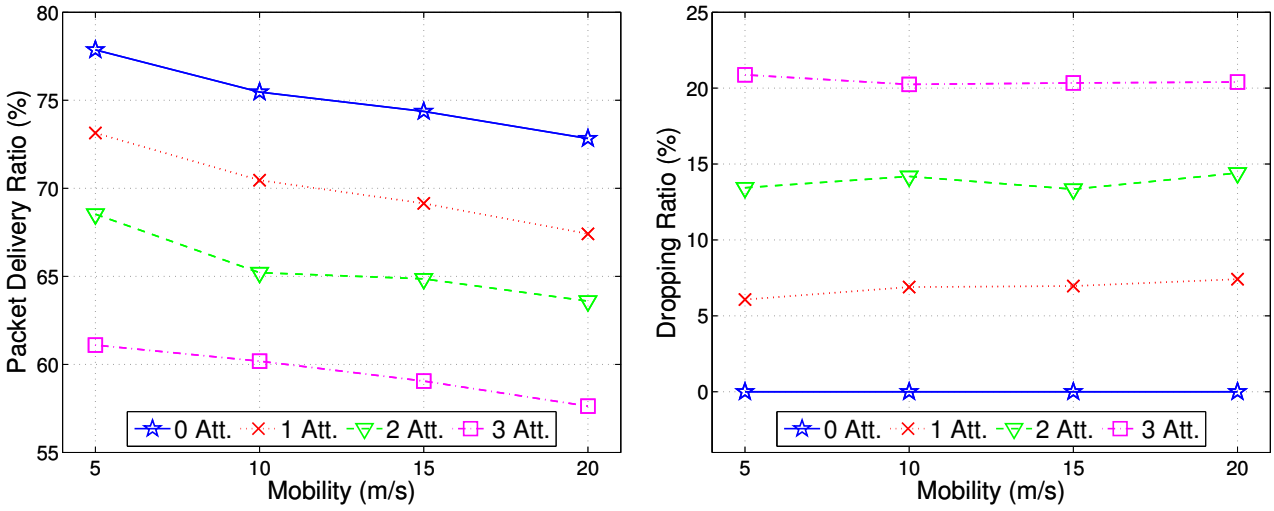
El en ataque de *delay* los nodos retrasan los paquetes de datos IP durante un cierto tiempo. Ésto puede afectar a distintos parámetros de QoS (retardo extremo-a-extremo, *jitter*, etc.), dando como resultado un pobre rendimiento de la red. La lista de parámetros de nuestra implementación es:

- `delayAttackProbability`: la probabilidad de retardar un paquete de datos, definida entre 0 y 1. Por defecto está fijada a 0, lo que implica un comportamiento normal del nodo atacante, *i.e.*, no se aplica ningún retardo extra.
- `delayAttackValue`: el tiempo de retardo específico aplicado a cada paquete. Este parámetro puede especificarse de acuerdo a una distribución estadística. Por esta razón, el parámetro está definido como volátil, *i.e.*, es modificado cada vez que se accede a él. Por defecto, sigue una distribución normal con media 1 segundo y desviación típica de 0.1 segundos.

C. Ataque de Sinkhole

En un ataque de *sinkhole* los nodos atacantes envían información falsa de *routing*, proclamando que tienen una ruta óptima hacia el destino y provocando que otros nodos encaminen los paquetes de datos a través de los atacantes. Aquí, los atacantes falsifican las respuestas (`RREP`) para atraer tráfico. Los parámetros del *sinkhole* son:

- `sinkholeAttackProbability`: la probabilidad de responder a un mensaje de solicitud (`RREQ`) con una respuesta falsa (`RREP`), entre 0 y 1. Por defecto está



(a) PDR (b) DR

Fig. 2: PDR y DR en función de la movilidad y del número de atacantes.

fijada a 0, lo que implica un comportamiento normal del protocolo AODV.

- `sinkOnlyWhenRouteInTable`: si está fijado a *true*, el *sinkhole* sólo envía falsos `RREP` a solicitudes para las que el atacante tenga una ruta válida, *i.e.*, rutas existentes en su tabla de *routing*. En caso contrario (valor *false*), el nodo envía `RREP` falsos a cualquier `RREQ` que le llegue, incluso si no tiene una ruta válida.
- `seqnoAdded`: el falso número de secuencia generado por el nodo atacante. Dicho valor es añadido al número de secuencia observado en la solicitud. Puede ser distinto en cada ocasión si está especificado como una distribución estadística. Por defecto, sigue una distribución uniforme con valores entre 20 y 30.
- `numHops`: el falso número de saltos devuelto por el atacante. Por defecto está fijado a 1, indicando que el atacante alcanza el destino de la comunicación en un único salto.

V. RESULTADOS EXPERIMENTALES

En esta sección se presenta el entorno experimental utilizado para evaluar los ataques presentados en la sección anterior. Además, se han realizado distintos tests con el objetivo de verificar el funcionamiento correcto de cada ataque, midiendo su impacto en la red en base a distintas métricas.

Con esta evaluación se pretende presentar las capacidades de simulación de NETA, dejando de manifiesto su capacidad para facilitar la extracción de información sobre el funcionamiento de los ataques.

A. Entorno de Experimentación Común

Como caso de estudio, se simulan una serie de despliegues MANET. Los parámetros comunes a todos los escenarios se describen a continuación.

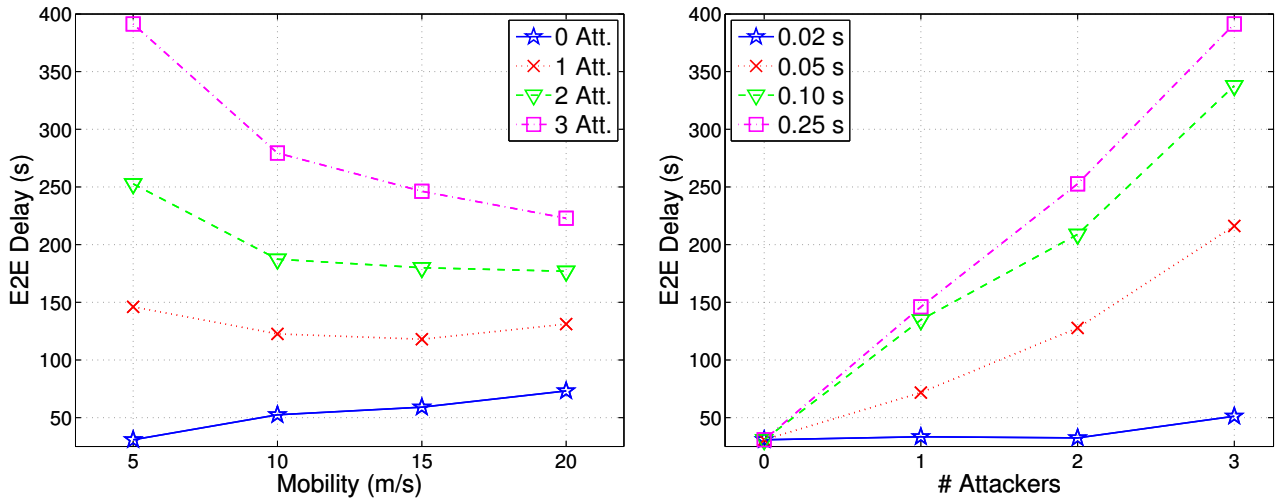
El área de simulación se restringe a un cuadrado de 1000x1000 metros. Cada nodo tiene una cobertura de 250 metros. El tiempo de simulación se fija a 300 segundos. Los resultados obtenidos se derivan promediando (con distintas semillas) 50 repeticiones de cada simulación.

Como protocolos MAC (*Medium Access Control*) y de *routing* se han elegido 802.11g y AODV respectivamente, así como el mecanismo RTS/CTS para el envío de paquetes. Esta última asunción es coherente con la propia movilidad de los nodos, dado que el hecho de no emplear la detección por portadora virtual en escenarios de movilidad podría implicar un gran número de colisiones debido al problema de la estación oculta (*hidden station*).

El número total de nodos es de 25, variando el número de atacantes entre 1 y 3. Los ataques son ejecutados durante todo el tiempo de la simulación, y su correspondiente *tasa de ataque* esta fijada al 100%, siendo esta tasa la probabilidad de que un nodo atacante realice el ataque.

El número de flujos con tráfico a nivel de aplicación está fijado a 21. Cada flujo consiste en una aplicación `UDPBasicBurst` que simula una conexión CBR (*Constant BitRate*) con una tasa de envío de 4 paquetes/segundo, teniendo cada paquete un *payload* de 512 bytes. Para cada flujo, la dirección destino es elegida aleatoriamente entre todos los nodos legítimos, manteniéndose el mismo destino para todo el tiempo de la simulación. Los flujos comienzan de forma aleatoria entre 0,5 y 1,5 segundos y terminan entre 290 y 295 segundos.

Se utiliza el modelo RWP (*Random WayPoint*) para simular el movimiento de los nodos. La velocidad mínima está fija a 1 metro/segundo y la velocidad máxima varía entre 5 y 20 metros/segundo, con un tiempo de pausa de 15 segundos, *i.e.*, una vez que el nodo alcanza el destino deseado, espera inmóvil durante el tiempo de pausa antes de elegir un nuevo



(a) (b)

Fig. 3: $E2ED$ para (a) distintas velocidades y número de atacantes, aplicando un *delay* de 0,25 segundos y (b) aplicando distintos *delays*, con una velocidad fija de 5 metros/segundo.

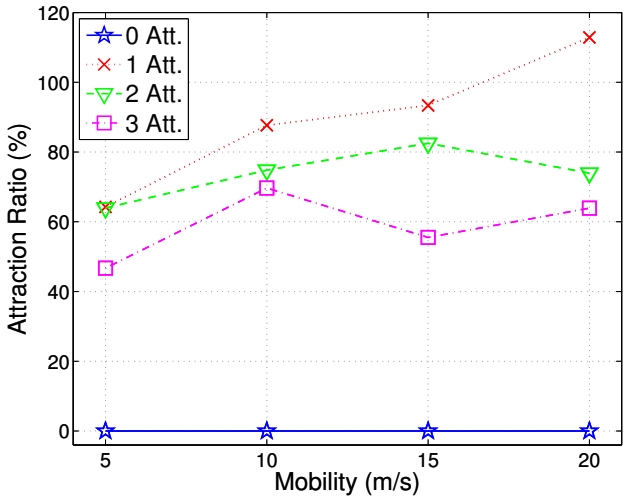


Fig. 4: AR para distintas velocidades y número de atacantes.

destino y repetir el proceso.

B. Evaluación del Ataque de Dropping

Para evaluar el funcionamiento del ataque de *dropping* se definen las siguientes métricas:

- ***Packet Delivery Ratio*, PDR (%)**: número total de paquetes de datos entregados correctamente, dividido por el número total de paquetes de datos enviados.
- ***Dropping Ratio*, DR (%)**: número total de paquetes de datos perdidos como consecuencia de la ejecución del ataque, dividido por el número total de paquetes de datos transmitidos.

Como puede verse en la Fig. 2, si el número de atacantes aumenta, el PDR se ve deteriorado, mientras que el DR crece. Además, puede verse cómo el PDR decrece con la movilidad, mientras que el DR permanece casi constante. Esto es debido a que un aumento en la movilidad implica un incremento en el número de paquetes perdidos por las colisiones y los errores del canal, mientras que el número de paquetes descartados como consecuencia del ataque permanece constante.

C. Evaluación del Ataque de Delay

Se emplean las siguientes métricas de rendimiento para evaluar el funcionamiento del ataque de *delay*:

- ***End-to-End Delay*, E2ED (segundos)**: tiempo medio empleado por un paquete de datos desde su transmisión hasta que alcanza su destino, incluyendo todos los posibles retrasos debidos a descubrimiento de rutas, colas, propagación, etc. Se calcula como el promedio de los E2ED de cada paquete en cada flujo, extrayéndose de esta forma el E2ED medio para toda la red.

Aquí se ha evaluado el ataque de *delay* en función (*i*) del número de atacantes (Fig. 3a), y (*ii*) del retardo aplicado por el atacante (Fig. 3b). En el primer caso se añade un retardo de 0,25 segundos, correspondiente al tiempo entre llegadas de la aplicación CBR. Como puede verse en la figura, el *delay* medio aumenta con el número de atacantes. En el segundo caso se fija la movilidad a 5 metros/segundo y se varía el retardo introducido por los atacantes. Los resultados muestran que, incluso introduciendo retardos inferiores al tiempo entre llegadas, esto puede dar lugar a un gran E2ED medio.

D. Evaluación del Ataque de Sinkhole

Para caracterizar el rendimiento de los nodos *sinkhole* se define la siguiente métrica:

- ***Attraction Ratio*, AR (%)**: la capacidad de atracción de los nodos *sinkhole* respecto de la atracción de los

nodos legítimos. Más específicamente puede verse como la relación entre el número medio de paquetes recibidos por los nodos *sinkhole* y el número medio de paquetes recibidos por los nodos legítimos. El AR se calcula cómo:

$$AR = \frac{\frac{1}{N_S}\sum_{i=1}^{N_S} pkt_i - \frac{1}{N_L}\sum_{j=1}^{N_L} pkt_j}{\frac{1}{N_S}\sum_{i=1}^{N_S} pkt_i} \cdot 100 \qquad (1)$$

siendo N_S y N_L el número de nodos *sinkhole* y legítimos respectivamente, y pkt_i el número total de paquetes recibidos por el nodo i.

La Fig. 4 muestra cómo los nodos *sinkhole* atraen un trafico superior al resto de nodos. Además, puede observarse que el AR decrece a medida que aumenta el número de atacantes. Esto es debido a que los atacantes tienen que competir entre sí para atraer el tráfico, resultando en un menor AR. Sin embargo, el número total de paquetes atraídos por todos los nodos *sinkhole* crece con el número de atacantes.

VI. CONCLUSIONES Y TRABAJO FUTURO

En este trabajo se ha propuesto NETA, un *framework* para la simulación de ataques en redes de comunicación desarrollado en base al *framework* INET y el simulador OMNeT++.

NETA presenta tres componentes principales: *controladores de ataque*, que gestionan la ejecución de los ataques; *módulos hackeados*, que implementan el comportamiento del ataque; y *mensajes de control*, encargados de transmitir la información de activación/desactivación, así como información de configuración desde los controladores de ataque a los módulos *hackeados*. Asimismo, y como prueba de concepto, se han implementado tres ataques: *dropping*, *delay* y *sinkhole*.

Como caso de estudio se han considerado escenarios de aplicación realistas, analizando una serie de despliegues MANET. Como puede comprobarse, los resultados experimentales obtenidos corroboran el funcionamiento correcto de los ataques implementados. Adicionalmente, se ha evaluado cómo afectan los distintos ataques al rendimiento normal de la red.

Sin embargo, esta primera versión del *framework* adolece de algunas limitaciones que se prevé serán tenidas en consideración con posterioridad con el fin de mejorar el mismo. Entre los puntos susceptibles de ser modificados en el futuro se destaca la implementación de nuevos ataques con una mayor complejidad junto con el desarrollo de diferentes métricas de rendimiento que puedan ser utilizadas para comparar soluciones de defensa, así como para analizar el rendimiento de éstas bajo las mismas condiciones.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el MICINN (Ministerio de Ciencia e Innovación) mediante el proyecto TEC2011-22579.

REFERENCIAS

[1] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in *Proceedings of the 2012 2nd International Conference on Advanced Computing & Communication Technologies*, ser. ACCT. IEEE Computer Society, Jan. 2012, pp. 535–541. [Online]. Available: http://dx.doi.org/10.1109/ACCT.2012.48

[2] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, May 2012. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2011.03.005

[3] J. Lessmann, P. Janacik, L. Lachev, and D. Orfanus, "Comparative study of wireless network simulators," in *7th International Conference on Networking*, ser. ICN. IEEE Computer Society, Apr. 2008, pp. 517–523.

[4] A. ur Rehman Khan, S. M. Bilal, and M. Othman, "A performance comparison of open source network simulators for wireless networks," in *IEEE International Conference on Control System, Computing and Engineering*, ser. ICCSCE. IEEE Computer Society, Nov. 2012, pp. 34–38.

[5] A. Kumar, S. Kaushik, R. Sharma, and P. Raj, "Simulators for wireless networks: A comparative study," in *International Conference on Computing Sciences*, ser. ICCS. IEEE Computer Society, Sep. 2012, pp. 338–342.

[6] H. Ehsan and F. Khan, "Malicious AODV: implementation and analysis of routing attacks in MANETs," in *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, ser. TrustCom. IEEE Computer Society, Jun. 2012, pp. 1181–1187.

[7] T. Gamer and M. Scharf, "Realistic simulation environments for IP-based networks," in *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, ser. SIMUTools. ACM, Mar. 2008, pp. 83:1–83:7.

[8] G. Dini and M. Tiloca, "ASF: an attack simulation framework for wireless sensor networks," in *IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications*, ser. WiMob. IEEE Computer Society, Oct. 2012, pp. 203–210.

JIE

Las **Jornadas de Inovación Educativa en Ingeniería Telemática (JIE)** cumplen su tercera edición desde que se celebraron, por primera vez, en Valladolid en 2010. Estas jornadas aparecieron durante la adaptación al Espacio Europeo de Educación Superior (EEES) y la implantación progresiva de los nuevos títulos de grado y posgrado en las universidades españolas, que han supuesto y todavía suponen todo un abanico de desafíos para la comunidad docente universitaria. El paradigma del aprendizaje centrado en el alumno, el desarrollo de competencias y la evaluación continua han exigido del profesorado un cambio profundo de mentalidad y la aplicación de nuevas tecnologías en el diseño de planes de estudios, la preparación de asignaturas, la planificación docente, la conducción de las clases y el seguimiento, tutorización y evaluación de los estudiantes.

Coincidiendo con la fase final de la implantación de los nuevos títulos, las **III Jornadas de Innovación Educativa en Ingeniería Telemática (JIE 2013)** son organizadas en esta edición por el Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada. Estas jornadas se presentan como una oportunidad para crear un foro de encuentro e intercambio de experiencias de innovación docente entre profesores en el ámbito de la Ingeniería Telemática, así como el uso y aplicación de las tecnologías de la información y las comunicaciones en la docencia universitaria en general y en la docencia de la telemática en particular.

Esta sección recoge las contribuciones que fueron aceptadas para su presentación en las jornadas. Tras un riguroso proceso de revisión en el que se aseguró, bajo la coordinación del Comité de Programa, que cada artículo recibiera al menos 2 revisiones independientes, se aceptaron 12 artículos para su presentación oral. Estas presentaciones se han estructurado en 3 sesiones distribuidas durante los tres días en que tienen lugar las XI Jornadas de Ingeniería Telemática (JITEL 2013).

Quiero dar las gracias a los miembros del Comité de Programa por su colaboración en las tareas organizativas y, especialmente, a los docentes que han participado en el proceso de revisión y que han permitido mejorar la calidad de las contribuciones. También quiero agradecer a los miembros del Comité Local su dedicación y entusiasmo, imprescindibles para el buen desarrollo de estas jornadas.

Finalmente, el área de Ingeniería Telemática de la Universidad de granada les da la más cordial bienvenida a las **III Jornadas de Innovación Educativa en Ingeniería Telemática**, esperando que su participación haga de ellas un éxito.

Jorge Navarro-Ortiz
Comité de Programa de JIE

Comité de programa

Ramón Agüero Calvo (Universidad de Cantabria)
Francisco Barceló Arroyo (Universitat Politècnica de Catalunya)
Fidel Cacheda Seijo (Universidade da Coruña)
Raquel Crespo García (Universidad Carlos III de Madrid)
Yannis Dimitriadis (Universidad de Valladolid)
Julián Fernández Navajas (Universidad de Zaragoza)
Alberto Eloy García Gutiérrez (Universidad de Cantabria)
José Manuel Giménez Guzmán (Universidad de Alcalá)
Guillermo Agustín Ibáñez Fernández (Universidad de Alcalá)
José Ángel Irastorza Teja (Universidad de Cantabria)
Martín Llamas Nistal (Universidad de Vigo)
Javier López Muñoz (Universidad de Málaga)
Elsa Macías López (Universidad de las Palmas de Gran Canaria)
Iván Marsá Maestre (Universidad de Alcalá)
Jesús Martínez Cruz (Universidad de Málaga)
Jorge Navarro Ortiz (Universidad de Granada)
Jaume Ramis Bibiloni (Universitat de les Illes Balears)
María Jesús Verdú Pérez (Universidad de Valladolid)

Repaso activo mediante el uso de mapas conceptuales: una experiencia de innovación docente

Norberto Fernández, Jesús Arias, Ivan Vidal, Jaime García-Reinoso, Luis Sánchez
Departamento de Ingeniería Telemática,
Universidad Carlos III de Madrid
Avda. Universidad, 30. Leganés, Madrid, España.
{berto,jaf,ividal,jgr,luiss}@it.uc3m.es

***Resumen*—En unidades didácticas que se extienden a lo largo de múltiples sesiones en el aula, separadas varios días entre sí, los alumnos se ven abocados a una situación de *pérdida de contexto*. Para hacer frente a esta situación, se pueden emplear técnicas de repaso en el aula para establecer nexos de unión con las clases anteriores. Uno de los mecanismos que se utilizan para hacer este repaso, consiste en recordar de manera verbal los conceptos presentados en las sesiones anteriores. Sin embargo, este mecanismo presenta algunas limitaciones, entre otras, que no hace participar activamente al alumno en el proceso ni favorece el aprendizaje visual. Para hacer frente a estas limitaciones, se ha llevado a cabo una experiencia de innovación docente en la que se ha propuesto que los alumnos participen activamente a la hora de hacer el repaso en el aula mediante la elaboración de mapas conceptuales. Los resultados de esta experiencia se detallan en el presente artículo.**

***Palabras Clave*—repaso en el aula, aprendizaje activo, mapas conceptuales**

I. INTRODUCCIÓN

En unidades didácticas que se extienden a lo largo de múltiples sesiones en el aula, separadas varios días entre sí, los alumnos se ven abocados a una situación de *pérdida de contexto*. Esta situación dificulta la asimilación de nuevos conceptos, puesto que a los alumnos les cuesta relacionarlos con los conceptos introducidos en clases anteriores, al recordar vagamente estos últimos.

Para hacer frente a esta situación, es habitual que en la denominada *fase inicial de la clase* [11] los profesores dediquen unos minutos a establecer nexos de unión con las clases anteriores, repasando los principales conceptos previos necesarios.

Una de las técnicas que se utilizan a la hora de hacer el repaso en el aula consiste en recordar brevemente, de manera verbal, los conceptos previamente tratados. A pesar de la ventaja que supone su sencillez, esta técnica presenta también algunas limitaciones, como por ejemplo: (1) convierte al alumno en un mero receptor pasivo de información y por tanto no fomenta el denominado aprendizaje activo [4], y (2) aunque el principal objetivo del repaso verbal es ayudar a recordar conceptos previos, este tipo de repaso ofrece un repertorio muy limitado de estímulos a la memoria visual, que es una de las piezas fundamentales de la memoria humana [2].

Así pues, con el objetivo de intentar mejorar el proceso de repaso en el aula, los autores de este artículo han llevado a cabo recientemente una experiencia de innovación docente en la Universidad Carlos III de Madrid. En dicha experiencia, se seleccionaron dos asignaturas de dos titulaciones distintas (relacionadas con el ámbito de las Tecnologías de la Información y las Comunicaciones) en las que los profesores utilizaban el repaso verbal a comienzo de clase como principal mecanismo para ayudar a los alumnos a recuperar el contexto perdido. Como alternativa a este mecanismo, se experimentó con la posibilidad de que los alumnos, en colaboración con el profesor o de manera independiente, elaboren mapas conceptuales [14], [15] a modo de repaso. Con ello se pretendía definir un mecanismo más activo para el alumno y de naturaleza más visual que el anteriormente utilizado para el repaso en el aula. Además, como objetivo secundario, se planteó llevar a cabo un análisis de la percepción que tienen los alumnos del proceso de repaso en el aula: si les parece positivo y necesario, qué técnicas suelen utilizar los profesores para llevarlo a cabo, cuáles de estas técnicas les parecen más adecuadas, etc. Este análisis se realizó por medio de encuestas en las que se vieron involucradas, además de las asignaturas antes mencionadas, otras dos más.

En este artículo se describe en detalle la experiencia llevada a cabo, así como los resultados alcanzados. Entre las principales conclusiones que se pueden extraer de la misma destacan que el proceso de repaso en el aula es percibido como fundamental por los alumnos, aunque, a tenor de los resultados, no siempre es habitual que los profesores repasen en clase. Además, la utilización de mapas conceptuales como medio de repaso en el aula no es frecuente, aunque se valora positivamente por parte de los estudiantes. Eso sí, esta valoración positiva está condicionada a otros aspectos, como por ejemplo su utilidad de cara a la evaluación de la asignatura.

El resto del artículo se estructura como sigue: en la sección II se introducirán una serie de conceptos previos y trabajos relacionados. La sección III describe en detalle las actividades llevadas a cabo como parte de la experiencia. Los resultados alcanzados en la misma se discutirán en la sección IV. Finalmente, la sección V presentará las principales conclusiones extraídas así como potenciales vías de mejora futura del presente trabajo.

II. CONCEPTOS PREVIOS Y TRABAJOS RELACIONADOS

A. Repaso en el aula y aprendizaje activo

Diferentes estudios en el ámbito de la psicología han tratado de abordar la problemática del funcionamiento de la memoria humana [19], [2]. Parte de estos estudios se centran en modelar la denominada *curva de olvido*, que indica cómo se pierde la información retenida si no se hace ningún intento por volver a recordarla. Según estos modelos, existe una variedad de factores que influencian la formación y mantenimiento de recuerdos, siendo uno de los más relevantes el tiempo transcurrido desde el estímulo que los genera. Así por ejemplo, uno de los primeros estudios en abordar este tema, debido a Hermann Ebbinghaus [7], establecía que la forma de dicha curva se podría asimilar a una exponencial decreciente con el tiempo.

Dado que, de acuerdo a la taxonomía de Bloom [3], la capacidad de recordar conceptos es una de las bases sobre las que se asientan procesos educativos de mayor complejidad, existe un claro interés por parte de los docentes en ayudar a la formación de recuerdos estables acerca de nuevos conceptos. Así pues, con el objetivo de frenar la evolución natural de la curva de olvido, los profesores pueden emplear técnicas de repaso en el aula.

Una de las técnicas empleadas habitualmente a la hora de hacer el repaso en el aula consiste en que el profesor presente verbalmente al inicio de clase los principales conceptos tratados en clases anteriores. Este tipo de repaso se caracteriza porque el grueso del esfuerzo recae en el profesor, convirtiendo al alumno en un mero receptor pasivo de información.

Esta situación contrasta con uno de los principales objetivos de la reforma del Espacio Europeo de Educación Superior (EEES) [8], que consiste en situar al alumno como centro del proceso educativo [18]. En el escenario del EEES, cobran especial relevancia las metodologías de aprendizaje activo [4], sobre las que existen evidencias de sus beneficios para el proceso de aprendizaje [16], [5]. En particular, algunos estudios recientes [10], [9] han puesto de manifiesto la importancia del proceso de recuperación activa (*active recall*) de conceptos memorizados a la hora de consolidar esos conceptos en la memoria a largo plazo.

Por tanto, teniendo todo esto en consideración, en esta experiencia de innovación docente se planteó la posibilidad de reemplazar el repaso verbal en el aula por un mecanismo más activo para el alumno. En particular se pretende que los alumnos lleven a cabo un proceso de recuperación activa de conceptos mediante la elaboración de sus propios mapas conceptuales como mecanismo para repasar los conceptos previamente presentados.

B. Mapas conceptuales

Los mapas conceptuales son herramientas gráficas para organizar y representar conocimiento [15]. Un mapa conceptual describe una serie de conceptos (representados usualmente por óvalos, círculos o cajas) y sus relaciones (que se muestran mediante líneas etiquetadas que conectan conceptos). La figura 1 muestra un ejemplo sencillo de mapa conceptual.

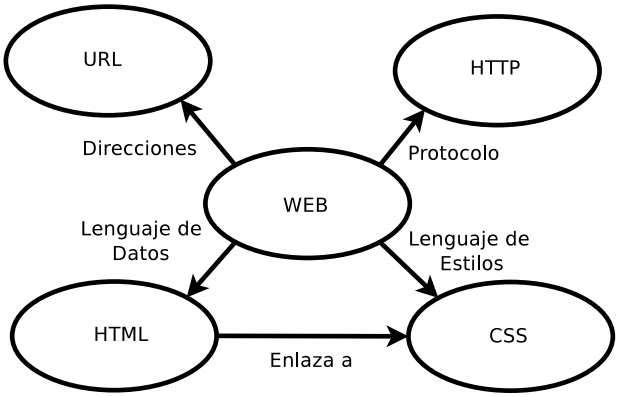


Fig. 1. Un mapa conceptual sencillo.

Esta técnica tiene su origen en la década de los setenta, en los estudios de Joseph Novak, de la Universidad de Cornell [15] y asienta su base teórica en el aprendizaje significativo de Ausubel [1]. Según esta teoría, los nuevos conceptos adquieren significado mediante su relación con los conceptos o ideas previamente adquiridos por el individuo. Es por ello por lo que los mapas conceptuales resultan una herramienta de utilidad para el aprendizaje significativo, al facilitar este proceso de interrelación de conceptos [15]. Su utilidad como herramienta educativa se ve refrendada por trabajos como [13] un meta-análisis donde, tras haber analizado 55 estudios acerca del uso educativo de mapas conceptuales, se concluía que su uso está asociado a una mejora en la capacidad de retención de conocimiento.

Debido a su flexibilidad, los mapas conceptuales han sido utilizados con diferentes finalidades dentro del proceso educativo [12]. Por ejemplo, [17] indica su uso como herramienta de evaluación sumativa, pero también como mecanismo para monitorizar la evolución de la estructura cognitiva de los alumnos a medida que avanza el proceso formativo. El uso de mapas conceptuales como mecanismo de evaluación, tanto formativa como sumativa, es también tratado en [20]. Más recientemente, un meta–análisis de estudios acerca del uso de mapas conceptuales en educación médica [6] destacaba, entre otros, su utilidad como recurso de aprendizaje, como mecanismo para proporcionar realimentación a los alumnos y también como mecanismo de evaluación.

En el caso de la experiencia detallada en este artículo, se planteó el uso de mapas conceptuales como herramienta de repaso en el aula. Dos son los principales motivos que sustentan la elección de esta herramienta. Por un lado, al hacer el repaso mediante un mapa conceptual se pretende que los alumnos construyan una estructura conceptual a la que poder anclar los nuevos conceptos que se van a presentar, facilitando de este modo el aprendizaje significativo. Por otro lado, al ser los mapas conceptuales herramientas gráficas, se pretende estimular la memoria visual, facilitando el proceso de recuperación y contribuyendo a frenar la evolución de la curva de olvido.

III. DESCRIPCIÓN DE LA EXPERIENCIA

A. Asignaturas involucradas

Las asignaturas involucradas en la experiencia fueron cuatro. La tabla I ofrece los datos básicos de dichas asignaturas.

Asignatura	Titulación	Curso	Tipo	Matriculados
Flujos de Información Multimedia (FIM)	Grado en Ingeniería de Sistemas Audiovisuales	4º	Obligatoria	35
Computación Web (CW)	Grado en Ingeniería Telemática	4º	Obligatoria	37
Procesamiento de Formatos en Aplicaciones Telemáticas (PFAT)	Grado en Ingeniería Telemática	3º	Obligatoria	49
Sistemas de Información (SI)	Ingeniería de Telecomunicación	4º	Optativa	18

Tabla I
DESCRIPCIÓN BÁSICA DE LAS ASIGNATURAS INVOLUCRADAS EN LA EXPERIENCIA.

Como se indicó en la sección de introducción, estas cuatro asignaturas tuvieron dos niveles de participación diferentes en la experiencia. Las dos primeras asignaturas descritas en la tabla I se vieron involucradas fundamentalmente en el análisis por medio de cuestionarios del proceso de repaso en el aula, mientras que en las dos últimas es donde se llevó a cabo la experiencia al completo.

B. Estado previo de las asignaturas

Anteriormente a la puesta en marcha de la experiencia de innovación docente descrita en el presente artículo, las cuatro asignaturas involucradas empleaban fundamentalmente las siguientes estrategias de repaso:

- Repaso verbal en la etapa inicial de clase, en el que el profesor recuerda a los alumnos los principales temas y conceptos de interés tratados en anteriores sesiones.
- Resolución de ejercicios o casos. Habitualmente se reserva un número reducido (entre 2 y 5) de sesiones en el aula por cuatrimestre para la resolución de problemas o ejercicios de tipo práctico y de naturaleza similar a los que los alumnos pueden encontrar en los exámenes de la asignatura.
- Uso de técnicas de evaluación continua. A lo largo del curso se llevan a cabo una o varias pruebas de evaluación por medio de exámenes escritos o tipo test. Aunque el objetivo fundamental de estas pruebas es recabar información sobre la evolución de los alumnos, contribuyen también al repaso del curso, puesto que motivan a los alumnos a estudiar para los exámenes y favorecen por tanto que lleven la asignatura al día.

De todas estas técnicas, la más frecuentemente utilizada era la primera, debido a su sencillez y su flexibilidad.

C. Desarrollo de la experiencia

Como se indicó en la sección III-A se pueden distinguir dos niveles de participación de las asignaturas en la experiencia: participación parcial (sólo a nivel de análisis de la etapa de repaso) y participación plena (análisis y cambios en el proceso de repaso).

Obviamente, dependiendo del nivel de participación, las actividades realizadas como parte del proyecto de innovación han sido distintas. Además, en las dos asignaturas que han implantado la experiencia al completo, también se han seguido estrategias de desarrollo distintas. Así pues, tenemos tres diferentes implementaciones de la experiencia, que se detallan a continuación por separado.

1) Asignaturas con participación parcial: En las asignaturas que participaron únicamente en la etapa de análisis del proceso de repaso, la actividad llevada a cabo como parte de la experiencia consistió en que el profesor, tras describir brevemente qué es un mapa conceptual (bien de manera verbal, bien ofreciendo a los alumnos un ejemplo realizado por él) solicitó a los alumnos que rellenasen una encuesta de manera voluntaria y anónima.

La figura 2 muestra el cuestionario que fue ofrecido a los alumnos para ser rellenado. Como se puede ver, el cuestionario se centra fundamentalmente en los siguientes aspectos:

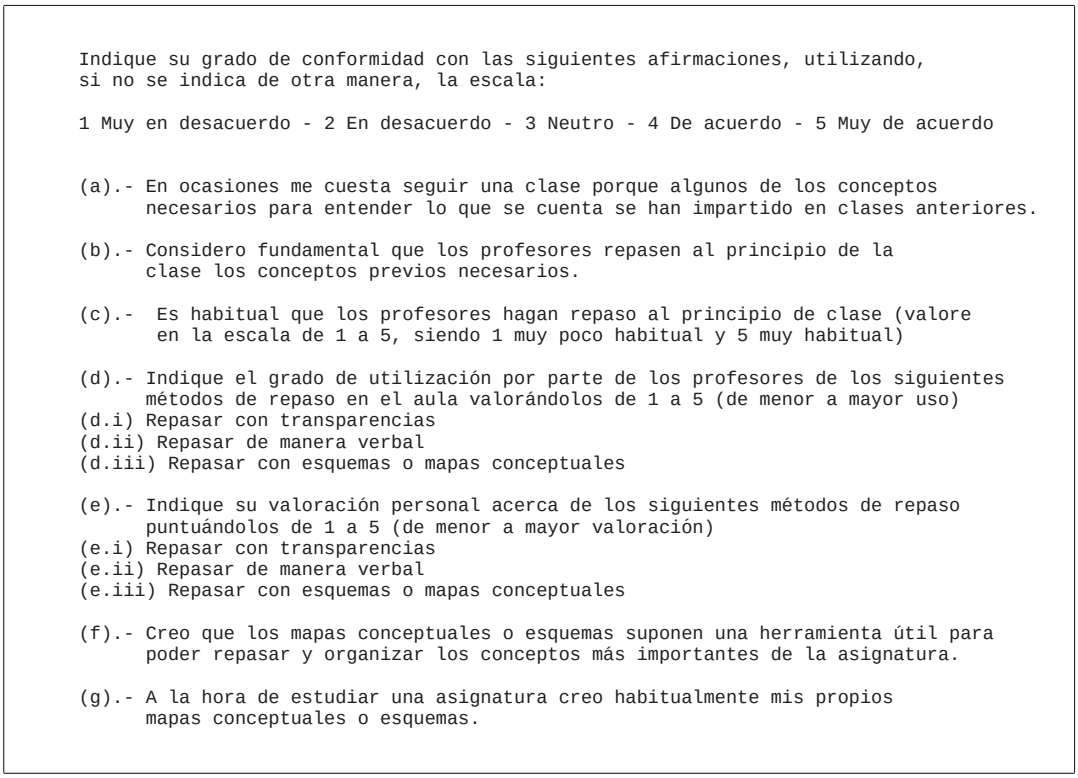
- Evaluar la gravedad del problema de pérdida de contexto (cuestión *(a)*).
- Obtener información sobre el repaso (preguntas *(b)* a *(e)*).
- Recabar la opinión de los alumnos sobre el uso de mapas conceptuales (preguntas *(f)* y *(g)*).

2) Sistemas de información: En esta asignatura el mecanismo seguido a la hora de implantar el proyecto de innovación docente consistió en la realización de dos tipos de actividades:

- A lo largo del cuatrimestre, cada vez que, debido a su longitud, una unidad didáctica requería ser impartida a lo largo de varias sesiones en el aula, se utilizaron mapas conceptuales a la hora de hacer el repaso en lugar de repaso verbal. El mecanismo seguido por el profesor en este caso, para involucrar activamente a los alumnos, consistió en un proceso de elaboración colaborativa del mapa. El profesor dibuja en la pizarra un concepto o un número limitado de conceptos semilla y a partir de ahí, a través de preguntas realizadas a los alumnos, les invita a que sean estos los que continúen con la construcción del diagrama del mapa. De este modo se pretendía obtener las ventajas que suponían contar por un lado con la participación activa de los alumnos y, por otro, con la guía del profesor.
- Al final del cuatrimestre se solicitó a los alumnos que rellenasen de manera anónima y voluntaria, el cuestionario presentado en la figura 2.

3) Procesamiento de formatos en aplicaciones telemáticas: El procedimiento seguido en este caso constó de las siguientes etapas:

(a) El primer día de clase el profesor introdujo brevemente la experiencia, sus objetivos y los mapas conceptuales. Se les indicó a los alumnos que, de manera opcional, cuando el profesor lo indicase, podrían realizar individualmente un mapa conceptual resumiendo los principales



Indique su grado de conformidad con las siguientes afirmaciones, utilizando,
si no se indica de otra manera, la escala:

1 Muy en desacuerdo - 2 En desacuerdo - 3 Neutro - 4 De acuerdo - 5 Muy de acuerdo

(a).- En ocasiones me cuesta seguir una clase porque algunos de los conceptos necesarios para entender lo que se cuenta se han impartido en clases anteriores.

(b).- Considero fundamental que los profesores repasen al principio de la clase los conceptos previos necesarios.

(c).- Es habitual que los profesores hagan repaso al principio de clase (valore en la escala de 1 a 5, siendo 1 muy poco habitual y 5 muy habitual)

(d).- Indique el grado de utilización por parte de los profesores de los siguientes métodos de repaso en el aula valorándolos de 1 a 5 (de menor a mayor uso)
(d.i) Repasar con transparencias
(d.ii) Repasar de manera verbal
(d.iii) Repasar con esquemas o mapas conceptuales

(e).- Indique su valoración personal acerca de los siguientes métodos de repaso puntuándolos de 1 a 5 (de menor a mayor valoración)
(e.i) Repasar con transparencias
(e.ii) Repasar de manera verbal
(e.iii) Repasar con esquemas o mapas conceptuales

(f).- Creo que los mapas conceptuales o esquemas suponen una herramienta útil para poder repasar y organizar los conceptos más importantes de la asignatura.

(g).- A la hora de estudiar una asignatura creo habitualmente mis propios mapas conceptuales o esquemas.

Fig. 2. Cuestionario utilizado en la experiencia de evaluación docente.

conceptos tratados en la clase anterior. Para fomentar su participación, se estableció que, en caso de entregar sus mapas, estos serían calificados y tenidos en cuenta de cara a la evaluación sumativa de la asignatura. Sin embargo, para no penalizar a los no participantes, se indicó que en cualquier caso la nota sería extra, y que se podría obtener la máxima calificación sin realizar los mapas. A continuación, dentro de la misma sesión, el profesor solicitó a los alumnos que rellenasen la encuesta presentada en la figura 2, que de esta forma sirvió a modo de pre-test para recabar la opinión inicial de los alumnos sobre el repaso y el uso de mapas conceptuales.

(b) En la primera clase en la que fue necesario llevar a cabo repaso en el aula de conceptos previos, el profesor elaboró un mapa conceptual, con el objetivo de que éste sirviese de ejemplo a los alumnos a la hora de elaborar los suyos propios en el futuro.

(c) Posteriormente, a lo largo del curso, el profesor solicitó en varias ocasiones a los alumnos que elaborasen mapas conceptuales a modo de resumen de la clase anterior. En general no se siguió un esquema periódico a la hora de asignar esta tarea, sino que se prefirió solicitar la elaboración de mapas conceptuales cuando se consideró necesario (fundamentalmente en unidades didácticas largas, con varias sesiones separadas). De este modo se pretendía no sobrecargar de tareas a los alumnos ni al profesor involucrados en la experiencia.

Tras recoger los mapas entregados por los alumnos, el profesor presentaba un mapa elaborado por él mismo a modo de repaso. De este modo, los estudiantes que participaban voluntariamente en la experiencia tenían una referencia para comparar con sus propios mapas y, al mismo tiempo, se minimizaba el posible impacto sobre los no participantes, al poder repasar estos con el mapa del profesor.

(d) Al final del curso, se les pidió a los alumnos participantes que rellenasen otra encuesta (que se muestra en la figura 3) con el objetivo de servir de post-test para intentar detectar posibles evoluciones en la opinión de los alumnos debidas a la experiencia.

IV. ANÁLISIS DE LOS RESULTADOS

En esta sección se detallan los resultados obtenidos a través de los cuestionarios realizados en las diferentes asignaturas y se lleva a cabo un análisis e interpretación de los mismos.

La tabla II muestra los resultados obtenidos en el test de la figura 2 para las asignaturas con participación parcial y *Sistemas de información*. La tabla III refleja los resultados obtenidos en la asignatura *Procesamiento de formatos en aplicaciones telemáticas*, separados entre pre-test (izquierda) y post-test (derecha). En ambas tablas se muestra, para cada pregunta, el número total de respuestas (N) y la media (μ) y desviación típica (σ) de los valores obtenidos.

En cuanto a los resultados para la encuesta de la figura 2, que se recogen en la tabla II, para las asignaturas de *Computación Web*, *Flujos de información multimedia* y *Sistemas de información* y en la parte izquierda (pre-test) de la tabla III para *Procesamiento de formatos en aplicaciones telemáticas*, se puede observar que:

- En general los alumnos manifiestan opiniones neutras (en las asignaturas de *Computación Web*, *Procesamiento de formatos en aplicaciones telemáticas* y *Sistemas de información*) o de ligero desacuerdo (*Flujos de información multimedia*) a la hora de evaluar la gravedad del problema de pérdida de contexto (pregunta *(a)*), lo

```
Indique su grado de conformidad con las siguientes afirmaciones, utilizando,
si no se indica de otra manera, la escala:

1 Muy en desacuerdo - 2 En desacuerdo - 3 Neutro - 4 De acuerdo - 5 Muy de acuerdo

(a).- Me ha costado seguir algunas clases de la asignatura porque los conceptos
      necesarios para entender lo que se contaba se habían impartido en clases anteriores.

(b).- Considero fundamental que los profesores repasen al principio de la
      clase los conceptos previos necesarios.

(c).- Indique su valoración personal acerca de los siguientes métodos de repaso
      puntuándolos de 1 a 5 (de menor a mayor valoración)
(c.i) Repasar con transparencias
(c.ii) Repasar de manera verbal
(c.iii) Repasar con esquemas o mapas conceptuales

(d).- Creo que los mapas conceptuales o esquemas suponen una herramienta útil para
      poder repasar y organizar los conceptos más importantes de la asignatura.

(e).- A la hora de estudiar la asignatura he utilizado los mapas conceptuales o
      esquemas que se han presentado en clase.

(f).- A la hora de estudiar la asignatura he creado mis propios mapas conceptuales
      o esquemas.

(g).- Creo que este tipo de iniciativas de innovación docente son útiles y deberían
      repetirse en otras asignaturas.

      Sugerencias o comentarios adicionales sobre la experiencia de innovación:
--------------------------------------------------------------------------------
```

Fig. 3. Cuestionario utilizado como post-test en la asignatura de *Procesamiento de formatos en aplicaciones telemáticas*.

que se podría interpretar como que, aún reconociendo su existencia, no perciben el problema como muy grave.

- Sin embargo, existe acuerdo a la hora de valorar como fundamental el repaso a principio de clase (pregunta *(b)*), como se muestra especialmente en *Computación Web* y *Sistemas de información*, con valores medios por encima de 4.
- Son descatables también los resultados de *Computación Web* y *Sistemas de información* en la pregunta *(c)*. Estos resultados (próximos al 2 de media) indican que no es tan habitual como cabría pensar que los profesores hagan repaso a principio de clase. Una tendencia similar (aunque más próxima a la respuesta neutra) se muestra también en *Procesamiento de formatos en aplicaciones telemáticas*. Nótese que en el caso del grupo de *Flujos de información multimedia* la opinión en esta pregunta ha sido más positiva (media 3.55), lo que contribuiría a explicar los resultados de ligero desacuerdo manifestados en la cuestión *(a)*.
- En los resultados de los grupos de cuestiones *(d)* y *(e)*, centrados en las técnicas de repaso en el aula, se observa que las técnicas más habitualmente empleadas son el repaso verbal y el repaso por medio de transparencias. El repaso por medio de esquemas o mapas conceptuales se emplea menos habitualmente, según reflejan los resultados de la cuestión *(d.iii)*. En cuanto a las preferencias de los alumnos, se puede observar que el uso de mapas conceptuales ha recibido una valoración destacada, salvo en el caso de *Flujos de información multimedia*, donde no se manifiesta una preferencia clara (todas las técnicas propuestas han recibido valoración positiva y similar). Se puede observar también que la valoración más positiva (media 4.42) se ha obtenido en la asignatura de *Sistemas de información*, donde la encuesta se pasó a los alumnos al final del cuatrimestre y tras haber realizado ya la experiencia de innovación en el aula.
- Por último, se puede constatar en los resultados de las cuestiones *(f)* y *(g)* que, en general, en todas las asignaturas, los alumnos valoran positivamente el uso de mapas conceptuales (de nuevo destacando ligeramente los resultados de *Sistemas de información*). Sin embargo, se puede observar también que los valores medios obtenidos son menores cuando se les pregunta acerca de si ellos mismos crean sus propios mapas conceptuales a la hora de estudiar la asignatura.

Dado que para la asignatura *Procesamiento de formatos en aplicaciones telemáticas* se dividió el proceso de recabar la opinión de los alumnos en una etapa de pre-test y otra de post-test, se pueden comparar los resultados obtenidos en ambas encuestas, recogidos en la tabla III.

Se puede observar que los resultados de las preguntas *(a)* y *(b)* no han variado apenas de la etapa de pre-test a la de post-test. Este es un resultado esperable, puesto que la respuesta de esas preguntas no depende de la ejecución de la experiencia en sí, sino de la valoración global sobre la importancia y necesidad del repaso.

En cuanto a la valoración personal de las técnicas de repaso, (grupo *(e)* en el pre-test y *(c)* en el post-test), las valoraciones se han mantenido para el caso del repaso con transparencias y se han reducido levemente para el caso del repaso verbal y por medio de mapas conceptuales. Sin embargo, realizando un test t-Student de diferencia de medias en los tres casos, se obtiene como resultado que no se puede descartar la hipótesis de igualdad de medias, así que las diferencias observadas

no pueden considerarse estadísticamente significativas con un nivel de significancia de $\alpha = 0.05$. La misma situación se produce también a la hora de comparar los resultados de la pregunta *(g)* del pre-test con la *(f)* del post-test: los participantes muestran una opinión neutra sobre crear sus propios mapas conceptuales.

Sin embargo, donde sí se observan diferencias estadísticamente significativas es en la percepción de utilidad del mecanismo de repaso basado en mapas conceptuales (pregunta *(f)* en el pre-test y *(d)* en el post-test). El valor ha descendido, lo que indica que los alumnos tenían inicialmente expectativas altas (media del pre-test 3.97), que no se vieron del todo atendidas (media del post-test 3.1). Para intentar explicar este resultado, se llevó a cabo un análisis del texto introducido por los alumnos en el cuadro de sugerencias y comentarios del post-test. Este análisis reflejó que, dado que la evaluación de la asignatura se realizaba por medio de ejercicios de naturaleza fundamentalmente práctica, los alumnos preferían dedicar más tiempo a resolver ejercicios en el aula, y menos a repaso teórico, que era lo que se perseguía mediante el uso de mapas conceptuales. Nótese que esta respuesta está en consonancia con los valores indicados en la cuestión *(e)* del post-test, en la que los alumnos se manifiestan ligeramente en desacuerdo (media 2.8) con la afirmación de haber utilizado los mapas conceptuales a la hora de estudiar la asignatura: al consistir la evaluación en la resolución de ejercicios, los estudiantes prefieren centrar sus esfuerzos en preparar ese aspecto y no perciben beneficio en invertir parte de su tiempo organizando los conceptos teóricos de la asignatura por medio de mapas conceptuales.

Finalmente, a pesar de los resultados anteriores, los datos obtenidos para la pregunta *(g)* del post-test, indican que los alumnos han valorado de manera ligeramente positiva (media 3.4) la experiencia de innovación.

V. CONCLUSIONES Y LÍNEAS FUTURAS

En este artículo se ha descrito una experiencia de innovación docente en la que se ha analizado la posibilidad de introducir cambios en el mecanismo de repaso en el aula para convertirlo en un proceso más pariticipativo para los alumnos.

En la experiencia, que se desarrolló a lo largo del curso 2012/2013, se vieron involucradas cuatro asignaturas de tres titulaciones distintas. En dos de estas asignaturas, se llevó a cabo un análisis por medio de cuestionarios para recabar información de los alumnos sobre el proceso de repaso en el aula. En las otras dos, se llevaron a cabo cambios en el mecanismo seguido para repasar al inicio de clase y se utilizaron también encuestas para evaluar la opinión de los estudiantes sobre estos cambios.

A modo de resumen, algunas conclusiones que se pueden extraer de esta iniciativa son:

- El repaso en el aula es considerado como un proceso fundamental por los estudiantes que, sin embargo, no perciben la pérdida de contexto como un problema grave.
- Los resultados en algunos de los grupos encuestados parecen indicar que, a pesar de su importancia para los estudiantes, el repaso en el aula no se realiza de manera tan habitual como cabría suponer.
- El uso de mapas conceptuales no es un mecanismo común a la hora de hacer el repaso en el aula, a pesar de que los alumnos encuestados lo valoran positivamente.
- A pesar de esta valoración, en general positiva, el valor percibido por los alumnos del uso de mapas conceptuales depende también de otros factores, como la naturaleza de la asignatura y su evaluación. En particular, en una de las asignaturas analizadas, al ser la evaluación de naturaleza fundamentalmente práctica, los alumnos prefieren emplear el tiempo en el aula resolviendo ejercicios y valoran menos el repaso teórico mediante mapas conceptuales.

En lo relativo a posibles líneas futuras de trabajo, hay que indicar que uno de los aspectos que la experiencia descrita en el artículo no ha cubierto es el de analizar el posible impacto sobre los resultados académicos (evaluación sumativa) que tiene el uso de los mecanismos de repaso basados en mapas conceptuales. El análisis de este potencial impacto se plantea como una posible línea de continuación del trabajo aquí descrito.

Adicionalmente, otra posible línea de continuación podría consistir en realizar un análisis del estado del arte de herramientas software para la elaboración de mapas conceptuales. El objetivo de este análisis sería el de sugerir a los alumnos el uso de una (o un conjunto limitado de) herramientas para elaborar sus mapas, algo que la presente experiencia no ha considerado (se usó pizarra o papel para elaborar y presentar los mapas).

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el proyecto regional de la Comunidad de Madrid eMadrid (S2009/TIC-1650). Los autores quieren expresar su gratitud hacia los profesores José Jesús García Rueda y Carmen Fernández-Panadero por sus valiosas sugerencias acerca de este artículo.

REFERENCIAS

[1] David Ausubel, Joseph Novak, Helen Anesian. “Educational Psychology: A cognitive view”, Holt, Rinehart, and Winston, New York, 2nd edition, ISBN: 78-0030899515, 1978.
[2] Alan Baddeley, “Human Memory: Theory and Practice, Revised Edition”, Allyn & Bacon, ISBN: 978-0205279487, 1997.
[3] Benjamin Bloom, “ Taxonomy of educational objectives: the classification of educational goals”, New York, Longmans, Green, 1956.
[4] C. C. Bonwell, J. A. Eison, “Active Learning: Creating Excitement in the Classroom”, ASHEERIC Higher Education Report No. 1, George Washington University, Washington DC, 1991.
[5] Isabelle D. Cherney, “The effects of active learning on students’ memories for course content”, Active Learning in Higher Education, vol. 9 n. 2, pp. 152-171, 2008.
[6] B. J. Daley, D. M. Torre. “Concept maps in medical education: an analytical literature review”, Medical Education, vol. 44, issue 5, pp. 440–448, 2010.
[7] Hermann Ebbinghaus. “Memory: A Contribution to Experimental Psychology”. Translated by Henry A. Ruger & Clara E. Bussenius (1913) Originally published in New York by Teachers College, Columbia University, 1885.
[8] Espacio Europeo de Educación Superior: Documentación básica. Disponible en: http://www.eees.es/es/documentacion (20/Mayo/2013)
[9] David Glenn, “Close the Book. Recall. Write It Down”, The Chronicle of Higher Education, vol. 55, issue 34, pp. A1, 2009.
[10] Jeffrey D. Karpicke, Henry L. Roediger, “The Critical Importance of Retrieval for Learning”, Science, vol. 319, n. 5865, pp. 966-968, 2008.
[11] Manuel Mahamud López, Juan María Menéndez Aguado. “Utilización de grabaciones en vídeo para aumentar la eficacia de las clases”, Jornadas de intercambio de experiencias en docencia universitaria en la Universidad de Oviedo, ISBN 978-84-8317-626-9, págs. 227-236, 2007.

Asignatura →	**FIM**			**CW**			**SI**		
Cuestión ↓	N	μ	σ	N	μ	σ	N	μ	σ
(a)	12	2.33	0.98	32	3.23	0.90	14	2.93	0.73
(b)	18	3.44	0.92	32	4.03	1.13	14	4.43	0.51
(c)	18	3.55	0.78	31	2.24	1.21	14	2.21	0.80
(d.i)	18	3.67	0.68	32	3.53	1.14	12	2.67	1.15
(d.ii)	18	4.22	0.94	32	3.57	1.04	12	2.75	0.62
(d.iii)	18	2.55	1.15	32	2.1	1.32	12	1.75	0.75
(e.i)	18	3.67	0.97	32	2.9	1.27	12	2.92	0.67
(e.ii)	18	3.61	1.09	32	3.27	1.23	12	2.25	0.87
(e.iii)	18	3.61	0.85	32	3.93	1.08	12	4.42	0.51
(f)	18	4.17	0.62	32	4.07	0.94	12	4.36	0.50
(g)	18	3.61	1.46	32	3.43	0.82	12	3	1.04

Tabla II

RESULTADOS DE LAS ENCUENTAS DE EVALUACIÓN DE LA EXPERIENCIA EN LAS ASIGNATURAS CON PARTICIPACIÓN PARCIAL Y *Sistemas de información*.

Test →	**Pre-test**		
Cuestión ↓	N	μ	σ
(a)	32	3.28	1.22
(b)	32	3.94	1.01
(c)	33	2.85	1.06
(d.i)	33	2.91	1.13
(d.ii)	33	3.24	1.03
(d.iii)	33	2.64	1.41
(e.i)	33	2.54	1.23
(e.ii)	33	3.54	0.75
(e.iii)	33	3.88	1.05
(f)	33	3.97	0.85
(g)	33	3.30	0.98

Test →	**Post-test**		
Cuestión ↓	N	μ	σ
(a)	20	3.2	1.28
(b)	20	3.9	1.07
(c.i)	20	2.65	1.14
(c.ii)	20	3.1	1.25
(c.iii)	20	3.2	1.4
(d)	20	3.1	1.16
(e)	20	2.8	1.15
(f)	20	3	1.26
(g)	20	3.4	0.94

Tabla III

RESULTADOS DE LAS ENCUENTAS DE EVALUACIÓN DE LA EXPERIENCIA EN *Procesamiento de formatos en aplicaciones telemáticas*.

[12] Marco Antonio Moreira. “Mapas conceptuales y aprendizaje significativo”, traducción al castellano del artículo publicado en *Cadernos do Aplicação*, Porto Alegre, 11(2), pp. 143-156, 1998.

[13] John C. Nesbit, Olusola O. Adesope, “Learning With Concept and Knowledge Maps: A Meta-Analysis”, Review of Educational Research, vol. 76, n. 3, pp. 413-448, 2006.

[14] Josep D. Novak. “Conocimiento y aprendizaje: los mapas conceptuales como herramientas facilitadoras para escuelas y empresas”. Alianza Editorial, ISBN: 978-84-206-2901-4, 1998.

[15] Joseph D. Novak, Alberto J. Cañas. “The Theory Underlying Concept Maps and How to Construct and Use Them”, Technical Report IHMC CmapTools 2006-01, Rev 2008-01, Florida Institute for Human and Machine Cognition, 2008.

[16] Michael Prince, “ Does Active Learning Work? A Review of the Research”, Journal of Engineering Education, vol. 93, issue 3, pp. 223–231, 2004.

[17] Alberto Regis, Pier Giorgio Albertazzi, Ezio Roletto. “Concept Maps in Chemistry Education”, Journal of Chemical Education, vol. 73, n. 11, November 1996.

[18] Joan Rué, “Enseñar en la Universidad: El EEES como reto para la Educación Superior”, Editorial Narcea, ISBN 978-84-27715585, 2007.

[19] Daniel L. Schacter. “The seven sins of memory: how the mind forgets and remembers”. Boston: Houghton Mifflin, ISBN 0-618-21919-6, 2001.

[20] Jennnifer Turns, Cynthia J. Atman, Robin Adams. “Concept maps for engineering education: a cognitively motivated tool supporting varied assessment functions”, Education, IEEE Transactions on, vol. 43, issue 2, 2000.

Modelo Cognitivo para la Docencia de Diseño de Redes mediante un Sistema de E-learning Inteligente

Elena Verdú Pérez, Luisa Regueras Santos, María Jesús Verdú Pérez, Juan Pablo de Castro Fernández
Departamento de Teoría de la Señal y Comunicaciones e Ingeniería Telemática,
Universidad de Valladolid
Campus Miguel Delibes, Paseo Belén 15, 47011 Valladolid.
elever@tel.uva.es, luireg@tel.uva.es, marver@tel.uva.es, jpdecastro@tel.uva.es.

Resumen- **Este artículo presenta un modelo cognitivo para la docencia de la asignatura "Laboratorio de Diseño y Configuración de Redes" que se imparte en la Universidad de Valladolid. El modelo se propone dentro del contexto del proyecto INTUITEL (*Intelligent Tutoring Interface for Technology Enhanced Learning*), un proyecto co-financiado por la Comisión Europea, cuyo objetivo es mejorar los sistemas de e-learning con el fin de que éstos sean capaces de ofrecer caminos de aprendizaje adaptados a las características y necesidades de los estudiantes.**

***Palabras Clave*- modelo cognitivo, aprendizaje personalizado, ontología pedagógica, virtualización de asignaturas**

I. INTRODUCCIÓN

La creación del Espacio Europeo de Educación Superior (EEES) ha supuesto un punto de inflexión en la educación universitaria en el que se adopta un modelo donde el estudiante es el centro del proceso de aprendizaje y tiene un papel mucho más activo. Paralelamente a este proceso de transformación, las universidades europeas están integrando sistemas de gestión del aprendizaje o LMS (*Learning Management Systems*) en sus estructuras, con el doble fin de facilitar la gestión docente y proporcionar herramientas que promuevan el aprendizaje activo.

Siendo el estudiante la parte central del proceso de aprendizaje, los LMS deberían ser capaces de adaptarse a las características y necesidades de los estudiantes; ya que el aprendizaje es una actividad cognitiva que difiere de un estudiante a otro, tal y como sostienen diversos autores [1] [2]. Puesto que no todos los estudiantes procesan y perciben la información de la misma forma, el uso de sistemas de aprendizaje que se adapten a las necesidades y características de los estudiantes mejora su satisfacción y sus resultados académicos y, en definitiva, consigue procesos de aprendizaje más eficientes y efectivos [3] [4]. Por otra parte, junto con la personalización, el uso de ontologías integradas en los LMS aumenta la efectividad de los sistemas de *e-learning* [5] y, más aún, es un elemento clave en los sistemas modernos de *e-learning*.

Los sistemas de *e-learning* personalizados deben adaptarse a las características de los estudiantes y de su entorno de aprendizaje así como a los conceptos ya adquiridos. Ésta es la idea de personalización que desarrolla el proyecto INTUITEL. Para guiar a los estudiantes en su proceso de aprendizaje, INTUITEL utilizará una ontología pedagógica integrada dentro del modelado de diferentes dominios específicos de conocimiento. Asimismo, en base a este modelado cognitivo, monitorizará el progreso del estudiante con el fin de ofrecerle caminos de aprendizaje adaptados a los conceptos que ya conoce y a sus características especiales.

Este artículo se centra en la descripción de un modelo cognitivo para la asignatura de "Laboratorio de Diseño y Configuración de Redes" que se imparte en la Universidad de Valladolid, el cual está integrado con una ontología pedagógica previamente definida por expertos pedagogos. La definición de este modelo permitirá personalizar los caminos de aprendizaje en función de las preferencias de aprendizaje y de los estados cognitivos de los estudiantes.

El uso de ontologías con fines de clasificación y aplicación a técnicas de resolución de problemas y razonamiento inductivo está muy extendido. Sin embargo, su uso para fines didácticos tiene connotaciones especiales, debido a la naturaleza de los procesos educativos. Por ello, parece conveniente trabajar en el desarrollo de ontologías específicas para el aprendizaje, como un paso fundamental hacia la creación de sistemas educativos adaptativos [6]. En el ámbito de la ingeniería, y sobre todo en el área de la programación, hay definidas varias ontologías para contextos educativos. En [7] y [8] se describe el proceso de diseño de una ontología para la enseñanza de los lenguajes de programación Java y C, respectivamente. En el ámbito de las redes de comunicaciones, en [1] se define una ontología para un curso sobre Ethernet, que se emplea en un sistema de personalización del proceso de *e-learning*. Sin embargo, en la definición de ninguna de estas ontologías se toma como base una ontología pedagógica, tal y como se propone en INTUITEL.

En el siguiente apartado se describe el proyecto INTUITEL, dentro del cual se desarrolla este trabajo. A continuación se describe el dominio de conocimiento para el que se va a desarrollar el modelado cognitivo, el cual será definido en el siguiente apartado junto con la ontología pedagógica sobre la que se sustenta dicho modelado. Finalmente, se exponen los resultados que esperan obtenerse tras la finalización de este trabajo.

II. El Proyecto INTUITEL

INTUITEL[1] es un proyecto de investigación cofinanciado por la Comisión Europea que persigue mejorar los sistemas de *e-learning* ofreciendo un sistema inteligente capaz de guiar y proporcionar un *feedback* a los alumnos a lo largo de su proceso de aprendizaje.

El objetivo de INTUITEL es mejorar el contenido *e-learning* y los LMS ofreciendo características propias de los tutores humanos. Un sistema habilitado INTUITEL (*INTUITEL-enabled*) proporcionará un entorno de aprendizaje integrado que se configurará y adaptará a las necesidades de los estudiantes. Este sistema monitorizará su proceso de aprendizaje y su progreso con el fin de ofrecer un *feedback* formativo basado principalmente en el perfil del estudiante y en modelos pedagógicos relevantes. En concreto, el sistema analizará la actitud y el estilo de aprendizaje del estudiante, el contexto cultural y emocional en el cual tiene lugar el proceso de aprendizaje y factores ambientales y técnicos relevantes tales como ruido ambiental, ancho de banda disponible y características de la interfaz (como por ejemplo el tamaño de la pantalla).

El sistema INTUITEL está compuesto de cuatro componentes principales, tal y como puede verse en la Fig. 1. Un elemento clave es la ontología pedagógica, escrita en el lenguaje de ontología Web OWL, la cual proporcionará una forma unificada para describir el material y los caminos de aprendizaje. Asimismo, usando como base la ontología pedagógica, podrán definirse diversas ontologías específicas de cada dominio de conocimiento con un formato acorde a INTUITEL, proporcionando así al sistema un modelo cognitivo detallado.

Otro componente clave es el LMS integrado con INTUITEL (*INTUITEL-enabled* LMS) mediante unas interfaces apropiadas y específicas para cada LMS. El proyecto diseñará interfaces para la integración de INTUITEL con distintos LMS propietarios y de código abierto tales como Moodle e ILIAS. Esta integración permitirá a INTUITEL medir el progreso de aprendizaje del estudiante, interactuar directamente con él y recomendarle los objetos de aprendizaje óptimos, en función de su estado cognitivo actual y el resto de factores contextuales anteriormente mencionados.

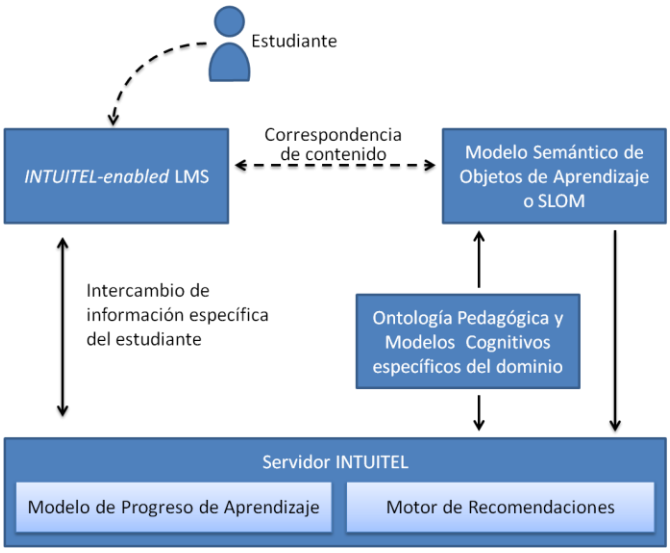


Fig. 1. Estructura de INTUITEL [Fte: elaboración propia, basada en www.intuitel.de/structure]

Asimismo, para facilitar el intercambio del material de aprendizaje, se ha especificado un nuevo formato contenedor, el SLOM (*Semantic Learning Object Model*). Este modelo define cómo empaquetar contenidos y metadatos de un curso habilitado INTUITEL. Pero el objetivo principal de SLOM es proporcionar el modelado de los metadatos que relacionarán los materiales de aprendizaje disponibles en el LMS con el modelado específico del dominio de conocimiento y el modelo pedagógico. De esta forma proporcionará al servidor INTUITEL la información necesaria para el proceso de razonamiento.

Finalmente, para guiar de forma óptima a cada usuario a través del material de aprendizaje, el Modelo de Progreso de Aprendizaje o LPM (*Learning Progress Model*) deducirá la posición actual del estudiante en el modelo cognitivo. A partir de esta posición y usando diversos metadatos sobre el estudiante así como también información contextual, el Motor de Recomendaciones creará indicaciones sobre cuál es el material de aprendizaje que el estudiante debería estudiar a continuación, ayudándole así a seguir el camino de aprendizaje más eficiente para abordar con éxito la asignatura.

III. El Dominio de Conocimiento: Asignatura "Laboratorio de Diseño y Configuración de Redes"

La asignatura de "Laboratorio de Diseño y Configuración de Redes" es una asignatura obligatoria de 6 ECTS de tercer curso de la mención en Ingeniería Telemática del Grado en Ingeniería de Tecnologías Específicas de Telecomunicación que se imparte en la E.T.S.I. de Telecomunicación de la Universidad de Valladolid. Es una asignatura de orientación eminentemente práctica dentro del bloque de materias específicas de telemática, donde se aplican conceptos de redes de datos que han sido vistos en otras asignaturas como "Conmutación y Encaminamiento", "Ingeniería de Protocolos" y "Redes y Servicios Telemáticos". Asimismo, está directamente relacionada con las asignaturas "Administración y Gestión de Redes de Comunicaciones", "Teletráfico" y "Seguridad en Redes de Comunicaciones", proporcionando entre las cuatro la base para abordar de forma práctica el diseño, planificación y gestión de una red de comunicaciones (ver Fig. 2). El principal objetivo de esta asignatura es que el alumno sea capaz de aplicar los conceptos adquiridos en otras asignaturas sobre protocolos, redes y servicios telemáticos en el diseño y configuración de una red IP real.

Dado su carácter práctico, esta asignatura no incluye ninguna clase teórica, sino que todas las actividades docentes son principalmente prácticas, con un alto porcentaje de carga docente presencial en el laboratorio. Concretamente, el 75% de la docencia se imparte en el laboratorio y el resto está dedicado a la realización de seminarios (3 y 1 hora semanales, respectivamente).

En las clases de laboratorio los alumnos realizan por parejas una serie de prácticas de diferente naturaleza: desde prácticas de configuración y simulación con la herramienta

[1] www.intuitel.eu

OPNET Modeler 17.5 hasta prácticas de configuración con equipos reales, así como un proyecto de diseño de un Sistema de Cableado Estructurado (SCE).

Fig. 2. Contextualización de la asignatura "Laboratorio de Diseño y Configuración de Redes" dentro de su plan de estudios.

Asimismo, en los seminarios se abarcan cuestiones claves de la asignatura pero desde un enfoque práctico y centrado en el trabajo en equipo y el diálogo entre profesor-alumno y alumno-alumno. En concreto, en los seminarios los alumnos trabajan en aspectos relacionados con conceptos claves en el diseño de redes a partir del desarrollo de actividades de aprendizaje colaborativo y de ejercicios guiados. Así, por ejemplo, para abordar los principios de diseño de red, los alumnos son divididos en grupos siguiendo una estrategia de aprendizaje llamada *jigsaw* o puzle donde a cada miembro del grupo se le asigna como experto un apartado de un capítulo de un libro sobre diseño de red [9], el cual tiene que preparar junto con el resto de expertos para explicárselo posteriormente a sus compañeros de grupo. Finalmente, y con el fin de verificar que se han alcanzado los objetivos de aprendizaje, cada alumno tiene que responder una serie de preguntas generales sobre el tema.

La asignatura se desarrolla con el apoyo de una plataforma Moodle ubicada en el Campus Virtual de la Universidad de Valladolid. Este LMS se utiliza como repositorio del material de aprendizaje (documentación, enunciado de los seminarios y laboratorios…), como forma de comunicación y como herramienta de gestión de la asignatura.

IV. Modelado Cognitivo

En INTUITEL, el modelado cognitivo de cada asignatura o curso consiste en modelar el dominio de conocimiento específico siguiendo el formato unificado definido en una ontología pedagógica previamente desarrollada por expertos pedagogos. Por tanto, antes de abordar el modelo cognitivo, es necesario conocer cuáles son las bases de dicha ontología pedagógica.

A. *Ontología pedagógica*

La ontología pedagógica describe cómo se clasifica e interrelaciona el material de aprendizaje para hacerlo compatible y utilizable por INTUITEL.

La ontología pedagógica define tres niveles de objetos de aprendizaje [10]:

1) Dominio de conocimiento (KD – *Knowledge Domain*): se corresponde con la asignatura o curso.
2) Contenedor de concepto (CC – *Concept Container*): equivalente a un tema o lección.
3) Objeto de conocimiento (KO – *Knowledge Object)*: contenido propiamente dicho (actividades, presentaciones, documentos, foros…). Los KO se describen mediante un tipo de conocimiento (orientación, explicación, tarea,…) y un tipo de medio (vídeo, texto, audio, tabla, blog, chat, formulario,…).

Un KD contiene uno o más CC, que a su vez están formados por uno o más KO. Los CC y los KO se relacionan entre sí formando caminos de aprendizaje (LP – *Learning Path*). La pedagogía ontológica definida en INTUITEL incluye unos caminos de aprendizaje básicos que serán empleados por el motor de razonamiento de INTUITEL. Concretamente, se utilizan dos niveles para los caminos de aprendizaje: 1) las relaciones entre CC, las cuales conforman caminos de aprendizaje de macro-nivel o macro LP, y 2) las relaciones o secuenciación de KO dentro de un CC que forman caminos de aprendizaje de micro-nivel o micro LP. La pedagogía ontológica define dos tipos principales de macro LPs: el jerárquico y el secuencial. Los diseñadores pueden crear macro-LPs de nuevos tipos o utilizar alguno de los dos predefinidos. Para ello, la pedagogía ontológica proporciona dos relaciones básicas entre CC (macro-nivel) para modelar caminos de tipo jerárquico ('*hasTopDownLikeRelation'* y '*hasBottomUpLikeRelation*') y otras dos para modelar caminos de tipo secuencial ('*hasFromOldToNewLikeRelation*' y '*hasFromNewToOldLikeRelation*'). Para definir un macro LP el diseñador puede elegir una de las relaciones existentes, la que más se aproxima al camino propuesto y usarla tal cual o crear una subpropiedad de la misma, asignándole un nombre, un título y una breve descripción. El poder crear subpropiedades facilita la definición de múltiples macro LPs del mismo tipo. Asimismo, las relaciones definidas para conectar KO (micro-nivel), dentro de un CC, permiten expresar diferentes aproximaciones pedagógicas: aprendizaje multi-estado (tanto basado en simulación como en buenas prácticas) y aprendizaje basado en investigación (abierto y estructurado). La clasificación de KO por tipos de medio y la definición de otras nuevas relaciones entre KO permiten también establecer caminos de aprendizaje teniendo en cuenta el nivel de abstracción o concretización de los KO. Para conocer más detalles de esta parte de la pedagogía ontológica, se recomienda consultar [10].

B. *Modelo cognitivo*

El modelo cognitivo propuesto para la asignatura "Laboratorio de Diseño y Configuración de Redes" consiste en la definición de dos caminos de aprendizaje de macro-nivel. El primero sigue un esquema próximo al camino cronológico y el segundo se aproxima más al camino jerárquico:

1) Camino de Aprendizaje Clásico (Fig. 3): relación '*hasLogicalNextStep1*' (subpropiedad de '*hasFromOldToNewLikeRelation*').
2) Camino de Aprendizaje Jerárquico Alternativo (Fig. 4): relación '*hasHierarchicalNextStep1'* (subpropiedad de '*hasTopDownLikeRelation*').

Las Fig. 3 y Fig. 4 muestran los CC pertenecientes al KD "Diseño de Red" así como las relaciones existentes entre ellos para los dos macro LP propuestos. Hay que tener en cuenta que el motor INTUITEL sólo trabaja con secuencias de CC, por lo que las relaciones se establecen entre cada 2 CC formando secuencias de CC y el nombre de la relación es lo que identifica el macroLP correspondiente. Las cajas moradas y azules claras se usan para los CCs que pertenecen exclusivamente al Camino de Aprendizaje Clásico y al Jerárquico Alternativo, respectivamente; mientras que las cajas azules representan CCs que se usan en los dos caminos (es decir, son compartidos por ambos).

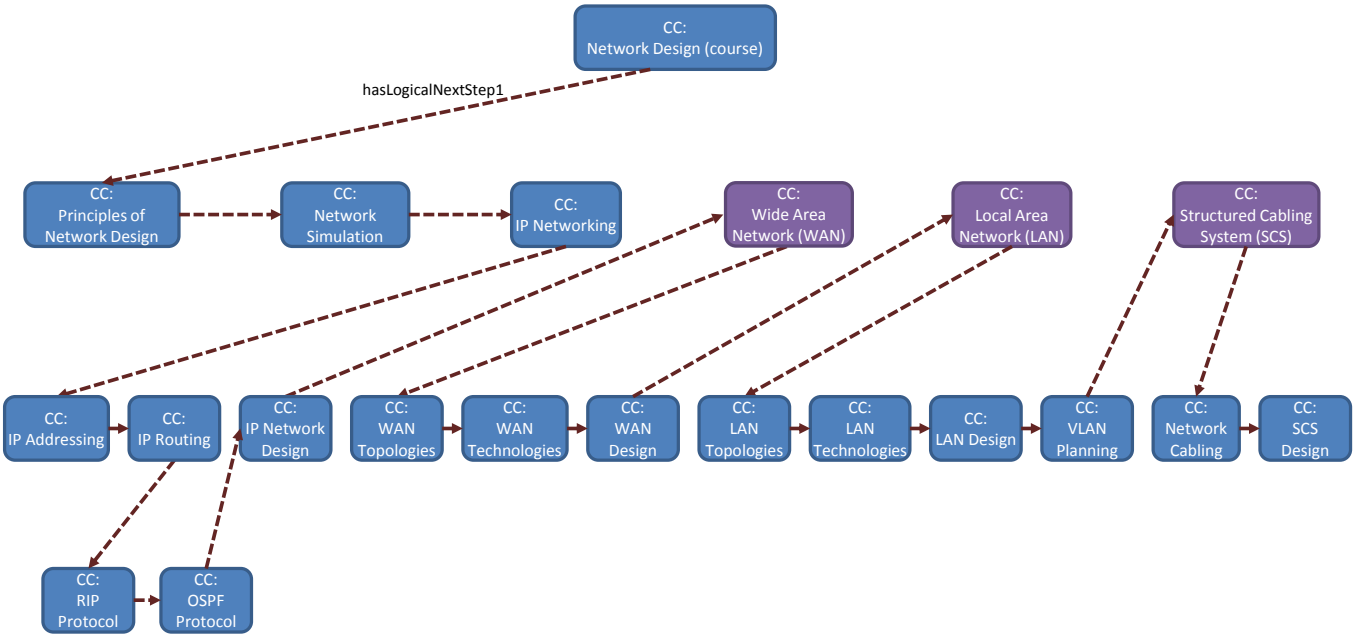


Fig. 3. Camino de Aprendizaje Clásico para el dominio de conocimiento "Diseño de redes"

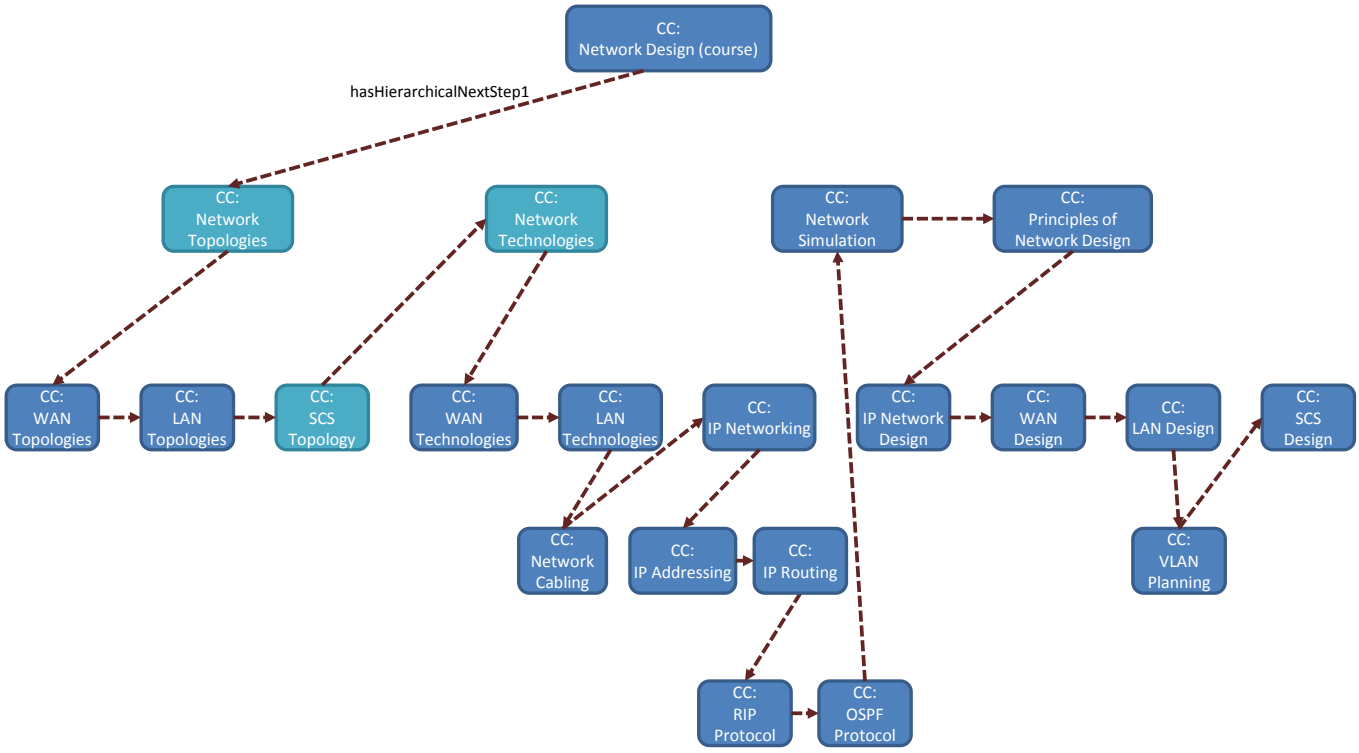


Fig. 4. Camino de Aprendizaje Jerárquico Alternativo para el dominio de conocimiento "Diseño de redes"

Por otra parte, cada CC puede contener uno o más KO de diferente naturaleza o tipo de conocimiento (presentaciones, ejercicios guiados…) y de diferentes características o tipo de medio (texto, imagen, vídeo…) lo cual permitirá definir varios caminos de aprendizaje (micro-nivel).

Así, por ejemplo, para aprender el concepto de cableado de red a los alumnos se les puede ofrecer dos caminos de aprendizaje con diferentes actividades cada uno (ver Fig. 5), uno basado en un camino de aprendizaje multi-estado de buenas prácticas y otro basado en un camino de aprendizaje de investigación estructurada. Por un camino (relaciones en azul), los alumnos reciben una explicación de los diferentes tipos de cableado de red a través del uso de una presentación y una tabla resumen realizadas por el profesor; mientras que por el otro camino (relaciones en granate), a los estudiantes se les presentan varias preguntas sobre diferentes fotos de tipos o elementos de un cableado de red y deben ser ellos quienes los identifiquen, estudien y presenten al resto de compañeros los resultados obtenidos. En ambos casos, posteriormente se les proporciona un ejemplo guiado sobre cómo se debe realizar el cableado de una red a través de un tutorial basado en texto y otro en video (generando así nuevamente dos posibles caminos de aprendizaje) y en un último paso son los propios alumnos los que deben hacer un ejercicio en el que se encarguen de realizar el cableado de una red. Las flechas rosas y verdes identifican distintas aproximaciones o subcaminos a seguir: desde más concreto (vídeo o tabla) hasta más abstracto (texto o presentación con diapositivas) o viceversa. La elección de una u otra aproximación se producirá por una elección del alumno, al ser consultado por INTUITEL, o teniendo en cuenta su historial.

Finalmente, en la Tabla I se puede observar una muestra de cuál sería el comportamiento esperado tanto por parte de los alumnos como por parte del sistema INTUITEL para un fragmento de los caminos de aprendizaje vistos anteriormente.

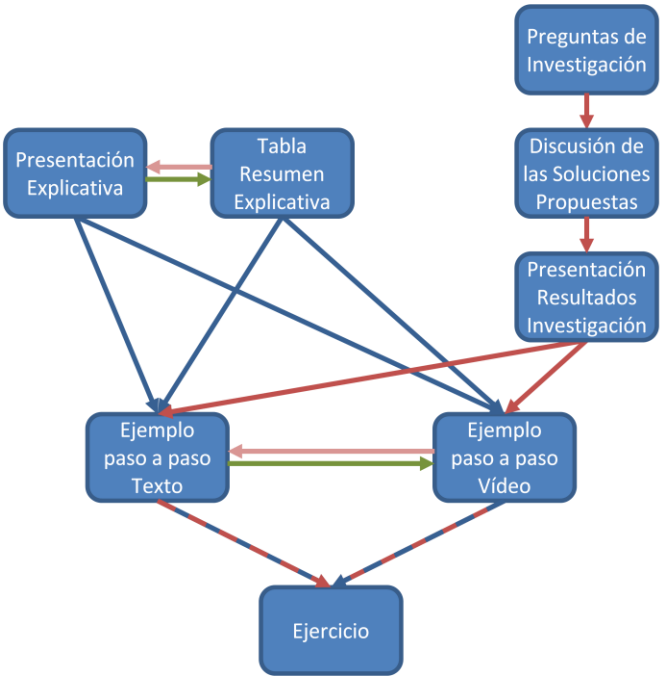


Fig. 5. Ejemplo de diferentes caminos de aprendizaje (micro-nivel) dentro del "CC: *Network Cabling*".

Tabla I
EJEMPLO DE COMPORTAMIENTO ESPERADO POR EL ESTUDIANTE Y POR INTUITEL PARA DIFERENTES KOS DENTRO DEL "CC: NETWORK CABLING"

KO	Comportamiento esperado del estudiante	Comportamiento esperado de INTUITEL
Presentación Explicativa sobre Cableado de Red (KO_01)	Ver y leer las transparencias durante 8 minutos	Comprobar si el estudiante ya ha completado el KO_02: -Si: Recomendar KO_03 -No: Recomendar KO_02 con un mensaje indicando que este nuevo KO es una visión más concreta del mismo tipo de conocimiento
Tabla Resumen Explicativa sobre Cableado de Red (KO_02)	Ver la tabla y leer su contenido durante 3 minutos	Comprobar si el estudiante ya ha completado el KO_01: -Si: Recomendar KO_03 -No: Recomendar KO_01 con un mensaje indicando que este nuevo KO es una visión más abstracta del mismo tipo de conocimiento

V. CONCLUSIONES

En este trabajo se ha presentado un modelo cognitivo para la docencia de una asignatura de diseño de redes con soporte en una plataforma Moodle habilitada con interfaces INTUITEL que permitirá ofrecer a los alumnos recomendaciones sobre cuál es el mejor camino de aprendizaje a seguir en cada caso.

El modelo cognitivo creado no es un mapa conceptual completo o una réplica de la estructura de las redes de comunicaciones sino que refleja la visión de los autores sobre los bloques conceptuales que es importante estudiar y conocer en la asignatura de Laboratorio de Diseño y Configuración de Redes así como los caminos de aprendizaje que se pueden seguir.

Actualmente, el modelo está siendo validado, a la vez que se diseñan otros componentes de INTUITEL. El sistema completo estará disponible en el curso 2014-2015, cuando podrá completarse la validación del modelo propuesto.

En el estado actual de validación, los modelos cognitivos se están evaluando mediante discusiones en un *Focus Group* y evaluaciones entre pares mediante cuestionarios. El objetivo es comprobar la completitud de los modelos y si son adecuados para poder ser utilizados por el sistema INTUITEL. Cuando el primer prototipo del sistema esté disponible se podrá evaluar su respuesta aplicando casos de prueba basados en el modelo de conocimiento definido, en los que se describirá la respuesta deseada respecto a posibles comportamientos del estudiante (casos de prueba ficticios), así como pruebas con estudiantes reales que utilizarán el sistema INTUITEL durante el curso 2014-2015. La validación del sistema permitirá comprobar si el modelo cognitivo especificado para el aprendizaje del diseño de redes, constituye un *input* de conocimiento pedagógico eficaz que, junto con otros *inputs* de naturaleza contextual o técnica, posibilita que INTUITEL pueda recomendar caminos de aprendizaje adecuados a los alumnos.

AGRADECIMIENTOS

La investigación que ha dado lugar a estos resultados ha recibido financiación del Séptimo Programa Marco de la

Unión Europea (PM7/2007-2013) en virtud del acuerdo de subvención nº 318496. El contenido de esta publicación es responsabilidad exclusiva de los autores y en ningún caso debe considerarse que refleja los puntos de vista de la Unión Europea.

REFERENCIAS

[1] P. Gomes, B. Antunes, L. Rodrigues, A. Santos, J. Barbeira, y R. Carvalho, "Using Ontologies for eLearning Personalization". En Proceedings of the 3rd ELearning Conference-Computer Science Education, 2006.

[2] M-G. Lee, "Profiling students' adaptation styles in Web-based learning", Computers & Education, vol. 36, n. 2, pp. 121-132, 2001.

[3] E. Verdú, L.M. Regueras, M.J. Verdú, J.P. de Castro, y M.A. Pérez, "An analysis of the Research on Adaptive Learning: The Next Generation of e-Learning", WSEAS Transactions on Information Science & Applications, vol. 5, n. 6, pp. 859-868, 2008.

[4] M. Gaeta, F. Orciuoli y P. Ritrovato, "Advanced ontology management system for personalised e-Learning", Knowledge-Based Systems Contents, vol. 22, pp. 292-301, 2009.

[5] S.R. Heiyanthuduwage y D.D. Karunaratne, "A Learner Oriented Ontology of Metadata to Improve Effectiveness of Learning Management Systems", Special Issue of the International Journal of the Computer, the Internet and Management, vol. 14, no. SP1, pp. 42.1-42.6, 2006.

[6] S. Sosnovsky, y T. Gavrilova, "Development of educational ontology for c-Programming," International Journal Information Theories & Applications, vol. 13, n. 4, pp. 303-308, 2006.

[7] G. Ganapathi, R. Lourdusamy y V. Rajaram, "Towards Ontology Development for Teaching Programming Language", En Proceedings of the World Congress on Engineering 2011, vol. 3, pp. WCE 2011, 2011.

[8] S. Sosnovsky y T. Gavrilova, "Development of Educational Ontology for C-programming", International Journal Information Theories & Applications, vol. 13, pp. 303-308, 2006.

[9] C. Long, IP Network Design, McGraw-Hill, 2001.

[10] C. Swertz, A. Schmölz, A. Forstner et al. "A Pedagogical Ontology as a Playground in Adaptive Elearning Environments", En Proceedings of the 5th International Conference on Advanced Science and Technology, 2013 (en prensa).

Aprendizaje Social y Gamificación en una Asignatura de Redes de Ordenadores

M. E. Sousa-Vieira, J. C. López-Ardao, M. Fernández-Veiga, M. Rodríguez-Pérez
Departamento de Ingeniería Telemática,
Universidad de Vigo,
c/Maxwell, s/n, Campus Universitario, Vigo.
estela@det.uvigo.es, jardao@det.uvigo.es, mveiga@det.uvigo.es, miguel@det.uvigo.es

***Resumen*—Resulta ampliamente aceptado que nos encontramos ante una generación de estudiantes caracterizada por encontrarse ante un espectacular desarrollo de las tecnologías de la información y las comunicaciones, los llamados "nativos digitales", y que como consecuencia de ello poseen diferentes patrones de trabajo, atención y preferencias de aprendizaje, y más aptitudes para afrontar procesos de aprendizaje social. Por ello, parece lógico que los profesores y sistemas educativos desvíen parte de sus esfuerzos docentes en este sentido. Aunque las redes sociales constituyen un instrumento poderoso para incorporar dimensión social a los sistemas clásicos de enseñanza online, en concepto no toman en cuenta las especificidades de la educación, por lo que en los últimos años hemos estado trabajando en el desarrollo de un sistema software que extiende las funcionalidades básicas de una red social para adaptarla a su uso en entornos educativos, incorporando actividades colaborativas de tipo social y mecanismos de recompensa basados en la teoría de juegos y en la comparación social, con la convicción de que pueden aumentar la motivación de los alumnos y mejorar sus procesos de aprendizaje. En esta comunicación describimos la experiencia de uso del sistema llevada a cabo en la asignatura "Redes de Ordenadores" de 2º curso del Grado de Ingeniería de Telecomunicación.**

***Palabras Clave*—Aprendizaje informal, gamificación, aprendizaje social, redes sociales.**

I. INTRODUCCIÓN

Si bien con retraso respecto a lo ocurrido en otros ámbitos socioeconómicos, finalmente el impacto transformador de las tecnologías de la información ha comenzado a sentirse en el campo de la educación, incluidas las instituciones de enseñanza superior, y viene sustentado tanto por el lado de la oferta como por el de la demanda.

Los estudiantes actuales, que pertenecen a la generación de los llamados "nativos digitales" por no haber conocido el mundo sin Internet, poseen nuevos patrones de atención, trabajo y preferencias de aprendizaje y más aptitudes para afrontar procesos de aprendizaje informal y social [1], [2], [3], [4]. Son intuitivamente competentes explorando y probando nuevas cosas con ayuda de la tecnología. La multitarea forma parte de su idiosincrasia y esto puede ocasionar aplazamiento de los objetivos, pérdida de la capacidad de abstracción y visión superficial de la información, en lugar de una comprensión más profunda y sosegada. Sin embargo, son más sociales y se comunican constantemente, creando con suma facilidad nuevas relaciones principalmente en la red. Además son inteligentes, eficientes en la consecución de sus objetivos cuando están motivados y capaces de localizar y movilizar gran cantidad de recursos materiales y humanos para sus propósitos.

La necesidad de satisfacción rápida es una de las características de los nuevos estudiantes que tiene mayores implicaciones en la enseñanza, entre ellas la dificultad con materias que impliquen el desarrollo de estructuras de conocimiento complejas o que demanden mucha dedicación y práctica, por lo que disponer de entornos de aprendizaje que hagan más atractivo y gratificante el estudio de estas disciplinas puede ser de gran ayuda para ellos. La motivación también puede surgir del reconocimiento social por haber resuelto un problema o haber conseguido un objetivo de manera satisfactoria, tanto de manera individual como por haber colaborado en un grupo. La comparación social [5] también puede resultar una herramienta muy efectiva como impulsora y motivadora del aprendizaje. En este sentido, el empleo de simulaciones [6], juegos [7], [8] o elementos del diseño de juegos (lo que se conoce como gamificación [9], [4]) en la enseñanza puede dar lugar a experiencias con gran éxito.

Otra característica esencial del comportamiento de los nativos digitales es que aprenden fundamentalmente en el contexto, en respuesta a una demanda o para resolver un problema particular, lo que motivó también que en los últimos años se dedicasen muchos esfuerzos investigadores en el área del aprendizaje basado en problemas. Pero una vez más, la forma de enfrentarse a sus problemas es sobre la marcha, en la modalidad multitarea buscando en Internet para encontrar información, vídeos, juegos o cualquier otro material relacionado. Alternativamente, exploran en sus redes sociales en la búsqueda de una persona que les pueda ayudar. Ello da lugar a que ocurran en paralelo múltiples experiencias de aprendizaje fragmentadas, relativamente cortas (debido al corto espacio temporal de atención mostrado por el aprendiz) y en muchos casos no hay ninguna necesidad percibida para aprender o memorizar algo para su uso posterior, ya que se puede repetir la búsqueda cuando sea necesario.

En resumen, mientras este nuevo modo de aprendizaje de la generación Internet puede ser considerado por algunos como una evidencia de la caída en la superficialidad, otros ven en ello una evolución natural en el desarrollo de nuestro conocimiento colectivo, tratando este tipo de aprendizaje como una tendencia a tener en cuenta, aceptar y adaptarse a ella.

Tengamos en cuenta que el aprendizaje tradicional es esencialmente formal, es decir, estructurado y dirigido por el profesor en torno a conocimiento explícito, y se halla recogido en medios de diversa índole (libros, vídeos, textos, audio, etc.). Frente a este tipo de conocimiento se encuentra el aprendizaje informal, cuyo objetivo es la adquisición de

conocimiento tácito, no explícito, sin estructurar, difícil de expresar y transmitir. Se trata del conocimiento obtenido en el día a día, resultado de nuestra interacción con la sociedad, conocimiento que es intrínseco a cada persona, del que incluso no siempre se es consciente.

A pesar de que el conocimiento adquirido informalmente resulta fundamental en la formación continua de una persona (en [2] se indica que el 80% del conocimiento adquirido por una persona a lo largo de su vida se encuentra soportado por actividades informales), hasta hace poco resultaba difícil incorporarlo al aula por la dependencia obvia que tiene este aprendizaje en las relaciones sociales. En este sentido, las redes sociales han supuesto una revolución, convirtiéndose en una herramienta de enorme potencial para el aprendizaje social, ya que impulsan el aprendizaje en colaboración con otros, la imitación de conductas y prácticas consuetudinarias y la recomendación mutua tanto de los contenidos como de la reputación de los integrantes [5].

La incorporación de las TIC a la educación motivó que cada vez resultara más habitual el uso de plataformas software de soporte y apoyo a la docencia. No obstante, los sistemas tradicionales de aprendizaje (Learning Management Systems (LMS), ej. Moodle) fueron desarrollados para el aprendizaje formal y no tienen en cuenta las relaciones sociales ni las interacciones con el exterior del aula. Ante este inconveniente, el profesorado más innovador ha optado por llevar al aula soluciones más o menos ingeniosas, resultado de integrar distintos servicios y herramientas de la Web 2.0 (blogs, wikis, foros, etc.).

Recientemente, la necesidad de disponer de una plataforma educativa integrada con soporte para ambos tipos de aprendizaje motivó la aparición de un nuevo concepto, el entorno de aprendizaje social (Social Learning Environment (SLE)) que es una plataforma educativa construida sobre una red social, la formada por la comunidad educativa, y que debería incorporar herramientas y mecanismos diseñados específicamente para el aprendizaje, tanto formal como informal. Prueba de la importancia que está adquiriendo el aprendizaje social es que muchas de las plataformas de e-learning aparecidas en los últimos años están basadas en redes sociales. Sin embargo, cabe destacar que se trata de plataformas de red social genérica que incorporan a mayores la funcionalidad tradicional de los LMS, sin incluir herramientas ni mecanismos específicos para el aprendizaje informal: motivación, incentivo, reconocimiento social, recomendación social o aprendizaje personalizado.

En este contexto, en los últimos años hemos estado trabajando en el desarrollo de SocialWire [10], un entorno de aprendizaje social que extiende la funcionalidad básica de un popular motor de desarrollo de redes sociales (Elgg [11]) de código abierto, para poder realizar los procesos de aprendizaje social e informal antes comentados. Además de los módulos típicos de un LMS tradicional (tareas, tests, cuestionarios, formularios, encuestas, libro de calificaciones, rúbricas, e-portafolios) que también hemos desarrollado enriqueciéndolos con las funcionalidades que nos aporta el disponer de un entorno social, hemos creado módulos específicos para poder incorporar actividades colaborativas de tipo social y gamificación (retos, competiciones, mecanismos de recompensa, comparación social, autoexpresión, etc.). Esta plataforma social enriquecida puede asímismo resultar útil para mejorar indirectamente algunas competencias transversales de los estudiantes, como su capacidad crítica y sus dotes de liderazgo.

El tipo de actividades que contemplamos como posibles en una plataforma como ésta consisten en la propuesta de tareas que los estudiantes tendrán que resolver de forma individual o en grupo con la posibilidad de poder plantearlas como un juego. Por tareas entendemos el encargo de actividades que sean concretas, aunque no necesariamente formales (por ejemplo, responder a una pregunta o buscar información adicional sobre un tema o aspecto), medibles, en el sentido de que toda tarea debe producir un resultado (un texto, documento o recurso como respuesta, por ejemplo, o un programa de ordenador o cualquier producto objetivo de esta actividad), abiertas, esto es, con posibilidad de recibir múltiples respuestas, todas válidas.

Venimos realizando pruebas del sistema en un entorno real en nuestra escuela desde el curso 2010-2011, con alumnos de grado y máster, en asignaturas relacionadas con la materia Redes de Ordenadores, y nos consta que lleva dos años siendo utilizado por profesores de nuestra universidad de distintas áreas en materias de distinto tipo. Los resultados y realimentación obtenidos hasta el momento han sido muy motivadores y nos han animado a mejorar la funcionalidad inicial desarrollando nuevos módulos.

En esta comunicación describimos la experiencia llevada a cabo durante el curso 2012-2013 para introducir mecanismos de aprendizaje social y gamificación en la asignatura Redes de Ordenadores de 2º curso del grado de Ingeniería de Telecomunicación. Para ello, en primer lugar en la siguiente sección resumimos las funcionalidades de los distintos módulos que, como extensiones, hemos desarrollado para completar las posibilidades de interacción social y de aprendizaje basado en juegos de nuestra plataforma.

II. GAMIFICACIÓN DE ELGG

Nuestra plataforma se basa en Elgg, un popular motor de desarrollo de redes sociales de código abierto.

El núcleo de Elgg usa un modelo de datos unificado para manejar los diferentes objetos que pueden existir en el ecosistema de una red social. La clase ElggEntity contiene los atributos básicos y más generales de cualquier objeto, y la extensibilidad y flexibilidad de Elgg se basa en otras tres clases. La clase ElggRelationship puede conectar virtualmente objetos, estableciendo relaciones entre ellos (amistad, compartición de información, pertenencia a un grupo, etc.). La clase ElggMetadata permite añadir datos a los objetos para refinar sus atributos, aportando gran flexibilidad para crear objetos con funcionalidad diversa. Finalmente, la clase ElggAnnotation permite definir nuevas acciones sobre los objetos, dando a los usuarios la posibilidad de interactuar con ellos (hacer comentarios, votar, etc.).

Así, combinando objetos de estas clases, Elgg se puede extender fácilmente a un entorno social de aprendizaje, desarrollando módulos que soporten las funcionalidades requeridas.

Un inconveniente de Elgg de cara a su uso en entornos educativos es la falta de soporte para subgrupos, es decir, comunidades de estudiantes a los que se le asigna la misma tarea o con intereses compartidos. En este sentido, los módulos de

gestión de subgrupos que hemos desarrollado constituyen una extensión fundamental para poder dar soporte a actividades colaborativas.

Otra tarea que decidimos abordar de forma prioritaria fue la gamificación de Elgg. A continuación describimos algunos de los módulos que permiten la introducción de herramientas, técnicas y dinámicas de juego en el aprendizaje que hemos desarrollado.

En [12] puede verse una decripción detallada de otros módulos docentes que hemos añadido a Elgg.

A. Módulo preguntas

A través de este módulo cualquier miembro del grupo (profesor ó alumno) puede plantear una pregunta. Si el autor es un alumno, la pregunta deber ser aprobada y puntuada por un profesor del grupo antes de que se abra el período de respuesta. Durante el tiempo que permanece abierta la pregunta todos los miembros del grupo, de forma individual o colectiva, pueden contestar, corregir y comentar las respuestas que vayan surgiendo (en caso de que sean visibles), y los profesores pueden destacarlas.

En cualquier momento, los profesores pueden cambiar la visibilidad de las respuestas, tanto del contenido como de los autores, como un mecanismo básico para introducir competitividad o restringir inapropiados o vagos hilos de discusión. El momento de cierre es configurable, según el propósito de la actividad (por ejemplo, se puede conseguir competitividad cerrando la pregunta tan pronto como se obtenga la primera respuesta correcta). Y también lo es el momento de puntuación, porque aunque lo más usual será hacerlo cuando la pregunta esté cerrada, puede puntuarse también durante el período de respuesta para inducir otras dinámicas de juego. Eso sí, cuando se cierra una pregunta ya no es posible modificar las respuestas aunque sí añadir comentarios.

Los puntos asignados a las preguntas y a las respuestas cumplen dos propósitos simultáneamente. Por un lado, sirven para clasificarlas y medir su interés (el módulo permite ordenarlas por relevancia y por puntuación). Por otro, este módulo interacciona con el ránking de puntos de forma que las puntuaciones se ven reflejadas en el ránking del grupo, en momentos que también son configurables.

B. Módulo concursos

Un concurso se puede ver como un juego de estrategia que persigue recoger pistas, ideas, soluciones completas o sugerencias sobre un problema complejo o con solución múltiple. Aunque estos juegos se pueden plantear de forma cooperativa, es decir, el objetivo de un concurso es conseguir de forma colaborativa la solución de un problema, o competitiva, en cuyo caso se podría incentivar confundir o aprovecharse de otros participantes, en nuestro caso asumimos que son siempre del primer tipo.

Las respuestas pueden ser individuales o colectivas y en cualquier momento los profesores pueden cambiar la visibilidad de las mismas, tanto del contenido como de los autores.

A la hora de puntuar existen varias posibilidades. Una opción es que el profesor pueda distribuir puntos entre las respuestas de acuerdo con su calidad, completitud u otros criterios acordados. De forma alternativa, las respuestas (posiblemente corregidas o filtradas por los profesores) entran en un período de votación donde los demás miembros del grupo pueden distribuir votos siguiendo distintos criterios (en este caso puede ser conveniente que no sea visible la identidad de los autores para evitar comportamientos no deseados). El contexto, objetivo y tema del concurso determina la mejor opción de puntuación.

Dado que este módulo también interactúa con el ránking de puntos, finalmente, se asignan puntos proporcionalmente a los votos obtenidos por cada alumno.

C. Módulo ránking de puntos

Uno de los principales motivos que nos llevó a desarrollar SocialWire fue el convencimiento de que la interacción social online entre estudiantes fomenta la eficacia del aprendizaje. En los sistemas online, donde los usuarios no pueden interactuar cara a cara, la posibilidad de poder comparar los logros propios con los de otros participantes es de crucial importancia para motivar a los estudiantes. Uno de los mecanismos más sencillos, pero también más eficientes, para impulsar la dinámica de grupos es el uso de ránkings de miembros, que muestran varias cosas simultáneamente. En primer lugar, muestran los logros de cada usuario en el sentido de que la posición en el ránking es un buen referente de cómo un alumno llevó a cabo un trabajo en comparación con sus compañeros. En segundo lugar, se establece una jerarquía en el grupo. Una vez que se conoce, el ránking influye de forma inconsciente sobre todo el grupo: las respuestas, tareas y en general las contribuciones de los miembros que ocupan posiciones destacadas en el ránking probablemente serán tomadas más en consideración por el resto. Y en la dirección opuesta, dichos miembros estarán obligados a hacer trabajo de alta calidad en futuras actividades si quieren mantener su puesto en el ránking.

El módulo ránking de puntos que hemos desarrollado organiza toda la información sobre los puntos recibidos por cada miembro del grupo, mostrando el detalle de los puntos obtenidos en cada actividad así como quién los ha asignado.

III. APLICACIÓN

Como apuntamos en la introducción, venimos haciendo pruebas de la plataforma en asignaturas de grado y máster relacionadas con la materia Redes de Ordenadores desde el curso 2010-2011.

Concretamente en la asignatura Redes de Ordenadores de 2º curso del grado de Ingeniería de Telecomunicación desde el curso 2011-2012 (primer año de impartición) y nuestra idea es extenderla a otras asignaturas de cursos superiores relacionadas, como pueden ser Arquitectura y Tecnología de Redes, Teoría de Redes y Redes Multimedia, que representan una unidad temática coherente y desarrollan con distintos niveles de complejidad la disciplina de las redes de comunicaciones. La implementación secuencial nos permitirá observar la respuesta de nuestros estudiantes a este tipo de actividades y detectar la posible mejora (en hábitos de trabajo, participación, resultados, etc.) y el aumento o disminución de la reputación social previa.

Fig. 1. Preguntas del curso.

A continuación describimos las actividades propuestas durante el curso 2012-2013 para introducir aprendizaje social y gamificación en la asignatura Redes de Ordenadores.

- **Resolución colaborativa de dudas.**
  Esta actividad consiste en el planteamiento y resolución de dudas, problemas y preguntas de la materia a través del módulo de preguntas, a lo largo de todo el curso. Las preguntas son creadas por los alumnos y eventualmente por los profesores.
  De las creadas por los alumnos, cada pregunta pertinente y no repetida se premia con un punto de juego y cada respuesta más o menos satisfactoria (no quiere decir que sea del todo correcta, se valora también el esfuerzo por responder y que la respuesta aporte algo de interés con respecto a la pregunta) y no repetida (puede haber varias que se complementen o una que matice con sentido una respuesta anterior) se premia también con un punto de juego o excepcionalmente con dos si la respuesta es realmente buena o destacada.
  Las respuestas a las preguntas creadas por los profesores se premian con más puntos, 5 o 10, dependiendo de la dificultad de la pregunta (se pueden plantear como pequeños retos) o del efecto que se quiera conseguir (por ejemplo, dinamizar el juego o tratar de evitar o contrarrestar estrategias que disminuyen su utilidad). Además, puede premiarse la rapidez de la respuesta para aumentar la competitividad del juego.
  Los profesores van matizando y guiando las respuestas de los alumnos y finalmente indican la o las correctas o dan una respuesta en caso de que ninguna de las de los alumnos lo sea. El ránking parcial es público.
  En la Figura 1 se muestra una vista parcial del módulo preguntas. A lo largo de todo el curso, los alumnos plantearon 49 preguntas y los profesores 2, y la calidad de las respuestas fue bastante satisfactoria, siendo 0.45 la tasa de respuestas de 2 puntos frente al total.
  En cuanto al grado de participación, los pequeños cambios introducidos en el planteamiento y dinámica del juego durante este curso con respecto al anterior, en el que también propusimos esta actividad, orientados principalmente a aumentar la motivación de los alumnos (mayor frecuencia de la realimentación por parte de los profesores y bajada del valor de las respuestas a las preguntas planteadas por los profesores para no romper en exceso la dinámica del juego) parece que resultaron efectivos por lo menos en ese sentido, ya que observamos un incremento de participación del 50%.
- **Trabajo colaborativo en grupos temáticos.**
  Para realizar esta actividad, cada alumno debe seleccionar algún subgrupo temático relacionado con los contenidos de la materia (de entre los propuestos por los profesores). Durante dos meses, los alumnos deben buscar y compartir en el subgrupo, pero para toda la clase, recursos relacionados con el tema de su subgrupo (noticias de actualidad, enlaces a artículos interesantes, material de estudio, ejercicios, actividades, esquemas, vídeos, tutoriales, presentaciones, animaciones, etc.) incluyendo junto al recurso una breve descripción del mismo y dónde se halla su interés. Finalmente, entre todos los miembros del subgrupo deben escribir una entrada de blog comentando los recursos seleccionados. Se valora la variedad y calidad de los recursos y la actividad se premia con un máximo de 20 puntos, que en principio, se asignan por igual a todos los miembros del subgrupo, salvo que se observen claros desequilibrios en el trabajo realizado por cada uno.
  En cuanto a los resultados obtenidos, aunque el grado de participación fue un poco menor que en el juego anterior, la calidad de los recursos seleccionados fue altamente satisfactoria, constituyendo una valiosa fuente de recursos complementaria para la preparación y estudio de la asignatura.

Además de las que ya hemos ido apuntando, podemos destacar otras ventajas de las actividades de aprendizaje social propuestas:

- Altruismo: En la primera actividad, la resolución de dudas y problemas habituales ayuda a la comprensión conjunta de la materia. En la segunda, los alumnos aprenden tanto al hacer la búsqueda de sus recursos como al leer las contribuciones de sus compañeros.
- Espíritu crítico: En la primera actividad, se potencia a la hora de contestar las preguntas o hacer comentarios a las respuestas de los compañeros. En la segunda, a la hora de seleccionar los recursos.
- Autoexpresión: La necesidad de oportunidades para expresar originalidad e incluso identidad en el grupo se puede cubrir con las dos actividades.
- Reducción de las consecuencias de los fallos: No pasa nada si la respuesta a una pregunta no es correcta, los fallos también son necesarios para aprender.

En la Figura 2 se muestra el ránking final de los puntos conseguidos por los participantes en las dos actividades.

La calificación obtenida en esta actividad representa un cuarto de la calificación de la parte de evaluación continua de la asignatura (una tarea de programación llevada a cabo durante el último mes del curso supone otro cuarto y el resto

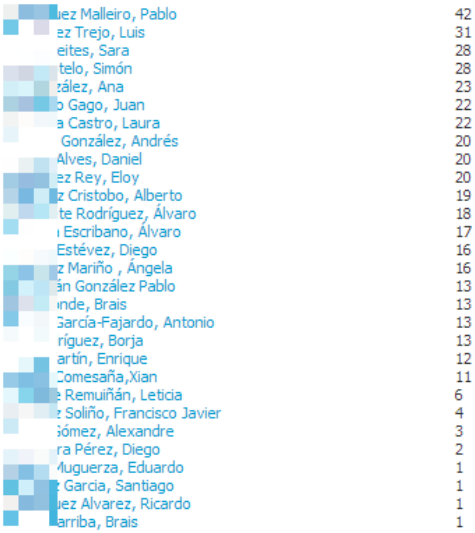


Fig. 2. Ránking de puntos.

recae en un examen parcial realizado a mediados de curso). A su vez, la calificación de la evaluación continua representa un 40% de la calificación de la asignatura, correspondiendo el 60% restante a un examen final de todo el contenido de la asignatura.

Por tanto, es necesario pasar los puntos del ránking a un valor entre 0 y 1. Para ello, si $med(P)$ es el número medio de puntos de juego de los alumnos participantes y $max(P)$ el máximo, se obtiene $M = min(med(P), max(P)/2)$. A este valor M se le asigna un 0.5, obteniendo un 1 todo alumno que tenga $2M$ o más puntos de juego. El resto de los alumnos obtendrá como calificación el resultado de dividir sus puntos entre $2M$. De esta forma, conseguimos evitar los efectos indeseados de un peso excesivo de los extremos del ránking a la hora de recompensar la participación en los juegos.

Observando la tabla de calificaciones de las tres partes de la evaluación continua podemos extaer las siguientes conclusiones:

- Los alumnos que ocupan posiciones destacadas en el ránking de puntos obtuvieron en general buenas calificaciones en la tarea de programación y en el examen parcial.
- Algunos de los alumnos que están entre los primeros del ránking habían obtenido malos resultados en el examen parcial, y trataron de mejorar la nota de la evaluación continua participando activamente en los juegos.
- Los alumnos que consiguieron menos puntos (generalmente los debidos a alguna pregunta planteada al principio del cuatrimestre) no realizaron las demás tareas de la parte de evaluación continua.
- Sólo un alumno de los que no participaron en los juegos tiene calificaciones altas en el examen parcial y en la tarea de programación.

Finalmente, apuntar que como continuación de este trabajo haremos un análisis más detallado que incluya también comparaciones con los alumnos que no han realizado las tareas de la parte de evaluación continua (dado que no es obligatoria), cuando dispongamos de los resultados de los exámenes finales.

AGRADECIMIENTOS

Este trabajo ha sido financiado por la Universidad de Vigo a través del proyecto de innovación educativa “Neoludismo: Juegos y Aprendizaje Informal como Estrategia Docente”.

REFERENCIAS

[1] S. Johnson, “Everything Bad Is Good for You”, Penguin, 2005.
[2] J. Cross, ”Informal Learning: Rediscovering the Natural Pathways that Inspire Innovation and Performance”, Pfeiffer, 2006.
[3] J. Vassileva, “Toward Social Learning Environments”. En IEEE Transactions on Learning Technology, vol. 1, n. 4, pp. 199-214, 2008.
[4] J. Lee and J. Hammer, “Gamification in Education: What, How, Why Bother?”. In Academic Exchange Quarterly, vol. 15, n. 2, pp. 1-5, 2011.
[5] L. Festinger, “ A Theory of Social Comparison Processes”. En Human Relations, vol. 7, n. 2, pp. 117-140, 1954.
[6] C. Aldrich, “Simulations and the Future of Learning”, John Wiley, 2004.
[7] M. Prensky, “Digital-game Based Learning”. McGraw-Hill,2001.
[8] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey, J. M. Boyle, “A Systematic Literature Review of Empirical Evidence on Computer Games and Serious Games”. En Computers & Education, vol. 59, n. 2, pp. 661-686, 2012.
[9] S. Deterding, D. Dixon, R. Khaled, L. Nacke, “ From Game Design Elements to Gamefulness: Defining Gamification”. En Mindtrek 2011.
[10] http://socialwire.es
[11] http://elgg.org
[12] M. E. Sousa, J. C. López, M. Rodríguez, M. Fernández, C. López, “Enabling Social Learning Environments at the College Level: A Toolbox”. En IEEE Global Engineering Education Conference, 2012.

Herramientas *open-source* para docencia en planificación de redes de comunicaciones

Jose-Luis Izquierdo-Zaragoza, Pablo Pavon-Marino
Departamento de Tecnologías de la Información y las Comunicaciones
Universidad Politécnica de Cartagena
Cuartel de Antiguones, Plaza del Hospital 1, 30202 Cartagena, España
{josel.izquierdo, pablo.pavon}@upct.es

***Resumen*- Este trabajo presenta la herramienta Net2Plan y la librería JOM, así como su aplicación como recursos docentes en el campo del diseño y planificación de redes de comunicaciones. Net2Plan está diseñada para ayudar al usuario en la definición y evaluación comparativa de sus propios algoritmos de planificación, así como en la simulación de algoritmos de control de admisión de conexiones, esquemas de protección y restauración, o algoritmos que reaccionan a fluctuaciones de tráfico. Por su parte, JOM es una librería que permite modelar problemas de optimización en lenguaje Java, promueve el prototipado rápido siguiendo una notación vectorial similar a la de lenguajes como MATLAB, y es una interfaz con *solvers* comerciales o de dominio público para obtener soluciones numéricas al modelo. Combinando Net2Plan y JOM, los usuarios obtienen un entorno completo para simular, analizar, dimensionar, optimizar y evaluar las prestaciones de sus propios diseños de red. Ambas herramientas están disponibles de forma gratuita en sus respectivos sitios web, junto con un repositorio completo de ejemplos.**

Palabras Clave*- Planificación de redes, optimización de redes, simulación por eventos discretos, Java, *open-source

I. INTRODUCCIÓN

La planificación y la optimización son procesos críticos en el despliegue y operación de redes de comunicaciones, pues requieren el mantenimiento de un cierto grado de compromiso entre prestaciones y coste. En este sentido, los estudiantes de titulaciones afines a la Ingeniería Telemática deben adquirir los conocimientos fundamentales que les permitirían realizar tareas de planificación y operación de redes, por ejemplo, dentro de una operadora o un proveedor de servicios de Internet.

Las tareas de planificación de red requieren del uso de herramientas software específicas [1]. Algunas están orientadas a la industria como OPNET, Cariden MATE Design, RSoft MetroWAND o WANDL IP/MPLSView. Entre ellas, quizás la más conocida sea OPNET, que dispone de licencias académicas gratuitas para universidades. En cuanto al campo de la investigación, las herramientas de planificación se reducen a implementaciones de algoritmos para problemas de planificación concretos, que algunos investigadores distribuyen públicamente con mayor o menor documentación.

Desafortunadamente, las herramientas actuales tienen importantes limitaciones como recursos docentes. Las implementaciones de algoritmos de planificación provenientes de la investigación resultan poco apropiadas didácticamente, ya que se enfocan en problemas muy concretos y avanzados. Por otro lado, las herramientas comerciales de planificación, carecen de flexibilidad para ejecutar diferentes algoritmos de diseño, restringiendo al usuario a utilizar los que incorpora la herramienta. Más aún, estos algoritmos no son conocidos ya que el software oculta su funcionamiento interno, y las empresas no publican detalles de sus implementaciones. En el caso de OPNET, las licencias académicas además prohíben explícitamente la comparación de sus resultados con los de otras herramientas competidoras [2]. No menos importante es que las herramientas comerciales se focalizan en *tecnologías concretas*, y tienen poca flexibilidad para ser utilizadas en estudios prospectivos sobre tecnologías futuras o variantes de problemas en tecnologías actuales, no incluidos dentro de los parámetros de uso estándar de la herramienta.

Desde un punto de vista docente, en este trabajo motivamos la importancia de promover una enseñanza, en la disciplina de diseño y planificación de redes, centrada en el aprendizaje de conceptos transversales: la optimización y evaluación de prestaciones en redes y el diseño de algoritmos. Esta estrategia se ha seguido en los temarios de las asignaturas "Teoría de redes de telecomunicaciones" y "Planificación y gestión de redes" para el Grado en Ingeniería de Sistemas de Telecomunicación (GIST) y el Grado en Ingeniería Telemática (GIT) de la Universidad Politécnica de Cartagena. El aprendizaje transversal se complementa con un estudio exhaustivo de algunas tecnologías relevantes, en otras asignaturas de los planes de estudio.

Las herramientas Net2Plan y JOM que se describen en este trabajo, nacieron en este contexto. Net2Plan [3] es una herramienta de planificación *open-source*, distribuida bajo la licencia de software libre LGPL. Está diseñada como una herramienta generalista, en el sentido de que no está restringida a ninguna tecnología concreta, lo cual habilita su aplicación a cualquiera de ellas. Además, permite a los usuarios ejecutar sus propios algoritmos de planificación, u otros ya integrados en la herramienta. Los diseños de red generados pueden ser analizados desde la interfaz gráfica. Asimismo se incluyen diversas herramientas de post-análisis, como un generador de informes (extensible por el usuario), un simulador de disponibilidad ante fallos, o un simulador de la evolución de la red ante fluctuaciones de tráfico.

Por otro lado, debido a que los algoritmos de planificación pueden formularse como problemas de optimización con restricciones (por ejemplo, problemas lineales, enteros, convexos…), también se ha desarrollado la librería JOM (Java Optimization Modeler) [4]. JOM permite modelar los problemas de optimización a un alto nivel

utilizando una sintaxis similar a MATLAB, interactuando con *solvers* gratuitos como GLPK o IPOPT, y comerciales como CPLEX, para obtener soluciones numéricas.

El objetivo del presente trabajo es describir las principales características y funcionalidades que proporciona el entorno formado por Net2Plan y JOM.

El resto del artículo se organiza de la siguiente manera. En las secciones 2 y 3 se describen las principales características de Net2Plan y JOM, respectivamente. En la sección 4, se realiza un caso de estudio práctico, utilizando las herramientas presentadas. En la sección 5, se relata la experiencia docente en el uso de dichas herramientas. Finalmente, en la sección 6 se presentan las conclusiones extraídas de este trabajo.

II. Net2Plan: Herramienta de planificación de redes open-source

Net2Plan está programada en lenguaje Java, y se distribuye bajo la licencia GNU Lesser General Public License (LGPL). Net2Plan tiene su origen en septiembre de 2011, como recurso docente para asignaturas de diseño y planificación de red en la Universidad Politécnica de Cartagena. Las primeras versiones, actualmente discontinuadas, se desarrollaron como una *toolbox* de MATLAB, sin embargo desde febrero de 2013 se migró a Java, lo que permitió conseguir una aplicación multiplataforma e independiente de software privativo.

La herramienta está específicamente diseñada para que los estudiantes puedan integrar sus propios algoritmos como clases Java, utilizando una interfaz de entrada/salida claramente definida. De esta forma, Net2Plan está concebida para que los estudiantes completen de forma progresiva sus propios diseños de red, encadenando algoritmos de forma sucesiva (Fig. 1). Por ejemplo, se parte de una red que solo contiene los nodos, y un algoritmo se encarga de definir los enlaces de acuerdo a una figura de mérito. Tras ello, otro algoritmo puede decidir de forma conjunta el encaminamiento y la capacidad de los enlaces, dada una matriz de tráfico. Como resultado, Net2Plan se convierte en una herramienta poderosa, ya que los estudiantes pueden ver paso a paso cómo sus diseños crecen, para posteriormente evaluarlos utilizando varias herramientas de post-análisis.

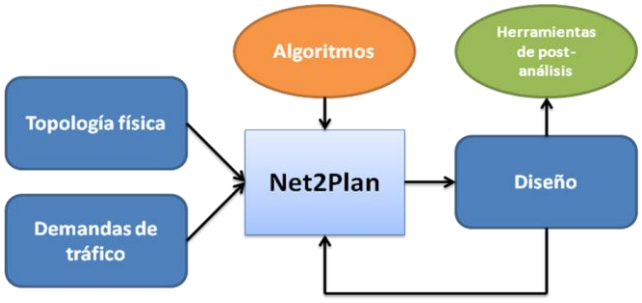


Fig. 1. Flujo de diseño con Net2Plan.

A. Marco teórico

Net2Plan define un formato de representación de red basado en conceptos abstractos como nodos, enlaces, rutas, demandas de tráfico y capas de red, con independencia de la tecnología. Esta es la idea clave que permite a Net2Plan no estar restringida a ninguna tecnología y, por tanto, poder aplicarse a cualquiera de ellas. Así, los problemas de planificación de redes reciben parte de esta información como parámetro de entrada (por ejemplo, topología de red y demandas de tráfico) y tratan de optimizar otros (por ejemplo, capacidades de los enlaces y encaminamiento).

El número de posibles variantes y familias de problemas de diseño de red es infinito. Más aún, los diseños aplicados a tecnologías particulares añaden sus propias restricciones y peculiaridades. En un intento de organizar didácticamente la enorme diversidad de los problemas que pueden aparecer, en la documentación de Net2Plan adoptamos la siguiente clasificación de los problemas de diseño de red, que es una extensión de la taxonomía clásica establecida por Kleinrock [5]:

- Problemas de diseño de topología (TA, *Topology assignment*): Los nodos y/o enlaces en la red son variables de decisión a optimizar.
- Problemas de asignación de capacidad (CA, *Capacity assignment*): Las capacidades de los enlaces son variables de decisión a optimizar.
- Problemas de definición del encaminamiento (FA, *Flow assignment*): El encaminamiento de las demandas de tráfico es la variable de decisión a optimizar.
- Problemas de asignación de ancho de banda o control de congestión (BA, *Bandwidth assignment*): El tráfico cursado para cada demanda es la variable de decisión a optimizar.

En la realidad (y en Net2Plan), estos problemas pueden aparecer de manera combinada. Por ejemplo un problema de tipo CFA (*Capacity and flow assignment*) implica la obtención conjunta de encaminamiento y capacidad de los enlaces.

B. Algoritmos y librerías

La filosofía de Net2Plan facilita la reutilización de software, ya que los algoritmos pueden ser modificados o reutilizados como parte de otros. Además, junto con Net2Plan se distribuyen un gran número de ejemplos, y su código fuente, los cuales se encuentran descritos de forma exhaustiva en el repositorio de ejemplos de la página web de la herramienta [3]. Los repositorios abiertos y la filosofía de código abierto favorecen la validación y la verificación, lo que implica un mayor grado de confianza en los resultados obtenidos.

Además, junto con Net2Plan se proporciona un conjunto librerías que ayudan en las tareas de creación y evaluación de algoritmos, como por ejemplo árboles de expansión, algoritmos de camino más corto, y otros de teoría de grafos. Para un listado completo y su API, el lector puede consultar [3].

C. Herramientas

Net2Plan proporciona dos interfaces de usuario: un entorno gráfico, y línea de comandos. En cualquiera de estos modos, la versión actual (0.2.1) dispone de seis herramientas:

- Diseño de red (*Network design*): Se utiliza para evaluar los diseños de red generados por algoritmos de planificación, ya sean los integrados o los desarrollados por el usuario, tratando aspectos como la topología de red, el encaminamiento del tráfico o la capacidad de los enlaces.
- Generación de matrices de tráfico (*Traffic matrix generation*): Se utiliza para generar y normalizar matrices de

tráfico, por ejemplo utilizando modelos aleatorios que pueden encontrarse en la literatura [6].

- Simulador de disponibilidad ante fallos (*Resilience simulation*): Se utiliza para evaluar la disponibilidad de red ante fallos aleatorios en nodos y/o enlaces. El simulador se basa en un algoritmo que define el patrón estadísitico de aparición de fallos y reparaciones, y el algoritmo de protección/restauración que determina cómo se reacciona ante ellos. En ambos casos, el usuario puede elegir un algoritmo integrado en Net2Plan o crear uno propio. Net2Plan calcula automáticamente una serie de estadísticos, como la disponibilidad de conexiones, o la fracción de tráfico que sobrevive en la red.
- Simulación de tráfico variable en el tiempo (*Time-varying traffic simulation*): Se utiliza para evaluar las prestaciones de algoritmos que reaccionan a variaciones en el volumen de tráfico a lo largo del tiempo (por ejemplo anomalías de tráfico, o fluctuaciones normales –lentas– de tráfico durante el día). El simulador se basa en un algoritmo que define el patrón estadístico de variación de tráfico, y el algoritmo de provisión que define cómo la red reacciona ante estos fallos. En ambos casos, el usuario puede elegir un algoritmo integrado en Net2Plan o crear uno propio.
- Simulación de control de admisión (*Connection-admission-control simulation*): Se utiliza para evaluar las prestaciones de algoritmos de control de admisión (CAC, *Connection Admission Control*), en que los recursos se reservan de forma dinámica bajo demanda. De manera similar a las anteriores, se basa en un algoritmo generador de conexiones, y un algoritmo CAC, pudiendo ambos ser definidos por el usuario.
- Generación de informes (*Reporting*): Net2Plan permite la generación de informes, ya sean integrados o definidos por el usuario, a partir de cualquier diseño de red. Esta herramienta se encuentra integrada dentro de todas las anteriores funcionalidades. Algunos de los informes integrados son: informe de retardo, de disponibilidad ante fallos, de probabilidades de bloqueo, robustez y supervivencia de tráfico ante fallos múltiples, o medidas topológicas de la red.

Toda la información sobre las distintas funcionalidades, así como el manual de uso, está disponible en la web de Net2Plan [3].

III. JOM: JAVA OPTIMIZATION MODELER

Con frecuencia los problemas de diseño de redes son resueltos mediante el modelado como problemas de optimización (por ejemplo, problemas lineales, lineales entero-mixtos…), y posteriormente la llamada a un *solver* para obtener la solución numérica del problema. En este contexto, las herramientas de modelado facilitan la definición de las variables de decisión, restricciones y función objetivo, constituyendo una interfaz con las, en general complejas, librerías de los *solvers*. AMPL y GAMS son ejemplos de herramientas de modelado comerciales.

Debido a que Java es un lenguaje de programación de propósito general, la sintaxis no resulta cómoda para el análisis matemático, sobre todo si se compara con un lenguaje específico para análisis matemático como MATLAB. No obstante, existe una gran diversidad de herramientas *open-source* para modelado en Java, pero en la opinión de los autores, ninguna de ellas es adecuada para su uso combinado con Net2Plan: bien porque generalmente es necesario el aprendizaje de un API concreto para cada tipo de problema (lineal, cuadrática…), como por ejemplo JOptimizer; o bien porque incluso requieren su propio compilador Java, como OptimJ. Por ello, en el momento de realizar la migración de Net2Plan de MATLAB a Java, se comenzó el desarrollo de JOM.

JOM es una librería *open-source* desarrollada en Java que puede comunicarse con varios *solvers* utilizando una sintaxis vectorial similar a MATLAB, lo que permite por ejemplo la introducción de restricciones en una única línea de código. La versión actual de JOM (0.1.8) puede comunicarse con GLPK (gratuito) y CPLEX (comercial) para resolver problemas lineales entero-mixtos, y con IPOPT (gratuito) para problemas diferenciables no-lineales, todo ello utilizando un API común. JOM se comunica directamente con las librerías precompiladas (.DLLs en Windows, .SOs en Linux), por medio de la librería Java Native Access (JNA).

En cualquier caso, JOM es independiente de Net2Plan y puede usarse para cualquier tipo de problema de optimización. Por su parte, Net2Plan utiliza JOM en todos los algoritmos de diseño de red basados en formulaciones. En la web de Net2Plan [3] se incluyen un gran número de ejemplos que usan JOM.

En la siguiente sección se utilizan de forma combinada Net2Plan y JOM para optimizar y analizar un diseño de red.

IV. CASO DE ESTUDIO: PROBLEMA DE ASIGNACIÓN DE TRÁFICO

En esta sección resolvemos un problema clásico de encaminamiento de demandas de tráfico en una red [7], para mostrar cómo los usuarios pueden modelar y resolver un problema de optimización utilizando Net2Plan y JOM.

El problema de encaminamiento que describimos decide los caminos de la red por los que se cursará el tráfico de un conjunto de demandas, tal que todo el tráfico sea cursado, sin que ningún enlace se sature. El objetivo de diseño será minimizar la congestión de red, medida como la utilización de red en el enlace cuello de botella (el enlace con mayor utilización en la red). La formulación completa se muestra a continuación:

Variables de decisión:	ρ, x_p	$p \in P$	
Función objetivo:	minimizar ρ		
Restricciones:	$\sum_{d \in D} \sum_{p \in P_d \cap P_e} x_p \le \rho \cdot u_e$	$\forall e \in E$	(1)
	$\sum_{p \in P_d} x_p = h_d$	$\forall d \in D$	(2)
	$0 \le \rho < 1$		(3)
	$x_p \ge 0$	$\forall p \in P$	(4)

donde *G(N, E)* es un grafo dirigido que representa la topología de nodos *N* y enlaces *E* de la red, u_e es la capacidad del enlace *e*, *D* es el conjunto de demandas de tráfico, h_d es el volumen de tráfico medio ofrecido para la demanda *d*. En este modelo, existe un conjunto *P* de caminos pre-computados, llamados caminos admisibles, y que son candidatos a poder cursar tráfico. P_d es el conjunto de caminos candidatos para cursar tráfico de la demanda *d* ($P_d \subseteq$ P), P_e es el conjunto de caminos candidatos que atraviesan el enlace *e* ($P_e \subseteq$ P). Por

otro lado ρ representa la utilización del enlace más ocupado, y x_p es el volumen de tráfico que cursa el camino p.

Las restricciones (1) fijan la utilización máxima de los enlaces, mientras que las restricciones (2) garantizan que todo el tráfico ofrecido se cursa. La restricción (3) limita la máxima utilización de los enlaces. Por último, aparecen las restricciones de no-negatividad del tráfico cursado (4).

En el listado 1, se muestra el fragmento de código utilizado para resolver en Net2Plan el problema de optimización, utilizando la librería JOM y GLPK (consultar [3] para más información sobre implementación de algoritmos). Destaca la simplicidad del código para ejecutar el algoritmo y encontrar la solución, comparada con soluciones alternativas como modelado en AMPL, o aprendizaje de la sintaxis propia de cada *solver*. Además, JOM permite el acceso a toda la librería Java y a las clases de usuario. Por ejemplo, con la clase *CandidatePathList* de Net2Plan se realiza automáticamente la creación y gestión de la lista de caminos candidatos para la formulación del problema. Aunque no se muestra en el ejemplo, JOM da acceso a los multiplicadores de Lagrange (variables duales) de las restricciones. Esto permite a los alumnos aprender el uso de estos multiplicadores para estimar cómo variaría la función objetivo ante cambios en las restricciones (por ejemplo el efecto en la congestión de un aumento de volumen de una demanda).

```
// Calcular un conjunto de caminos candidatos utilizando el algoritmo de
// los k-caminos más cortos sin ciclos para cada demanda de tráfico (k = 3)
CandidatePathList cpl = new CandidatePathList(netPlan, "K", "3");
int P = cpl.getNumberOfPaths();

// Crear un problema de optimización
OptimizationProblem op = new OptimizationProblem();

// Definir los parámetros de entrada
op.setInputParameter("u_e", netPlan.getLinkCapacityInErlangsVector(), "column");
op.setInputParameter("h_d", netPlan.getDemandOfferedTrafficInErlangsVector(), "column");
op.setInputParameter("delta_dp", cpl.computeDemand2PathAssignmentMatrix());
op.setInputParameter("delta_ep", cpl.computeLink2PathAssignmentMatrix());

// Definir las variables de decisión
op.addDecisionVariable("x_p", false, new int[] {P, 1}, 0, Double.MAX_VALUE);
op.addDecisionVariable("rho", false, new int[] {1, 1}, 0, 1);

// Definir las restricciones
op.addConstraint("delta_ep * x_p <= rho * u_e", "maximumLinkUtilizationConstraints");
op.addConstraint("delta_dp * x_p == h_d", "carryAllTrafficConstraints");

// Definir la función objetivo
op.setObjectiveFunction("minimize", "rho");

// Resolver el problema utilizando el solver GLPK
op.solve("glpk");
if (!op.solutionIsOptimal()) throw new RuntimeException("No se pudo encontrar solución");

// Obtener la solución e incluirla en el diseño de red
netPlan.removeAllRoutes();
netPlan.addRoutes(cpl, op.getPrimalSolution("x_p").to1DArray(), false);
```

Listado 1. Fragmento de código para resolver el problema de asignación de tráfico.

En las siguientes figuras se presenta la herramienta de diseño de red utilizada para resolver el problema de asignación de tráfico. El espacio de trabajo se divide en tres áreas: área de entrada de datos, ejecución e informes (parte derecha); panel de visualización de topología (parte superior izquierda); área de información general del diseño (parte inferior izquierda). En la Fig. 2 se muestra el proceso de ejecución del algoritmo: en primer lugar, se carga la topología y el conjunto de demandas de tráfico asociado; posteriormente, se selecciona el algoritmo deseado y se configuran sus parámetros; y finalmente se ejecuta. Los usuarios pueden explorar los resultados de manera gráfica, por ejemplo visualizando la(s) ruta(s) que cursa(n) tráfico de una demanda (Fig. 3). Los resultados del algoritmo para la red de referencia NSFNET (incluida en Net2Plan) determinan un encaminamiento tal que la utilización máxima de los enlaces es del 53.7%. Como muestra de los datos obtenidos de los informes de Net2Plan, podemos observar que el retardo medio de red para un paquete extremo a extremo es de 12.6 ms (Fig. 4). Si cada demanda fuese una fuente de peticiones de conexión con un patrón de llegadas tipo Poisson, asumiendo un modelo de estimación de bloqueo tipo *load sharing*, la probabilidad de bloqueo ante peticiones de circuitos virtuales bajo demanda se estima como despreciable (Fig. 5). Por otro lado, la disponibilidad de red para fallos simples y dobles de enlace se estima del 99.99%, asumiendo una disponibilidad de enlace del 99.86% y un modelo de fallos independientes (Fig. 6). Para este caso, se asume que los caminos se implementan como circuitos virtuales en una red MPLS con un algoritmo de restauración MPLS Fast Reroute.

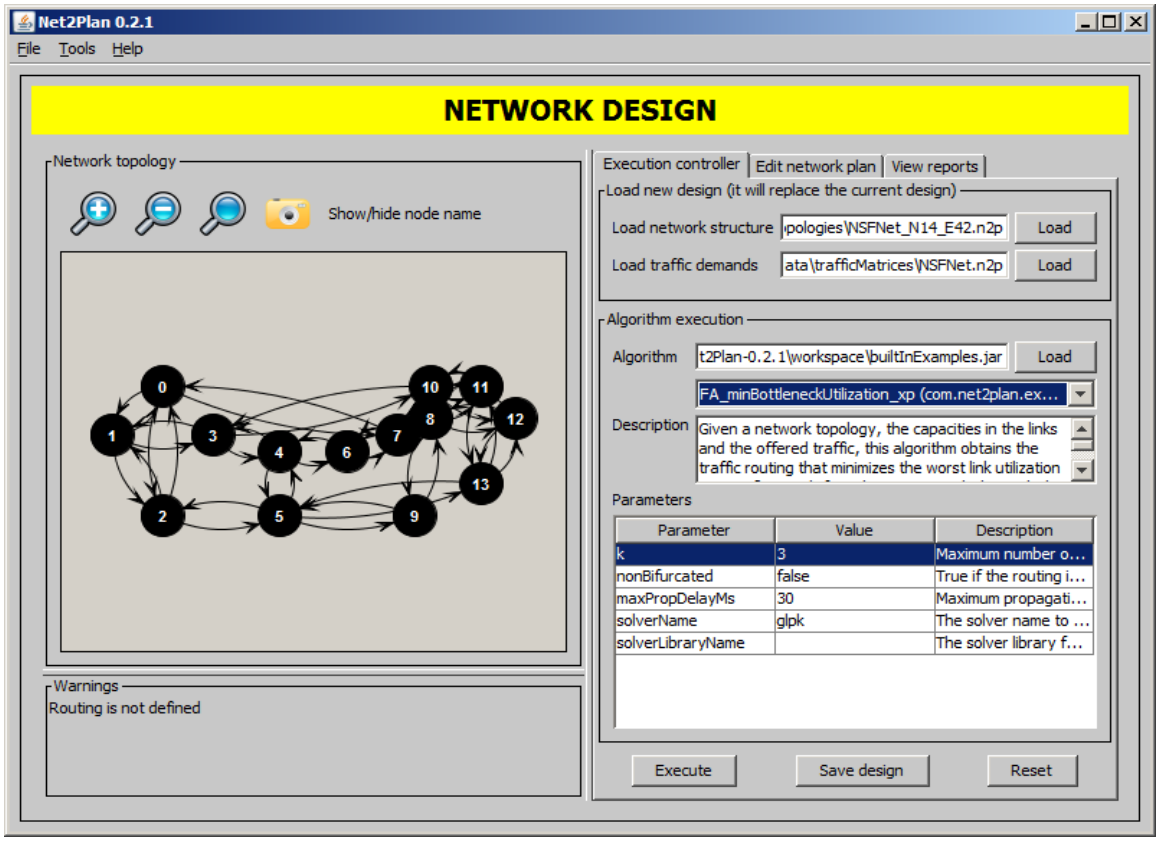


Fig. 2. Ejecución de un algoritmo de asignación de rutas.

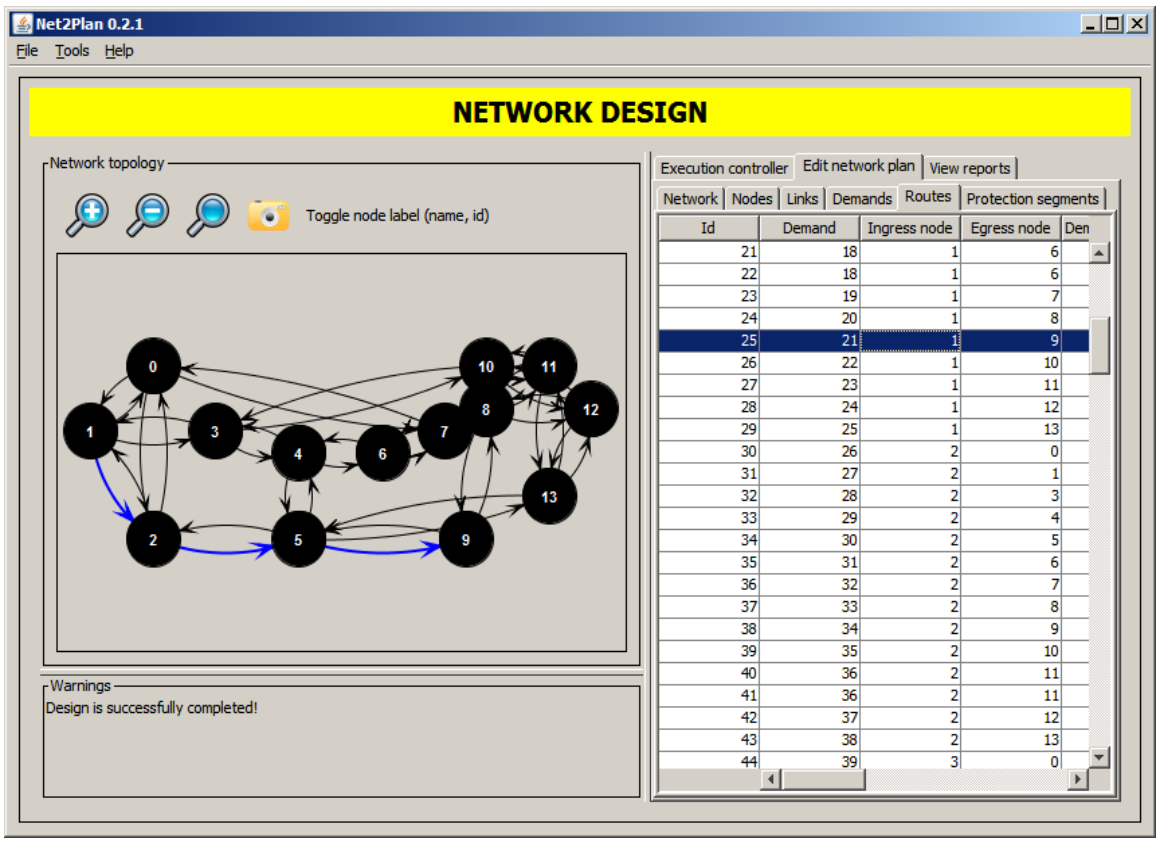


Fig. 3. Visualización de rutas utilizando la herramienta de diseño.

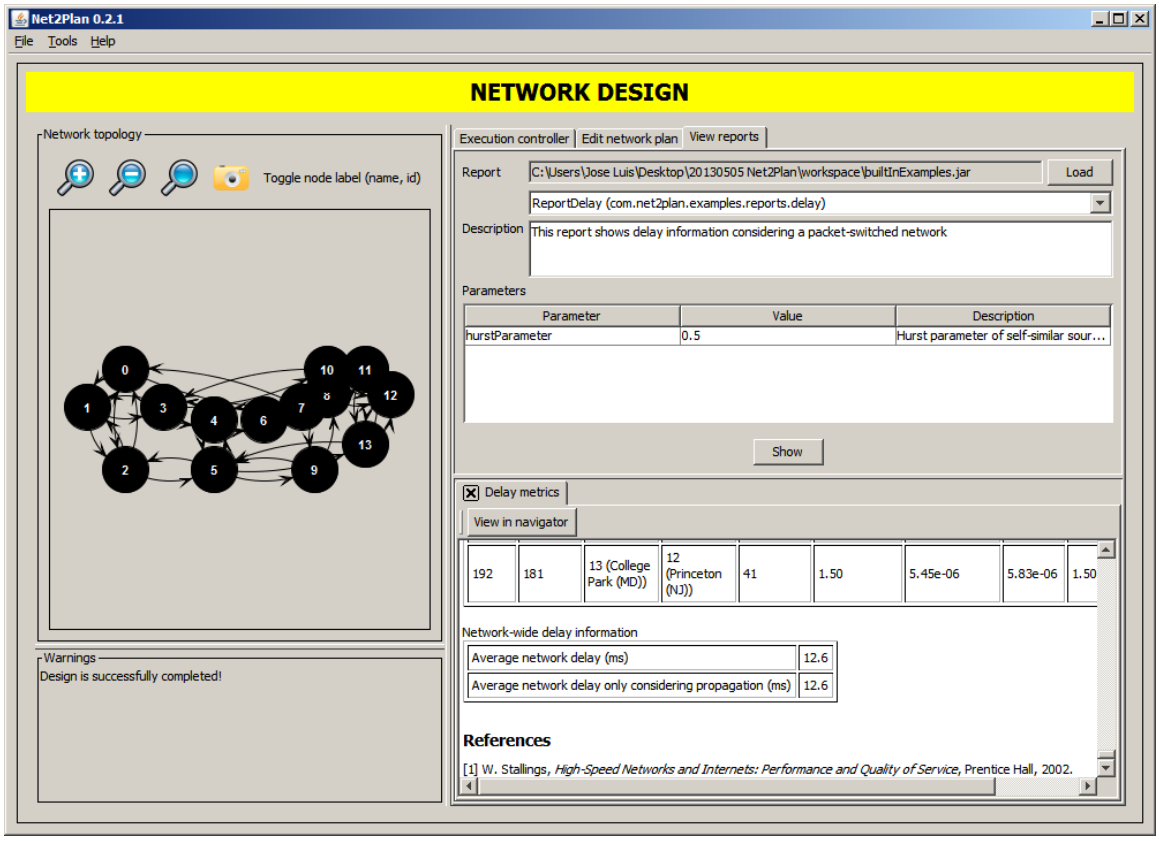


Fig. 4. Informe de retardo de paquetes.

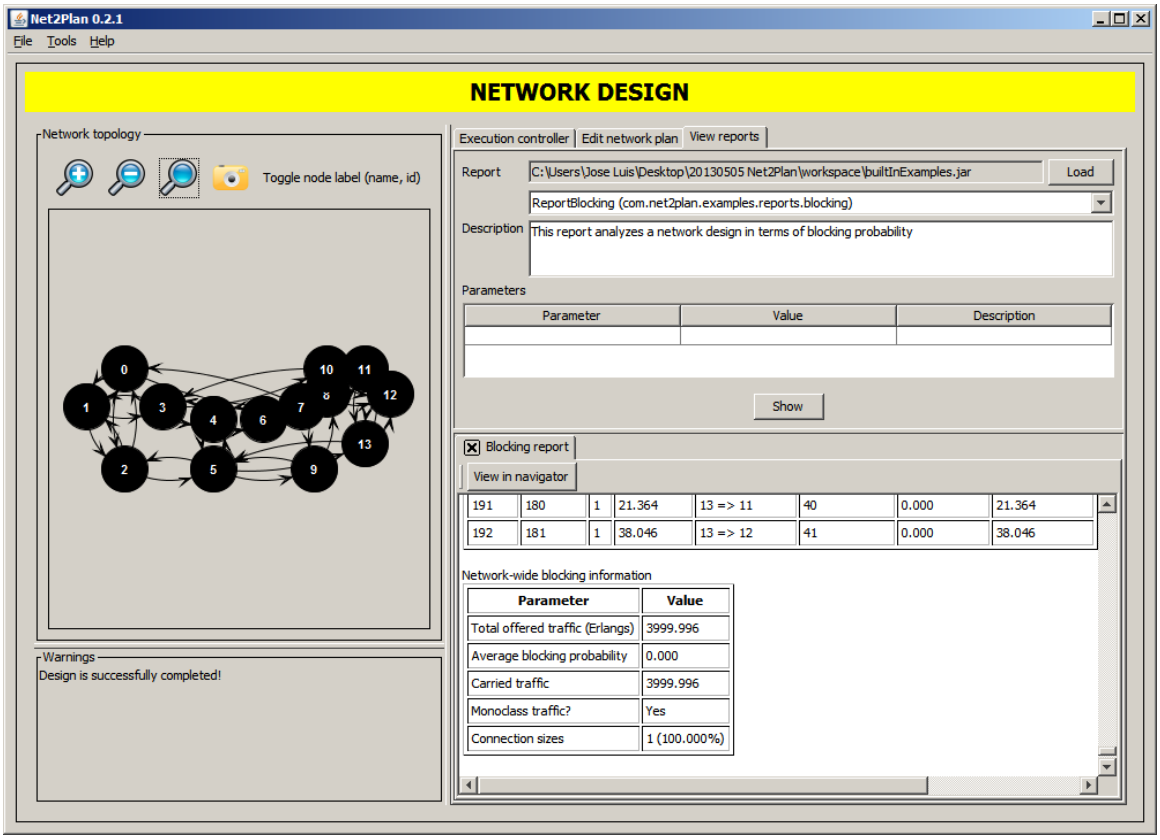


Fig. 5. Informe de bloqueo de conexiones.

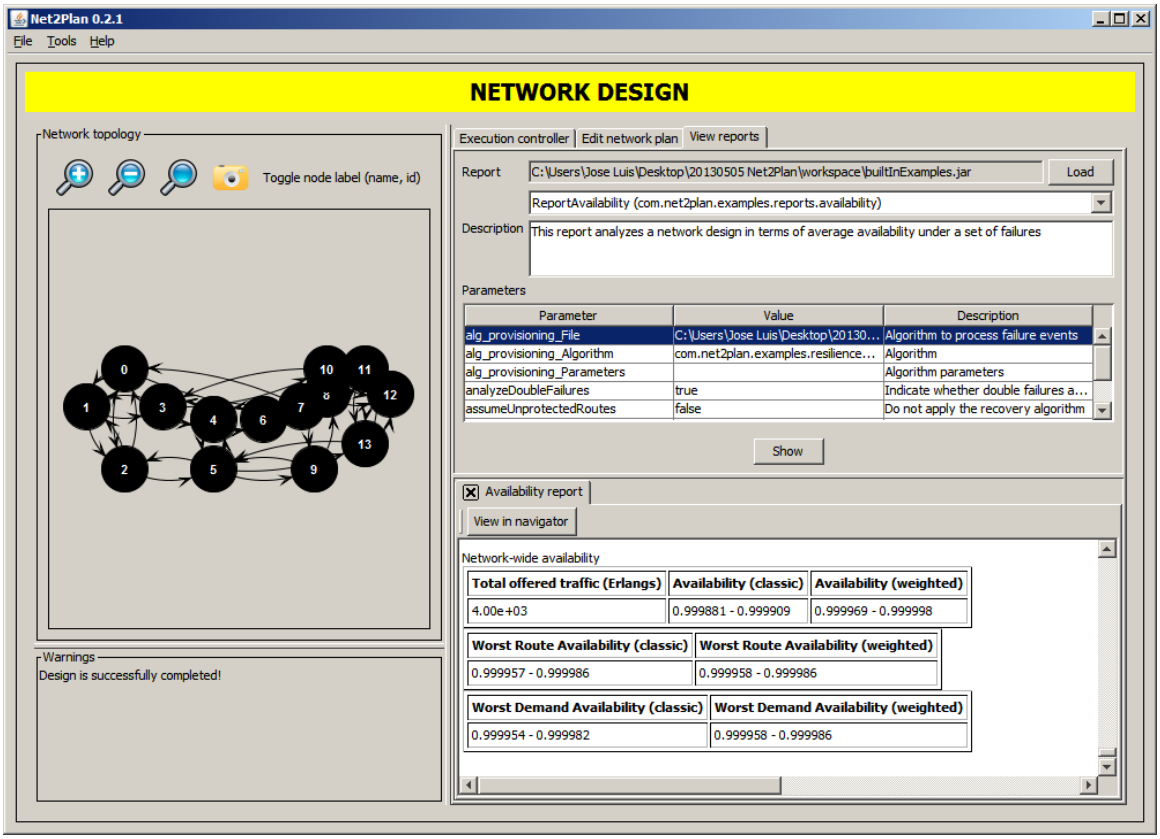


Fig. 6. Informe de disponibilidad.

V. Experiencia docente

En el curso 2012-2013, Net2Plan y JOM se han usado en las asignaturas "Teoría de Redes de Telecomunicaciones" (2º curso GIT y GIST) y "Planificación y gestión de redes" (3º curso GIT), en la UPCT, acumulando un total de 50 horas de prácticas de laboratorio y 150 alumnos aproximadamente. Los enunciados de gran parte de las prácticas se encuentran disponibles en [3]. Además, está prevista su utilización en la asignatura "Operación e Ingeniería de Red" en el Máster en Ingeniería de Telecomunicación (habilitante) que se implantará en el curso 2013-2014.

La organización de las asignaturas se ha realizado de forma que los estudiantes se van adentrando progresivamente en el diseño y planificación de redes. En la asignatura de segundo curso, se introducen conceptos de optimización matemática aplicada al diseño de redes: problemas FA, CA, BA, TA y sus combinaciones. Los alumnos modelan y resuelven numéricamente todos estos diseños con Net2Plan y JOM. Aprenden las relaciones entre (i) el tráfico, capacidades, y topologías de las redes, con (ii) las medidas de prestaciones en redes como el retardo, la probabilidad bloqueo, el coste y la justicia en el reparto de recursos (por ejemplo para problemas de control de congestión). La optimización de redes es el corpus matemático utilizado. Los modelos de optimización introducen en el diseño resultados de retardo y bloqueos extraídos de la Teoría de Colas, como puedan ser las estimaciones Erlang-B de bloqueo, retardos M/M/1, o estimaciones sencillas de retardo medio en enlaces para tráfico autosimilar. Se estudia la convexidad de estas estimaciones respecto a las capacidades de los enlaces o el tráfico que circula en ellos. Este concepto toma importancia, ya que permite aplicar los potentes resultados de optimización convexa para analizar, entender y resolver muchos problemas de diseño de red.

En la asignatura de tercer curso, los estudiantes aprenden conceptos avanzados de planificación, como la fiabilidad de red. Desarrollan algoritmos heurísticos (por ejemplo algoritmos genéticos, *tabu search* o *GRASP*) para problemas de planificación, incluyendo la planificación de redes con mecanismos de protección o restauración ante fallos. La utilización de heurísticos está motivada por una particularidad habitual en la planificación de redes: los problemas abordados son de complejidad algorítmica NP-*hard*, y no es posible encontrar las soluciones óptimas en un tiempo de cómputo asumible, salvo en redes triviales.

Algunas de las prácticas de laboratorio de las asignaturas "Teoría de redes de telecomunicaciones" y "Planificación y gestión de redes" se encuentran disponibles como recursos docentes [3].

A. *Métodos de evaluación*

La valoración del aprendizaje en el diseño y planificación de redes es una tarea difícil, porque debe basarse en una combinación de diferentes méritos del estudiante. En el curso 2012-13, en la asignatura "Teoría de Redes de Telecomunicaciones", un 40% de la nota final del alumno se obtuvo de un examen de 1:30 horas individual en el laboratorio. En él, el alumno utiliza Net2Plan para (i) resolver varios problemas básicos de manipulación de matrices de tráfico, y utilización de algoritmos ya integrados en Net2Plan para diseñar y evaluar redes, (ii) desarrollar un algoritmo propio que resuelva un problema de diseño de red a través de JOM.

Además, los alumnos podían sumar un 20% extra a su nota final de la asignatura, realizando dos trabajos opcionales consistentes en modelar y resolver con JOM problemas orientados a estimular habilidades avanzadas de modelado (no solo modelado para problemas de redes). Por ejemplo, en el curso 2012-13, se les planteó a los alumnos hacer un algoritmo que resuelva sudokus, y otro que resuelva un problema de asignación de frecuencias a estaciones base evitando interferencias. En ambos casos, 3 alumnos fueron capaces de modelar el problema correctamente, y entregar el algoritmo que resolvía el problema con JOM.

La asignatura "Planificación y gestión de redes", tiene dos partes, una centrada en gestión (tipo SNMP) de una red (45% nota final), y otra la planificación de redes (55% nota final), con especial atención al diseño de esquemas de protección y restauración. La parte de planificación de red utilizó la herramienta Net2Plan. Un 15% de la nota final del alumno se basó en un examen de 2:30 horas en el laboratorio en el que los alumnos debían desarrollar con Net2Plan un algoritmo para un problema de planificación concreto, evaluando las prestaciones de la red resultante. Un 10% de la nota final provenía de un caso de estudio relativamente complejo a desarrollar por los alumnos. En el curso 2012-13 los alumnos diseñaron independientemente algoritmos para determinar los pesos OSPF de una red IP, tal que se minimice la congestión de red resultante, un problema clásico de ingeniería de tráfico.

En este caso, la nota de los estudiantes se calculó a partir de dos méritos: (1) realización de una entrevista personal en que se evaluaba la originalidad y profundidad técnica de los algoritmos propuestos, (2) posición del alumno dentro de un ranking con las mejores soluciones encontradas para el problema, en unas topologías y tráficos de referencia.

B. Grado de satisfacción de los estudiantes

La retroalimentación recibida por parte de los estudiantes es muy positiva. Por un lado, destacan la comodidad, simplicidad y flexibilidad de la herramienta para ejecutar tanto los algoritmos e informes incluidos por defecto, como los desarrollados por ellos mismos. Así pueden centrarse en conceptos de planificación y diseño de red, sacando el máximo partido a las asignaturas. Por otro lado, los estudiantes se sienten estimulados ya que plantean los ejercicios como una competición. Algunas de las soluciones propuestas por los alumnos sobresalen por su creatividad y profundidad técnica, e incluso algunos algoritmos se encuentran ya integrados en Net2Plan, de forma que otros estudiantes puedan usarlos.

VI. CONCLUSIONES

En este trabajo se han presentado dos herramientas de software libre desarrolladas en la Universidad Politécnica de Cartagena. Por un lado, Net2Plan es una herramienta de planificación de redes que facilita a los usuarios diseñar, optimizar y simular redes de comunicaciones sin enfocarse en ninguna tecnología específica, lo cual permite que pueda aplicarse a cualquiera de ellas, implementando algoritmos propios o utilizando alguno de los integrados en la herramienta. Por otro lado, JOM es una librería para el modelado de problemas de optimización que conecta con varios *solvers* comerciales y de libre distribución. La combinación de Net2Plan y JOM permite a los docentes y estudiantes disponer de un entorno completo para el aprendizaje de técnicas de modelado y optimización de redes de comunicaciones.

AGRADECIMIENTOS

Este trabajo ha sido financiado por el proyecto nacional TEC2010-21405-C02-02/TCM (CALM) y el Programa de Formación del Profesorado del Ministerio de Educación, Cultura y Deporte (ref. FPU12/04571). Asimismo, se ha desarrollado en el contexto del "Programa de Ayudas a Grupos de Excelencia de la Región de Murcia", de la Fundación Seneca (Plan Regional de Ciencia y Tecnología 2007/2010).

REFERENCIAS

[1] M.A. Rahman, A. Pakštas, F.Z. Wang, "Network modelling and simulation tools", *Simulation Modelling Practice and Theory*, vol. 17, no. 6, págs. 1011-1031, Julio 2009.

[2] OPNET Technologies, "Research with OPNET Requirements", OPNET University Program [Online]. Disponible: http://www.opnet.com/university_program/research_with_opnet/research_requirements.html [Último acceso: Mayo 2013]

[3] Net2Plan – The open-source network planner [Online]. Available: http://www.net2plan.com/ [Último acceso: Mayo 2013]

[4] JOM – Java Optimization Modeler [Online]. Disponible: http://ait.upct.es/~ppavon/jom/ [Último acceso: Mayo 2013]

[5] L. Kleinrock, *Queueing Systems, Volume 2: Computer Applications*, Wiley, 1976

[6] R.S. Cahn, *Wide Area Network Design: Concepts and Tools for Optimization*, Morgan-Kaufmann, 1998

[7] M. Pióro, D. Medhi, *Routing, Flow, and Capacity Design in Communication and Computer Networks*, Morgan-Kaufmann, 2004

Uso de un entorno colaborativo en la asignatura de Programación I

Mary Luz Mouronte López
Departamento de Ingeniería y Arquitecturas Telemáticas
Universidad Politécnica de Madrid
E. U. I. T. de Telecomunicación. Carretera de Valencia km. 7. 28031 Madrid
mouronte.lopez@upm.es

***Resumen*—Este documento describe la experiencia de innovación docente realizada durante el curso 2012-2013 en la asignatura Programación I. Esta asignatura es común a los grados de Ingeniería Telemática, de Ingeniería Electrónica de Comunicaciones, de Ingeniería de Sistemas de Telecomunicación y de Ingeniería de Sonido e Imagen, en la Escuela Universitaria de Ingeniería Técnica de Telecomunicación de la Universidad Politécnica de Madrid. La experiencia desarrollada utiliza una metodología fundamentada en elementos motivacionales y en su ejecución a través de herramientas colaborativas. Los resultados arrojados sobre la docencia-aprendizaje han sido positivos.**

***Palabras Clave*—Innovación educativa, TIC, Entorno Colaborativo**

I. INTRODUCCIÓN

La formación a través de las **T**ecnologías de **I**nformación y **C**omunicación (TIC) resulta imprescindible para aprovechar las ventajas que ellas nos ofrecen en la implementación de nuevas metodologías de aprendizaje.

Si atendemos al informe elaborado por la Fundación Telefónica en 2008, a partir de la realización de 17.576 encuestas a alumnos, profesores y directores de centros de educación primaria y secundaria, se puede observar como el uso de las TIC en las aulas es poco habitual en los centros educativos españoles de este tipo. Así, sólo el 4,9% de alumnos usan los ordenadores y únicamente un 3,9% utilizan Internet en el aula a diario. Hay un 28,5% de profesores que nunca emplean las TIC en las aulas, mientras que un 26,4% lo utilizan semanalmente. Una gran parte de profesores usan las TIC en el aula como apoyo a la exposición oral (78,7%), presentaciones de contenido (62,3%) y para proporcionar guías y orientaciones (57,5%). Por su parte los alumnos, realizan en gran porcentaje búsquedas de información (89,5%) y realización de ejercicios (69%).

En referencia a la enseñanza universitaria en el año 2011, la **C**onferencia de **R**ectores de las **U**niversidades **E**spañolas (CRUE) en su informe UNIVERSITIC, cuyos datos fueron recogidos a partir de una encuesta dirigida únicamente a las universidades presenciales, con una tasa de respuesta del 87%, estableció que el equipamiento básico (conexión a internet y proyector multimedia) estaba disponible en el 53,4% de las aulas, existía un promedio de 37 alumnos por cada ordenador fijo, 295 estudiantes por cada portátil accesible en préstamo y 359 alumnos por ordenador dedicado a aula móvil (sistema de ordenadores portátiles utilizables en diferentes aulas). También determinó que sólo el 63% de los estudiantes universitarios españoles se conectaban a la WiFi de la universidad; siendo el total de conexiones WiFi en las universidades que participaron en la encuesta de casi dos millones.

Por su parte, el Informe Horizon 2012, elaborado por **N**ew **M**edia **C**onsortium (NMC) en colaboración con **E**DUCAUSE **L**earning **I**nitiative (ELI), describió las seis tecnologías emergentes que están llamadas a tener un gran impacto en el aprendizaje, la enseñanza y la expresión creativa en los campus universitarios. Este informe consideraba que las Aplicaciones para los Dispositivos Móviles y las Tabletas serían implantadas en los centros universitarios en el plazo medio de un año, mientras que el Aprendizaje Basado en Juegos y las Analíticas de Aprendizaje lo harían en dos o tres años. Habría que esperar unos cuatro o cinco años para asistir a la introducción de la Informática basada en Gestos y de Internet de las Cosas en las universidades.

En el nuevo contexto europeo de educación el uso de las TIC y el trabajo colaborativo constituyen un componente esencial en los procesos de enseñanza-aprendizaje, además de ser unas de las competencias fundamentales a desarrollar por los estudiantes en la mayoría de las titulaciones universitarias. Como resultado de lo anterior, deben producirse modificaciones tanto en el papel desempeñado por el alumno como por el profesor.

La socialización del conocimiento logra la capacitación de los alumnos para acometer tareas conjuntamente. Este tipo de aprendizaje, exige una cuidada planificación de la clase, clarificación de los objetivos docentes, empleo de nuevas estrategias de aprendizaje y aprovechamiento del carácter activo del alumnado, requerimientos que exigen aumento en la creatividad del profesor.

El término *Innovación Educativa* se refiere a ideas, procesos y estrategias sistematizadas, mediante los que se pretende introducir cambios en las prácticas docentes. En este trabajo analizamos la utilización de un entorno colaborativo para la enseñanza universitaria de la asignatura Programación I. Este entorno está constituido por la plataforma *Moodle* y diversas herramientas para programación colaborativa.

Moodle es una plataforma virtual interactiva adaptada a la formación y empleada como apoyo a la docencia.

Programación Colaborativa significa que varios programadores trabajan conjuntamente sobre el mismo código. Investigadores como Nosek [7], Williams, Kessler, Cunningham y Jefries [9], Nawrocki y Wojciechowski [8] entre otros, afirman que mediante el empleo de este tipo de programación se logran mejores resultados si se tienen en consideración métricas como tiempo de desarrollo y eficiencia del código implementado. Surge la necesidad de emplear métodos que se fundamenten en la programación

colaborativa para el desarrollo del software.

Por otro lado, las compañías de desarrollo software pretenden incrementar su rendimiento compartiendo información y simplificando procesos, con el fin de conseguir minimizar el tiempo de disponibilidad de sus productos en el mercado (*time to market*), los entornos colaborativos se convierten en imprescindibles. La formación del alumno universitario en el conocimiento teórico y práctico de dichos entornos cobra especial relevancia.

La experiencia aquí descrita logra mejorar el proceso educativo, por utilización de nuevas modalidades de aprendizaje a través de las nuevas TIC. Se consigue no sólo, que el estudiante conozca el editor, el compilador, el sistema operativo, el manejo de datos y las estructuras básicas de un lenguaje de programación, sino también, que maneje un entorno colaborativo para distintas tareas, tales como: diálogo con los participantes en la asignatura, realización de ejercicios, recepción de calificaciones, implementación y realización de las entregas de las prácticas. Se fomenta así, la colaboración, la participación, la evaluación continua y el acercamiento al mundo empresarial de los alumnos.

II. ENSEÑANZA DE LA ASIGNATURA DE FUNDAMENTOS DE PROGRAMACIÓN

A. La asignatura de Programación I

La programación constituye una herramienta básica para cualquier graduado en ingeniería. Particularmente, tiene aplicación en el desarrollo de aplicaciones telemáticas, en el procesado digital de señales y está presente en la mayoría de los sistemas de telecomunicación.

Programación I es una asignatura común a los grados de Ingeniería Telemática, de Ingeniería Electrónica de Comunicaciones, de Ingeniería de Sistemas de Telecomunicación y de Ingeniería de Sonido e Imagen en la Escuela Universitaria de Ingeniería Técnica de Telecomunicación (E.U.I.T. Telecomunicación) de la Universidad Politécnica de Madrid (UPM). Esta asignatura supone el primer contacto de los estudiantes con la programación, disciplina que desarrollarán a lo largo de la carrera. En esta asignatura se efectúa una introducción a la programación, asentando los fundamentos del diseño descendente como método elemental en el desarrollo de aplicaciones. Posteriormente, en otras asignaturas, el alumno estudiará técnicas diferentes de diseño (por ejemplo el diseño basado en objetos), que no suponen una alternativa al diseño descendente, sino que son métodos complementarios, cada uno con su campo de aplicación específico.

La asignatura de Programación I durante el curso 2012-2013 fue impartida por doce profesores y cursada por cuatrocientos cincuenta estudiantes. En esta asignatura el alumno debe:

- Adquirir los conocimientos precisos para efectuar el análisis y diseño de procedimientos.
- Conocer el lenguaje de programación C y aplicarlo en la codificación de algoritmos.

La asignatura tiene seis créditos lo que se traduce en ciento sesenta horas de trabajo total, concentradas en unas doce semanas. El alumno puede escoger entre dos itinerarios de evaluación, excluyentes y definitivos:

- Itinerario de evaluación continua. La superación de la asignatura se realiza a través de la evaluación continua. Es el itinerario por defecto.
- Itinerario de sólo prueba final. En este itinerario no se realiza ninguna prueba de evaluación continua, pero los alumnos deben efectuar las prácticas de laboratorio y entregar al final de semestre las memorias de las mismas. La evaluación final, en este caso, consiste en dos pruebas: examen de laboratorio y examen de teoría.

Si el estudiante opta por el itinerario de evaluación continúa, el trabajo que debe efectuar incluye la asistencia activa a las clases presenciales de teoria y de laboratorio, el estudio personal, las búsquedas bibliográficas, la realización de las pruebas de autoevaluación, la implementación de las prácticas y la resolución de ejercicios. La asignatura se imparte mediante b-learning, es decir, combinando la enseñanza presencial y la no presencial.

Durante el curso 2012-13, se han introducido en la asignatura Programación I iniciativas innovadoras en los métodos docentes y evaluadores. Dentro de estos cambios destacan como puntos básicos la utilización del aprendizaje colaborativo, la realización de evaluación continua con cinco evaluaciones parciales, así como el empleo de nuevas tecnologías TIC: plataforma *Moodle* y herramientas de programación colaborativas (*Subversion* [2] y *Eclipse* [3]).

Uno de los condicionantes tenidos en cuenta a la hora de ejecutar estos cambios fue la mejora de la motivación de los alumnos, considerando la interacción entre las metas que ellos persiguen con su trabajo académico y con los modos preferibles de afrontamiento del mismo.

B. Motivación del alumno

Es conocido por todos los profesores que la motivación con que los estudiantes desarrollan las tareas académicas constituye uno de los factores clave del proceso de aprendizaje. El alumno motivado emprende antes las actividades, se concentra más, es más insistente y emplea más tiempo y esfuerzo en ellas. Por consiguiente, es muy importante potenciar el interés de los alumnos por la asignatura de Programación I. Para mejorar la motivación del estudiante es preciso chequear y estimar los criterios de actuación académica en relación con su influencia sobre dicha motivación, efectuando una retroalimentación sobre las prácticas docentes a partir de sus resultados sobre el aprendizaje.

Existen diferentes investigaciones que han tratado de analizar tanto la repercusión de las diferentes motivaciones de los alumnos sobre el aprendizaje, como la dependencia que posee una motivación de las características personales del alumno ([10], [11], [5]; [4]). Partiendo de estos trabajos los intereses de los estudiantes pueden resumirse en:

- Aprobar la asignatura. En el contexto de la E.U.I.T. de Telecomunicación este interés es el más extendido, esto está especialmente causado por la circunstancia de que los cursos iniciales de la carrera han sido tradicionalmente los más difíciles, con un alto grado de fracaso universitario. Este nivel de motivación es independiente de los contenidos de la asignatura, pero las acciones que puedan ser percibidas por el estudiante como facilidades para la aprobación de la asignatura consituirán un aliciente para su estudio.

- Adquisición de conocimientos útiles para el ejercicio de la profesión. Varios investigadores han estudiado este aspecto ([10], [11], [5]) concluyendo que al alumno universitario le interesan aquellos conocimientos cuya utilidad para la consecución de objetivos profesionales posteriores perciba claramente y, que además supongan una aplicación real.
- Profundización en contenidos específicos.

Sobre los tres puntos mencionados desempeñan un papel relevante tanto los propios contenidos de la asignatura como la aceptación por parte de los estudiantes de la metodología docente utilizada.

III. INNOVACIONES METODOLÓGICAS Y EVALUADORAS

En el diseño de las modificaciones aplicadas a los métodos de enseñanza-aprendizaje se han considerado tanto los objetivos docentes, como los elementos motivacionales del alumno, lo que constituye una mejora sustancial de la asignatura de Programación I.

Durante el curso 2012-2013 se empleó un entorno de programación con las características seguidamente.

A. Ordenadores

- Memoria: 4GB,
- Sistema Operativo Windows de 64 bits,
- Procesador: 1,5 GHz,
- Disco: 440 GB

La infraestructura descrita era la ya existente en los laboratorios, los cuales son compartidos por diversas asignaturas en la E.U.I.T. de Telecomunicación. Esta circunstancia condicionó la elección de la plataforma sobre la que se ejecutarían las herramientas en el entorno de programación utilizado.

B. Herramientas Software

1) Subversion: herramienta de software libre que se publica bajo una licencia *Apache*. Esta utilidad permite un entorno de programación colaborativo, de forma que diversos desarrolladores pueden trabajar simultaneamente sobre un mismo código, compartiendo las modificaciones software. *Subversion* aporta un mecanismo de control de versiones a través del almacenamiento de todos los archivos que integran un proyecto y de los cambios que se efectúen sobre ellos a lo largo del tiempo. Es posible recuperar versiones anteriores y revisar los cambios implementados previamente a su publicación. Describimos la estructura de directorios del repositorio y las operaciones más utilizadas:

- **Estructura de directorios *Subversion***. Las siguientes carpetas componen el primer nivel de directorios de su repositorio:
  - Trunk: Rama de desarrollo principal,
  - Tags: Rama de gestión de versiones,
  - Branches: Rama con evoluciones paralelas a Trunk.
- **Operaciones utilizadas en *Subversion***
  - **Trabajo en equipo**. Se utilizó la modificación paralela de código del repositorio que permite *Subversion*, de modo que varios alumnos pudieron trabajar simultaneamente sobre la misma zona del código sin producir interferencias. Cuando dos alumnos modificaron un elemento idéntico simultaneamente, *Subversion* integró las modificaciones automaticamente, obligando al estudiante a realizarlo manualmente sólo cuando el conocimiento humano fue el único modo que garantizó la correcta integración.
  - **Cierre de versión** (”Creación de Tag”). En ciertos momentos del ciclo de vida de un proyecto industrial puede ser conveniente el cierre de una versión para continuar con su evolución en el ámbito de la versión siguiente. Este cierre de versión nos permitirá volver a versiones anteriores en situaciones que lo requieran. Esta funcionalidad se utilizó para aquellas prácticas que suponían una ampliación de otras.
    En idioma *Subversion*, el cierre de versión se denomina ”crear un Tag” de la versión desarrollada. Esto implica llevar una copia de la versión a cerrar a la rama de gestión de versiones.
  - **Ramificación del Código** (”Creación de Branch”). Existen situaciones en las que el ciclo de vida de un proyecto industrial implica una evolución paralela de su código. *Subversion* permite habilitar entornos separados para estos desarrollos mediante la creación de Branches. Los cambios efectuados en los entornos paralelos pueden ser fusionados en cualquier instante mediante la operación de Fusión de cambios. Esta funcionalidad no fue utilizada durante las prácticas.
  - **Fusión de cambios**. En ocasiones, en un proyecto industrial, tras una ramificación, los cambios realizados en una rama deben aplicarse a algún desarrollo paralelo. *Subversion* ayuda a este proceso mediante un comando específico, que aplica todos los cambios producidos entre dos revisiones en una rama a otra rama cualquiera del repositorio. Por ejemplo, en el caso de que se efectúe una bifurcación para la resolución de un fallo (en una rama correctiva) de forma paralela al desarrollo de la siguiente versión (en una rama evolutiva), deberán fusionarse las moficaciones efectuadas en la rama correctiva con las que hayan aparecido simultáneamente en la rama evolutiva. Esta funcionalidad fue empleada en algunas prácticas.

En la asignatura de Programación I *Subversion* se utilizó para que:

- Los alumnos descargasen datos de cada una de las prácticas (esquema del proyecto, ficheros de tipos y

definiciones) elaborada por el profesor, realizasen las entregas de sus programas, recibiesen la realimentación docente y efectuasen prácticas en grupo (donde los distintos estudiantes implementan partes diferentes del código),
- El profesor depositase los datos de cada una de las prácticas, descargase los programas implementados por los estudiantes e informase a éstos de sus correcciones.

Respecto al uso en red de esta herramienta:

- El *Servidor Subversion* se instaló en un *ordenador* de los laboratorios,
- Se desplegó un *Cliente Subversion* en los ordenadores de los laboratorios donde los estudiantes desarrollaron sus prácticas y en los ordenadores de los docentes,
- Se elaboró un manual de usuario para el alumno y otro para el profesor. En estos documentos se indicaban los mecanismos de operación:
  - Bajar por primera vez una copia de trabajo -*SVN Checkout*-,
  - Subir una copia de trabajo modificada -ŚVN Commit-,
  - Actualizar una copia de trabajo existente -*SVN Update*-.
  - Fusionar cambios -*SVN Merge*-

  Se proporcionó una referencia para localizar un manual completo sobre *Subversión* y el ejecutable: http://tortoisesvn.net,
- Se configuró *Subversion* para realizar una compilación automática de los programas cada vez que un alumno efectuase una entrega.
- Un profesor asumió el papel de administrador del repositorio *Subversion*.

2) Eclipse: para programar en un lenguaje de alto nivel como es C se requiere disponer de: un editor de texto, un compilador y de manera opcional de un depurador. Existen programas que integran estas herramientas en un solo paquete y que además disponen de un interfaz gráfico. A estos programas se les denomina **E**ntornos de **D**esarrollo **I**ntegrado (EDI). Ejemplos de este tipo de programas son *Eclipse*, *NetBeans* o *Visual Studio*.

En nuestro caso se utilizó el entorno integrado *Eclipse* combinado con **Min**imalist **G**NU for **W**indows (*MinGW*), para poder utilizar el compilador *gcc* y el depurador *gdb*).

MinGW es una implementación del compilador *gcc* y el depurador *gdb* para la plataforma Windows, que permite, entre otras funcionalidades, compilar, depurar y enlazar programas escritos en C.

Eclipse Es software libre. Esta herramienta fue creada principalmente para el desarrollo de aplicaciones Java, si bien, ofrece la posibilidad de añadir funcionalidades al editor, a través de nuevos módulos (*plugins*), para programar en otros lenguajes de programación distintos de Java como C/C++, PHP, Python, Ruby, Cobol, etc.

Respecto al uso de *Eclipse* en la asignatura de Programación I:

- Se elaboró un manual básico describiendo:
  - Qué es un entorno de programación en C,
  - Instalación y Configuración de MinGW. Ejecutable: http://sourceforge.net/projects/mingw,
  - Cómo instalar *Eclipse* 4.2 (Juno). Ejecutable: http://www.eclipse.org/downloads),
  - Cómo escribir un programa C en *Eclipse*:
    - Crear un proyecto,
    - Crear el código fuente,
    - Compilar, enlazar y ejecutar un programa,
    - Cómo asociar un fichero codificado con un proyecto,
    - Cómo importar un proyecto existente
- Se proporcionó al estudiante un esquema de proyecto realizado por el profesor para cada práctica.
- Se le enseñó al alumno a realizar un uso básico del depurador.

El alumno pudo instalar *Eclipse* y *Subversion* en su ordenador personal para trabajar con ellos en su casa. En las guia de uso de *Subversion* se indicó el conjunto de comandos que debían de ejecutarse en el proceso típico de trabajo escuela $->$ casa $->$ escuela.

3) Moodle: se utilizó la plataforma *Moodle* como depósito de material docente (textos académicos, cuestionarios de autoevaluación, etc.) y como foro donde los estudiantes intercambiaron experiencias sobre las problemáticas surgidas durante la realización de las prácticas. En este foro los docentes resolvieron distintas dudas e informaron de eventos de interés. También se utilizó la plataforma para realizar tutorías a distancia, y para suministrar a los alumnos realimentación sobre ejercicios.

C. Esquema de práctica

Se describe a continuación el guión habitual de realización de una práctica:

Tipo 1: Práctica individual:

1) Leer el enunciado de la práctica,
2) Realizar una copia de trabajo - *SVN Checkout* - (se obtiene proyecto, tipos y variables),
3) Efectuar la implementación en la copia de trabajo, compilarla con la herramienta *Eclipse* y verificar su funcionamiento,
4) Publicar los cambios -*SVN Commit*-.

Tipo 2: Práctica en grupo:

1) Leer el enunciado de la práctica,
2) Realizar una copia de trabajo - *SVN Checkout* - (se obtiene proyecto, tipos y variables),
3) Escoger uno de los bloques que en el enunciado se muestran como implementables por un único individuo,
4) Efectuar la implementación asignada en la copia de trabajo, compilarla con la herramienta *Eclipse* y verificar su funcionamiento,
5) Publicar los cambios -*SVN Commit*-,
6) Una vez que el resto de miembros del grupo publiquen sus implementaciones, fusionar cambios -*SVN Merge*-,

7) Actualizar la copia de trabajo existente - *SVN Update* -.

D. Beneficios

Es importante hacer notar que, en las actuales empresas de desarrollo software, se utilizan estructuras de datos y entornos colaborativos de desarrollo que gestionan automaticamente los cambios y el intercambio de datos requerido. Disponer de entornos de desarrollo, que por su fiabilidad y rapidez de respuesta, permitan tomar decisiones y realimentarse a etapas previas para ajustar modificaciones, es lo que logra eficacia en el desarrollo de productos.

El entorno de desarrollo utilizado en la asignatura de Programación I se emplea en distintas compañías de construcción de productos software, por lo que en esta asignatura, el alumno además de adquirir conocimientos de programación se familiariza con un paquete de herramientas colaborativas propias del sector industrial.

Los beneficios logrados con el uso del entorno colaborativo descrito fueron los siguientes:

- Contraste de experiencias que fueron discutidas y consensuadas. El intercambio efectuado quedó registrado alentando la reflexión y la comunicación,
- Eliminación de las fronteras espaciales y temporales favoreciendo la comunicación entre múltiples usuarios,
- Potenciación del papel del grupo como elemento dinamizador de la docencia-aprendizaje, como coordinador y elemento recopilador de conclusiones,
- Mejora del proceso de enseñanza-aprendizaje. El entorno colaborativo permitió que los alumnos trabajasen en grupo aunque conservando su propia autonomía, lo que facilitó el proceso educativo,
- Favorecimiento de los procesos cooperativos. Mientras que en los grupos tradicionales existen reuniones presenciales, el entorno colaborativo permitió la realización de encuentros virtuales, realimentaciones docentes e intercambio de impresiones en forma on-line,
- Agilización de la interacción profesor-alumno. Rápido acceso a ficheros compartidos (esquema de proyectos, definición de tipos y variables), optimización del tiempo de recepción de calificaciones y comentarios sobre las prácticas y ejercicios entregados,
- Aumento de la productividad. Los conocimientos en el alumno se construyeron más facilmente al utilizarse un entorno dinámico: se posibilitó su acceso a contenidos, se alento su participación, se realizó un trabajo cooperativo y se incentivó su motivación. El rendimiento del profesor se incrementó por la agilización de la gestión de los estudiantes así como de la correción de ejercicios y prácticas. También por posibilitar el seguimiento continuado e individualizado de los alumnos (evaluación continua).

IV. RESULTADOS

La dificultad de establecer relaciones causales entre el uso de las TIC y la mejora del aprendizaje, ha llevado a algunos autores [6], [1] a estudiar el modo en que la incorporación de las TIC a los procesos de aprendizaje puede modificar las prácticas educativas. El razonamiento que fundamenta este cambio de perspectiva es que carece de sentido pretender establecer una relación directa entre la incorporación de las

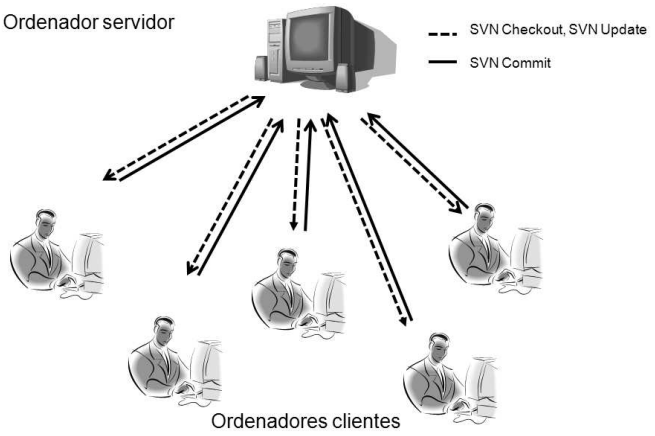


Fig. 1. Entorno de programación colaborativa.

TIC y los resultados del aprendizaje, puesto que la misma estará modulada por el enorme y complicado conjunto de aspectos que conforman las prácticas educativas. Se propone, que lo que se requiere es averiguar cómo, en que magnitud y bajo qué circunstancias las TIC pueden modificar las prácticas educativas a las que se incorporan.

Las consecuencias de este cambio de perspectiva son evidentes: por una parte, el foco de interés se mueve desde el estudio de las potencialidades ofrecidas por las TIC para la enseñanza y el aprendizaje, hacia el estudio empírico de la utilización efectiva que docentes y estudiantes efectúan de dichas tecnologías; y por otra, se vinculan las posibles mejoras del aprendizaje a la participación e implicación de los alumnos en estas tareas, donde el uso de las TIC es un único rasgo relevante entre los muchos aspectos importantes implicados.

Resumiendo, según este enfoque no es en las TIC ni en sus características específicas, sino en las tareas efectuadas por profesores y estudiantes gracias a las posibilidades de comunicación, intercambio, acceso y procesamiento de la información que ofrecen las TIC, donde hay que localizar el estudio para comprender y valorar su impacto sobre la enseñanza y el aprendizaje.

En referencia a nuestra experiencia docente, ésta es un trabajo en curso, en el que se constata que existen resultados preliminares basados en opiniones subjetivas de profesores y alumnos, los cuales se cuantificarán en los cursos próximos. Así, con el fin de evolucionar la asignatura de forma correcta en sucesivos cursos, cada año se analizarán las encuestas docentes. El estudio de estas encuestas, la recopilación de las opiniones de los profesores y las estadísticas de las calificaciones obtenidas, permitirán comprobar la tendencia de las mejoras existentes tras la modificación de las prácticas de aprendizaje. Esta verificación posibilitará efectuar una apropiada retroalimentación sobre dichos métodos.

Con respecto al curso 2012-2013 el número de aprobados ha experimentado un aumento en relación con los anteriores (del orden del 10% sobre una muestra de cuatrocientos cincuenta estudiantes).

Los profesores y los alumnos, en general, han manifestado su satisfación con la nueva metodología docente, si bien han sugerido algunas vías de mejora especialmente relativas a

Subversion.

Según alumnos y profesores, el uso de esta herramienta aportó los beneficios siguientes:

- Posibilitó el seguimiento histórico de las modificaciones sufridas por los archivos (implicando copias y renombrados).
- Permitió la realización de modificaciones atómicas (si alguno de los ficheros integrantes de la actualización no puede ser cambiada toda la operación es anulada).
- Referente a las operaciones de sincronización únicamente se transmiten aquellos ficheros que sufren modificaciones, lo que supuso ahorro en el tráfico de red.
- La creación de ramas y etiquetas fue una operación muy eficiente, ya que por cada rama se utiliza un árbol diferencial de cambios.
- Permitió bloquear archivos y carpetas individualmente evitando que fuesen editados por más de un usuario.

Respecto a la herramienta *Eclipse*, docentes y alumnos destacaron como beneficios su neutralidad con respecto a la plataforma empleada y la realización íntegra del proceso de desarrollo software (desde el análisis de requerimientos hasta la distribución y el mantenimiento).

La experiencia docente realizada en la asignatura de Programación I:

- Cubre los tres niveles motivacionales del alumno:
  - Mayor número de aprobados que en cursos anteriores,
  - Adquisición de conocimientos utilizables en el ejercicio profesional: fundamentos básicos de programación, metodología de desarrollo software y uso de herramientas industriales,
  - Ampliación de conocimientos sobre contenidos específicos consiguida a través de la consulta de enlaces y documentos en *Moodle* complementada con el diálogo on-line con el docente.
- Permitió al alumno desarrollar las siguientes competencías:
  - Mejora en la utilización de las TIC,
  - Habilidades para el aprendizaje autónomo,
  - Capacidad de expresión correcta oral y escrita. La comunicación eficaz y correcta con los demás, argumentando con claridad, con lógica y con precisión, es mejorada por medio de la metodología y herramientas utilizadas (uso de foros, exposiciones en público, etc.)
  - Conocimiento y utilización de fundamentos de arquitectura, metodología de diseño, verificación y validación de software,
  - Formación básica sobre uso y programación de ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación a la ingeniería.
- Logró que se adquiriesen los siguientes resultados de aprendizaje:
  - Definir el concepto de procesador, diseño, entorno y acciones.
  - Establecer el concepto de dato y su representación en el ordenador. Utilizar tipos de datos básicos, definir y utilizar tipos de datos estructurados. Identificar los datos necesarios para resolver un problema y asociarlos a los tipos correspondientes,
  - Manejar las operaciones de entrada/salida,
  - Operar con ficheros,
  - Utilizar operadores (aritméticos, relacionales, lógicos y a nivel de bit), expresiones,
  - Acciones, sentencias de asignación, selección e iteración,
  - Diseñar algoritmos que den solución a problemas de complejidad sencilla, utilizando diseño descendente partiendo de una especificación,
  - Identificar clases y tipos de parámetros,
  - Determinar los mecanismos de paso de parámetros en argumentos y resultado de funciones,
  - Analizar la corrección de los algoritmos usando técnicas sencillas de verificación,
  - Codificar y realizar pruebas a partir del diseño de un algoritmo,
  - Estructurar un programa en funciones y conocer el uso del paso de funciones como argumentos de otras funciones,
  - Usar memoria dinámica y aritmética de punteros para resolver problemas sencillos,
  - Explicar el concepto de módulo: utilizar funciones de biblioteca y de otros módulos,
  - Familiarizarse con el manejo básico de herramientas para desarrollar programas: editor, compilador, enlazador y depurador,
  - Manejar entornos integrados de desarrollo y acostumbrase a documentar programas,
  - Preparar y organizar memorias de trabajos. realizados.

V. CONCLUSIONES

La experiencia descrita demuestra que es posible diseñar y aplicar una metodología fundamentada en la potenciación de la motivación y en el desempeño de un trabajo colaborativo para mejorar los resultados de la docencia-aprendizaje. También se concluye que existen tecnologías que aunque son empleadas en la industria son aplicables en el entorno educativo.

VI. TRABAJOS FUTUROS

Al ser la experiencia docente aquí descrita un trabajo aún en evolución, la tendencia de sus resultados se cuantificará en los cursos académicos siguientes. En cursos próximos se incorporarán otras herramientas al aprendizaje:

- Utilidad para la confección de mapas mentales,
- Herramienta para elaborar ejercicios interactivos basados en páginas web,
- Utilidad para que el profesor cree *ebooks* con el material docente, los estudiantes podrán visualizarlos en sus dispositivos personales.
- Herramienta para que los estudiantes construyan un *blog* donde expondrán sus trabajos y recibirán comentarios.

REFERENCIAS

[1] D. Jonassen, J. Howland, J. Moore, and R. M. Marra, "Learning to Solve problems with technology: A constructivist perspective upper Saddle River", NJ: Pearson Education, 2003.

[2] http://subversion.apache.org/. May 2013.
[3] http://www.eclipse.org/. May 2013.
[4] J. A. Sánchez, "Técnicas centradas en el trabajo en equipo", Curso: Técnicas Alternativas para la Enseñanza Universitaria, Universidad Politécnica de Madrid, 22, 2007.
[5] J. A. Tapia, "Motivar para aprender y mejorar el interés de los alumnos", Curso: ¿Qué se debe hacer para motivar a los alumnos? Motivar para aprender y mejorar el interés de los alumnos, Universidad Politécnica de Madrid, vol. 69, 2007.
[6] J. L. Moore et all. ?The relationship between situated cognition and anchored instruction: A response to Tripp. Educational Technology?, The Cognition and Technology Group at Vanderbilt, vol. 34, n. 8, pp. 28-32, 1994.
[7] J. T. Nosek, "The case for collaborative programming", Communications ACM, vol. 41, n. 3, pp. 105-108, 1998.
[8] J. Nawrocki and A. Wojciechowski, "Experimental evaluation of pair programming", European Software Control and Metrics (Escom), pp. 99-101, 2001.
[9] L. Williams, R. R. Kessler, W, Cunningham y R. Jefries, "Strengthening the case for pair programming", IEEE Software, vol. 17, n. 4, pp. 19-25, 2000.
[10] M. V. Convington, "Goal theory, motivation and school achievement: An integrative review", Annual Review of Psychology, vol. 51, pp. 171-200, 2000.
[11] R. M. Ryan, y E. L. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development and well being", American Psychologist, vol. 55, n. 1, pp. 68-78, 2000.

Organización de docencia cooperativa usando Google drive

Elsa Macías, Álvaro Suárez

Grupo de Arquitectura y Concurrencia, Departamento de Ingeniería Telemática
Universidad de Las Palmas de Gran Canaria
Campus Universitario de Tafira, Edificio de Electrónica y Telecomunicación, Pabellón C, España
emacias@dit.ulpgc.es, asuarez@dit.ulpgc.es

***Resumen*- El *Espacio Europeo de Educación Superior* (*EEES*) ha dado lugar al uso de muchas técnicas de enseñanza y al uso de muchas herramientas telemáticas (sólo basta observar las actas de los congresos de docencia para constatar la gran cantidad de experiencias que se han dado en esta dirección en los últimos años). Nosotros hemos aprovechado las bondades del modelo universal de trabajo cooperativo para crear un modelo de trabajo aplicado al proceso de enseñanza-aprendizaje implicando en ello a los responsables de juntas de centros docentes (escuelas, facultades o institutos universitarios), los profesores y los alumnos. La idea básica es mejorar el rendimiento de los alumnos facilitándoles la adquisición de conocimientos de forma autónoma y por otro lado reducir el impacto de la creciente burocratización de las tareas del profesor usando Google Drive que permite ahorros de costes muy considerables para las universidades. Hemos aplicado nuestro modelo a un conjunto muy variado de asignaturas durante los últimos 4 años obteniendo unos resultados de satisfacción muy buenos tanto para alumnos como profesores.**

***Palabras Clave*- EEES, trabajo cooperativo, Nube, Google drive, ahorro costes, burocratización, satisfacción.**

I. INTRODUCCIÓN

Actualmente está en marcha en todas las universidades españolas sistemas de enseñanza en el marco del EEES. Este sistema de enseñanza establece que el alumno debe ser el intérprete de su aprendizaje y que el profesor es el que guía ese aprendizaje mediante técnicas adecuadas de enseñanza. Este aprendizaje se suele estructurar en dos partes diferenciadas: a) presencial del alumno en las instalaciones de la Universidad y b) no presencial. Generalmente los equipos rectorales han diseñado reglamentos de docencia en los que se obliga a hacer proyectos docentes de las asignaturas en los que se especifica exhaustivamente las horas que un alumno debe dedicar al estudio individual, en grupo (con otros alumnos) a cada tema de la asignatura, las horas de evaluación que el profesor debe dedicar presencialmente y en algunos casos el trabajo personal del alumno.

Las clases presenciales de las asignaturas del Área de Ingeniería Telemática suelen estar estructuradas en varias partes muy bien diferenciadas: a) Teoría, b) Problemas en el Aula, c) Prácticas de Laboratorio y d) Tutorías en grupos muy reducidos de alumnos. Salvo las tutorías en grupos reducidos, el resto de actividades suele tener su propia evaluación individualizada para cada alumno. La evaluación puede ser continuada (típica que se hace para problemas en el aula y prácticas de laboratorio) o a final del curso (es el caso de la evaluación de teoría o problemas en el aula).

Las universidades han hecho y están haciendo esfuerzos importantes en la formación de los profesores para el EEES, generación de herramientas que faciliten la planificación de las actividades de las asignaturas semanalmente (exámenes de evaluación continua, tutorías en grupo y clases presenciales)... También han proliferado estudios de adaptación de asignaturas al EEES, como por ejemplo [1] que pone de manifiesto el poco eco que tienen las nuevas metodologías de enseñanza en el EEES; y se ha trabajado en proyectos educativos interuniversitarios para desarrollar modelos de evaluación de asignaturas tales como el trabajo de fin de grado [2]. Sin embargo, no se detecta que haya habido un estudio concreto para asignaturas del área de Ingeniería Telemática globalmente. Por otro lado, no cabe duda que existe un esfuerzo importante por evaluar la satisfacción de los alumnos y los profesores en la adaptación al EEES. Después de los primeros años de adaptación al EEES, se han producido varios estudios en este sentido: en [3] se presenta un análisis cualitativo de las titulaciones EEES frente a las previas (del sistema anterior) observando una serie de variables que tratan de medir la satisfacción de 179 alumnos de últimos años (de Administración de Empresas y Derecho de la Universidad de Vigo), con: a) la titulación elegida, el profesorado, el grado de cumplimiento de las expectativas del alumno antes de entrar en el primer curso, los conocimientos aprendidos, la aplicación de los conocimientos aprendidos y la calidad de la docencia. Para todas estas variables se observa si presenta diferencias significativas respecto a las titulaciones previas (pre-EEES). El resultado mostró que en general el alumno estaba satisfecho con sus profesores y aplicación de los conocimientos, pero no con la titulación EEES respecto a la pre-EEES puesto que la calidad de la docencia no aumentaba. En [4] se muestra un estudio de la moderada satisfacción mostrada por los alumnos de Ingeniería de Edificación de la universidad del País Vasco, antes y después de implantar dicha asignatura en el EEES. En [5] se analiza la adaptación de asignaturas al EEES en el área concreta de la docencia de asignaturas de Ingeniería y la satisfacción del alumno en cuanto a si serían capaces de desarrollar las competencias adquiridas en la Empresa. En [6] se muestra la baja satisfacción de los profesores ante el cambio al EEES. Resultado que se ha visto complementado recientemente en

informes sobre la Calidad de la docencia universitaria en la que se observa un nivel creciente de burocratización de las tareas del profesorado. Finalmente, es de destacar que en [7] se muestra un ejemplo, en el ámbito de las asignaturas de Ingeniería, de la dificultad práctica que supone la puesta en marcha de metodologías de aprendizaje cooperativo entre alumnos. Esto es especialmente acentuado entre los alumnos de Ingeniería a los que tradicionalmente se les ha acostumbrado a trabajar de forma individual o por parejas sobre todo en los temas de teóricos.

Si bien es demostrable que a nivel de Gobierno de la Universidad se hacen esfuerzos para que los profesores adapten su forma de impartir clases, no se detecta que exista un nivel de formación adecuado en el manejo de herramientas telemáticas que favorezcan el proceso de aprendizaje de los alumnos (haciéndoles intérpretes a ellos de su proceso de aprendizaje). Y también es constatable que los centros docentes también están haciendo esfuerzos por generar herramientas que faciliten la planificación global de las clases presenciales; pero no profundizan en la implantación de modelos de coordinación cooperativa entre profesores. Nosotros pensamos que la adaptación al EEES se debe hacer con una visión sistémica y con la mirada puesta en una solución que fomente la cultura innovadora que facilite la implantación de metodologías de trabajo cooperativo de todos los agentes implicados en ello. Nosotros identificamos 3 agentes principales (circunscribiendo la solución a nivel de departamentos y centros docentes): la Junta de centros docentes, Profesor y Alumno. Entendemos que el papel del Consejo de Departamento no entra en esta solución porque generalmente no tiene competencias administrativas para organizar la docencia verticalmente con visión global de todas las asignaturas de la Titulación.

En este trabajo presentamos una aportación concreta que hemos desarrollado en cursos anteriores (dentro y fuera del marco del EEES) que fomenta el trabajo cooperativo entre profesores y alumnos con apoyo de la Junta de centro docente. En concreto hemos diseñado herramientas de trabajo cooperativo a nivel de profesores y la Junta de centro docente para planificar la docencia presencial de las asignaturas y por otro lado hemos utilizado Google Drive para organizar la docencia mediante modelos de aprendizaje cooperativo entre los alumnos. En asignaturas con pocos alumnos los resultados son espectaculares: tanto los alumnos como los profesores muestran su satisfacción; sin embargo, a medida que aumenta el número de alumnos los resultados no son tan espectaculares, pero sí buenos en general.

II. Modelo de trabajo cooperativo

Como en todos los sistemas de enseñanza que se han usado hasta el momento, en el EEES existen puntos fuertes y débiles. Ello ha llevado a que las distintas universidades se esmeren en analizar la satisfacción del alumnado. Además de la satisfacción que se muestra en las encuestas publicadas, es verdad que en general los alumnos suelen quejarse de la carga excesiva de actividades que se suelen evaluar de forma continua y el número elevado de horas presenciales que deben cumplir en algunas semanas del curso (por ejemplo, las prácticas de laboratorio o las tutorías presenciales se suelen concentrar al final del curso haciendo que los alumnos

Fig. 1. Ejes principales del proceso de enseñanza-aprendizaje del EEES.

tengan una carga lectiva semanal muy elevada). Cuando esto ocurre en varias asignaturas simultáneamente el alumno no puede llevar a cabo su proceso de aprendizaje con garantías de éxito. Aunque las Juntas de centro docente suelen velar para que esto no se produzca ajustando la planificación temporal de los proyectos docentes de las asignaturas distribuyéndolo equilibradamente a lo largo de todo el semestre de impartición, esta es una tarea muy complicada de implantar en la práctica de manera efectiva, porque las soluciones no suelen contemplar la participación cooperativa de todos los profesores que imparten las asignaturas.

Otro problema que se suele producir es el desajuste del proceso de enseñanza de los distintos profesores de una asignatura. Esto es, en algunos casos no es posible impartir los temas de teoría tal como se ha planificado inicialmente por varias causas justificadas: por ejemplo que existan días no lectivos o de huelga imprevistos en el momento en el que se planificó la impartición de los temas de teoría del proyecto docente, o bien simplemente no ha sido posible terminar un tema debido a la participación activa de los alumnos que ha requerido más tiempo para terminar de explicar adecuadamente el tema. Esto puede llevar asociado un cambio en la planificación de la docencia de problemas en el aula e incluso de prácticas de laboratorio que deberían ser adecuadamente coordinadas de manera cooperativa por todos los profesores de la asignatura de forma dinámica. Y debe contar con el mecanismo ágil de información a la Junta de centro docente para que contemple posibles mecanismos de coordinación vertical entre asignaturas al objeto de que la carga presencial semanal del alumno no sea excesiva y pueda llevar a cabo con garantías su proceso de aprendizaje.

Por último, entre los alumnos de una asignatura suele ocurrir que el trabajo en grupo produce desajustes temporales catastróficos para su proceso de aprendizaje. Esto es, en muchos casos los alumnos no son capaces de cooperar entre ellos para apoyarse en la realización de un trabajo en grupo debido a que, aunque cuentan con herramientas telemáticas muy potentes de comunicación en tiempo real, no las suelen usar para hacer dichos trabajos de forma efectiva. Se observa una falta de cultura de trabajo en grupo preocupante.

Estos problemas anteriores suele tener unos efectos demoledores en el comportamiento docente alumnado y profesorado. A título de ejemplo exponemos algunas de ellas: a) desánimo, lo que lleva a que los profesores no cambien sus hábitos docentes pre-EEES y pierden el interés por cambiar su forma de impartir docencia según el nuevo modelo; y a que los alumnos intenten coger atajos que les permitan "soportar" la gran cantidad de tareas que deben realizar en solitario (y en un intervalo de tiempo dado), y b) mala gestión del tiempo dedicado a tareas de coordinación, lo que produce que el profesor termine por "llevar" individualmente el control de las tareas que el alumno debe realizar, sus tareas de evaluación, puesta de notas y coordinación con sus compañeros de asignatura (escritura de informes) para no perder tiempo en reuniones de coordinación largas y faltas de eficacia; y que el alumno prefiera ir por libre sin explotar sus relaciones personales ni de estudio con sus compañeros para tener la sensación de que no pierde el tiempo en relaciones que no le aportan frutos de aprendizaje claros (aprobar las asignaturas). Lo anterior lleva directamente a la desmotivación por el aprendizaje cooperativo y la cultura del trabajo individual. Lo cual es un problema de importancia mayúscula en la Sociedad del Conocimiento y la Globalización.

La solución a los problemas anteriores debe ser de tipo sistémica (aprovechando la jerarquía subyacente del sistema educativo), debido a que entre esos problemas hay inter-relaciones que hacen que las soluciones particulares en un nivel dado no sean efectivas en la práctica. En la Fig. 1 se muestra un esquema en el que se muestran las relaciones jerárquicas del sistema. En el primer nivel de jerarquía, la Junta de centro debe ser capaz de organizar a los profesores de una titulación para que la planificación de la docencia se lleve a cabo con éxito. En el segundo nivel de jerarquía, los profesores deben guiar adecuadamente a los alumnos (que estarían en un tercer nivel de jerarquía), para que puedan llevar a cabo el proceso de aprendizaje de forma autónoma y según lo establecido en el proyecto docente. Nótese que el esquema contempla la posibilidad de que los alumnos puedan realimentar con sus comentarios, quejas y sugerencias al primer nivel jerárquico el funcionamiento del sistema (es de suponer que esto se hace cuando falla la comunicación de esos problemas entre alumnos y profesores, o bien cuando entre profesores y alumnos no es posible dar solución simple a un problema concreto de manera directa). En los siguientes apartados presentamos los distintos niveles a los que se puede dar solución a este tipo de problemas.

A. Organización cooperativa de la planificación de la docencia

En la Fig. 2 se muestra que, bajo la supervisión de la Junta de centro, los profesores deben ser capaces de reaccionar a cualquiera de los problemas que surjan en la alteración de la planificación de la asignatura: los responsables de la Junta de centro mediante el uso de herramientas telemáticas deben estar inmediatamente informados de esos problemas (haciendo uso de mensajes cortos o correos electrónicos enviados por la herramienta). Esta herramienta debe disponer de la posibilidad de que los alumnos puedan también informar a esos responsables de cualquier deriva en la planificación del proyecto docente.

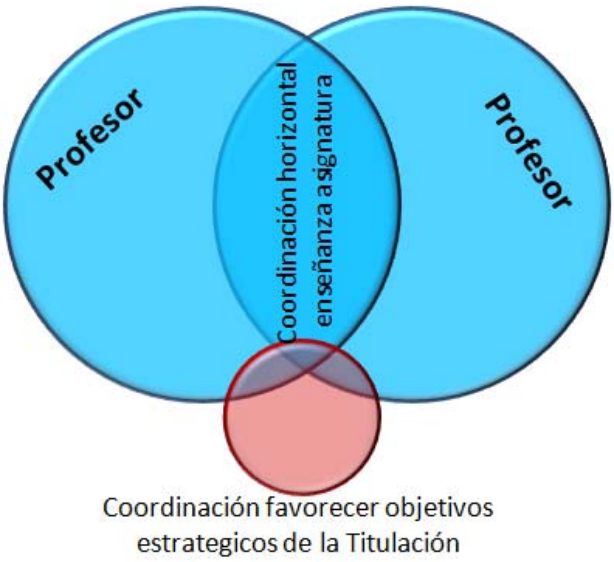


Fig. 2. Esquema de cooperación entre alumnos.

Una característica de esta herramienta es que debe tener una interfaz muy simple, ubicua con acceso inalámbrico y Web y además permitir que únicamente un notario electrónico conozca la identidad del alumno para permitir libertad en la realimentación del funcionamiento del sistema y seguridad a la hora de que no se hagan sugerencias carentes de fundamento [8].

En el caso del centro docente: *Escuela de Ingeniería de Telecomunicación y Electrónica* (*EITE*) de la *Universidad de Las Palmas de Gran Canaria* (*ULPGC*) actualmente se utiliza *Joomla* [9] para hacer la planificación de las asignaturas y que los profesores modifiquen dicha planificación en caso necesario. Pero no se permite la participación de los alumnos. Por otro lado, la interfaz de trabajo es poco amiga del usuario y se requiere mucho tiempo para hacer modificaciones muy simples. En general se requeriría mayor nivel de automatización y agilidad de estos procesos a la vez que se simplifiquen las tareas a realizar cooperativamente por parte de los agentes.

B. Coordinación cooperativa de los profesores

En la Fig. 2 se indica que los profesores deben llevar a cabo las acciones de coordinación de una asignatura concreta que tienen permisos para modificar y realizar las operaciones que estimen oportunas. Nótese que el conjunto de asignaturas puede ser vista por todos los profesores de la Titulación favoreciendo de esta manera el trabajo en abierto [10] y facilitando la coordinación vertical de asignaturas de manera distribuida proactiva (minimizando la intervención de los responsables de la Junta de Centro en caso de conflictos entre asignaturas: por ejemplo muchos exámenes parciales en una semana de distintas asignaturas). Además, la misma herramienta usada por los responsables de la Junta de centro docente podría usarse para estas tareas. Ejemplo de acciones que podrían llevar a cabo son cuando se:

a) Elabora el proyecto docente, normalmente cuando se reparte la docencia en los departamentos, todos los profesores, usando una única instancia del proyecto

Fig. 3. Esquema de cooperación entre profesores.

docente pueden cooperar en la edición, en tiempo real y on line de dicha instancia.

b) Está impartiendo y se produce una alteración haciendo uso de servicios de comunicación en tiempo real entre profesores y con responsables de la Junta de Centro.

c) Elaboran pruebas de evaluación de cualquier tipo (teoría, laboratorio, problemas...) compartiendo una instancia de la prueba a realizar para su edición y comentarios cooperativos.

d) Ponen las notas obtenidas por los alumnos (en el mejor de los casos, normalmente se suele hacer mediante el envío rotativo de un archivo por correo electrónico) compartiendo un archivo con las notas y sus ítems.

e) Elabora el informe final de la asignatura (normalmente también mediante rotación por correo electrónico de dicho informe), compartiéndolo durante todo el curso para que cada profesor pueda anotar a modo de bitácora los temas concretos impartidos y detalles concretos a destacar en su docencia que el resto de profesores deba conocer.

En la EITE actualmente las acciones b a e se llevan a cabo en distintas herramientas que no tienen ninguna relación entre ellas (*Moodle* [11] por un lado y Joomla por otro). La acción a se lleva a cabo en una herramienta separada de las anteriores que maneja el equipo de Gobierno de la ULPGC. Son todas herramientas Web que carecen de interfaces amigas del usuario y acceso ubicuo inalámbrico.

Sería deseable que existiera una herramienta que tuviera una interfaz muy sencilla y además permitiera compartir la información rápidamente en una nube privada con acceso inalámbrico ubicuo porque ahorra mucho tiempo de burocracia, a la vez que produce inmediatez en el uso y motivación por cooperar. Esta herramienta debe contener servicios de *Voz sobre Internet Protocol* (*VoIP*) (para localizar a cualquiera de los profesores en tiempo real para consultar o aclarar dudas), una pizarra compartida (para que en el caso de que se disponga de un terminal adecuado se pueda explicar una idea gráficamente) y mensajería en diferido tradicional (para comunicar o explicar acciones cuya urgencia en el tiempo es baja), gestión de agendas y tiempos de realización de tareas marcadas por el coordinador de la asignatura o responsable de la Junta de Centro. El principal objetivo es eliminar pérdidas de tiempo en la coordinación o inmediatez en la solución de problemas. Aunque a día de hoy hay entornos integrados de gestión de la docencia que son capaces de proporcionar estos servicios, el problema que tienen es que adaptarlos para casos particulares es tedioso y su interfaz de manejo suele ser muy engorrosa. Por eso, un requisito adicional es que la herramienta sea muy simple de usar y mantener.

C. Aprendizaje cooperativo entre alumnos

El uso de herramientas de gestión de la docencia tipo Moodle permite que los alumnos puedan realizar pruebas de evaluación, ejercicios, publicar información, discutir entre ellos mediante foros, elaborar apuntes mediante wikis... El avance producido en este campo en los últimos años es espectacular. Por ello, se puede utilizar este tipo de herramientas para facilitar el aprendizaje cooperativo entre los alumnos (con o sin supervisión del profesor). El software de redes sociales, blogs y microblogs son otros elementos que se suelen utilizar para estos menesteres. Curiosamente, en las asignaturas de Ingeniería, en general, se advierte el poco entusiasmo que despierta el uso de estas herramientas en los alumnos y en los profesores, porque al ser normalmente expertos en su uso detectan fallas o falta de potencia para hacer determinadas tareas muy útiles. Además, suelen tener interfaces bastante complejas que impiden que puedan ser usadas eficazmente con terminales móviles.

Ejemplos de tareas que suelen ser muy difíciles de encontrar en las herramientas analizadas son: a) edición cooperativa en tiempo real y on line de documentos ricos en contenidos multimedia, para elaborar apuntes en los que se permita, por ejemplo, usar un teléfono móvil para dibujar sobre la marcha un esquema de clase, b) establecer una llamada de VoIP con otros alumnos o profesores que les permitan aclarar dudas rápidamente, c) usar una video-conferencia desde un terminal móvil para exponer un problema, por ejemplo con la elaboración de una práctica de laboratorio, o d) elaborar rápidamente un mapa conceptual de un tema a desarrollar con ayuda de otros compañeros.

En la Fig. 3 se muestra que el profesor, usando una herramienta telemática adecuada sería capaz de orientar a los alumnos en su trabajo cooperativo de forma sencilla y eficaz. El uso de una herramienta que permita compartir información con instancias únicas modificables por cualquier alumno o profesor permitiría a los alumnos ahorrar tiempo y gestionar mejor su tiempo de estudio. La herramienta que posibilita llevar a cabo estas tareas debe permitir a los profesores guiar a los alumnos en la solución de los problemas que se les planteen y también fomentar el aprendizaje cooperativo entre ellos. Esta herramienta debe operar en abierto para todos los profesores y alumnos de la Titulación al objeto que cualquier profesor pueda aportar su punto de vista en un tema concreto a la vez que se facilita que entre todos los profesores exista flujo real de los conocimientos que se están impartiendo en cada asignatura. Lo mismo es aplicable a las pruebas de evaluación y los temas tratados en las clases presenciales.

Juntando todo se obtiene el modelo de la Fig. 4 en la que se muestra que la Junta de Escuela (Centro docente) es la

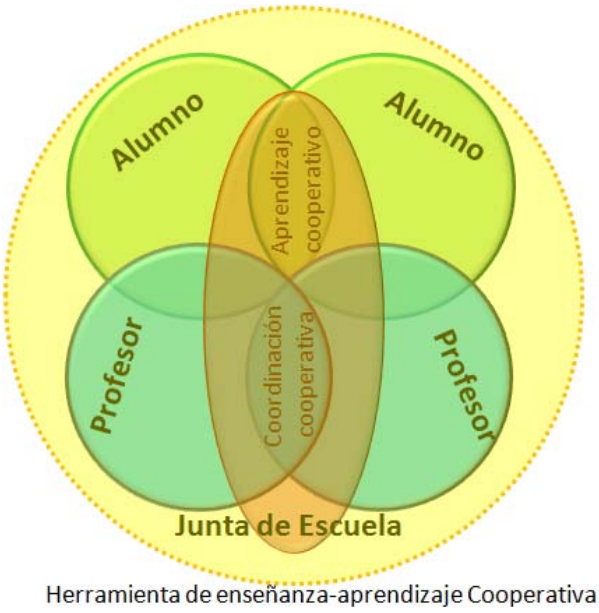


Fig. 4. Herramienta telemática de ayuda al proceso enseñanza-aprendizaje.

columna que vertebra las acciones coordinadas de los profesores de la misma o distinta asignatura que a su vez son los que coordinan el aprendizaje cooperativo de los alumnos. Usando certificados digitales se puede llevar a cabo toda la administración de forma electrónica eliminando por completo el papel y permitiendo que todas las acciones de trabajo a cualquier nivel pueda ser visto por todos los profesores y modificable por los de una asignatura concreta.

Nosotros en [12] presentamos una herramienta que permite planificar la docencia de las asignaturas con la participación de los tres niveles jerárquicos del sistema educativo. La herramienta tiene una interfaz de usuario sencilla, es fácil de manejar y permite la cooperación reducida entre los agentes del sistema. Sin embargo, no permite el trabajo cooperativo de los alumnos para su proceso de aprendizaje y su integración con el Moodle oficial de la ULPGC y con otras herramientas de la ULPGC no es sencilla debido a cuestiones técnicas y de gestión de los distintos organismos de la ULPGC.

Por ello, es necesario contar con una herramienta que no tenga los inconvenientes de implementación anteriores. Por otro lado, sería deseable que estuviera disponible las 24 horas de todos los días y que minimizara el ahorro energético de las máquinas que la implantan. El ahorro en gastos de administración y operación de la herramienta también es un factor crítico de diseño.

III. Google Drive para facilitar el proceso enseñanza-aprendizaje

El tipo de herramienta telemática candidata a cumplir con el modelo propuesto es aquella que se ejecute en la Nube y que sea ofertada por la Universidad o Empresa externa de forma gratuita a todos los agentes del EEES revisados en el apartado anterior.

No es nuevo que el Google Drive se está introduciendo rápidamente en la enseñanza en colegios públicos y diversas universidades de muchos países. La sencillez con la que se pueden emplear sus diversas herramientas para la enseñanza nos lleva a pensar que en general puede es muy útil para implantar el modelo expuesto.

El Google Drive permite desplegar una estructura básica para un curso on line que facilite el proceso enseñanza-aprendizaje de manera rápida y sencilla para usuarios que no necesitan tener grandes conocimientos de informática y comunicaciones. Al mismo tiempo, es apropiado para profesores y alumnos de ingenierías debido a que para ciertos usos es muy potente y ofrece una cantidad enorme de aplicaciones que pueden ser configuradas para potenciar su uso muy concreto. Sin embargo, tiene algunos inconvenientes que limitan su uso en la enseñanza. A continuación exponemos un conjunto de ventajas e inconvenientes de este entorno para su uso en asignaturas de Ingeniería Telemática.

Entre las ventajas de usar Google drive están: a) edición cooperativa de archivos de su plataforma ofimática de manera sencilla tanto on line como off line usando los servicios de sincronización con carpetas locales del usuario, b) editar y enviar encuestas rápidamente sobre una cuestión que no haya podido quedar clara en clase, c) obtener estadísticas sobre los resultados de evaluación de los alumnos o de su evaluación continuada de manera sencilla e integrada con el resto de herramientas, d) crear rápidamente información multimedia para el aprendizaje de conceptos complicados: por ejemplo, tomar una imagen de una pizarra electrónica y automáticamente subirla al drive, tomar fotos de un dispositivo diseñado en el laboratorio, un vídeo sobre cómo ha ido evolucionando el diseño de la interconexión de equipos heterogéneos a un encaminador de internet con sus *gateways* respectivos, subir un vídeo con un ejemplo de configuración de un servicio de correo electrónico... e) editar cooperativamente un mapa conceptual sobre un tema concreto usando aplicaciones como *Meinmeister*. De especial interés es la posibilidad de usar Google Drive para trabajar en tiempo real durante una clase o fuera de ella. Esto es, algunos alumnos pueden estar fuera de clase siguiéndola mediante un canal de VoIP en sus terminales móviles y colaborando con los alumnos de clase que en ese momento hacen uso de sus terminales móviles y una conexión *Wireless Fidelity* (*WiFi*) disponible en todas las aulas de las universidades. De esta forma la discusión de la solución a problemas en el aula puede enriquecerse enormemente con la aportación on line que hace cada uno de los alumnos usando un archivo compartido. Otro detalle interesante es que ésta es una forma de generar documentación sobre los problemas que permite una evaluación casi instantánea del alumno.

Entre las desventajas están: a) no tiene integrado un servicio de VoIP en la suite de drive directamente, con lo cual se ha de mantener en paralelo un sistema que permita usar al grupo de alumnos de una asignatura sincronizado con las herramientas externas de Google, b) el servicio de *hangout* de Google se debe usar también de forma separada a Google drive, c) la creación de grupos para compartir propiedades de edición de archivos se debe hacer manualmente lo cual pone limitaciones de configuración rápidas importantes, d) el establecemiento de dinámicas de aprendizaje en grupos dinámicos de tal manera que temporalmente los archivos sobre los que se trabajan no sean visibles a otros grupos es tedioso y propenso a errores

porque la configuración de esos grupos es engorrosa y lleva cierto tiempo que limita el poder hacerlo en tiempo real.

A pesar de las desventajas anteriores, nosotros hemos usado Google Drive en los últimos años para facilitar el proceso de enseñanza aprendizaje tal como exponemos en el siguiente apartado, debido a que en general, la respuesta es bastante satisfactoria en relación al tiempo y recursos que se dedican.

IV. Experiencia usando Google Drive

Nosotros hemos utilizado Google drive en distintas asignaturas de Ingeniería Telemática, tanto para la enseñanza como para llevar a cabo su coordinación horizontal. No hemos llevado a cabo la coordinación vertical ni tampoco las relaciones con los responsables de la Junta de centro docente por no haber sido posible hacerlo a nivel oficial. Dentro de la docencia dentro de una asignatura concreta, hemos utilizado el Google drive para: a) suministrar documentación a todos los alumnos, llevar a cabo la evaluación de los problemas en el aula, las prácticas de laboratorio y la teoría, b) elaborar documentación cooperativamente sobre temas concretos que a priori se clasifican como difíciles de entender por los alumnos por experiencia de cursos anteriores, c) llevar a cabo la enseñanza cooperativa de ciertos temas que requieren de una reflexión profunda por parte de los alumnos para ser asimilados. A continuación presentamos de forma detallada estos ejemplos y el proceso para lograr llevar a cabo estas tareas usando ejemplos de distintas asignaturas en distintas universidades.

La *Agencia Nacional de la Evaluación de la Calidad* y *Acreditación* (*ANECA*) requiere que por cada curso se elabore por cada asignatura un informe final de resultados de su impartición. Por tanto, la coordinación entre los profesores de una asignatura, no sólo tiene interés por elevar la calidad de la docencia ofertada sino que además debe quedar reflejada en un documento final que se debe elaborar especificando las actividades que realiza cada uno de los profesores que la imparten. A la hora de elaborar o mejorar el proyecto docente de la asignatura procedemos a publicarlo en Google Drive entre los profesores recién asignados por el Consejo del Departamento. Se discute presencialmente o mediante VoIP aspectos concretos antes de proceder a publicarlo en la herramienta de la ULPGC. Para la coordinación durante el curso se procede a compartir un documento en Google drive que permite que diariamente cada profesor escriba lo que ha impartido en clase y si ha tenido algún tipo de incidente o hecho que quiera destacar. La ventaja de hacerlo de esta manera es que en caso que haya habido algún suceso extraordinario, inmediatamente el coordinador puede hacer una multi-conferencia VoIP con todos los profesores disponibles en ese momento para discutir el problema. Un ejemplo típico se produce cuando en una semana no ha sido posible impartir una clase de teoría debiendo retrasar en ese momento el resto de clases para que queden debidamente sincronizadas. Para que el alumno quede perfectamente informado de hechos como éste, se comparte con ellos un archivo con el temario a impartir estructurado por semanas: cuando existe un problema de retraso, simplemente se actualiza este archivo y se envía una notificación (correo electrónico a todos), para que queden enterados. Nótese que en caso que la Junta de centro docente lo permitiera, esto sería muy fácilmente escalable al resto de asignaturas, haciendo que existiera un archivo compartido con los temarios de todas las asignaturas o simplemente una carpeta con todos los archivos de cada asignatura.

Un detalle importante que permite motivar el aprendizaje cooperativo emocional y social es la provisión de una bitácora de las clases impartidas diariamente. En documento compartido con una estructura de plantilla previa se permite que el profesor: a) exponga brevemente lo que se ha hecho en clase después de impartirla (destacando los puntos importantes que a su juicio han surgido) y b) presente cuál ha sido su impresión acerca del ambiente que ha detectado en clase (si ha detectado des-interés, interés, que no se ha entendido algo, o si se ha entendido o simplemente su opinión sobre su propio trabajo en clase). El alumno tiene libertad para expresar sus propias opiniones en esta bitácora, pudiendo utilizarla para hacer anuncios sobre eventos extra-curriculares que entienda serían de interés para todos. Por ejemplo, es típico que anuncie que no puede ir a clase un día determinado y pida ayuda a sus compañeros con el material de clase, y lo más frecuente es que anuncien novedades tecnológicas relacionadas con lo que se explica en clase. En algunos casos esta bitácora se convierte en un almacén de sugerencias para mejorar aspectos particulares de la docencia de algunos temas que tienen un valor enorme. Está claro que aplicando esta técnica al resto de asignaturas de la Titulación se puede obtener una forma de realimentación positiva muy importante.

La evaluación tiene varias facetas diferentes que se puede llevar a cabo con la ayuda de Google drive: a) la preparación de las pruebas de evaluación se hace compartiendo un archivo con las preguntas a realizar entre los profesores de la asignatura. Durante un plazo se modifican y se comentan hasta asegurar que se cumplen las competencias y el alumno obtendría los resultados del aprendizaje. b) La evaluación se hace compartiendo un examen (archivo PDF) de sólo lectura que se comparte justamente unos minutos antes de empezar la prueba de evaluación. En una plantilla de respuesta aparte el alumno puede responder a cada una de las preguntas. Esta plantilla está hecha mediante una hoja de cálculo que el alumno debe primero copiar en su carpeta personal y a continuación responder a las preguntas. Una vez finalizado el plazo de respuestas, el profesor corrige on line y actualiza la puntuación de cada una de las preguntas. Automáticamente la plantilla de hoja de cálculo obtiene la nota final obtenida en esa prueba. Subrayar que en esa plantilla hay casillas protegidas para que el alumno no las pueda escribir (puntuación, nombre de la asignatura...). c) En una plantilla de hoja de cálculo privada compartida entre todos los profesores se actualiza la nota obtenida por cada alumno en cada prueba (cada profesor actualiza la parte que ha evaluado) y automáticamente obtiene la nota final del alumno que se le publica a medida que va haciendo evaluaciones continuadamente. Este proceso es propenso a errores en plataformas como Moodle debido a que un profesor puede alterar la nota puesta por otro involuntariamente. Para solucionar esto, cada casilla de la hoja de cálculo que puede actualizar un profesor determinado está perfectamente protegida (con los permisos adecuados), para que los otros no puedan alterarlas. Esto se podría llevar a cabo con ayuda de la Junta de centro docente

para todas las asignaturas de tal manera que se ahorra tiempo del profesor al poder re-utilizar muchas plantillas estándar de evaluación en asignaturas similares. Las notas obtenidas son fácilmente exportables a las herramientas de la ULPGC para publicar las notas oficialmente a los alumnos.

La bitácora permite conocer aquellos detalles que no han quedado claros en las clases de teoría: los alumnos suelen dejar claro lo que no han entendido por si alguno de sus compañeros desean ayudarles respondiendo a sus preguntas concretas. Esto realimenta positivamente la impartición de las clases de problemas en el Aula, porque en primer lugar el profesor publica los enunciados de los problemas en una carpeta compartida. En esa carpeta además pone información que él considera relevante para resolver el problema y se permite que los alumnos pongan información que consideren puede ser de ayuda a resolver ese problema. Con esa información entre todos los alumnos opinan como resolver el problema antes de que sea discutida en las clases presenciales de problemas en el Aula. Ya en esa clase el profesor pide discutir soluciones posibles. Las posibles soluciones que se discutan y cada alumno particularice son subidas a su carpeta personal como respuesta personal al problema. Haciendo esto es muy sencillo averiguar el grado de información buscada y discutida en grupo entre los alumnos: estos dos parámetros puntúan en la nota final del alumno en la ULPGC.

La misma técnica seguida para las clases de problemas en el aula se sigue para las clases prácticas de laboratorio: primero se publica el enunciado de la práctica, después los alumnos buscan información para resolverla, se discute a través de Google drive y finalmente en las clases de prácticas de laboratorio cada alumno da su solución particular que sube a su carpeta personal. Además, responde a un cuestionario propuesto por el profesor sobre el desarrollo de la práctica.

Tanto en las clases de problemas en el aula como en la de prácticas de laboratorio el alumno se acostumbra a discutir en grupo y formular soluciones cooperativamente. Un punto importante del Google drive es que permite ir un paso más allá en las clases de teoría y la forma de enfocar la impartición de los temas. Para algunos de los apartados más relevantes por su dificultad de aprendizaje, en primer lugar el profesor publica información relativa a ese tema parcialmente antes de empezar la clase presencial. Invita a los alumnos a hacer un repaso previo de la información publicada después de los primeros 10 minutos de haber sido enfocado el tema en la clase presencial de teoría. En esa misma clase presencial, después de 10 minutos que los alumnos han revisado el material disponible, el profesor procede a explicar el tema y acto seguido se invita a que entre todos los alumnos (estructurados en grupos de 3 a 5 alumnos como máximo) hagan sus propios esquemas conceptuales de lo que han aprendido en un total de 10 a 15 minutos mediante una herramienta de Google drive denominada *Meinmeister*. Como trabajo del alumno se ha de revisar todos los esquemas compartidos y generar su propio esquema del apartado ayudado por lo que el profesor hubiera explicado en la clase presencial. En la siguiente clase presencial se propone a los alumnos que elaboren un informe cooperativamente. Se da un plazo y finalizado ese plazo el profesor puede averiguar qué alumnos han participado en ese informe y corregirlo. Es importante aclarar que no se debe alterar la forma en que haya sido escrito pues es seguro que el alumno ha empleado su propio lenguaje para entender los conceptos. Por último, destacar que se avisa que esos informes generados son objeto de evaluación en el examen final de la asignatura lo cual hace que los alumnos se esmeren por cooperar con sus compañeros para no perder oportunidades de aprobar.

Nosotros hemos implantado esta técnica de enseñanza-aprendizaje desde el año 2009 cuando Google drive estaba todavía en un estado de funcionamiento muy básico (*Google docs* en conjunción de *Google groups*), en varias asignaturas de Ingeniería Telemática de la ULPGC: a) en la Titulaciones de Ingeniero de Telecomunicación de la EITE pre-EEES: 1) Sistemas Multimedia en Tiempo Real, 2) Redes de ordenadores, b) en el Grado EEES de Ingeniería de Telecomunicación de la EITE: 1) Arquitectura de Redes, 2) Aplicaciones de Red, c) en el Master EEES de Tecnologías de Telecomunicación de la EITE: 1) Tecnologías Internet de Nueva Generación y 2) Ingeniería de Aplicaciones Móviles y d) en estudios de doctorado. Además se ha empleado en asignaturas de Master de la Universidad Politécnica de Valencia y en la Escuela Politécnica del Litoral (Ecuador). La muestra de asignaturas es importante porque son muy variadas, desde el tercer al quinto curso de titulaciones pre-EEES a grado y master del EEES y doctorado en España (distintas universidades) y fuera de España. El número de alumnos es muy variado: desde 2 alumnos de doctorado hasta los 65 alumnos de segundo curso del grado. La temática de las asignaturas también es variada: tecnologías de redes hasta programación pasando por sistemas multimedia. Por último, el número de profesores ha variado: en algunas asignaturas sólo había un profesor y en otras 2, 3 y hasta 9 en una de ellas.

Entre las ventajas aportadas por este modelo y herramienta de enseñanza-aprendizaje, en general, es el aumento de interés que se ha producido en todos los casos por el contenido de las asignaturas y la motivación por el aprendizaje autónomo y la enseñanza y aprendizaje cooperativos. Por otro lado, se observa que la evaluación de las competencias de los alumnos se mejora considerablemente debido a que se facilita enormemente su gestión por un lado y la captura de evidencias de evaluación por otro. En particular, cuanto menor es el número de alumnos mejor es el modelo porque básicamente el índice de aprobados es del 100% y el abandono de las asignaturas es nulo. En concreto para la asignatura de doctorado se probó la realización de clases presenciales mediante video-conferencia (VoIP) con un alumno que estaba en Italia pero que cooperaba con los de Gran Canaria mediante Google drive en tiempo real para discutir temas concretos de algunos temas de teoría. Un detalle final es que la coordinación de todas esas asignaturas con distintos equipos de profesores se pudo llevar a cabo con una gestión del tiempo de coordinación extremadamente eficiente. En todos los casos el uso de la bitácora fue muy útil. La satisfacción del profesorado en tareas de coordinación es muy elevada porque permite reducir enormemente los procesos burocráticos asociados a la coordinación y la puesta de notas burocrática de los alumnos.

Sin embargo, para que el uso de Google drive sea del todo eficiente quizás se deberían mejorar algunos aspectos concretos: a) compartir información con distintos alumnos es

un proceso lento (y propenso a errores) en el caso que sean necesarios permisos particulares para distintos grupos de alumnos. Ello significa que hay que preparar bien ese aspecto de las clases presenciales para no perder tiempo en la clase presencial. b) Actualizar permisos para archivos individuales dentro de una carpeta es un proceso engorroso si en la asignatura existen muchos alumnos. c) Mientras que es muy simple proteger celdas concretas de una hoja de cálculo para que solo ciertos alumnos las puedan modificar, es cierto que esto no es posible hacerlo para partes concretas de un archivo de texto a ser editado cooperativamente. Esto es importante puesto que puede aportar beneficios muy grandes al evitar posibles errores involuntarios de eliminación de información.

V. Conclusiones

El EEES ha creado un nuevo esquema de enseñanza-aprendizaje basado en nuevas relaciones alumno-profesor. La diferencia con respecto al modelo anterior es que se intenta que el alumno sea el intérprete de su propio proceso de aprendizaje. Esto significa que se ha de crear los mecanismos adecuados para que el alumno sea capaz de interpretar adecuadamente los conocimientos que el profesor y otros medios le aportan. Entre la gran cantidad de técnicas de enseñanza y aprendizaje (puzzle, basadas en problemas, dirigida por portafolios...) nosotros creemos que el modelo cooperativo es uno de los más interesantes.

El modelo cooperativo es aplicable a otros esquemas de trabajo entre profesor y alumno puesto que es un modelo de trabajo general. Los alumnos pueden cooperar entre ellos de manera autónoma para adquirir conocimientos y los profesores pueden cooperar entre ellos para generar el conocimiento y administrar su impartición de tal manera que obtengan una gestión de su tiempo eficiente. Precisamente, la gestión eficiente del tiempo es uno de los problemas que se produce en el EEES ya que los profesores suelen quejarse de que se exige una gran dedicación a la burocracia para preparar reuniones de docencia, para evaluación, preparación de proyectos docentes, coordinaciones puntuales para resolver problemas concretos que surgen al día a día: todo lo cual conlleva la generación de actas de reuniones y escritos oficiales... Lograr que el alumno esté satisfecho es otro de los objetivos que combinado con elevar la calidad de la docencia para lograr niveles muy altos (especialmente en las ingenierías en las que tradicionalmente este nivel siempre ha sido muy elevado) es una de las máximas preocupaciones oficiales actualmente. Con el modelo cooperativo se permite que el alumno pueda adquirir modos de trabajo necesarios en la Sociedad del Conocimiento y la Globalización.

En este trabajo hemos diseñado un esquema o modelo de trabajo cooperativo a tres niveles que permite sintonizar adecuadamente el trabajo de las juntas de centros docentes, los profesores y el alumno usando Google drive. Mediante este modelo y herramienta se puede organizar de forma muy sencilla (en un muy poco tiempo) la gestión de las asignaturas a través de la Nube. Este modelo tiene varias ventajas: permite ahorrar energía en los centros docentes, disponibilidad continua del servicio en la Nube, y una facilidad enorme de uso ubicuo e inalámbrico. La experiencia variada que hemos obtenido en los últimos años ha demostrado que estas ventajas se ven contrastadas con la insuficiente capacidad de Google drive para compartir eficazmente partes de documentos y rapidez a la hora de reconfigurar permisos de acceso a documentos. En cualquier caso el balance de uso es muy positivo por los buenos resultados obtenidos tanto en las titulaciones antiguas como en las del EEES, con número variable de alumnos y de profesores.

Referencias

[1] Carmen Florido, Juan Luis Jiménez, Jordi Perdiguero, Cómo (no) adaptar una asignatura al EEES: Lecciones desde la experiencia comparada en España, e-pública Revista electrónica sobre la enseñanza de la Economía Pública, 24-28, Nº 10, febrero, 2012.

[2] Prácticas Hacia la Excelencia de los Trabajos Fin de Grado. Elaboración de un catálogo de prácticas basadas en el cotejo con el marco nacional e internacional y experimentadas en el campo de la Ingeniería. Análisis de la proyección y transferencia a otros contextos. Davinia Hernández-Leo (Coordinadora). Programa de Estudios y Anàlisis 2011 Ministerio de Educación, Cultura y Deporte (EA2011-0088).

[3] Carmen Otero Neira, Carlos Ferro Soto y Mercedes Vila Alonso, Satisfacción del alumnado ante la implantación del Modelo de EEES. Análisis comparativo, Revista Educativa Hekademos, 12, Año V, diciembre 2012

[4] Maria Luisa Cantonnet Jordi, Jasmina Berbegal Mirabent, Juan Carlos Aldasoro Alústiza, Análisis de la adaptación al espacio europeo de educación superior (EEES) a través de las encuestas de satisfacción del alumnado. El caso de la asignatura de seguridad y prevención de ingeniería de la edificación de la universidad del País Vasco (España), tendencias pedagógicas nº 21, 119-131, 2013

[5] Virginia Gutiérrez, Isabel Sánchez, Rafael Betancor, Metodología de adaptación al EEES y análisis de la asignatura bases de datos desde la perspectiva de las competencias profesionales del ingeniero en informática, http://redaberta.usc.es/aidu/index2.php?option=com_docman&task=doc_view&gid=441&Itemid=8

[6] http://www.euatm.upm.es/calidad/encuestas/informe_satisfaccion_pdi-1.pdf, disponible mayo 2013.

[7] J. K. Espinosa, J. Jiménez, M. Olabe1, Y X. Basogain, Innovación docente para el desarrollo de competencias en el EEES, http://campus.usal.es/~ofeees/ARTICULOS/p216.pdf

[8] Carlos Espino Yagüe, Servidor de correo electrónico anónimo, Álvaro Suárez Sarmiento (director), Proyecto Final de Carrera, Universidad de Las Palmas de Gran Canaria, Escuela Universitaria de Ingeniería Técnica de Telecomunicación, 2002.

[9] http://www.joomla.org/, disponible mayo 2013.

[10] David González Dorta, Herramienta web basada en XML para la elaboración de proyectos docentes universitarios, Álvaro Suárez Sarmiento (director 2001), Proyecto final de Carrera, Universidad de Las Palmas de Gran Canaria, Escuela Universitaria de Ingeniería Técnica de Telecomunicación, 2001.

[11] https://moodle.org, disponible mayo 2013.

[12] Elsa María Macías López, Álvaro Suárez, J. Rodríguez, Herramienta telemática para la planificación temporal de la docencia de asignaturas en el EEES. Jornada de Innovación Educativa en Ingeniería Telemática (JIE 2011), Santander, septiembre 2011.

Herramienta Web para el Seguimiento y Evaluación de los Trabajos Fin de Grado

Davinia Hernández-Leo, Verónica Moreno

USQUID Escuela Superior Politécnica, Universitat Pompeu Fabra
c/Roc Boronat 138 08018, Barcelona

davinia.hernandez@upf.edu , verónica.moreno@upf.edu

***Resumen*— Las peculiaridades académico-formativas del Trabajo Fin de Grado (TFG) requieren del establecimiento de directrices tanto organizativas como pedagógicas que aseguren la adquisición y evaluación de los niveles de logro competenciales propios del grado. Con el objetivo de dar respuesta a esta necesidad, la Escuela Superior Politécnica de la Universidad Pompeu Fabra ha diseñado una Guía para el Seguimiento y Evaluación de los TFGs asociados a los grados que imparte. Esta guía recoge una propuesta orientada a un seguimiento continuo y una evaluación basada en el uso de rúbricas. Este artículo presenta una herramienta Web que facilita el uso de dicha Guía. Además de visualizar su contenido, permite generar rúbricas cumplimentadas y simular calificaciones en función de los niveles de logro de las competencias consideradas. El artículo también describe unos primeros indicadores de uso.**

***Palabras clave*— Trabajo Fin de Grado, rúbricas, evaluación de competencias, herramienta Web**

I. Introducción

La Escuela Superior Politécnica de la Universitat Pompeu Fabra (ESUP) está trabajando desde hace varios años para alcanzar los objetivos y propósitos recogidos, no solo en la LOU [1], sino también en la Declaración de Bolonia [2] así como en ordenaciones oficiales como el BOE núm. 206 [3], etc. Se puede afirmar que las acciones planteadas, implementadas y evaluadas en aras de alcanzar dichos objetivos han seguido un orden cronológico respetando la secuencia natural en la implementación de los nuevos Grados. Es decir, las primeras acciones respondían, generalmente, a elementos que impactan sobre los primeros cursos/fases de adaptación de los planes de estudio (diseño competencial, metodológico y evaluativo) [4-5]. En esta línea, el diseño del Trabajo Fin de Grado (TFG) como asignatura de último curso, ha sido planteado especialmente en el último bienio. Mientras que en la mayoría de las disciplinas el TFG aparece como un gran reto, en las Ingenierías existe experiencia previa con lo que hasta el momento se denominaba Proyecto Fin de Carrera (PFC). Aún así, ha sido preciso revisar substancialmente su diseño para que el TFG tenga un planteamiento explícito basado en competencias [6-7] y evaluado, no solo como producto sino también como proceso.

La ESUP basó su trabajo de diseño del TFG en diferentes referentes y directrices tales como el Marco de Referencia para el Diseño de los Planes de Estudio de Grado, la ordenación de las universidades oficiales recogida en el REAL DECRETO 1393/20071, los Libros Blancos editados por la ANECA [9], el estudio resultante del proyecto *Tuning Educational Structures in Europe* [10], otras recomendaciones provenientes de organismos internacionales [11] y en los marcos académicos más recientes que establecen los requisitos para la verificación de los títulos universitarios oficiales que habilitan para el ejercicio de la profesión [12].

Considerando estas bases sobre las que se fundamenta cada una de las asignaturas de un Grado, incluida el TFG, se observa que es necesario considerar, por lo menos, estos tres elementos: las competencias en sí mismas (tanto específicas como instrumentales), la metodología de trabajo (que favorezca el logro de los objetivos formativos) y por último la evaluación (flexible y rigurosa).

Desde esta perspectiva es indudable la necesidad de diseñar un plan formativo que responda a estas necesidades. Por ello, la ESUP decidió generar una Guía que orientara tanto el Seguimiento como la Evaluación de los TFGs [13] instrumentalmente apoyada en rúbricas. Este recurso fue experimentado en múltiples ocasiones con el objetivo de ir mejorándolo y aproximándolo al máximo a las necesidades de los destinatarios, no solo a nivel de contenido, sino también a nivel de formato del recurso. En esta línea se percibió que era necesario encontrar un formato fácilmente aplicable, amigable en su uso para maximizar su adopción. Para ello, se decidió diseñar y desarrollar una versión Web de la Guía que facilita la aplicación de las rúbricas para el Seguimiento y Evaluación de los TFGs.

Este artículo se centra en presentar dicha herramienta, a la vez que en revisar los aspectos más relevantes de la Guía. Tanto la guía [13], como la herramienta Web (http://www.usquidesup.upf.edu/tfg/index.es.php) resultante está disponible en acceso abierto a toda la comunidad educativa (ESUP, UPF y externamente). Mientras la Guía se ha utilizado en pruebas piloto en cursos anteriores, este curso se está aplicando por primera vez el uso de la herramienta Web. Tanto el profesorado como el estudiantado de la ESUP, pueden acceder a la herramienta tanto para revisar los criterios

de evaluación, y simular (auto-)evaluaciones con rúbricas y cálculo de calificaciones.

El resto del artículo se estructura de la siguiente manera. La Sección II presenta la metodología de trabajo seguida hasta llegar a la herramienta Web. Seguidamente, en la Sección III se presenta el resultado obtenido, es decir, la herramienta y unos primeros indicadores de uso. La Sección IV describe las principales conclusiones del artículo.

II. Motivación y Metodología

La metodología seguida para diseñar la herramienta Web sigue un esquema alineado con las metodologías de desarrollo de software. Para realizar el análisis de los principales requisitos de la Guía, se parte de la propia descripción de la misma, así como de su contexto de uso y necesidades de los usuarios.

A. Contexto de uso

El TFG es un trabajo que realizan los alumnos durante el 4º curso de sus estudios, de forma autónoma y guiados por un director o tutor. En el caso de los planes de estudio de la ESUP, la carga lectiva es de 20 ECTS (Grado en Ingeniería Telemática, Grado en Ingeniería de Sistemas Audiovisuales, Grado en Ingeniería en Informática) o 18 ECTS (Grado en Ingeniería Biomédica). La asignatura no cuenta con clases presenciales, aunque sí se organizan unas sesiones sobre aspectos transversales como el uso de las referencias.

La temática de los TFGs puede ser diversa. Pero, en cualquier caso, debe servir de iniciación a la realización de proyectos en el ámbito profesional como futuros ingenieros, y debe permitirles poner en práctica competencias (transversales y específicas) asociadas al Grado que se está cursando y obtener una valoración integrada de estas competencias.

La estructura de los planes de estudio contempla que el TFG se realice durante todo el curso, pero con una carga diferente según el trimestre. Típicamente se espera más dedicación el último trimestre del curso, pero esto es flexible y puede depender de la casuística concreta del estudiante en función de las asignaturas matriculadas (combinación de optativas elegidas, prácticas en empresa, etc.). De acuerdo con su director, el alumno deberá hacer una planificación temporal del TFG teniendo en cuenta su caso concreto. Al final del curso, el estudiante debe entregar la memoria que recoja el trabajo realizado en el TFG y defenderlo delante de un tribunal.

B. Guía para el Seguimiento y Evaluación de TFGs

La Guía para el Seguimiento y Evaluación de TFGs de la ESUP [12] trata los dos aspectos fundamentales que se indican en el propio título de la Guía.

En cuanto a la temporización, la Guía sugiere que todo TFG debe considerar una fase de inicio y planificación, otra de ejecución o desarrollo y otra de fin. En cada fase se describen tareas típicas que se espera que el alumno realice, poniendo en práctica una serie de competencias que el director evaluará de manera iterativa, ofreciendo retroalimentación al estudiante durante su progreso. Las tareas son orientativas, pudiendo revisarse en función las características y temática de cada TFG. Alineado con los ECTS del TFG, la Guía indica una estimación de horas de dedicación del estudiante por fase. Se trata de una estimación que puede ajustarse según el caso concreto y desgranarse por tareas. En cada fase el alumno deberá entregar a su director al menos un informe de progreso y el director deberá realizar al menos una evaluación formativa de las competencias trabajadas.

La evaluación del TFG tiene dos perspectivas. La primera se refiere al seguimiento y evaluación continua por parte del director. La Guía propone una serie de indicadores asociados a competencias transversales y requiere que profesor y alumno negocien y formulen las competencias específicas que se trabajarán con más énfasis en el TFG. Para cada indicador, se describen cuatro niveles orientativos de logro (rúbricas de evaluación [15]). Para el caso de las competencias específicas los niveles de logro puede definirlos el propio profesor, considerando aspectos como dificultad, aplicabilidad, etc., según el caso. La evaluación continua tiene un peso del 30% en la calificación del TFG.

La segunda perspectiva se trata de la evaluación por parte del tribunal. Como en la evaluación continuada se definen una serie de indicadores y niveles de logro asociados a competencias. Algunos indicadores son similares a los incluidos para el seguimiento, pero otros se refieren a competencias que solo pueden evaluarse en el momento de la defensa del trabajo, como la competencia de comunicación oral. La evaluación por el tribunal tiene un peso del 70% en la calificación del TFG, distribuyéndose ese porcentaje a partes iguales entre las competencias transversales y específicas.

Los apéndices de la Guía listan todas las rúbricas de evaluación asociadas a cada uno de los indicadores.

C. Necesidades de los usuarios

Los usuarios de la Guía son tanto profesores como alumnos. Sus necesidades básicas son poder acceder a la Guía desde cualquier navegador y dispositivo (incluidos dispositivos tipo tabletas o teléfonos móviles). Además de que estos dispositivos son utilizados de manera habitual por ambos actores, el escenario de la presentación del TFG hace especialmente necesario que el tribunal pueda acceder a la Guía desde este tipo de dispositivos.

Por otro lado, las experiencias piloto del uso de la Guía y otras rúbricas en formato documento ponen de manifiesto la necesidad de herramientas que faciliten la aplicación de rúbricas [14] tanto por el tutor, en el seguimiento, y del tribunal, en la evaluación final, como del propio estudiante cuando realice ejercicios de autoevaluación para reflexionar sobre el nivel de logro que va consiguiendo en la realización del trabajo.

D. Requisitos

La descripción de la propia Guía, su contexto de uso y necesidades de sus usuarios llevan a una serie de requisitos funcionales fundamentales que se han tenido en cuenta en el diseño y desarrollo de la herramienta Web de apoyo.

- Acceso la información básica a tener en cuenta en el seguimiento y evaluación de la Guía. Aunque el documento en versión PDF de la Guía está disponible para su consulta, un acceso rápido a la información

esencial agilizará y facilitará el conocimiento de esta información.

- Plantillas para el planteamiento de la temporización descargables. La Guía está disponible en versión PDF, conteniendo una plantilla para la temporización que no puede editarse directamente.
- Consulta ágil de las rúbricas de evaluación. Dado el alto número de indicadores y, por tanto, de descripciones de niveles de logro, las páginas del apéndice de la Guía que contienen las rúbricas son relativamente numerosas.
- Indicación interactiva de niveles de logro en plantillas de seguimiento y evaluación, y descarga de las mismas. Añadido a la problemática de la Guía en versión PDF, las consultas iterativas de rúbricas por indicador para asociar niveles de logro puede resultar incómoda y llevar a errores (asociados a los cambios de página entre plantillas de evaluación y rúbricas en apéndices).
- Cálculo de calificación considerando los porcentajes asociados a cada bloque de competencias (transversales / específicas) y fase del TFG (seguimiento / evaluación final por tribunal).
- Herramienta multilingüe disponible en las tres lenguas de trabajo de la UPF (catalán, castellano, inglés) para respetar la normativa al respecto de la universidad y facilitar el uso plural (Ej., también para estudiantes Erasmus).
- Comunicación con los creadores de la Guía y la herramienta para realizar consultas o proponer mejoras.

E. Proceso de Diseño e Implementación

Como en la propia elaboración de la Guía, en el diseño y desarrollo iterativo de la herramienta han participado tanto los miembros de la USQUID-ESUP, incluyendo una técnica pedagoga, como profesores de los Grados que han participado en sesiones sobre la herramienta y están utilizándola actualmente. El programador de la USQUID encargado de la herramienta se encarga de mantenerla y actualizarla según los aspectos y necesidades que van emergiendo. La tecnologías utilizadas para la implementación de la herramienta son PHP, HTML, CSS y JavaScript. La herramienta incorpora un formulario para que los usuarios (profesores y estudiantes) puedan comunicar de forma sistemática sus comentarios, sugerencias y/o observaciones.

La siguiente sección muestra el resultado actual del diseño e implementación de la herramienta Web para facilitar el uso de la Guía según los requisitos listados en el apartado anterior.

III. Herramienta Web para la Asignatura TFG

La herramienta Web está disponible públicamente en http://usquidesup.upf.edu/tfg. Como se observa en la Fig. 1, la entrada a la herramienta muestra "Información general" sobre la propia herramienta. Incluye un vídeo explicativo que muestra las diferentes opciones y menús para navegar por la Web. En el menú superior izquierdo se puede cambiar el idioma, estando disponible todo el material –incluidas las rúbricas- en las tres lenguas oficiales de la UPF (catalán, español e inglés).

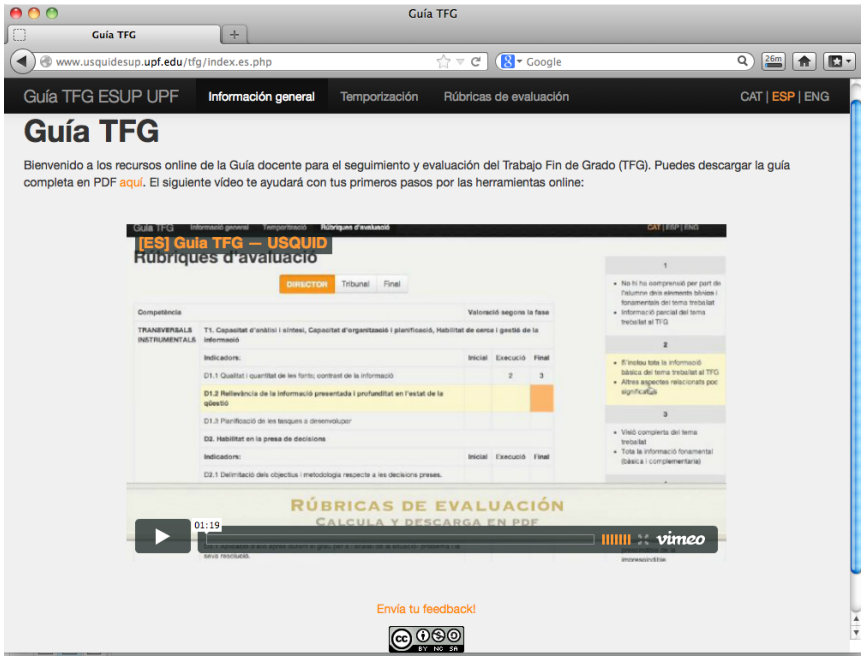


Fig. 1. Entrada a la herramienta Web para el seguimiento y gestión de TFG

El menú "Temporización" permite navegar por las tres fases básicas en las que se propone dividir la planificación global de un TFG. Además de una visión global de la temporización sugerida y la plantilla descargable para que cada tutor-estudiante la adapten a su caso, cada una de las fases incluye las tareas típicas asociadas a la fase. También se listan las competencias que se trabajan en la realización de estas tareas y cuyo desarrollo debe seguirse y evaluarse a lo largo de la fase. La Fig. 2 muestra una captura de la fase de ejecución.

La estructura de la Web permite facilitar información de diferente tipo ubicada alrededor del menú inicial. Por ejemplo, en esta página el usuario puede ver con claridad que se encuentra en la fase de ejecución tanto porque el título así lo

indicada, como por el menú de la izquierda en el que queda destacada la fase que se visualiza en cada momento. Por otro lado, a la derecha, se observa una aproximación a la distribución porcentual de cada una de las fases diseñadas así como una orientación en cuanto a tareas generales y competencias. Se insiste en este aspecto ya que las rúbricas de evaluación están construidas en función de las fases aquí recogidas y contemplando las competencias definidas para cada caso. Tanto la visualización del texto, como del menú superior se auto-adapta en función del dispositivo donde se visualiza la Web (ordenador, tableta, teléfono móvil).

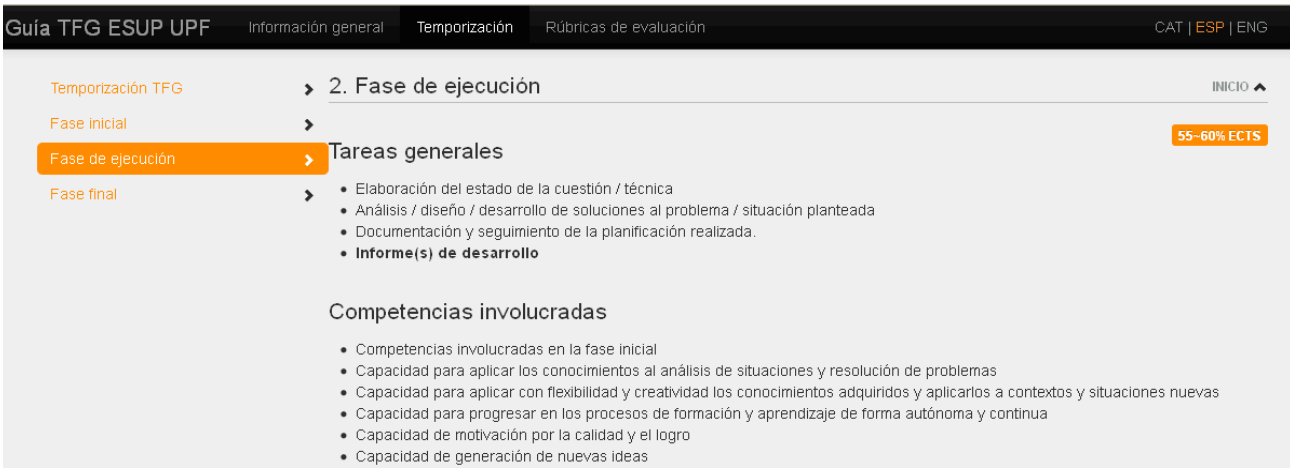


Fig. 2. Descripción propuesta para la fase de ejecución en la Temporización del TFG

El menú "Rúbricas de evaluación" contiene los diferentes indicadores a considerar en función del agente evaluador así como del momento: Director- evaluación del proceso, Tribunal- evaluación final. La Fig. 3 muestra parte de la plantilla de seguimiento por el director y la rúbrica para el seguimiento, mientras que la Fig. 4 muestra lo propio para la evaluación por el tribunal.

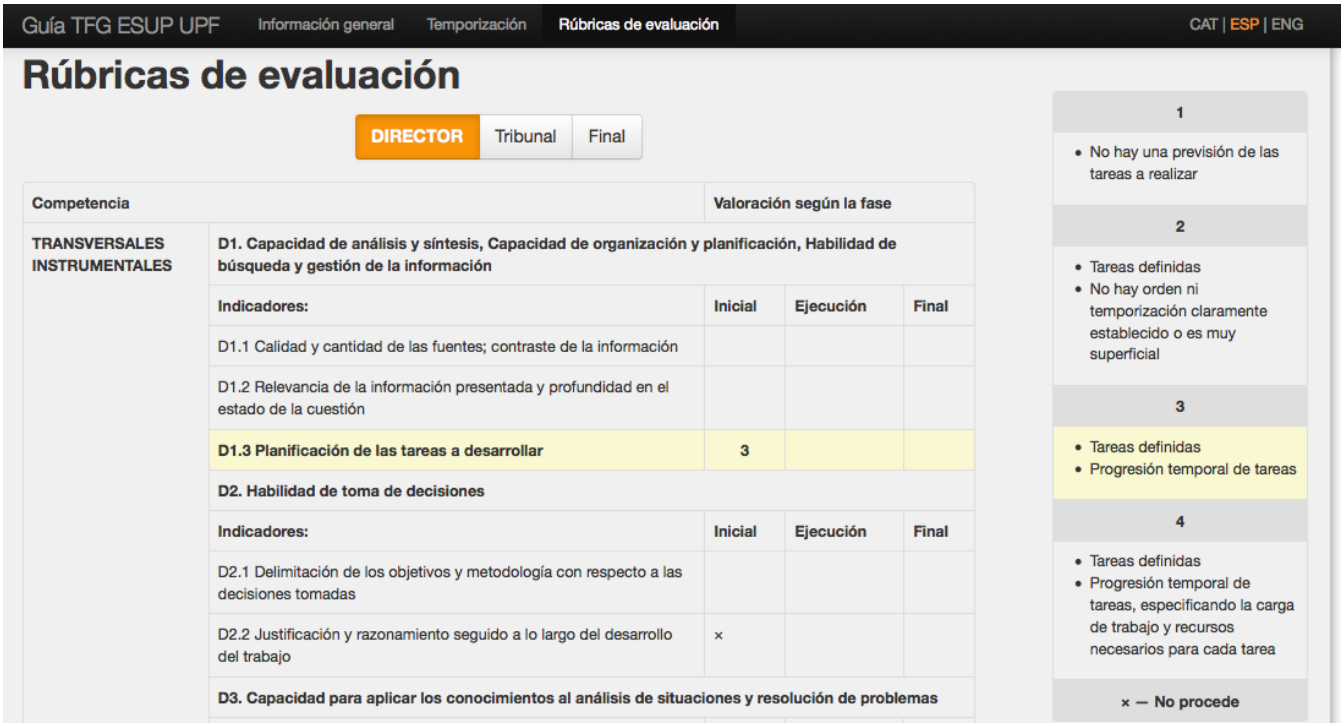


Fig. 3. Plantilla de indicadores (se muestra incompleta) para el seguimiento por el director del TFG. La rúbrica mostrada (a la derecha), con niveles de logro y su descripción, corresponde al indicador "Planificación de las tareas a desarrollar"

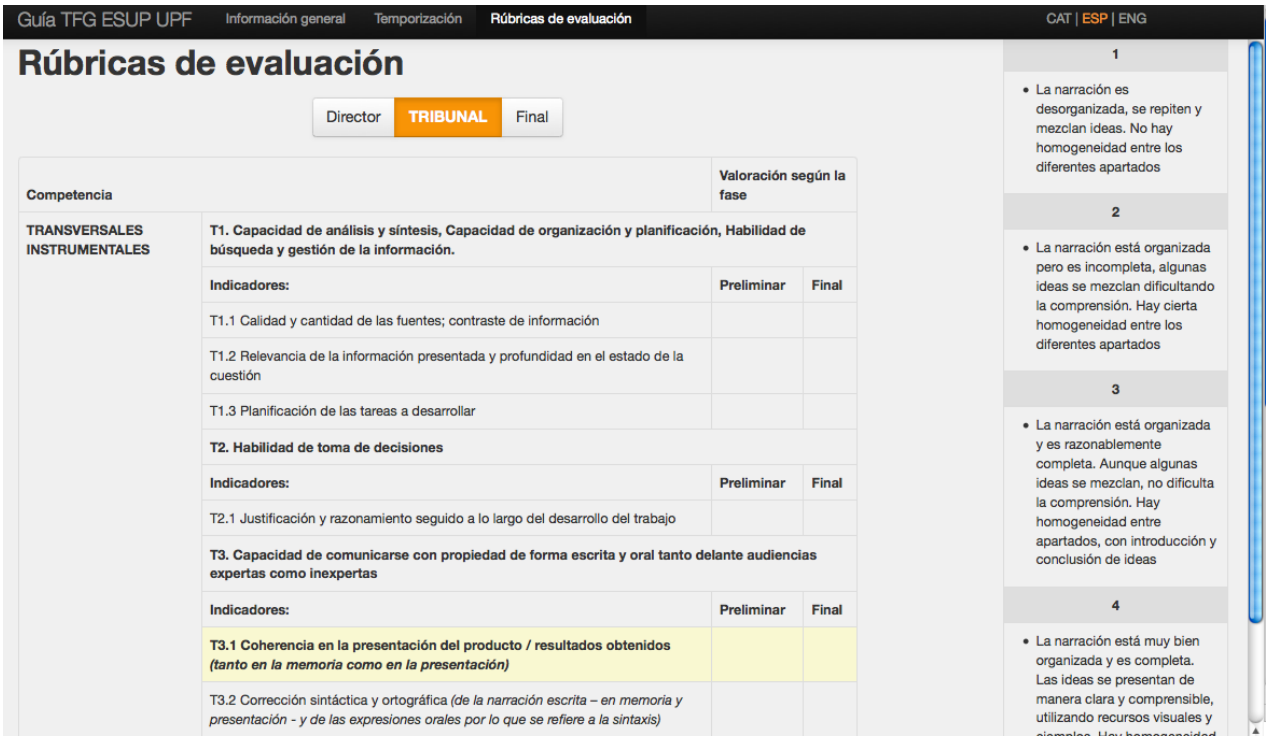


Fig. 4. Plantilla de indicadores (se muestra incompleta) para la evaluación por el tribunal del TFG. La rúbrica mostrada (a la derecha), con niveles de logro y su descripción, corresponde al indicador "Coherencia en la presentación del producto / resultados obtenidos (en memoria y presentación)"

En ambas figuras (3 y 4) se observa la distribución de la información en dos grandes partes, una más sintetizada en la parte central y otra parte más descriptiva que es la que facilita el correcto uso de la rúbrica. Concretamente la parte del centro, la tabla, consta de: en las filas las competencias/ grupos de competencias a evaluar destacadas y enumeradas ordinalmente. En el caso del ejemplo en la Fig. 3 se observa la competencia D1 que se corresponde con el primero de los bloques de competencias formado por: "Capacidad de análisis y síntesis, Capacidad de organización y planificación y Habilidad de búsqueda y gestión de la información". Se observa que este bloque de competencias se desgrana en tres indicadores que siguen la lógica de enumeración de la competencia a la que pertenecen (D1.1, D1.2 y D1.3).

Cuando el Director vaya a evaluar este bloque de competencias, y más concretamente el indicador D1.3 "Planificación de las tareas a desarrollar" destacado en la captura y que pueden seleccionar con un clic, deberá otorgar el nivel de logro que ha alcanzado el estudiante en cada una de las fases programadas (inicial, ejecución y final). Para ello dispone de una barra deslizante a la derecha (que aparece tras seleccionar el indicador) que contiene los descriptores clave para cada uno de los niveles. Seleccionando de nuevo con un clic el nivel que corresponda ese valor aparecerá automáticamente en la tabla de competencias/indicadores (en la Fig. 3 se selecciona el nivel de logro 3). Así, el director, en cada una de las fases podrá ir anotando cuál es nivel de logro alcanzado en el TFG respecto cada uno de los indicadores. El estudiante puede ser consciente también de qué debe hacer para conseguir mejor nivel de logro (ya que puede seguir las indicaciones de los descriptores de la derecha), promoviendo una mayor implicación sobre su propio proceso de aprendizaje así como la autorregulación.

Esta definición de descriptores está hecha para cada uno de los indicadores correspondientes a todas las competencias/ bloques de competencias que se contemplan en las rúbricas (tanto del director como del tribunal). Para responder también a la idiosincrasia de los trabajos existe la posibilidad de que alguno de los indicadores no sean contemplados en la evaluación porque no sea pertinente dada su naturaleza. En ese caso el Director/ Tribunal puede seleccionar la opción "no procede".

Una vez completada la rúbrica se puede obtener una calificación orientativa para los bloques de competencias evaluadas en cada fase. La calificación se calcula automáticamente según se ve en la Fig. 5. La Fig. 5 también muestra que no todos los indicadores proceden en todas las fases de la ejecución del TFG. La tabla de indicadores completada puede descargarse en formato PDF.

Finalmente la Fig. 6 muestra una funcionalidad de la herramienta que permite calcular la calificación final del TFG teniendo en cuenta los pesos propuestos para la evaluación de competencias transversales y específicas en función de los dos agentes (director y tribunal).

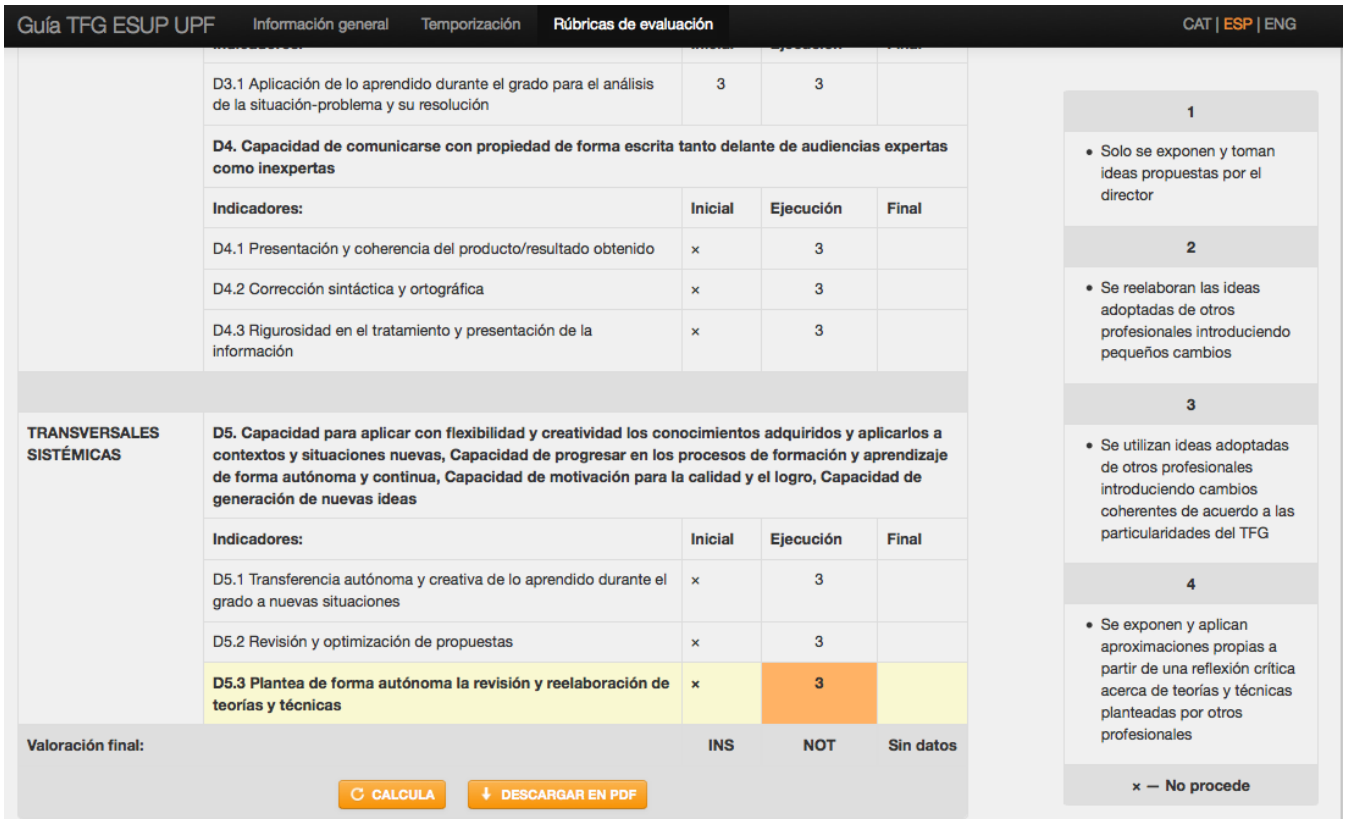


Fig. 5. Cálculo orientativo calificación competencias transversales por fases

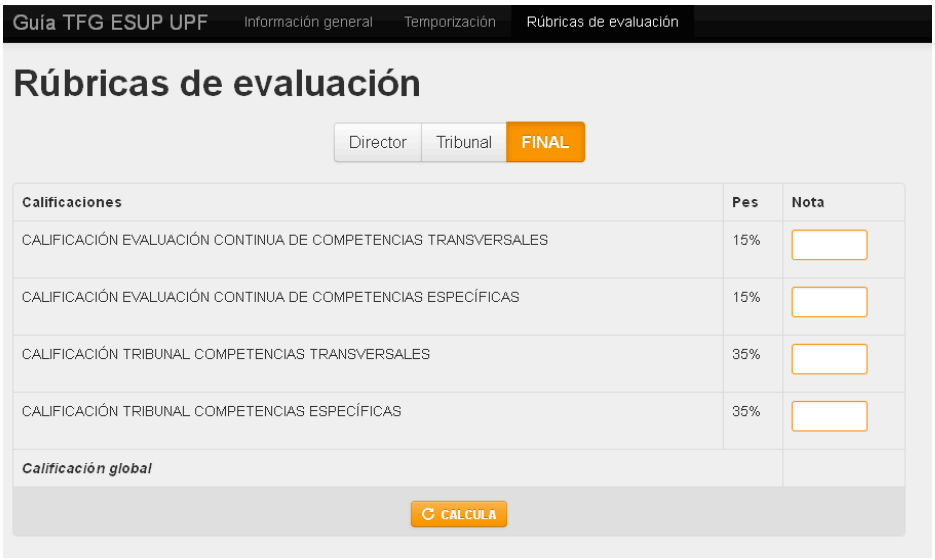


Fig. 6. Cálculo de la calificación del TFG

Como se observa en la Fig. 6 esta funcionalidad contempla la procedencia de las cualificaciones consideradas para el cómputo de la nota final. En la tercera columna es donde se deben poner las notas y, por último, hacer el cálculo final que está también automatizado.

Aunque se ha planificado una evaluación sistemática de la herramienta (que se realizará tras el cierre de los TFGs de este curso académico), las reacciones de los usuarios en las sesiones sobre la herramienta han sido positivas. El profesorado participante coincide en que la herramienta facilita la gestión del proceso de seguimiento y evaluación del TFG, y que la navegabilidad de la Web permite su uso de manera ágil. Por otro lado, hasta el momento, no se han recogido comentarios mediante el cuestionario disponible en la herramienta.

Un aspecto que resultaba especialmente interesante para los responsables del diseño e implantación de esta herramienta era conocer si estaba siendo consultada tanto por profesorado como por estudiantado. Los datos a este respecto se han

extraído usando *Google Analytics*. Lamentablemente no se dispone de datos del acceso a la herramienta desde el comienzo de curso al 15 de febrero de 2013. Desde esta fecha hasta el momento de la escritura de este artículo (mayo 2013), han accedido a la Web 208 usuarios, habiendo un total de 308 visitas y por tanto un 35% de usuarios que acceden a la herramienta en más de una ocasión. El 90% de las visitas se realizan desde España, un 70% del total desde Barcelona. Si se considera que el número de alumnos que están realizando el TFG no supera los 50, se puede interpretar que tanto los estudiantes como sus tutores están utilizando la herramienta o la han utilizado al menos una vez, posiblemente de manera complementaria a la Guía disponible en el repositorio electrónico de la UPF.

IV. Conclusiones

Este artículo ha presentado una herramienta Web que facilita la aplicación de la Guía para el seguimiento y evaluación de los TFGs en los Grados de la ESUP de la UPF. La acogida de la herramienta tanto por parte de la dirección de la Escuela como por parte del profesorado y estudiantado se valora inicialmente como positiva, ya que ha potenciado la propia adopción de la Guía – un reto dado la poca familiarización de los profesores con el uso de rúbricas, etc. A falta de una evaluación completa del uso de la herramienta, las primeras valoraciones indican que se concibe como una herramienta clara y que ayuda a consolidar procesos de planificación y organización del trabajo, motivar una mayor responsabilidad del estudiante sobre su propio proceso de aprendizaje y promover su autorregulación. En cuanto al impacto directo sobre la figura del director/tribunal, se valora la claridad de los indicadores y descriptores de los diferentes niveles de alcance así como la flexibilidad de la herramienta.

Los primeros trabajos se defenderán a finales del curso académico 2012-2013. Para entonces se ha planificado realizar una evaluación en profundidad del uso de la Guía y de la herramienta Web así como de la percepción de estudiantes y profesorado en cuanto a su usabilidad, propuestas de mejora, etc. Sus resultados serán compartidos oportunamente con la comunidad, y las mejoras iterativas de la herramienta continuarán accesibles públicamente.

V. Agradecimientos

Este trabajo ha sido parcialmente financiado por los proyectos E/A2011-0088, PlaQUID2010 y el apoyo directo de la Universitat Pompeu Fabra a las Unidades para el Apoyo a la Calidad e Innovación Docente. Las autoras quieren agraceder las aportaciones de los profesores de la ESUP que han participado en las pruebas pilotos de la Guía, y al becario de la USQUID-ESUP Vicenç Gascó por el trabajo realizado en la implementación de la herramienta Web.

VI. Referencias

[1] Ley Orgánica de la Universidad, consultado el día 10 de mayo de 2013 en: http://www.aneca.es/ANECA/Marco-legislativo

[2] Declaración Bolonia, consultado el documento oficial el día 10 de mayo de 2013 en: http://www.educacion.gob.es/dctm/boloniaeees/documentos/02que/declaracion-bolonia.pdf?documentId=0901e72b8004aa6a

[3] BOE núm. 206, Martes 30 de octubre de 2007.

[4] D. Hernández-Leo, V. Moreno, J. Dodero, A. Pardo, M.C. Romero-Ternero, Y. Dimitriadis, y J.I. Asensio-Pérez, "Aplicación de Recomendaciones para la Alineación de Competencias, Metodología y Evaluación en Asignaturas de Ingeniería Telemática, Informática y Electrónica," *IEEE Revista Iberoamericana de Tecnologías del Aprendizaje*, vol. 7, no.1, pp. 13-20, 2012.

[5] D. Hernández-Leo, E. Peig i Olivé, y V. Moreno Oliver, V. "Marco de evaluación por competencias para asignaturas de grado," *Jornada de la Red Estatal de Docencia Universitaria*, Madrid, 2013, http://repositori.upf.edu/handle/10230/20363

[6] A. Navio, "Propuestas conceptuales en torno a la Competencia Profesional," *Revista de Educación*, no. 337, pp 213-234, 2005.

[7] P. Sánchez, y J. Gairín, *Planificar la formación en el Espacio Europeo de Educación Superior*. Madrid: ICE de la Universidad Complutense de Madrid, 2008.

[8] SENA, *Metodología para la elaboración de normas de competencia laboral*. Dirección de Empleo, Bogotá, 2003.

[9] Libros Blancos, consultados el 10 de mayo de 2013 en: http://www.aneca.es/Documentos-y-publicaciones/Libros-Blancos

[10] Proyecto Tuning, consultado el 10 de mayo de 2013 en: http://www.unideusto.org/tuning/

[11] ACM Curricula Recommendations, consultado el día 20 de mayo de 2013 en: http://www.acm.org/education/curricula-recommendations

[12] Orden CIN/355/2009, de 9 de febrero, por la que se establecen los requisitos para la verificación de los títulos universitarios oficiales que habiliten para el ejercicio de la profesión de Ingeniero de Telecomunicación. Consultado el día 10 de mayo de 2010 en http://www.boe.es/boe/dias/2009/02/20/pdfs/BOE-A-2009-2897.pdf

[13] D. Hernández-Leo, V. Moreno, y I. Camps, *Guía docente para el seguimiento y la evaluación de los Trabajos Final de Grado*. Unidad de Apoyo a la Calidad e Innovación Docente, Escuela Superior Politécnica, Universitat Pompeu Fabra, Barcelona, 2012, http://repositori.upf.edu/handle/10230/20036

[14] D. Hernández-Leo, V. Moreno, y I. Camps, I. (Coords.). *Prácticas Hacia la Excelencia de los Trabajos Fin de Grado. Elaboración de un catálogo de prácticas basadas en el cotejo con el marco nacional e internacional y experimentadas en el campo de la Ingeniería. Análisis de la proyección y transferencia a otros contextos*. Informe final de proyecto E/A2011-0088. Unidad de Apoyo a la Calidad e Innovación Docente, Escuela Superior Politécnica, Universitat Pompeu Fabra, Barcelona, 2012. Disponible en: http://138.4.83.162/mec/ayudas/casaAva.asp

[15] M. S. Ibarra Saiz, G. Rodríguez Gómez, V. B. Álvarez Rojo, F. Aliaga Abad, "Hacia un sistema de evaluación del aprendizaje universitario basado en criterios, normas y procedimientos públicos coherentes", *Actas del XIII Congreso Nacional de Modelos de Investigación Educativa*, San Sebastián, 2007.

Dos casos del uso de rúbricas para la evaluación de Trabajos Fin de Grado

Verónica Moreno[1], Guillermo Carpintero[2], Davinia Hernández-Leo[3]

[1,3]Escuela Superior Politécnica, Universitat Pompeu Fabra
c/Roc Boronat 138 08018 Barcelona, España
[2]Escuela Politécnica Superior, Universidad Carlos III de Madrid
Av. Universidad 30, 28911-Leganés, Madrid
{veronica.moreno, davinia.hernandez;}@upf.edu, {guiller}@ing.uc3m.es

***Resumen*— Este artículo recoge la experiencia piloto llevada a cabo en los estudios de ingeniería de la Escuela Politécnica Superior de la Universidad Carlos III de Madrid (EPS) y la Escuela Superior Politécnica de la Universitat Pompeu Fabra (ESUP) sobre el diseño de un sistema de organización, gestión y evaluación de los Trabajos Fin de Grado (TFG) mediante el uso de rúbricas. Se enfatiza en el acompañamiento durante el desarrollo del trabajo del así como en la evaluación del producto final (memoria) y su presentación y defensa. La ESP basó sus rúbricas en las recomendaciones de la *Accreditation Board for Engineering and Technology* (ABET), mientras que la ESUP elaboró las susyas considerando trabajos previos relacionados. Así, el objetivo del artículo es presentar ambos modelos destacando diferencias, similitudes, fortalezas y debilidades y ofrecer propuestas de optimización a partir de la experiencia de ambas Escuelas.**

Palabras claves— **rúbricas, evaluación de competencias, trabajo fin de grado, estandarización, seguimiento**.

I. INTRODUCCIÓN

Como parte del trabajo realizado y acciones enfocadas a la inmersión de la educación superior en el Espacio Europeo de Educación, tanto la Escuela Politécnica Superior de la Universidad Carlos III de Madrid (a partir de ahora EPS) como la Escuela Superior Politécnica de la Universitat Pompeu Fabra - Barcelona (a partir de hora ESUP) han diseñado, desarrollado y evaluado un proceso académico-formativo enfocado a la medición de competencias adquiridas por el alumno [1]. Para esta experiencia se ha tomado como objetivo la asignatura de Trabajo Final de Grado (TFG), la cual se desarrolla en el último curso de los estudios de Grado diseñada para establecer un escenario formativo en el que el estudiante pueda integrar las competencias adquiridas a lo largo de los estudios. Ello la convierte en la asignatura ideal para medir las competencias adquiridas por el alumno a lo largo de sus estudios antes de insertarse en el mercado laboral.

Dado que es una asignatura común en todos los planes de estudio de ingeniería, aparece como reto fundamental el diseño de una herramienta de evaluación de competencias que tenga en cuenta tanto la temática específica de cada caso (ya que el contenido cambiará en función del TFG y por tanto adaptando también las competencias específicas a cada caso) como las competencias transversales (o generales), que las empresas están demandando en los recién graduados (por ejemplo, capacidad de síntesis o capacidad de comunicación oral). En esta asignatura el profesor adopta un rol claramente de orientador/acompañante dado que el número de horas de trabajo dirigido –fuera del aula- es significativo. Así, el TFG aparece como una asignatura en la que la evaluación, tanto de competencias específicas como sobre todo de transversales, es especialmente significativa. Además de todo lo anterior, actualmente se requiere explícitamente que el estudiante demuestre un mayor nivel competencial en las asignaturas de últimos cursos que en las asignaturas previas, concretamente, un nivel equivalente a las expectativas correspondientes a los indicadores de Dublín para el primer ciclo [2].

Por todo ello, el TFG es una asignatura particularmente exigente con su diseño, gestión y evaluación, ya que requiere de un esfuerzo, si cabe mayor, que el resto de asignaturas. En esta línea cabe destacar que en el TFG el estudiante asume un rol significativamente más activo y responsable. Considerando estas características del TFG, la opción tomada tanto por la ESP como por la ESUP fue recurrir al uso de rúbricas como instrumento de seguimiento y evaluación de los TFG. Las rúbricas permiten la formulación de un conjunto de criterios graduados; su uso como herramienta y recurso para la evaluación (y autoevaluación personal) resulta especialmente interesante para el desarrollo de un proceso integral y formativo [3].

Como se verá en las secciones siguientes, la EPS optó por el diseño de unas rúbricas para medir algunas de las competencias –*Student Outcomes*– establecidas por el *Accreditation Board of Engineering and Technology* (ABET) [4] para los estudios de ingeniería. Los *Student Outcomes* son once competencias, conocidas como las (a) a (k), que los estudiantes deben adquirir durante sus estudios. En el caso concreto del TFG, se miden los *Student Outcomes* (e) habilidad para identificar, formular y resolver problemas propios del ámbito de la ingeniería, (g) la habilidad para comunicarse de manera efectiva, y (k) la habilidad para usar las técnicas y herramientas de ingeniería necesarias en la práctica profesional. El hecho de utilizar estos *Student Outcomes* se basó en que ninguna otra asignatura del programa de estudios era capaz de evaluar al final de la carrera estas competencias. Por otra parte, el TFG resulta idóneo para el uso de estos *Students Outcomes* dado que el alumno debe resolver y documentar un problema de ingeniería. A partir de los *Student Outcomes* que se desea medir, se diseñaron diversas secciones en las rúbricas referentes tanto a la

memoria, como a la presentación del trabajo y al esfuerzo individual realizado por cada estudiante.

En el caso de la ESUP y como se ha presentado en el resumen, se diseñaron rúbricas fundamentalmente a partir del trabajo de Valderrama [5-8] separadas en función del agente evaluador (tutor y tribunal) dado que las del primero contienen criterios relacionados con el proceso de realización del trabajo que el tribunal no puede evaluar (porque no son competencias demostrables en la presentación/ defensa del trabajo). Del mismo modo, la rúbrica del tribunal contenía competencias evaluables sólo en la acción (entendiendo esta como presentación y defensa del proyecto).

En ambos casos (EPS y ESUP) las rúbricas recogen indicadores y criterios referentes a competencias transversales, que computan sobre la nota final de manera ponderada, en el primer caso en función de los criterios, en el segundo del agente. Los detalles se muestran en la Sección II: Objetivos y Metodologías de Trabajo, en la que se definen tanto los objetivos como las acciones clave llevadas a cabo, haciendo un especial apunte a las similitudes y diferencias entre ambos modelos para destacar las fortalezas y debilidades de cada caso. En la Sección III se muestran los Resultados obtenidos en los respectivos pilotajes con las rúbricas, y finalmente las conclusiones y elementos de discusión.

II. Objetivo y metodología de trabajo

Como se vislumbra de lo explicado a lo largo de la sección introductoria, el objetivo de ambas experiencias (ESP y ESUP) era diseñar un instrumento que permitiera sistematizar tanto el proceso de seguimiento como el de evaluación de las competencias adquiridas por el alumnos en los TFG mediante el establecimiento de criterios claros y rigurosos que fueran comunes a todos los trabajos a la vez que se respetara la idiosincrasia de cada uno de ellos. Es importante señalar, que en el Real Decreto 1393/2007, de 29 de octubre, en el que se establece la ordenación de las enseñanzas universitarias oficiales, se indica que los estudios de Grado deberán incluir un trabajo de fin de Grado (de entre 6 y 30 créditos) en la fase final del plan de estudios y que debe estar orientado a la evaluación de competencias asociadas al título.

En este punto cabe recordar que los planes de estudio de la mayoría de carreras del ámbito de la ingeniería recogían la realización del Proyecto Fin de Carrera (PFC). El PFC puede ser considerado como la asignatura en la que se plasmaba con mayor claridad la calidad y excelencia del nivel competencial de los egresados siendo así un inmejorable escenario en el que los estudiantes podían dedicar una carga de trabajo considerable para realizar un proyecto razonablemente completo.

Dicho esto, recordamos que el objetivo de este artículo es comparar diferentes medios para sistematizar el desarrollo, y sobre todo la evaluación de los TFGs, construyendo sobre lo aprendido en los anteriores PFCs. Para ello se aplican nuevas estratégicas pedagógicas más coherentes con la formación basada en competencias que rige hoy el sistema universitario español bajo el paraguas del Espacio Europeo de Educación Superior (EEES), elemento, ya recogido en trabajos previos [9] que ponen sobre la mesa distintos modelos adoptados por diferentes universidades de la geografía española.

Teniendo claro el objetivo general veamos en la Tabla I las características básicas del TFG tanto en la EPS como en la ESUP, dado que en algunos aspectos pueden resultar condicionantes de las acciones posteriormente experimentadas.

Tabla I
Características básicas del TFG en la ESP y la ESUP: Implicaciones

	TFG de la ESP	**TFG de la ESUP**
Competencias trabajadas	- Específicas: definidas en función cada TFG - Transversales (3) siguiendo los estándares ABET	- Específicas: definidas en función cada TFG - Transversales instrumentales (hasta un total de 6) y sistémicas (hasta un total de 4)
Temáticas/ Tópicos del TFG y otras características	- Diversidad de contenidos en función del TFG. - Trabajo obligatorio a desarrollar en el último curso del Grado. - Implica una carga crediticia de 12 ECTS - Ponderación sobre la nota final en función de la competencia.	- Diversidad de contenidos en función del TFG, se exige al estudiante un grado de responsabilidad en cuanto a su planificación y desarrollo significativamente superior que en el resto de asignaturas. - Trabajo obligatorio a desarrollar en el último curso del Grado. - Implica una carga crediticia de 20 ECTS. - Ponderación sobre la nota final en función de la competencia/ agente evaluador.
Agentes implicados en la evaluación	Tutor y Tribunal	Tutor y Tribunal

Como se observa en la Tabla I hay múltiples elementos que resultan comunes en ambas Escuelas, posiblemente por tratarse de elementos que se heredan del hasta ahora PFC, tradicional en estos estudios y que ha permitido rescatar algunas buenas prácticas y/o elementos para transferirlos a los TFGs. Algunos aspectos, como es el caso de la obligatoriedad resultan comunes a todos los estudios de grado. A nivel de implicaciones directas sobre las rúbricas en función de los tres elementos clave destacados en la primera columna, se destaca lo siguiente: se requiere de la consideración de criterios de evaluación diferenciados en función de la competencia y agente a evaluar/evaluador. Del mismo modo requiere que la formulación de los indicadores, criterios así como la definición de los diferentes niveles de logro sea clara, rigurosa y unívoca.

Sobre este particular resalta el indudable papel del estudiante como agente activo, responsable y gestor de su propio trabajo (contemplando no sólo el producto final sino también el proceso) y el rol del tutor que aparece más como orientador, mediador.

A. Diseño de las rúbricas de evaluación: criterios y niveles de logro

En lo previamente presentado se ha nombrado ya el concepto de rúbrica como instrumento de evaluación, pero, ¿qué sabemos de ellas?, ¿por qué confiamos en la rúbrica como instrumento riguroso?

Entre la literatura existente sobre este particular recogemos la definición de Zazueta y Herrera, [10] que definen las rúbricas como aquellos instrumentos que facilitan la calificación del desempeño del estudiante en aquellas tareas/ áreas curriculares que resultan complejas y/o imprecisas. Así, este proceso es llevado a cabo mediante el uso de un conjunto de criterios graduados que permiten valorar tanto el proceso de aprendizaje como los conocimientos y/o competencias alcanzadas por el estudiante. Fundamentalmente, una rúbrica es un medio para establecer de forma explícita cuáles son las expectativas que el evaluador tiene sobre el trabajo del estudiante de cara a su evaluación.

De esta forma, y al presentarse las rúbricas al estudiante desde el primer momento, se promueve que este, consciente de lo que se espera de él, pueda sistematizar su propio trabajo potenciando la asunción de la responsabilidad sobre su proceso de aprendizaje. Del mismo modo cabe destacar que el estudiante, sabiendo los diferentes niveles de logro de cada competencia a evaluar, pueda autoevaluarse y regular su dedicación y/o esfuerzo en aras a mejorar sus puntos más débiles y consolidar sus potencialidades. Cuando además, los resultados de la evaluación con el instrumento se comunican a los alumnos tras la evaluación, establecen una retroalimentación (*feedback*) al alumno para que sea consciente del nivel que ha alcanzado y cuáles son las competencias que debe desarrollar [11].

La creación de una rúbrica exige desarrollar sus tres elementos: dimensión, escala y descriptores, mostradas en la Fig. 1. La dimensión está relacionada con las competencias que la rúbrica va a evaluar, a través de los criterios que van a ser evaluados. La escala, muestra los diferentes niveles de logro utilizados para medir el nivel de adquisición de las competencias, y finalmente los descriptores, que describen lo más claramente posible qué significa la consecución de cada uno de los niveles de la escala. Este instrumento fomenta un ejercicio de reflexión por parte de los agentes evaluadores contemplando la perspectiva docente y discente, ya que estos pasan a ser conocedores de lo que se espera de ellos en cada uno de los indicadores definidos en las rúbricas.

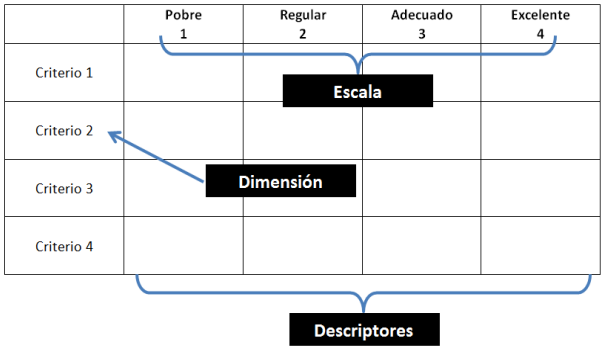


Figura 1: Elementos de una rúbrica

Una vez realizada esta breve definición de la concepción de las rúbricas como instrumento de evaluación, se procede a detallar qué uso se ha hecho de ellas en los casos que aquí se analizan y que corresponden a ESP y la ESUP. Como se recoge en la Tabla I, hay rúbricas diferenciadas para tutor y tribunal. Esto se debe a que la competencia a evaluar, o mejor dicho, el indicador de la competencia es o no observable en el proceso, en la memoria y/o en la defensa, por tanto, es o no visible para el tutor y/o el tribunal. Seguidamente se describe cómo se definen dichos indicadores así como los descriptores correspondientes a cada uno de los niveles de logro asociados, para ello tomaremos como ejemplo una de las competencias consideradas en las rúbricas de la ESP y de la ESUP respectivamente.

Recordemos que la ESP basó sus criterios en los estándares de *Student Outcomes* ABET, y se ciñeron en lo que respecta a la habilidad (e) identificar, formular y resolver problemas propios del ámbito de la ingeniería, (g) la habilidad para comunicarse de manera efectiva, y la (k) habilidad para usar las técnicas y herramientas de ingeniería necesarias en la práctica profesional. Una vez decididas las competencias a considerar se definieron una serie de criterios bajo los que evaluar cada una de las competencias. Como ejemplo, para evaluar la competencia (g), se establecieron varias dimensiones en la rúbrica (ver Fig. 1), que contemplaban tanto aspectos de la memoria presentada indicando que la memoria es evaluada a través de su organización y presentación, la manera en cómo se plantea el problema, la contribución y el presupuesto. Por otro lado, para esta competencia también se evalúan criterios concernientes a la presentación, evaluando el conocimiento demostrado por el estudiante respecto la temática de su trabajo durante la misma, así como la presentación y el tono de la exposición. La escala para medir

el nivel de logro de cada caso va de 1 a 4, siendo 1 el mínimo valor y 4 el máximo.

Para la obtención de la nota final se pondera la puntuación dada a cada criterio considerando que la memoria computa hasta un total de 4,4 puntos, la presentación hasta 2,8 y la contribución y esfuerzo de cada estudiante hasta el 2,8 restante, existiendo para esta última parte un informe que realiza cada director centrado en aspectos fundamentalmente relacionados con el proceso y progreso del estudiante. A continuación se muestra un ejemplo de la rúbrica diseñada en la ESP, concretamente este caso hace referencia a la **exposición oral** (Tabla II, reproducida según el formato común de las rúbricas). La evaluación de la exposición oral se complementa con indicadores adicionales relativos a la presentación de la solución y la defensa del trabajo. La rúbrica para la evaluación se encuentra publicada en la intranet de la EPS, de forma que los alumnos pueden acceder a este instrumento en cualquier momento para consultar los criterios y descriptores. Asimismo, pueden solicitar la rúbrica de su examen tras la evaluación.

Tabla II
SÍNTESIS DE LA RÚBRICA UTILIZADA POR LA ESP PARA LA EVALUACIÓN DE LA EXPOSICIÓN ORAL

1	2	3	4
La exposición se realiza con saltos bruscos entre trasparencias y pérdida del hilo de la misma. El volumen de voz empleado es muy bajo para ser percibido con claridad	El alumno sigue el hilo conductor de las transparencias pero presentando literalmente su contenido. El volumen de voz empleado en la exposición es adecuado	El alumno sigue el hilo conductor de las transparencias sin necesidad de recurrir a su lectura literal y dirigiéndose hacia el tribunal. El volumen de voz empleado en la exposición es adecuado	El alumno realiza una presentación con seguridad, dirigiéndose hacia el tribunal, manteniendo su atención y manejando las transparencias o cualquier otro medio con soltura

En cuanto al diseño de las rúbricas de la ESUP, como se mostraba en la Tabla I se consideraron un total de 10 competencias que fueron agrupadas en bloques para facilitar su evaluación y delimitación de criterios alcanzando un total de 5 bloques de competencias, 4 de ellos referentes a competencias instrumentales y 1 a sistémicas. La escala para medir el logro de cada uno de los criterios sigue la misma lógica que la propuesta por la ESP pero incluye un elemento diferenciador y es la periodicidad de la evaluación, es decir, que en el caso de la ESUP se evalúa cada indicador, como mínimo, tres veces por parte del tutor y dos por parte del tribunal, una de ellas en la entrega del borrador (unas semanas antes de la defensa) y la otra el día de la propia defensa. Así el trabajo es revisado en múltiples ocasiones y el estudiante recibe *feedback* concreto en cada caso para poder tener elementos claros que le ayuden a mejorar su trabajo.

Por otro lado, igual que en el caso de la ESP, la ESUP no tiene definidas rúbricas para las competencias específicas ya que la especificidad e idiosincrasia de cada trabajo no permite esta tarea (o no dando como fruto unos criterios aplicables de manera generalizada). Sí contempla su evaluación con el conjunto de las competencias transversales recogidas en las rúbricas y por tanto, en el cómputo de la nota final del TFG. Concretamente, para la ponderación se consideran los elementos agente y tipología de las competencias. Tanto la calificación correspondiente a la evaluación continuada de competencias transversales como específicas computan cada una un 15% sobre la nota final y la calificación del tribunal tanto en lo referente a las competencias transversales como a las específicas computan un 35%. Veamos ahora un ejemplo de las rúbricas diseñadas en la ESUP. Para seguir la lógica del ejemplo de la ESP, se presenta la rúbrica que corresponde a la evaluación de la competencia: Capacidad de comunicarse con propiedad de forma oral y escrita tanto delante de audiencias expertas como inexpertas. Esta competencia se divide en cuatro indicadores: la coherencia en la presentación del producto/ resultados obtenidos, corrección sintética y ortográfica y rigurosidad en el tratamiento y presentación de la información (los tres referentes tanto a la memoria escrita como a la presentación en sí) y un cuarto indicador que es el lenguaje no verbal, tono de la voz, cadencia y pronunciación. La Tabla III recoge una síntesis de la rúbrica utilizada por la ESUP para evaluar la **coherencia en la presentación**.

Tabla III
SÍNTESIS DE LA RÚBRICA UTILIZADA POR LA ESUP PARA LA EVALUACIÓN CORRESPONDIENTE A LA COHERENCIA EN LA PRESENTACIÓN

1	2	3	4
La narración es desorganizada, se repiten y mezclan ideas. No hay homogeneidad entre los diferentes apartados	La narración está organizada pero es incompleta, algunas ideas se mezclan dificultando la comprensión. Hay cierta homogeneidad entre los diferentes apartados	La narración está organizada y es razonablemente completa. Aunque algunas ideas se mezclan, no dificulta la comprensión. Hay homogeneidad entre apartados, con introducción y conclusión de ideas	La narración está muy bien organizada y es completa. Las ideas se presentan de manera clara y comprensible, utilizando recursos visuales y ejemplos. Hay homogeneidad entre apartados, con una buena introducción y conclusión de ideas

Se han seleccionado estos dos ejemplos porque la esencia competencial es la misma, es decir, que en ambos casos la competencia, de naturaleza transversal, hace referencia a la habilidad del estudiante para presentar su trabajo de manera coherente y respetando los elementos comunicativos básicos.

En el siguiente apartado se describe el proceso de experimentación llevado a cabo en ambas escuelas discerniendo las similitudes y diferencias.

B. Experimentación

Los primeros TFGs no serán presentados hasta finales del curso académico 2012-2013, es por ello que las pruebas piloto se han realizado en los tribunales de los hasta ahora PFCs y no como instrumento exclusivo para realizar la evaluación, es

decir, que se han facilitado como herramienta de soporte tanto a directores como tribunal con el objetivo, básicamente, de recoger su feedback en clave de retroacción y satisfacción respecto a futuro uso de la rúbrica. En lo que supone este proceso de implementación experimental de las rúbricas existen algunas diferencias que cabe considerar. En la Tabla IV se sintetizan algunos de los elementos más significativos a este respecto.

Tabla IV
ELEMENTOS CLAVE EN CUANTO A LA RECOGIDA DE INFORMACIÓN DURANTE LA EXPERIMENTACIÓN.

Elementos	TFG de la ESP	TFG de la ESUP
Número de registros	34 estudiantes 34 tribunales	19 estudiantes 15 profesores/ rol miembros de tribunal
Recogida de datos	- Las rúbricas se diseñan en función del objeto de evaluación (memoria y presentación). - La evaluación de las rúbricas se realiza mediante el uso de cuestionarios diseñados en función del destinatario (profesor y alumno)	- Las rúbricas se diseñan en función del agente evaluador ergo del momento de evaluación (tutor- evaluación continuada y director evaluación final). - La evaluación de las rúbricas se realiza mediante el uso de cuestionarios diseñados en función del destinatario (director/tribunal y alumno). - Realización de diversas pruebas piloto para recoger evidencias [12]
Formación	- Las rúbricas se desarrollaron inicialmente por el Subdirector de Desarrollo Académico - Se realizaron varias sesiones informativas, a alumnos, a personal de administración y servicios, y a los directores de departamento - Se incluyó una encuesta para recoger información de evaluación del instrumento - Toda la información se presentó en la intranet de la universidad para gestión de los PFC y TFG	- Se realizaron reuniones de presentación de la Guía elaborada para el seguimiento y evaluación de los TFGs [13] - Difusión de la Guía generada (incluyendo las rúbricas) mediante el repositorio digital institucional - Generación de una Web para el seguimiento y evaluación de los TFGs [14]

En el caso de la EPS, el proceso de experimentación ha sido realizado en todas las titulaciones de ingeniería, tanto superiores (Ingeniería de Telecomunicación, Ingeniería Industrial e Informática) como en titulaciones técnicas. El proceso se ha llevado a cabo desde la Dirección de la EPS, y el proceso de implantación ha culminado con su uso generalizado a nivel institucional en la EPS tanto para PFC como para TFG. Los objetivos a conseguir han sido:

- Clarificar a los alumnos el criterio con el que van a ser evaluados de antemano.
- Homogeneizar el proceso de evaluación.
- Medir el grado de adquisición de competencias, para proporcionar información a la institución.

C. Evaluación de la experiencia

Una vez llevada a cabo la experiencia piloto de uso de las rúbricas para la evaluación de los TFGs en los estudios de Ingeniería de la ESP y la ESUP se procedió a evaluar su impacto, siendo agentes informantes tanto el profesorado (director y tribunal) como el estudiantado participante. El objetivo era conocer cuál era la percepción de unos y otros en cuanto a la claridad de las rúbricas, su percepción de usabilidad así como el efecto que percibían podía tener sobre la mejora en el proceso de aprendizaje de los estudiantes. Sin embargo existen elementos específicos para cada caso, por ejemplo: en el caso de la ESP, se perseguía también conseguir informaciones que permitieran optimizar la rúbrica y poder institucionalizar su uso más allá de una prueba piloto (la ESUP realizó este tipo de pilotaje en una fase anterior). También se observan algunas diferencias en los criterios evaluados, veamos el detalle a continuación:

- La ESP centra la evaluación en cuestiones como la necesidad de consensuar la ponderación de la evaluación propuesta con la rúbrica, es decir, el peso concedido al rol del tribunal vs. tutor así como a cada una de las partes del trabajo explícitamente evaluadas con las rúbricas. Por otro lado, se solicita que se destaquen potencialidades y debilidades (tanto a profesorado como a estudiantes).
- En cuanto a la evaluación realizada por la ESUP destaca, en primer lugar, que fue realizada tanto desde la perspectiva del estudiante como del tutor/tribunal. En el primer caso, los indicadores más relevantes hacían referencia a la valoración que otorgaban a la necesidad de pautar el seguimiento del trabajo y a la importancia de conocer los criterios de evaluación desde el primer momento. En cuanto a la valoración por parte del tutor/tribunal destacar como indicadores clave la percepción de necesidad de pautar el seguimiento del TFG, la utilidad de tener una herramienta que sistematice tanto dicho proceso como la evaluación final y por último se les preguntaba sobre la claridad de las rúbricas (tanto en lo que refiere a la descripción de competencias como a los niveles de logro).

III. RESULTADOS OBTENIDOS

Este tercer bloque recoge los resultados obtenidos a partir de la experimentación detallada anteriormente y mediante la aplicación de los cuestionarios diseñados con ese fin.

Para facilitar la comprensión de ambos se presentan, mediante el uso de tablas/puntos los datos más significativos tanto para el caso de la ESP como de la ESUP. En la Tabla V, se recogen los resultados de la evaluación con respecto a la rúbrica de la EPS.

Tabla V
RESULTADOS DE EVALUACIÓN RESPECTO LA RÚBRICA DE LA EPS

Tribunal	
La rúbrica hace hincapié en aspectos que ya cuidaba con los PFC que he dirigido	4,29/5
La rúbrica puede expresar los elementos de juicio que he utilizado hasta ahora como evaluador de PFC	3,69/5
Estudiantado	
La rúbrica expresa los elementos de juicio que entiendo se han venido utilizando hasta ahora	3,71/5

En la EPS los resultados obtenidos han permitido evaluar diferentes aspectos de la herramienta, tanto a partir de los resultados de la herramienta en sí como a partir de la encuesta de evaluación adjuntada.

Uno de los aspectos que interesaba analizar era el consenso sobre los diferentes criterios establecidos en la rúbrica. Por este motivo se incluyeron en la propia rúbricas, cuestiones a este respecto, tanto para recoger la opinión de los profesores como la de los alumnos. Las respuestas presentadas en la Tabla V sugieren que tanto unos como otros reconocen que los criterios que se han propuesto coinciden con los que se han venido utilizando, de forma tácita, para la evaluación de los PFC. Como ventaja, los alumnos indican que los niveles de consecución de los criterios les permiten tener información sobre lo que se espera de ellos en la evaluación.

Más interesante resulta la coincidencia entre profesores y alumnos respecto a la ponderación que proponen para cada uno de los criterios de cara a establecer una nota de evaluación (datos recogidos en la Tabla VI). La mayor diferencia entre los criterios se produce en el criterio del presupuesto del proyecto. Este es un criterio muy controvertido entre el profesorado, habiendo quienes lo consideran fundamental y otros recomiendan eliminarlo de la evaluación.

Tabla VI
VALORACIÓN DE PROFESORADO Y ESTUDIANTADO CON RESPECTO A LA PROPUESTAS DE PONDERACIÓN DE LOS CRITERIOS DE LA RÚBRICA DE LA EPS

	Tribunal	**Estudiantado**
Criterios Memoria		
Organización / Presentación	1,84	1,67
Planteamiento del problema	1,90	1,70
Contribución	1,62	0,70
Presupuesto	0,65	1,80
Criterios Presentación		
Conocimiento	1,65	1,80
Presentación del tema	1,34	1,40
Tono de la exposición	1,00	0,95
PUNTUACION TOTAL	**10,00**	**10,00**

En cuanto a los resultados más significativos extraídos de la evaluación llevada a cabo por la ESUP destacan, desde la perspectiva del estudiante, el valor otorgado al trabajo realizado durante el desarrollo del TFG, es decir, el valor que otorgan a la necesidad de considerar el proceso en el cómputo de la nota final. En este caso, la media obtenida es de 4,53/5.

El hecho de conocer los criterios de evaluación es, desde la perspectiva del estudiantado, considerablemente importante, alcanzando su valoración una media de 3,74/5.

En lo que respecta a las valoraciones por parte de los directores/tribunal, destacan los siguientes elementos:

- Se percibe necesario el establecer un sistema de trabajo continuo asegurando el trabajo constante del estudiante.
- Otro elemento que se contempla como punto fuerte es la percepción del profesorado (rol tutor y tribunal) en cuanto a la facilidad del uso de la rúbrica, siendo explícita la claridad de las rúbricas, tanto en lo que respecta a la definición de las competencias como de los niveles de logro.
- Por último destacar que existe total acuerdo con el hecho que, el usar este tipo de instrumento, reduce la subjetividad en el proceso de evaluación. Es decir, que las rúbricas, al tener definido, no sólo el objeto (indicador) sino también los niveles de logro, permiten realizar este proceso con mayor rigurosidad.

Como se observa, tanto en la evaluación llevada a cabo por la ESP como en la ESUP, existe consenso en cuanto al valor que se le da al uso de este tipo de herramientas para sistematizar tanto el proceso como la evaluación final del TFG. Por otro lado aparecen también elementos para la reflexión y trabajo futuro que han permitido optimizar las herramientas y procesos enmarcados en la iniciativa descrita. Es en la siguiente sección en la que se concluye y se presentan dichos elementos.

IV. CONCLUSIONES Y ELEMENTOS DE DISCUSIÓN

Este trabajo presenta la experimentación llevada a cabo en la ESP y la ESUP en el marco del seguimiento y evaluación de los Trabajos Fin de Grado, concretamente en estudios de Ingeniería. El esfuerzo realizado tanto en la ESP como en la ESUP se ha centrado en el diseño de una herramienta que sistematice tanto el seguimiento como la evaluación de los TFGs. Posteriormente y gracias a la colaboración de los colectivos implicados (profesorado y estudiantado) se han realizado diversos pilotajes que han permitido la revisión de la herramienta hasta llegar a su versión final. Es esta versión de las rúbricas la que se está aplicando con la primera generación de TFGs.

A falta de una evaluación completa del uso de las rúbricas en el escenario real del TFG (recordemos que la experimentación se llevó a cabo con PFCs), las primeras evidencias recogidas son, tal y como se muestra en los resultados, alentadoras en tanto que profesorado y estudiantado consideran útil, aplicable y positivo el uso de un recurso tal como las rúbricas diseñadas tanto en una escuela como en la otra.

Adentrándonos más en el detalle de los resultados obtenidos y categorizando estos en función de su naturaleza se concluye con los siguientes aspectos:

- En cuanto a la aplicabilidad de las rúbricas como instrumento para el seguimiento y evaluación de los TFGs desde el punto de vista del profesorado y el estudiantado:
  - Resultan un instrumento útil y fácilmente aplicable.
  - Permite la homogenización de criterios y la reducción de la subjetividad en los procesos evaluativos.

- En cuanto a la percepción del impacto del uso de rúbricas para el seguimiento y evaluación de los TFGs sobre el proceso de aprendizaje de los estudiantes:
  - Los elementos considerados en las rúbricas son, globalmente, pertinentes y coherentes.
  - El hecho de conocer los criterios desde el inicio del TFG es un elemento que promueve la autorregulación del estudiante y motiva la asunción de la responsabilidad sobre su propio proceso de aprendizaje.
  - El dar y recibir feedback a lo largo del proceso impacta directamente sobre el proceso de construcción del trabajo, ergo sobre el aprendizaje del propio estudiante.

Como elementos de discusión cabe destacar, fundamentalmente dos cosas; por un lado, la evaluación de las competencias específicas y por el otro la ponderación de la evaluación, es decir, el valor que cobra cada competencia o bloque de competencias en la nota final. Con respecto al primero de los elementos y debido a las múltiples temáticas sobre las que se puede basar el TFG, hay que asumir la imposibilidad de listar todas y cada una de las posibles competencias específicas susceptibles a ser trabajadas en los TFGs. Esto supone que, o bien no se consideren en las rúbricas (en el caso de la ESP que contempla las competencias generales listadas al inicio de este trabajo) o bien facilitar la definición de estas por parte de cada tutor mediante el uso de ejemplos y ofreciendo el soporte pedagógico necesario (en el caso de la ESUP).

Por otro lado y en cuanto a la ponderación de cada uno de los elementos evaluados, se destaca aquí por ser un aspecto crítico en cuanto a que requiere un proceso de toma de decisiones complejo. En ambos casos y destacando como un elemento común, la cualificación final no sale de una media aritmética sino que se ha ponderado en función del elemento (competencia/ tipo de competencia/ agente evaluador/momento).

Una vez se hayan presentado los primeros TFGs (curso académico 2012-2013) podrá llevarse a cabo la evaluación completa de la aplicación ya sí, institucionalizada, de las rúbricas de seguimiento y evaluación de los TFGs.

V. Agradecimientos

Este trabajo ha sido parcialmente financiado por los programas de ayudas de las universidades UC3M y la UPF (PlaQUID) así como por el Proyecto de Estudios y Análisis financiado por el Ministerio de Educación (E/A2011-0088). Los autores quieren agradecer la participación en la experimentación tanto al profesorado como al estudiantado de ambas instituciones.

VI. Referencias

[1] Real Decreto 1393/2007, de 29 de octubre (BOE 30/10/2007), por el que se establece la ordenación de las enseñanzas universitarias oficiales y Real Decreto 861/2010, de 2 de julio (BOE 3/7/2010) por el que se modifica el RD 1393/2007.

[2] Organización de las Enseñazas Universitarias en España, Ministerio de Educación y Ciencia, 26 de septiembre de 2006, en: http://www.eees.ua.es/grados/Propuesta%20MEC%20organizaci%F3n%20titulaciones%20Sep06.pdf

[3] A. Conde, y F. Pozuelo, "Las plantillas de evaluación (rúbrica) como instrumento para la evaluación. Un estudio de caso en el marco de la reforma de la enseñanza universitaria en el EEES," *Investigación en la Escuela*, no. 63, pp 77-90, 2007.

[4] *Accreditation Board for Engineering and Technology, Engineering Criteria*, Septiembre, 2004, en: http://www.foundationcoalition.org/home/keycomponents/assessment_eval/ec_outcomes_summaries.html

[5] E. Valderrama, M. Rullan, J. Pons, et al, *Guia per a l'avaluació de competències als treballs de final de grau i de màster a les Enginyeries*. Barcelona: AQU Catalunya, 2009.

[6] E. Valderrama, M. Rullan, F. Sánchez, J. Pons, F. Cores y J. Bisbal, "La evaluación de competencias en los Trabajos Fin de Estudios," *XV JENUI - Jornadas de Enseñanza Universitaria de la Informática*. Barcelona, 2009.

[7] E. Valderrama, M. Rullan, F. Sánchez, J. Pons, C. Mans, F. Giné, L. Jiménez y E. Peig, "Guidelines for the Final Year Project Assessment in Engineering," *FIE - Frontiers in Education*. San Antonio, Texas, 2009.

[8] E. Valderrama, M. Rullan, F. Sánchez, J. Pons, C. Mans, F. Giné, G. Seco-Granados, L. Jiménez, et al., "La Evaluación de Competencias en los Trabajos Fin de Estudios," *IEEE Revista Iberoamericana de Tecnologías del Aprendizaje,* vol. 5, no. 3, pp. 107-114, 2010.

[9] D. Escudero y D. Hernández-Leo, "Aplicación de buenas prácticas para la mejora de la calidad de los trabajos de fin de grado en Ingeniería en Diseño Industrial," *Simposio Internacional sobre Innovación y Calidad en la Formación de Ingenieros*, Valladolid, 26-28 de abril de 2012.

[10] MA. Zazueta y LF. Herrera, "Rúbrica o matriz de valoración, herramienta de evaluación formativa y sumativa," *Quaderns Digitals*, no. 55, 2008. Disponible en: http://www.quadernsdigitals.net/index.php?Accionmenu=hemeroteca.visualizaarticuloiu.visualiza&articulo_id=10816

[11] G. Rogers, "Students are important too," en *Program Assesment of Student Learning*, 9 de Enero 2012. Disponible en: http://programassessment.blogspot.com.es/

[12] V. Moreno, D. Hernández-Leo, I. Camps y J. Melero, " Uso de rúbricas para el seguimiento y evaluación de los trabajos fin de grado," *II Congreso Internacional sobre Evaluación por Competencias mediante e-Rúbricas*, Málaga, 23-25 de octubre de 2012.

[13] D. Hernández-Leo, V. Moreno e I. Camps, *Guía docente para el seguimiento y la evaluación de los Trabajos Final de Grado*. Unidad de Apoyo a la Calidad e Innovación Docente, Escuela Superior Politécnica, Universitat Pompeu Fabra, Barcelona, 2012, http://repositori.upf.edu/handle/10230/20036

[14] D. Hernández-Leo y V. Moreno *Herramienta Web para el Seguimiento y Evaluación de los Trabajos Fin de Grado.* III Jornadas de Innovación Educativa en Ingeniería Telemática, Granada, 2013, (Web de la Guía disponible on-line en http://www.usquid.esup.upf.edu/tfg)

Desarrollo de herramientas para la enseñanza de seguridad en redes telemáticas

Enrique de la Hoz, Ivan Marsa-Maestre, Jose Manuel Gimenez-Guzman,
Isaias Martinez-Yelmo, German Lopez-Civera
Departamento de Automática,
Universidad de Alcalá
Alcalá de Henares, Madrid (Spain)
{enrique.delahoz,ivan.marsa,josem.gimenez,isaias.martinezy,g.lopez}@uah.es

***Resumen*- El estudio de la materia Seguridad en Redes Telemáticas es un tema de vital importancia en la Internet actual que requiere una importante labor práctica por parte del alumno y a ser posible, en laboratorios especializados con dicho propósito. Sin embargo, los laboratorios habitualmente usados para su impartición suelen ser entornos cerrados, irónicamente por cuestiones de seguridad de los centros donde se imparten, y carecen de la flexibilidad necesaria para su correcta impartición por lo que sería deseable la disponibilidad de entornos más específicos. En este artículo presentamos una herramienta que permite de manera flexible generar escenarios de red virtualizados que sirven para impartir docencia de seguridad en redes y sistemas informáticos. Las principales ventajas de usar este sistema virtualizado es que es un sistema de software abierto, modular, distribuido, escalar y flexible. Ilustramos el funcionamiento de la herramienta mediante un escenario de pruebas junto con los resultados obtenidos tras su uso en asignaturas de Seguridad pertenecientes a los nuevos grados del EEES.**

***Palabras Clave*- Seguridad, Redes y Sistemas, Docencia práctica, Virtualización.**

I. INTRODUCCIÓN

Los sistemas de información y comunicaciones desempeñan un papel fundamental en la actual sociedad de la información. El grado de integración de estos sistemas y redes en nuestras vidas es tal, que es difícil, si no imposible, imaginar nuestra sociedad desarrollada actual sin ellas. Además, estos sistemas y redes son elementos clave a nivel empresarial y gubernamental. Esta dependencia de la sociedad en los sistemas de información y comunicaciones convierte a la sociedad en tan vulnerable como lo son sus sistemas de información y redes telemáticas, lo que convierte su protección en un aspecto absolutamente crítico.

Para proteger estos sistemas y redes, hay que considerar dos tipos diferentes de amenazas: físicas y lógicas. Si se analizan los datos de los últimos años, podemos apreciar que ha habido un continuo incremento en el número y en la importancia de ataques lógicos a diferentes infraestructuras críticas de red [1-3]. Por estas razones, es necesario dedicar esfuerzos eficaces y efectivos para proteger nuestras infraestructuras contra estos posibles tipos de amenazas. Una de las estrategias críticas para alcanzar estos requisitos pasa por una enseñanza universitaria de alta calidad de las materias de seguridad en redes y sistemas. Sin embargo, esta estrategia no es nueva ya que desde la década de los 90, diferentes expertos han recomendado reforzar las asignaturas relacionadas con la seguridad en los planes de estudio universitarios relacionados con las Tecnologías de la Información y Comunicaciones (TIC), destacando que la enseñanza en estas materias es claramente insuficiente, ya que no cubre las necesidades reales [4].

Aunque hay diferentes maneras de abordar la docencia de seguridad en redes y sistemas en las asignaturas, la mayor parte de ellas distinguen dos bloques fundamentales: seguridad de la información, donde el énfasis se pone en la criptografía, y seguridad en sistemas de información [5]. Uno de los requisitos clave para proporcionar una educación completa y de calidad, especialmente en el caso de la seguridad de sistemas, consiste en disponer de un equipamiento adecuado para tal fin. Debido a la naturaleza eminentemente práctica de esta disciplina, es muy difícil conseguir una enseñanza efectiva sin disponer de un entorno de laboratorio donde puedan estudiarse los aspectos prácticos necesarios de la materia. Sin embargo, incluso en los casos en los que se dispone de suficientes recursos para construir este tipo de laboratorios, suele ser difícil proveer escenarios similares a entornos reales, lo que permitiría proporcionar a los estudiantes desafíos más cercanos a los que se enfrentarán en su futura vida profesional. Además, debido a la naturaleza de los temas tratados en este tipo de asignaturas, los administradores de red, por motivos de seguridad, se muestran reacios al despliegue de laboratorios de seguridad en campus universitarios, a menos que estén aislados del resto de la red, lo que limita su alcance. Por todas las razones anteriormente expuestas, la mayor parte de laboratorios de seguridad que se pueden encontrar en las universidades son bastante limitados, aunque la totalidad de los docentes coinciden en que el caso ideal sería disponer de entornos prácticos donde puedan interactuar con sistemas más realistas usando tecnologías que se encuentren en el estado del arte.

El diseño de laboratorios de seguridad realistas es, por tanto, una tarea fundamental para los docentes en el área de seguridad. En esta línea, nuestro trabajo se centra en el diseño de laboratorios de seguridad de escenarios realistas, sin que estos impacten de manera negativa en el funcionamiento de la red ni de los sistemas existentes en el campus universitario. Además, el diseño de estos laboratorios debe considerar la rápida evolución de esta disciplina, por lo

que las herramientas desarrolladas deben ser modulares y fácilmente extensibles a escenarios futuros. Este artículo contribuye a estos objetivos de diferentes maneras. En primer lugar, analizamos el problema de la docencia en seguridad en sistemas y redes usando escenarios de ejemplo, revisando las principales contribuciones que existen en este área. En segundo lugar, presentamos la herramienta NEMESIS, un modelo modular y jerárquico que permite definir escenarios para la docencia en seguridad en redes y sistemas de manera flexible y extensible. La arquitectura de NEMESIS se basa en máquinas virtuales distribuidas a lo largo de diferentes equipos físicos, lo que permite la implementación y estudio de escenarios complejos y escalables. Finalmente, incluimos un caso de uso detallado para la enseñanza de esta disciplina junto con los resultados obtenidos en diferentes asignaturas donde se ha empleado la herramienta descrita en comparación con los obtenidos cuando no se empleaba dicha herramienta.

II. Estado del arte en el desarrollo de laboratorios de seguridad

En esta sección se hace un breve resumen de las principales propuestas existentes para el despliegue de laboratorios de seguridad para la docencia de seguridad en redes y sistemas. Conforme a sus arquitecturas, dividiremos estas propuestas en: laboratorios *hardware*, laboratorios virtuales centralizados y laboratorios virtuales descentralizados.

La manera de alcanzar el máximo nivel de realismo en el diseño de un laboratorio de seguridad es el uso de *hardware* real. Así, los estudiantes pueden hacer uso de dispositivos reales (incluyendo componentes de red reales) y experimentar los problemas derivados del uso de tales componentes. A pesar de que este tipo de laboratorios proporcionan la experiencia más realista, también presentan importantes desventajas. Su principal problema radica en el coste económico de desplegar el sistema completo deseado. Además, existen también costes asociados al tiempo necesario para instalar y configurar cada escenario con el que se desee trabajar. Por otro lado, si consideramos la portabilidad, los estudiantes no pueden reproducir dicho entorno con facilidad, ya que se trabaja directamente con el *hardware* real. Finalmente, para el profesorado supone invertir un tiempo no despreciable en desplegar estos escenarios que van a emplearse para diferentes materias, titulaciones o incluso prácticas de laboratorio. Por lo tanto, este tipo de laboratorios, incluso aunque proporcionan la experiencia más cercana a la realidad, puede superar los recursos disponibles de la mayor parte de instituciones. Un ejemplo de este tipo de laboratorios es el *Georgia Tech's Hands-On Information Security Lab* [6]. En este entorno, y empleando las capacidades del equipamiento de red Cisco, es posible reconfigurar la infraestructura de red hasta cierto punto. Los autores reconocen que los requisitos impuestos por su implementación pueden hacer no factible su utilización para instituciones de tamaño mediano o pequeño.

Debido a los inconvenientes descritos anteriormente, muchos docentes no consideran los laboratorios de seguridad basados en *hardware* factibles o adecuados para sus propósitos. Las tecnologías de virtualización pueden ayudar a desplegar escenarios similares de manera mucho más sencilla y eficiente. En esta aproximación al problema, se puede emplear la infraestructura *hardware* para ejecutar máquinas virtuales donde desplegar el escenario de seguridad deseado. Además, estos entornos virtuales pueden ser migrados o replicados en diferentes equipos físicos de manera rápida y sencilla, permitiendo de esta manera replicar diferentes arquitecturas de red de manera eficiente. Con esta aproximación, podemos alcanzar un mayor nivel de estabilidad y tolerancia a fallos: dado que el estado de las máquinas virtuales puede almacenarse, los estudiantes pueden trabajar de manera más segura y autónoma con el escenario. Así, si tiene lugar alguna situación destructiva (bien sea accidental o intencionada), siempre se puede volver al último estado estable conocido. Básicamente, hay dos modelos diferentes para implementar este tipo de laboratorios. Por un lado, es posible almacenar imágenes de máquinas virtuales en un sistema de almacenamiento centralizado. Así, cuando un estudiante quiere ejecutar un escenario para una práctica de laboratorio concreta, debe descargar las imágenes a su equipo local y ejecutar dichas imágenes localmente con el motor de virtualización empleado. Una ventaja clave de este modelo es la abstracción que se hace del *hardware* real por medio de las máquinas virtuales. Otra fortaleza de esta aproximación es que cada estudiante puede reproducir su propio conjunto de máquinas virtuales en un entorno aislado. Sin embargo, esta estrategia presenta algunos inconvenientes a tener muy en cuenta, como el tiempo de descarga requerido previo al lanzamiento del escenario y la limitación en el número máximo de nodos que podrá tener el escenario, que vendrá determinado por las capacidades de cómputo, memoria y almacenamiento del equipo local donde se ejecutan las máquinas virtuales deseadas. Para subsanar estos inconvenientes podemos plantear un modelo diferente donde, en lugar de descargar un conjunto de máquinas virtuales a cada estación de trabajo, un único conjunto de imágenes se distribuye sobre un conjunto de estaciones de trabajo. De este modo, por ejemplo, si se pueden ejecutar 6 máquinas virtuales en cada estación de trabajo, podríamos simular el funcionamiento de una red de 30 *hosts* con 5 estaciones de trabajo. La principal ventaja de este método es permitir la agregación de recursos para simular redes más grandes, permitiéndonos estar más cerca de la experiencia de trabajo en un entorno real en producción. Respecto a la configuración de la red, las topologías sencillas pueden desplegarse de manera directa, pero para escenarios más complejos hay que hacer uso de técnicas que permitan la virtualización a nivel de enlace, como *Virtual Distributed Ethernet* (VDE), que permite interconexiones de *hosts* usando conmutadores y *routers* virtuales. Un ejemplo de laboratorio de este tipo es *TinkerNet* [7].

Otros modelos proponen el uso de un modelo centralizado para proporcionar un entorno de red virtual. Bajo este modelo, existe un servidor central que alberga las redes virtuales para todos los estudiantes. Aunque teóricamente este servidor centralizado podría soportar una virtualización tanto completa como de sistema operativo, para escenarios relativamente complejos las limitaciones en la potencia de cálculo de los equipos nos forzarán a usar virtualización de sistema operativo. Así, los estudiantes podrán acceder al servidor central y crear redes virtuales de hasta un tamaño moderado con un escaso impacto en las prestaciones del servidor. Además, esta técnica permitirá a los estudiantes acceder a los escenarios propuestos remotamente, con las ventajas que ello supone. En este tipo

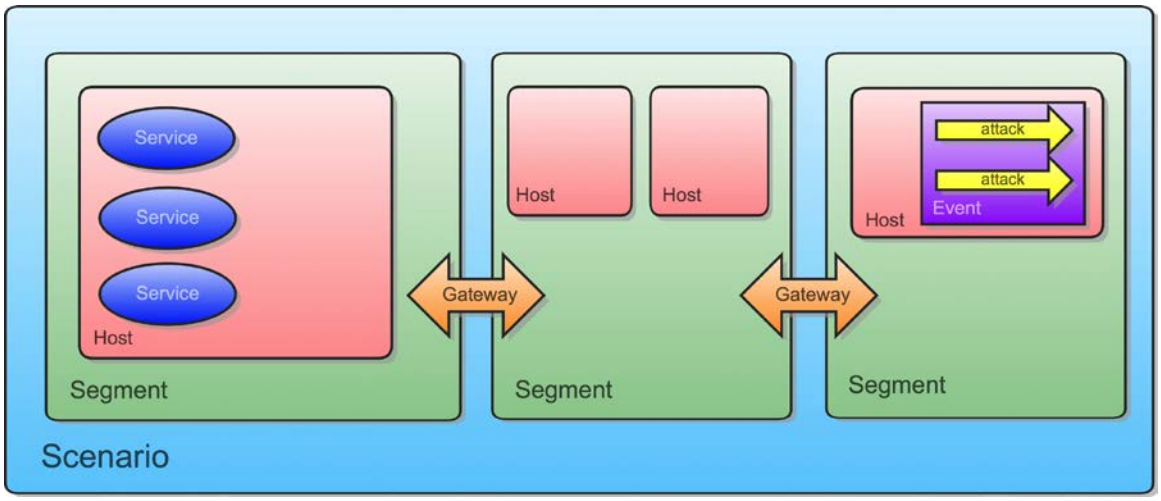


Fig. 1. Elementos de un scenario NEMESIS.

de laboratorios se pueden emplear *clusters* de equipos para incrementar la escalabilidad del sistema. La ventaja principal de este modelo es, sin duda, la simplicidad para la gestión del laboratorio. Sin embargo, al basarse en un único servidor centralizado, existe un riesgo de no disponibilidad mayor, requiriéndose además conectividad de red a dicho servidor para poder trabajar con los escenarios desarrollados.

III. NEMESIS: HERRAMIENTA DE GENERACIÓN DE ESCENARIOS DE SEGURIDAD

Como se ha visto, la mayor parte de propuestas en cuanto al diseño de laboratorios presenta limitaciones como falta de flexibilidad, escalabilidad o excesivo consumo de recursos. Para abordar estas limitaciones, hemos desarrollado una herramienta de generación de escenarios para la docencia de materias relacionadas con la seguridad de redes y sistemas, cuyo nombre es NEMESIS (*Network EMulator for Education on System and Internet Security* – Emulador de red para la docencia en seguridad de sistemas e Internet). Una descripción detallada de la arquitectura e implementación de NEMESIS queda fuera del alcance de este artículo pero está disponible en [8]. En los siguientes apartados, se destacarán los elementos clave de la arquitectura hasta el nivel de detalle necesario para comprender las posibilidades de la herramienta y sus posibilidades para la especificación y despliegue de escenarios de seguridad, así como su aplicación a un escenario concreto definido en el resto del artículo.

A. La arquitectura de NEMESIS

NEMESIS se basa en una arquitectura modular, que facilita su expresividad y flexibilidad además de asegurar su extensibilidad. Los elementos clave existentes en NEMESIS son los siguientes:

- *Host*: cada una de las máquinas del escenario de red considerado. Las características generales de las máquinas, como por ejemplo la versión deseada de un sistema operativo, puede seleccionarse entre diferentes plantillas disponibles.
- Segmento de red: incluye un conjunto de *hosts* que tienen conectividad entre todos ellos a nivel de enlace.
- Pasarela (*gateway*): un tipo especial de *host* que actúa como conexión entre dos o más segmentos de red. Puede ser un router o un elemento más complejo con más funcionalidades.
- Evento: en cada *host*, se pueden programar eventos o conjuntos de eventos. Entendemos por evento una secuencia de acciones (como por ejemplo la ejecución de un programa o servicio) que se ejecutan en instantes de tiempo especificados.
- Ataque: entre las diferentes acciones que puede iniciar un evento, los ataques son especialmente relevantes para los objetivos docentes en seguridad. Los ataques pueden seleccionarse de una librería disponible de ataques.

Los diferentes elementos lógicos de un escenario definido mediante NEMESIS, junto con las relaciones entre ellos, se muestran gráficamente en la Fig. 1.

La arquitectura *hardware* de NEMESIS consiste en máquinas virtuales que pueden distribuirse en diferentes máquinas físicas. Cada máquina física puede albergar uno o más segmentos de red, cada uno con una o más máquinas virtuales. Toda esta infraestructura se gestiona mediante un gestor de máquinas virtuales (VMM – *Virtual Machine Manager*) [9]. Los segmentos de red se interconectan por medio de sus correspondientes pasarelas virtuales. Gracias a esto, para los *hosts* es transparente el hecho de que un escenario esté distribuido entre diferentes máquinas.

Con una arquitectura virtual distribuida como la descrita, los problemas en cuanto a prestaciones pueden paliarse distribuyendo la carga computacional entre diferentes máquinas. Por otro lado, esta arquitectura permite, por ejemplo, desplegar las máquinas virtuales desde las que los estudiantes actuarán como "atacantes" en máquinas diferentes a las que albergan los segmentos de red a los que van a atacar, previniendo de este modo que se manipule el escenario de pruebas planificado para su impartición.

La implementación de esta arquitectura distribuida pone de manifiesto algunas cuestiones adicionales, como el control del inicio y parada de las máquinas virtuales, el aislamiento adecuado entre diferentes segmentos de red y la confidencialidad de las comunicaciones existentes entre las diferentes máquinas. Estas cuestiones han condicionado en gran medida la solución de virtualización adoptada.

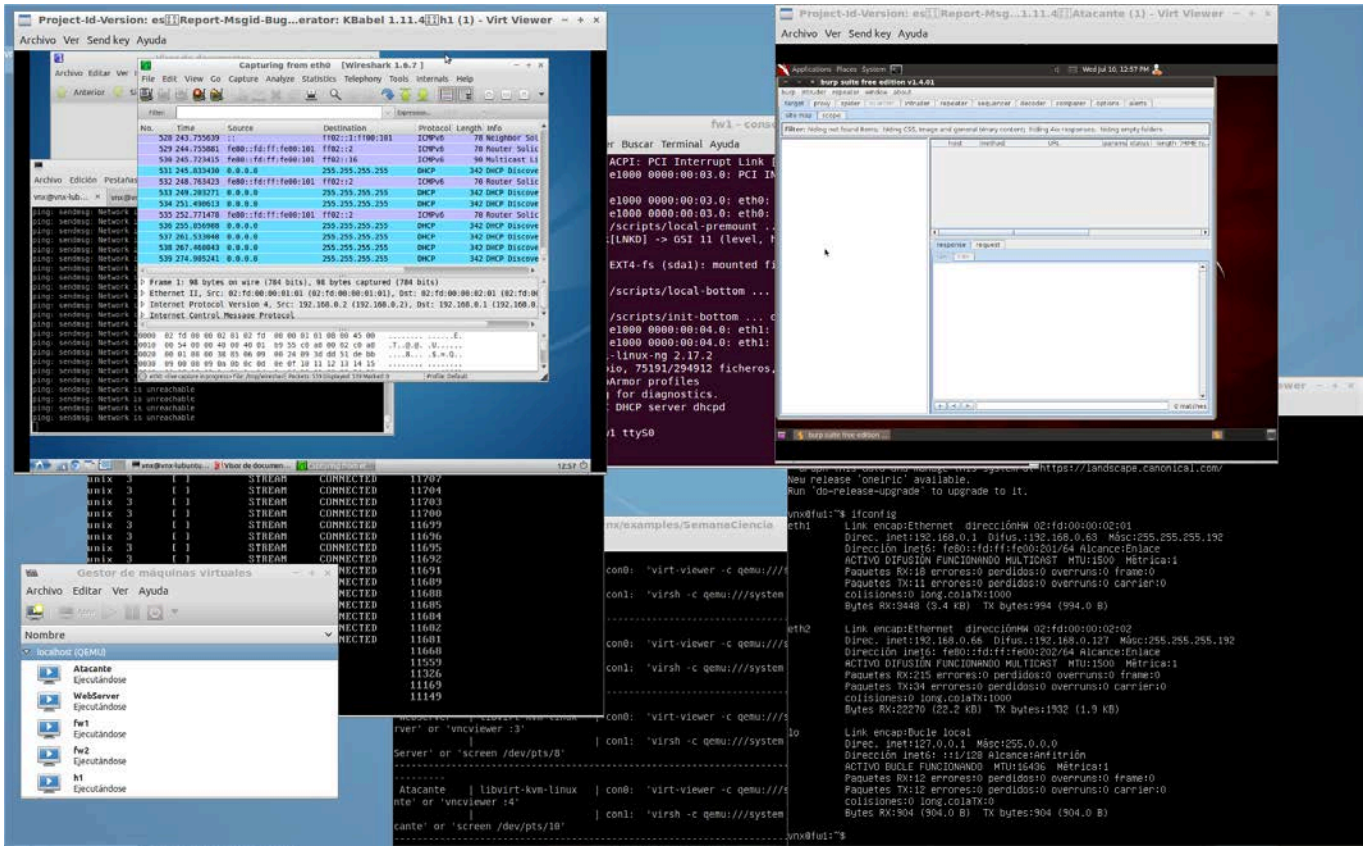


Fig. 2. Ejemplo de interfaz del sistema.

En una primera implementación de NEMESIS, nos planteamos el uso de diferentes tecnologías de hipervisor como VMWare (http://www.vmware.com) y Xen (http://www.xen.org), aunque finalmente la solución escogida fue KVM (http://linux-kvm.org). Para la implementación actual, se ha optado por la herramienta de emulación de redes VNX [10] a la que se han añadido las capacidades de definición y configuración de escenarios de seguridad.

B. Descripción del escenario, puesta en marcha y gestión

Un escenario NEMESIS se describe empleando un fichero XML. El escenario XML se carga por medio del agente gestor (AG), que lo analiza sintácticamente y envía las órdenes requeridas a un conjunto de agentes en las máquinas físicas, de modo que cada máquina física despliega su parte correspondiente del escenario.

Cada segmento de red, definido por el elemento `segment` en el fichero XML, se lanza en una máquina dada. Si varios elementos de red se lanzan en la misma máquina, debe especificarse un puerto como atributo adicional para cada segmento, de modo que este puerto se empleará para las comunicaciones que involucren a las máquinas virtuales que pertenezcan a ese segmento.

Los *hosts* pueden incluirse dentro de cada segmento de red, definiéndolos con el elemento `host`. Para cada host, hay que especificar la plantilla (`template`) que define el tipo de máquina virtual que quiere ser lanzada. Las diferentes plantillas se almacenan previamente en las máquinas. Dentro de cada *host*, podemos hacer uso del elemento `service` para definir servicios que se ejecuten en la puesta en marcha de la máquina virtual. Los segmentos de red se conectan por medio de `gateways`, usando plantillas previamente almacenadas, de manera similar a los *hosts*. Los eventos (elemento `event`) pueden definirse para que se ejecuten en un *host* en un instante de tiempo definido.

El elemento `config` puede usarse para especificar configuraciones más detalladas y complejas de los *hosts*, *gateways* y servicios, entre otros.

Por defecto, las máquinas virtuales se ejecutan sin interfaz gráfico. El elemento `display` puede emplearse para habilitar una interfaz gráfica para un *host* específico (de modo que, por ejemplo, un alumno pueda operar a través de dicho *host*) y especificar qué máquina física lanzará esta interfaz gráfica. Esto permite exportar interfaces de *host* a máquinas que no pertenezcan al escenario, lo que permite interactuar con el escenario sin dar acceso a las máquinas a las que el usuario no debería tener acceso, incluso cuando estén en el mismo segmento de red virtual.

Para más información acerca de la descripción de escenarios en NEMESIS, su puesta en marcha y gestión, se han publicado un conjunto de vídeos mostrando el uso de la herramienta en http://ww.youtube.com/user/telematicauah. Asimismo, la Fig. 2 muestra una captura de pantalla de la interfaz del sistema ejecutando un caso de uso.

IV. UN ESCENARIO DE EJEMPLO: SEGURIDAD PERIMETRAL

En esta sección se describe un ejemplo del empleo de NEMESIS para diseñar prácticas de laboratorio de seguridad perimetral. Hemos escogido específicamente este escenario debido a los especiales desafíos que supone tanto para el despliegue de la infraestructura de red como para el diseño de actividades adecuadas para la evaluación de los estudiantes. En primer lugar, la propia naturaleza de la seguridad perimetral requiere definir diferentes segmentos de red (cada

uno de ellos con su propio esquema de direccionamiento) e interconectarlos por medio de conmutadores y encaminadores. En segundo lugar, aunque este tipo de escenarios podrían emularse empleando otras alternativas, los estudiantes tendrían que solventar un elevado número de problemas relativos a la configuración y gestión del escenario. De acuerdo con nuestra experiencia docente, esta carga de trabajo adicional a menudo impide al estudiante concentrarse adecuadamente en los verdaderos objetivos docentes de la asignatura. En tercer lugar, para evaluar y validar los resultados en este tipo de entornos, es necesario generar patrones de tráfico específicos (e.g., para comprobar las capacidades de defensa frente a ataques DDoS), lo que puede interferir con algunos de los mecanismos de seguridad que suelen desplegarse en las redes universitarias. Por último, es deseable permitir a los estudiantes probar diferentes arquitecturas de seguridad perimetral (e.g., múltiples subredes filtradas, subredes separadas…). Por ello, creemos que este tipo de escenarios puede beneficiarse en gran medida del uso de NEMESIS y que, en consecuencia, son muy adecuados para mostrar las prestaciones de NEMESIS de forma clara.

Las asignaturas de seguridad ofertadas tradicionalmente en nuestra universidad siempre han incluido prácticas de seguridad perimetral. Normalmente, de una asignatura de 60 horas, se dedicaban cuatro horas (dos sesiones de dos horas de duración) a prácticas de seguridad perimetral, empezando con cortafuegos y terminando con sistemas de detección de intrusiones (*intrusion detection systems*, IDS). Estas prácticas se basaban en arquitecturas de cortafuegos de una sola máquina, que consistían en un encaminador con capacidad de filtrado de paquetes (normalmente una máquina Linux), y un equipo bastión en la red local. Las reglas de filtrado de paquetes en el encaminador tenían que ser tales que el equipo bastión fuera la única máquina de la red interna a la que pudieran conectarse máquinas en Internet (por ejemplo, para entregar correo electrónico). Por supuesto, sólo se permitía cierto tipo de conexiones. Cualquier sistema externo que intentase acceder a los sistemas y servicios internos debía pasar por el equipo bastión. Además, se incluían otros equipos en la red interna. Al estudiante se le pedía que configurara el filtrado de paquetes en el encaminador para permitir que los equipos internos pudieran abrir conexiones hacia equipos situados en Internet para ciertos servicios, y que se bloqueasen todas las conexiones desde el exterior salvo aquellas dirigidas a los servicios ofrecidos por el equipo bastión. En la segunda parte de la sesión, se introducían nuevas amenazas que no podían ser tratadas adecuadamente por un cortafuegos (e.g., ataques de fuerza bruta sobre contraseñas) y se sugería el empleo de un sistema de detección de intrusiones. Para afrontar estas amenazas, se pedía al estudiante que crease reglas para el IDS snort [11].

Tanto en el escenario de cortafuegos como en el de IDS, a los estudiantes se les pedía configurar el entorno y, posteriormente, se realizaba una evaluación (normalmente a mano) para comprobar que cumplía con los requisitos de la práctica. La evaluación del trabajo del estudiante era una combinación de corrección formal y cumplimiento de requisitos.

Este mecanismo, aunque permitía cumplir con los requisitos docentes básicos para estas sesiones, tiene algunas desventajas. Por un lado, existen limitaciones respecto de la complejidad de los escenarios que se pueden desplegar con este enfoque, debidas principalmente a los problemas derivados de montar configuraciones complejas de red (varias redes interconectadas por encaminadores y cortafuegos) de forma manual, ya sea en entornos de virtualización o con sistemas reales. Desde un punto de vista docente, esto limita el tipo de entornos con los que podemos trabajar, haciendo muy difícil, por ejemplo, trabajar con arquitecturas de múltiples subredes con filtrado de paquetes. Por otro lado, la evaluación del trabajo del estudiante es muy costosa para el personal docente, dado que la mayor parte de las pruebas se hacen de forma manual.

Para hacer frente a estas limitaciones, proponemos el uso de NEMESIS. A continuación ilustramos los beneficios que se derivan de emplear nuestra solución, presentando un escenario que hemos utilizado en docencia y que modela un caso de uso típico: una red corporativa de gran tamaño donde distintas áreas (administración, I+D, servidores externos…) tienen redes diferentes con requisitos de seguridad y control de acceso dispares. La complejidad de este escenario justifica el uso de NEMESIS.

Al estudiante se le presenta el caso de uso con los requisitos específicos para cada una de las áreas de la red, y se le proporciona un conjunto de alternativas de diseño entre las que debe escoger una de acuerdo con los requisitos planteados y con su propia comprensión del escenario planteado. Las alternativas de diseño citadas han sido creadas previamente por el equipo docente de la asignatura. Tanto la descripción del escenario NEMESIS (un fichero XML) para cada una de las alternativas como las máquinas virtuales necesarias (*hosts* bastión, estaciones de trabajo, *gateways*…) se proporcionan de antemano, de forma que el estudiante sólo tiene que ocuparse de la configuración del direccionamiento IP, lo que pueda hacerse con facilidad modificando el fichero de descripción correspondiente. Una vez completada esta sencilla configuración, los estudiantes pueden lanzar la simulación del escenario.

Sobre este escenario, se pide al estudiante que diseñe e implemente mecanismos de seguridad perimetral empleando primero únicamente cortafuegos, y añadiendo después sistemas de detección de intrusiones. Empleando la plantilla de NEMESIS `gateway` (mencionada anteriormente), el estudiante puede centrarse únicamente en aspectos de diseño y configuración, olvidándose de las tareas de instalación. La plantilla `gateway` está basada en GNU Linux e incluye los paquetes software *iptables* y *snort* [11, 12], para la gestión del filtrado de paquetes y la detección de intrusiones, repectivamente.

Para llevar a cabo esta práctica de laboratorio, contemplamos dos maneras diferentes de trabajar con NEMESIS. En primer lugar, es posible implementar la configuración de seguridad (reglas para el *firewall* y el IDS) por medio de descripciones de alto nivel, para que los estudiantes no tengan que realizar configuraciones de IDS o *firewalls* a bajo nivel. Esta alternativa es preferible para aquellas asignaturas en las que los estudiantes tienen poca experiencia en administración de sistemas operativos. Las descripciones de alto nivel permiten definir tanto reglas de filtrado (e.g. `'allow-dns'`) como reglas para que un IDS identifique amenazas (`'allow less than 5 login attempts'`) sin que sea necesario tener conocimientos sobre cómo se implementan realmente dichas reglas. Estas descripciones de alto nivel son parametrizables para permitir que se particularicen a distintas situaciones. Este enfoque hace posible centrarse en los aspectos de diseño de este tipo

de sistemas, dejando aparte los aspectos de implementación. En segundo lugar, está disponible una modalidad de descripción de bajo nivel (`'custom-rule'`) específica para cada sistema operativo, con la que se puede lograr la misma expresividad que permita el SO subyacente. Ambos tipos de descripciones se pueden incluir en un mismo fichero XML de descripción de escenario, o en otro XML referenciado desde el anterior: el estudiante puede incluso cargar y descargar diferentes conjuntos de reglas para evaluar el resultado de su aplicación. En definitiva, el uso de descripciones de alto o bajo nivel dependerá en general de las características de la asignatura en la que se desarrolle la práctica y de los estudiantes implicados.

Además del diseño y despliegue de los escenarios, es posible definir evaluaciones y validaciones automáticas. Al definir el escenario, pueden incluirse rutinas de validación para valorar el cumplimiento de los requisitos definidos. Estas rutinas de validación, que se definen en ficheros XML externos, no son más que tests automatizados predefinidos. Para realizar la validación propiamente dicha, estos tests toman como parámetros de entrada características del escenario, de forma que el profesor no necesita conocer de antemano los detalles específicos de configuración de red con los que trabajará el alumno. El objetivo de este tipo de rutinas es doble. En primer lugar, permite una validación formal del conjunto de reglas definidas por el estudiante para evaluar si son consistentes o no. Si esta validación tiene éxito, se comprueba el cumplimiento de los requisitos de la práctica. La comprobación consiste en un conjunto de tests automatizados, que emulan diferentes tipos de patrones de tráfico de red, ya sea legítimo o malicioso. Un ejemplo del primero podría ser `'access host 'web server' using http port 80 from Internet'` y un ejemplo del segundo podría ser `'Do SYN Flood over hosts in DMZ network'`.

Esta validación devuelve una puntuación detallada que refleja el grado de cumplimiento con los requisitos de seguridad del escenario. Esta puntuación le puede servir al alumno como realimentación sobre la adecuación de su solución, y también a los docentes como métrica de evaluación adicional.

V. Resultados del uso de NEMESIS en docencia

En esta sección analizamos nuestra experiencia con NEMESIS en docencia. En primer lugar describimos brevemente el marco de las asignaturas relevantes para la experiencia, para después pasar a presentar y discutir los resultados obtenidos.

A. Contexto de la asignatura

Tradicionalmente, *Seguridad en Internet* es una asignatura optativa del plan de estudios de Ingeniería Informática en la Universidad de Alcalá, que tiene 30 horas prácticas en laboratorio de un total de 60 horas. El objetivo de la asignatura es ofrecer a los alumnos unas bases sólidas sobre seguridad de la información, seguridad de redes y seguridad de sistemas. La mayor parte de las horas de teoría se dedican a criptografía, mientras que las clases prácticas se enfocan más hacia la seguridad de redes y sistemas. Los resultados académicos de la última década han puesto de manifiesto que los estudiantes adquieren más fácilmente los conocimientos de la parte de criptografía, mientras que las habilidades relacionadas con seguridad de redes y sistemas les resultan más difíciles de aprender. Nuestra hipótesis sobre estos resultados es que la seguridad de sistemas requiere una experiencia más realista, que permita a los estudiantes enfrentarse a algunos de los problemas de la disciplina en el mundo real. Teniendo esto en cuenta, en el último año rediseñamos la parte práctica de la asignatura para hacer las prácticas más realistas. No obstante, las restricciones de infraestructura y presupuesto limitaron en gran medida las mejoras que pudimos hacer a las prácticas de laboratorio.

Con la transición al Espacio Europeo de Educación Superior (EEES) en las universidades españolas, se ha invertido un gran esfuerzo en proporcionar a los estudiantes una formación más práctica y orientada a competencias. Hemos tomado esa transición como una oportunidad de desarrollar una plataforma que permita generar escenarios para prácticas de seguridad de forma realista y flexible. La plataforma que se describe en este documento se ha utilizado para la asignatura *Seguridad* (SEG), asignatura obligatoria del nuevo plan de *Grado en Ingeniería Telemática* y optativa en el plan de estudios de *Grado en Ingeniería Informática*, con 3 créditos ECTS prácticos de un total de 6. Los contenidos de la asignatura son muy similares a los de la asignatura *Seguridad en Internet* mencionada más arriba, lo que constituye una oportunidad única para la validación de la plataforma.

B. Resultados

Desde el punto de vista de los profesores, el uso de NEMESIS proporciona un mecanismo mucho más sencillo y flexible para el diseño y despliegue de escenarios para las prácticas de laboratorio, lo que permite ofrecer a los alumnos prácticas más realistas. Una prueba adicional de la flexibilidad y facilidad de uso de la plataforma es que hemos pedido a algunos estudiantes que diseñen escenarios para prácticas de seguridad, y han obtenido resultados de muy alta calidad en un tiempo razonable. Nuestra idea es incluir esos escenarios como prácticas opcionales en futuras ediciones de la asignatura.

Desde el punto de vista del estudiante, la percepción subjetiva sobre la experiencia fue muy positiva. En cualquier caso, para obtener una realimentación más objetiva de los estudiantes, se realizó una encuesta orientada a recabar la opinión de los estudiantes de SEG sobre el sistema. La Tabla I muestra el resultado, donde cada pregunta se valoraba en una escala del 1 al 5. Los resultados se han agregado por temas por razones de espacio, ya que la encuesta original tenía 27 preguntas que cubrían, además, otros aspectos de la asignatura. Los resultados muestran que los estudiantes están significativamente satisfechos con la plataforma:

Tabla I
Resultados de la encuesta para SEG (2012/2013)

Aspecto	Media
Flexibilidad para el trabajo (tiempo, ubicación)	4.823
Cobertura de los temas de la asignatura	4.241
Utilidad para reforzar conceptos y habilidades	4.428
Diversidad de prácticas e interés	4.567
Evaluación general de las prácticas	4.427

Finalmente, se ha analizado el rendimiento de los estudiantes tras seguir la asignatura optativa ya extinta *Seguridad en Internet* y el resultado de la actual asignatura

obligatoria SEG. Así, agregando los resultados académicos de los cursos 2010/2011 y 2011/2012 de *Seguridad en Internet* superaron (no superaron) la asignatura 24 (14) alumnos en primera convocatoria, lo que es una tasa de aprobados del 63.2%. Por otro lado, la asignatura SEG, incluso tratándose de una asignatura obligatoria para los alumnos del Grado en Ingeniería Telemática, ha tenido unos resultados en el curso 2012/2013 de 41 aprobados sobre un total de 42 alumnos, lo que da un porcentaje de éxito del 97.6%, lo que indica la mayor implicación por parte del alumnado en la asignatura.

VI. Conclusiones y trabajo futuro

El diseño de laboratorios de seguridad realistas es un desafío para los profesores de este tipo de asignaturas. Existen diferentes alternativas para abordar este desafío, desde los laboratorios puramente hardware al uso de diferentes técnicas de virtualización. Sin embargo, la mayoría de enfoques disponibles en la literatura tienen limitaciones serias, especialmente en cuanto a flexibilidad, extensibilidad y seguridad. Para dar respuesta a esas limitaciones, en este artículo presentamos NEMESIS, una plataforma para la generación y emulación de escenarios para la docencia de la seguridad de redes y sistemas. La plataforma hace uso de técnicas de virtualización existentes para facilitar la portabilidad de los escenarios, y presenta un diseño modular para garantizar su extensibilidad. Por otro lado, la plataforma se ha diseñado para permitir su despliegue distribuido en varias máquinas físicas, lo que mejora la escalabilidad de la solución. Finalmente, el diseño de escenarios hace uso de plantillas para *hosts*, servicios y ataques, y usa ficheros XML para la definición de escenarios de seguridad. Esto garantiza un cierto grado de expresividad y flexibilidad.

Aunque el uso de esta plataforma para el diseño de prácticas de laboratorio ha dado resultados satisfactorios (como se ha mostrado en el ejemplo de uso analizado), hay aún un amplio campo de investigación en esta línea. Estamos trabajando en la creación de plantillas para diferentes sistemas, servicios y ataques y en la mejora de la expresividad de las descripciones de escenarios. Finalmente, estamos interesados en crear un portal para el desarrollo de módulos para la plataforma, donde otros miembros de la comunidad de seguridad de sistemas puedan contribuir al crecimiento de NEMESIS.

Agradecimientos

Los autores de este trabajo quieren mostrar su agradecimiento al área de Ingeniería Telemática del Departamento de Automática de la Universidad de Alcalá y a la propia Universidad, que facilita la innovación educativa a los autores de este artículo por medio del proyecto de innovación educativa «UAH-EV548» de la convocatoria «Proyectos para el fomento de la innovación en el proceso de enseñanza-aprendizaje» de 2012-2013.

Referencias

[1] T. Mendyk-Krajewska y Z. Mazur, "Problem of network security threats", en 3rd Conference Human System Interactions (HSI), 2010.
[2] Jiang Wei, "Survey of network and computer attack taxonomy" en IEEE Symposium On Robotics and Applications (ISRA), 2012.
[3] United States Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented", http://www.gao.gov/assets/660/652170.pdf (accedido julio 2013).
[4] T. A. Yang, K. Yue, M. Liaw, G. Collins, J. T. Venkatraman, S. Achar, K. Sadasivam y P. Chen, "Design of a distributed computer security lab", J.Comput.Sci.Coll. 20(1), pp. 332-346. 2004.
[5] J. C. Higgins, "Information security as a topic in undergraduate education of computer scientists," en Proceedings of the 12th National Computer Security Conference, Baltimore, 1989, pp. 553-557.
[6] R. T. Abler, D. Contis, J. B. Grizzard y H. L. Owen. Georgia tech information security center hands-on network security laboratory. Education, IEEE Transactions On 49(1), pp. 82-87. 2006.
[7] T. Winters, R. Ausanka-Crues, M. Kegel, E. Shimshock, D. Turner y M. Erlinger, "TinkerNet: A low-cost and ready-to-deploy networking laboratory platform" En Proceedings of the 8th Australasian Conference on Computing Education - Volume 52. 2006.
[8] E. de la Hoz, I. Marsa-Maestre, M. Lopez-Carmona y M. T. Lopez-Merayo, "Herramienta para la generación de escenarios de apoyo a la docencia de la seguridad en redes" en Actas de las I Jornadas De Innovacion Educativa En Ingeniería Telemática (JIE 2010), Valladolid, 2010, pp. 16-23.
[9] J. Smith and R. Nair. Virtual Machines: Versatile Platforms for Systems and Processes 2005.
[10] Virtual Networks over linuX (VNX) web site. http://web.dit.upm.es/vnxwiki/ (accedido julio 2013).
[11] J. Koziol. Intrusion Detection with Snort (1st ed.) 2003.
[12] Netfilter. The netfilter.org project. 2012.

Validación por la Comunidad Docente de una Metodología de Aprendizaje Activo para Cursos de Programación

Iria Estévez-Ayres, Carlos Alario-Hoyos, Mar Pérez-Sanagustín, Raquel M. Crespo-García, Derick Leony, y Hugo A. Parada G.
Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid
Avda. de la Universidad, 30, 28911, Leganés, Madrid, España
{ayres, calario, mmpsanag, rcrespo, dleony, hparada}@it.uc3m.es

***Resumen*—En este artículo se presenta y evalúa una metodología para cursos de programación, basada en el aprendizaje activo y el aprendizaje basado en proyectos. Esta metodología se centra en el trabajo continuo, día a día, del alumno. Por un lado, ofrece pautas para que los alumnos organicen su tiempo, promoviendo el autoaprendizaje y el trabajo individual. Por otro, durante el proyecto los alumnos desarrollan sus capacidades de trabajo en equipo, fomentando el desarrollo de competencias transversales como el aprendizaje colaborativo. La metodología descrita se ha aplicado durante varios cursos en una asignatura de programación en C de segundo curso de los cuatro grados de Ingeniería de Telecomunicaciones. Para poder evaluar, ajustar y mejorar el proceso de enseñanza-aprendizaje propuesto, se utilizan mecanismos de realimentación y seguimiento del alumnado y del profesorado. En este artículo, la implantación de la metodología es evaluada por 40 profesores de distintas universidades españolas que imparten asignaturas en cursos de ingeniería, con objeto de validar su aplicabilidad en otros contextos.**

***Palabras Clave*—Aprendizaje Activo, Metodología, Curso de Programación, Arquitectura de Sistemas.**

I. INTRODUCCIÓN

La demanda de desarrolladores de software ha experimentado un importante crecimiento en los últimos años [1]. En la industria del desarrollo software, caracterizada por el cambio constante debido a la aparición frecuente de nuevas herramientas y métodos de desarrollo, se requieren profesionales cada vez más preparados para adaptarse al cambio, proactivos, críticos, con habilidades como el liderazgo y con una gran capacidad de trabajo en equipo [2].

Para formar profesionales para esta industria las metodologías clásicas de enseñanza, normalmente basadas en la combinación de presentaciones de conceptos teóricos y ejercicios prácticos aislados, no son suficentes [1]. La aplicación de metodologías como el aprendizaje activo [3] y el aprendizaje basado en proyectos [4] proporcionan una solución parcial para cubrir estas necesidades. Sin embargo, estas metodologías presentan algunas limitaciones. Por una parte, no son capaces de capturar la diversidad de conocimientos previos, ritmos de trabajo y objetivos de aprendizaje característicos de los grupos de los primeros cursos de formación universitaria. Por otra, estas metodologías no incluyen técnicas ni mecanismos para hacer un seguimiento cercano de los alumnos y detectar así problemas como la pérdida de interés o los conflictos del trabajo en equipo [5]. En este contexto, es necesario proponer nuevas metodologías para la enseñanza del desarrollo software capaces de capturar e integrar las necesidades de la industria y superar estas limitaciones.

Con este objetivo, en este artículo se propone una metodología basada en el aprendizaje activo y el aprendizaje basado en proyectos para cursos de programación en un entorno universitario. La metodología propuesta permite adaptar de forma dinámica aspectos principales de una asignatura como temas, actividades de aprendizaje, configuración de grupos y actividades de evaluación. Esta metodología se ha aplicado en la asignatura Arquitectura de Sistemas (AS)[1]. Esta asignatura tiene como objetivo principal aprender a programar en lenguaje C, y se imparte de forma transversal en el segundo curso de los grados en castellano y bilingüe (inglés) de Ingeniería Telemática, Sistemas Audiovisuales, Sistemas de Comunicaciones y Tecnologías de las Telecomunicaciones de la Universidad Carlos III de Madrid. Además de mostrar cómo se aplica la metodología propuesta en un contexto real, este artículo presenta los resultados de una encuesta sobre su aplicabilidad a otros contextos, que ha sido completada por 40 docences de cursos de ingeniería de 6 universidades españolas distintas.

Este artículo se organiza como se especifica a continuación. Primero se describe la asignatura AS (sección II) y cómo se ha aplicado la metodología propuesta en este contexto (sección III). A continuación se presentan los resultados obtenidos de la validación de la metodología por un grupo de docentes del ámbito de ingenierías (sección IV), y se discuten las decisiones tomadas, con el fin de refinar la metodología (sección V). Finalmente, la sección VI resume las principales contribuciones y conclusiones de este trabajo.

II. DESCRIPCIÓN DE LA ASIGNATURA

La asignatura Arquitectura de Sistemas (AS) se imparte en el segundo año de los cuatro grados de Ingeniería de Telecomunicaciones en la Universidad Carlos III de Madrid, en español y en inglés. El número aproximado de alumnos matriculados cada edición oscila entre 200 y 275 y la plantilla docente la forman cada año entre 6 y 9 profesores.

Tal y como se detalla en [6], los cuatro objetivos específicos a cubrir por la asignatura son:

[1] http://www.it.uc3m.es/labas

1. diseñar y desarrollar aplicaciones en el lenguaje de programación C;
2. aplicar técnicas de trabajo en equipo para desarrollar una aplicación en un dispositivo móvil;
3. usar herramientas de desarrollo de aplicaciones como el controlador de versiones Subversion[2] y máquinas virtuales, entre otras;
4. desarrollar técnicas de autoaprendizaje.

La asignatura se organiza en lecciones *magistrales* o de grupos grandes y en clases *prácticas* de laboratorio o de grupos reducidos. Las primeras se realizan en aulas convencionales y las segundas se llevan a cabo en salas con ordenadores. Cada grupo, tanto magistral como reducido, tiene un profesor responsable. La asignatura sigue un sistema de evaluación continua pero los alumnos tienen la opción de hacer un examen final si no desean seguir este esquema.

III. METODOLOGÍA APLICADA EN AS

Esta metodología toma como uno de sus pilares fundamentales el aprendizaje activo. Los estudiantes que cursan AS se encuentran, generalmente por primera vez, con un curso que les exige trabajar de forma autónoma, con la guía del profesor como material de referencia, pero sin tantas clases teóricas y mucha más dedicación de trabajo individual previo a la clase y de trabajo colaborativo durante y después de la clase. Así, motivar, convencer e implicar a los estudiantes es uno de los grandes retos de cada edición, y en cada una de ellas encontramos que los estudiantes pasan por prácticamente todas las fases descritas por Woods en [7]: (1) conmoción; (2) rechazo; (3) resistencia y retirada; (4) rendición y aceptación; (5) esfuerzo y exploración; (6) retorno de la confianza en sí mismo; (7) integración y éxito.

Para establecer un vínculo con el futuro mercado laboral, la asignatura de AS se estructura durante todo el curso alrededor de un escenario que simula una situación de trabajo real. Desde el primer día, se explica a los alumnos que forman parte de un departamento de diseño de aplicaciones (objetivo 1) de una empresa ficticia, donde deberán trabajar en equipo (objetivo 2) con distintas herramientas (objetivo 3). Tal y como ocurre en una empresa, aunque hay cursos de formación (clases magistrales en el contexto de AS), los empleados tendrán que usar manuales tanto en castellano como en inglés como documentación básica (objetivo 4) para realizar algunas las tareas asignadas. A partir del escenario se refuerza la percepción de que la materia y los problemas que se plantean durante la asignatura tienen una relación directa con el entorno laboral.

Además, en AS se considera prioritario mantener a los alumnos informados sobre las decisiones metodológicas principales tomadas en el desarrollo la asignatura. Con este objetivo se aplica un principio de transparencia que incluye desde la presentación de la metodología docente al inicio del curso (con referencias que avalan dicha metodología), hasta el uso de rúbricas en la evaluación, pasando por la definición de un calendario detallado de sesiones con todo el material disponible al comienzo de la asignatura.

A continuación se detallan los aspectos clave de la metodología del curso, como son el aprendizaje activo (apartado III-A), el trabajo colaborativo (apartado III-B), las herramientas de desarrollo empleadas (apartado III-C), el sistema de evaluación (apartado III-D) y la realimentación sobre la metodología por parte de alumnos y cuerpo docente (apartado III-E).

III-A. *Aprendizaje Activo*

Para promover el aprendizaje activo, los alumnos pueden acceder al cronograma de la asignatura desde el inicio del cuatrimestre[3], así como a la descripción detallada de las actividades que se les pedirán cada semana. Además, se les indica el tiempo que se espera que dediquen a la asignatura semana a semana. Por otra parte, los alumnos tienen disponible todo el material de la asignatura en forma de apuntes elaborados por los profesores desde el inicio de curso[4]. De esta manera se anima a los alumnos a que se organicen desde el principio y que tengan una idea de los objetivos e hitos del curso.

III-A1. Esquema de trabajo semanal: en la descripción de la asignatura[5] se sugiere a los estudiantes un esquema de trabajo (Fig. 1). Éste consta de dos sesiones de estudio intercaladas por una de consultas personalizadas al profesor para resolver dudas.

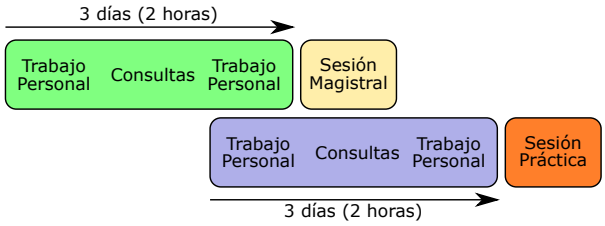


Figura 1. Esquema de trabajo semanal.

Para cada sesión se publican actividades previas y actividades a realizar en clase, con el tiempo estimado que requieren por parte del alumno para su resolución. Las actividades previas guían a los alumnos a través de los apuntes, indicando qué ejercicios o programas deben realizar en cada momento, así como qué apartados de teoría de los apuntes deben leer antes de cada sesión. La descripción de la actividad incluye una lista de recursos (enlaces a documentos auxiliares), un plan de trabajo, un criterio de evaluación y un tiempo estimado de resolución.

Como evaluación formativa de las tareas previas se suelen incluir ejercicios de autoevaluación y mencionar el uso que se va a hacer con los resultados durante la siguiente sesión. Con este esquema se pretende que los estudiantes asistan a clase con el trabajo realizado y así sacar el máximo partido a las sesiones tanto magistrales y prácticas.

III-A2. Metodología docente: al principio de la clase magistral, el profesor explica aquellos aspectos más importantes de la teoría. Después resuelve las dudas de los alumnos sobre las actividades previas, intercalando ejercicios, unas veces resueltos por el profesor, otras por los alumnos en grupos de trabajo (que se corrigen y explican en pizarra al final de cada clase).

[2]http://subversion.apache.org

[3]http://www.it.uc3m.es/labas/info/material_es.html
[4]http://www.it.uc3m.es/labas/course_notes/index_es.html
[5]http://www.it.uc3m.es/labas/info/syllabus_es.html

En el caso de las sesiones de prácticas, el profesor explica las actividades a desarrollar, y resuelve grupo a grupo las dudas que hayan surgido durante la resolución de las actividades previas. Esto sucede mientras el resto de grupos trabajan en las actividades determinadas para la sesión.

III-A3. Uso del foro: las actividades de los apuntes que no han sido definidas como actividades previas se proponen como ejercicios en el foro. Estos ejercicios se corrigen por parte del profesor si y sólo si los alumnos aportan previamente una solución en el foro. Dicha solución se discute en el foro de forma colaborativa. En el caso de ejercicios relacionados con la programación, se proponen además correcciones o mejoras al código propuesto por los estudiantes. Todas las dudas planteadas por los alumnos en el foro se tratan en un máximo de 24 horas.

III-A4. Atención al alumnado: además del horario de atención obligatorio al alumnado dispuesto por normativa de la universidad (el cual se dedica a tutorías individuales), algunos profesores de los grupos magistrales han incluido, de forma voluntaria, tutorías grupales dentro de su metodología. Los alumnos acuden más a estas tutorías grupales, en las que se resuelven dudas y ejercicios, que a las tutorías individuales y, en general, son bien recibidas por parte del alumnado.

III-B. Trabajo colaborativo

Uno de los objetivos transversales de AS es que los alumnos desarrollen capacidades y competencias de trabajo en equipo. Con este objetivo, se introdujo un trabajo en grupo en la parte más práctica de la asignatura: el laboratorio. Durante el curso, en las sesiones prácticas, el trabajo de los alumnos se organiza de la siguiente manera:

- en la primera mitad del curso, mientras toman contacto con el lenguaje C y aprenden sus fundamentos, trabajan en parejas, formadas libremente por los estudiantes;
- en la segunda mitad, el aprendizaje se basa en proyecto, y el trabajo se realiza en equipos de cuatro personas formados por el profesor.

III-B1. Formación de los equipos: una de las metas más importantes de AS es preparar al alumnado para su futuro profesional, en el cual tendrán que trabajar con personas que no conocen previamente, solucionar de forma proactiva los conflictos que puedan surgir y ponerse de acuerdo para conseguir terminar en tiempo y forma un determinado proyecto. Un estudio de Deibel, K. [8] sostiene que, en grupos de alumnos formados por el profesor, se establece una interacción mayor entre los alumnos y se aprende más que en equipos formados por los propios alumnos. Tomando como referencia este estudio, la formación de los grupos en AS la realiza el profesorado, basándose en las notas de los alumnos obtenidas durante la primera mitad del curso y agrupando a aquéllos con notas similares.

III-B2. Puesta en marcha y seguimiento: la primera sesión del trabajo en equipo se dedica a describir qué se entiende por trabajo en equipo, a enfatizar la dificultad de conseguir un rendimiento elevado y a anticipar los posibles conflictos que suelen aparecer conforme se avanza en esta fase y reducir así el número de situaciones que requieren la intervención de la plantilla docente. En relación a este último objetivo, se incluye como parte de las lecturas previas un extracto de un artículo que trata sobre posibles conflictos [9].

Durante la primera sesión se analizan los distintos roles que pueden aparecer en un equipo disfuncional (adaptados del trabajo [10]): "el jeta" (*hitchhiker*), "el manta" (*couch potato*) [9], miembros del equipo que se intentan aprovechar de una manera más o menos manipuladora del resto y "la locomotora", aquel alumno aventajado que se carga con todo el trabajo y no comparte sus decisiones con los demás. También se analiza qué debería hacer cada equipo para funcionar de manera correcta y se dan unas pautas sobre cómo enfrentarse, si se da el caso, con estos problemas.

Típicamente, el trabajo colaborativo implica roces y conflictos más o menos graves y, aunque los alumnos parten de que no van a tener problemas con sus compañeros, al final siempre acaba habiendo algún tipo de malentendido. Por este motivo, cada semana se les pasa un cuestionario individual anónimo donde sólo tienen que indicar el grupo de trabajo en el que están y valorar con una escala Likert-5 la intensidad de los siguientes conflictos en el equipo (0 no hay, 4 grado máximo):

- *un jeta*. Uno o más miembros del equipo afirman que su compromiso con el equipo es total, pero su desempeño es siempre bajo y con alguna excusa.
- *no integración*. Algún miembro no se integra porque es difícil hablar con él/ella.
- *una locomotora*. Uno o más miembros del equipo dominan la materia más que el resto y, además, les molesta que los demás no sigan su ritmo. El resto del equipo está molesto porque no se les toma en cuenta.
- *diferentes objetivos*. Existen diferentes perspectivas sobre cómo llevar a cabo el proyecto, pudiendo aparecer malestar mutuo con el tiempo.

Estos cuestionarios cortos son de gran utilidad para detectar los conflictos que surgen y poder ayudar a los alumnos a resolverlos.

III-C. Herramientas de desarrollo

A lo largo de la asignatura, los alumnos utilizan diversas herramientas de desarrollo:

- máquina virtual. Proporciona a los alumnos el mismo entorno de trabajo que en el laboratorio, sin obligarles a instalar Linux, ni todas las herramientas necesarias.
- gestor de versiones (subversion). El uso de esta herramienta en la asignatura cumple dos funciones. Por una parte, familiariza a los estudiantes con entornos de trabajo colaborativo semejantes a los que pueden encontrar en una empresa y les prepara para otras asignaturas posteriores que usan estas herramientas. Por otra parte, facilita la corrección de las pruebas de laboratorio y poder ofrecer realimentación a los alumnos de los errores cometidos. Además, facilita la gestión de los directorios de trabajo de los alumnos y proporcionarles a todos los mismos códigos fuente que se tomarán como referencia.

III-D. Sistema de evaluación

AS consta de 14 pruebas, incluyendo tanto individuales como grupales. La evaluación se organiza en dos partes. La primera parte corresponde al 30 % de la nota global de la asignatura y comprende:

- pruebas individuales: 2 exámenes de programación de 10 minutos en papel (un pequeño fragmento de código) y 2 de programación de 30 minutos, también en papel.
- pruebas por parejas: 3 tests en papel de 10 minutos en el laboratorio y 1 entrega de código en el laboratorio por parejas.

La segunda parte de la asignatura, correspondiente al aprendizaje basado en proyecto, tiene un peso del 70 % en la nota global de la asignatura e incluye:

- pruebas individuales: 2 exámenes de programación de 1 hora en papel y 1 examen individual de 30 minutos sobre el proyecto en el laboratorio.
- pruebas en equipo: entregas parcial y final del proyecto, y presentación oral del trabajo realizado.

Este formato de evaluación concede más peso a la parte individual frente a la parte en grupo (donde la nota es compartida), para evitar que un alumno, gracias al trabajo de sus compañeros, apruebe sin tener conocimientos de la asignatura. Las pruebas iniciales obligan al estudiante a trabajar diariamente desde el principio de curso, aunque no tienen mucho peso en la nota final para evitar abandonos al comienzo de la asignatura.

III-D1. Información de progreso: los alumnos disponen de información actualizada acerca de cómo progresan en la asignatura y de cómo se evalúa dicho progreso. Así, se establece un máximo de tiempo de una semana para la corrección de cada prueba y el uso de rúbricas tanto en los exámenes escritos (se les envía a los alumnos conjuntamente con la nota de cada examen) como en el proyecto (disponible para los alumnos desde el primer día de la asignatura). Además, las entregas de laboratorio se corrigen sobre el código fuente de los alumnos y se les da realimentación indicándoles sus errores y sugerencias de cómo evitarlos. Las rúbricas, además de fomentar la transparencia en la evaluación, ayudan a homogeneizar los criterios de evaluación de la plantilla docente, mejorando la coordinación de la misma.

III-E. Realimentación sobre la metodología

Como parte de la metodología, el profesorado reflexiona constantemente sobre la calidad del curso, no sólo al finalizar cada edición, sino también durante su ejecución. Esta reflexión continua tiene como propósito adaptar sobre la marcha aspectos clave de la asignatura (p.ej. temas y actividades de aprendizaje), reforzando las carencias detectadas en los alumnos. Para que la reflexión y las decisiones tomadas sean efectivas se debe consultar a todos los actores involucrados en el proceso de enseñanza-aprendizaje. Así, durante el curso se realizan cuestionarios dirigidos tanto al alumnado como al profesorado; y al finalizar el curso se analizan los resultados de las encuestas oficiales de la universidad.

III-E1. Por parte de los alumnos: tres veces durante el curso se les ofrece la posibilidad de comentar, de forma totalmente anónima, qué puntos mejorarían y qué defectos ven en la asignatura a través de un breve cuestionario web [11]. El formulario solicita que se describa el aspecto crítico más positivo y el más negativo de lo que va de curso (o desde el formulario anterior). Las respuesta se limitan a 300 caracteres para forzar a los estudiantes a pensar detenidamente sobre uno de los múltiples aspectos y expresarlo de forma concisa. Estas respuestas sirven, por ejemplo, para detectar carencias en la formación previa del alumnado, partes a mejorar en el material de la asignatura o excesiva carga de trabajo de los alumnos. Además, los cuestionarios sirven para que los estudiantes perciban la implicación del profesorado, siendo ésta otra forma más de aumentar su motivación, según la opinión de los propios estudiantes.

III-E2. Por parte de la plantilla docente: al final de cada edición se pide a la plantilla docente que indique, de forma anónima, su grado de satisfacción con la metodología de la asignatura así como si, desde su punto de vista, se han alcanzado los objetivos planteados.

III-E3. Reuniones metodológicas de la plantilla docente: se llevan a cabo varias reuniones con el objetivo de analizar los cuestionarios anteriores y tomar decisiones.

- Durante el curso la plantilla docente se reúne al menos 3 veces para la toma de decisiones acerca de la marcha de la asignatura. Durante estas reuniones, los resultados de los cuestionarios al alumnado se revisan y se analiza si se deben tomar medidas correctivas y de qué tipo.
- Al finalizar el curso se realizan varias reuniones donde se revisan los resultados de los cuestionarios al alumnado y al profesorado de forma global conjuntamente con los resultados de las encuestas oficiales de la universidad, y se estudia la efectividad de las medidas tomadas. También se deciden las mejoras a adoptar en la siguiente edición, tanto en el material como en la metodología empleada.

IV. VALIDACIÓN DE LA METODOLOGÍA

Para validar cómo se podría aplicar esta metodología a otras asignaturas de ingeniería, se ha distribuido un cuestionario a docentes completamente ajenos a AS de distintas universidades españolas. Un total de 40 docentes han cumplimentado la encuesta, procedentes de 6 universidades (Universidad Carlos III de Madrid, Universidad de Jaén, Universidad de Valladolid, Universidad Politécnica de Madrid, Universidade de Vigo y Universitat Pompeu Fabra). Los encuestados pertenecen al área de conocimiento de Ingenierías (92,5 %) y Ciencias (7,5 %), donde la gran mayoría, 80 %, imparte asignaturas directamente relacionadas con la programación.

La mayoría de los encuestados tienen una amplia experiencia docente. El 77,5 % lleva ejerciendo como docente más de 6 años (Fig. 2). Además, gran parte de los encuestados imparten asignaturas de una complejidad organizativa y un tamaño similares a los de AS (Fig. 3). La mayoría de los encuestados imparte docencia en asignaturas con un gran número de alumnos matriculados (el 30 % en asignaturas con más de 160 estudiantes y el 28 % en asignaturas de entre 80 y 160 estudiantes) y, además, en un 58 % de los casos con más de 3 profesores.

El cuestionario plantea una serie de preguntas a los docentes en una escala Likert-6, ofreciéndoles la posibilidad de no contestar o de indicar que la pregunta no es aplicable a las asignaturas que el encuestado imparte. A continuación, se presentan los resultados de cada uno de los aspectos sobre los que se ha preguntado a los docentes, así como su opinión global de la metodología.

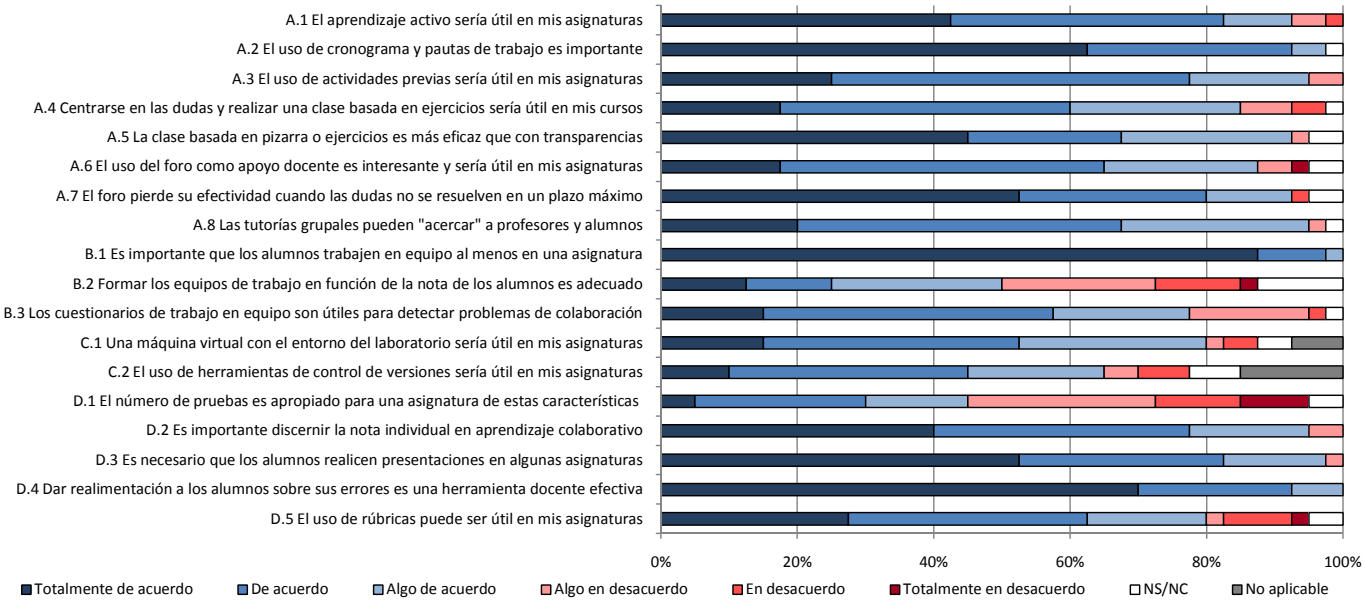


Figura 4. Opiniones sobre la metodología de aprendizaje.

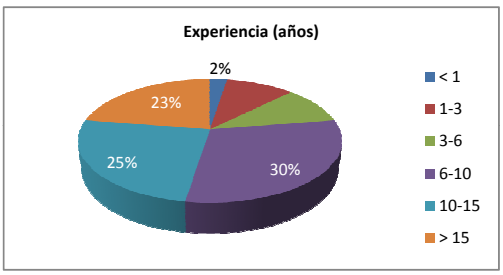


Figura 2. Experiencia docente de la población de docentes encuestada.

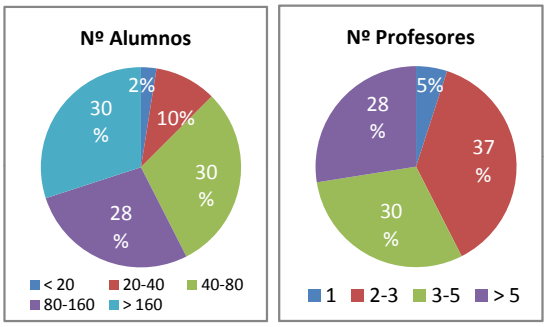


Figura 3. Número de alumnos y profesores en las asignaturas impartidas.

IV-A. Resultados sobre el aprendizaje activo

Tal y como se muestra en las respuestas a las preguntas del bloque A de la Fig. 4, los encuestados respaldaron de forma mayoritaria la metodología de aprendizaje activo seguida en esta asignatura.

Se observa que el 92 % de los profesores opinaron que el aprendizaje activo puede ser beneficioso para las asignaturas que imparten (Fig. 4, A.1), con tan sólo 3 respuestas *en desacuerdo* o *algo en desacuerdo*. Si se analiza según el número de alumnos por asignatura, todos los profesores con asignaturas de más de 80 alumnos consideraron beneficiosa esta metodología para sus asignaturas.

Asimismo, la totalidad de los profesores que se pronunciaron estuvieron de acuerdo en la importancia de proporcionar a los alumnos un cronograma y unas pautas de trabajo (Fig. 4, A.2).

Con respecto al esquema de trabajo semanal, el 95 % de los profesores consideraron que el planteamiento de proporcionar a los alumnos unas tareas previas a cada sesión puede ser beneficioso para las asignaturas que imparten (Fig. 4, A.3), estando únicamente 2 de ellos *algo en desacuerdo*.

En relación a la pregunta sobre la dinámica de las clases, sólo un profesor se manifestó *algo en desacuerdo* con la afirmación de que la clase basada en pizarra o en ejercicios es más eficaz que basar la docencia en transparencias (Fig. 4, A.5). De la misma manera, un 85 % manifestó que centrarse en dudas y realizar una clase basada en ejercicios podría ser de utilidad en las asignaturas que imparten (Fig. 4, A.4).

El planteamiento del foro como herramienta de apoyo docente propuesto en la metodología fue considerado interesante y la mayoría de los docentes consultados (87, 5 %) consideraron que podría ser de utilidad en las asignaturas que imparten (Fig. 4, A.6). Todos los profesores con asignaturas con más de 80 alumnos se mostraron favorables a esta afirmación. Asimismo, excepto un profesor, todos coincidieron en que si las dudas planteadas en un foro no se resuelven en un plazo máximo, el foro pierde su efectividad (Fig. 4, A.7).

Finalmente, preguntados por la utilidad de las tutorías grupales como ayuda para "acercar" a profesores y alumnos y que éstos pierdan su "miedo" a hacer preguntas, un 95 % de las respuestas fueron positivas (Fig. 4, A.8).

IV-B. Resultados sobre el trabajo colaborativo

Todos los docentes encuestados consideraron importante que, en al menos una asignatura del currículum, los estudiantes trabajen en grupo (Fig. 4, B.1).

IV-B1. Formación de los equipos: El criterio utilizado para la formación de equipos ha sido uno de los puntos más criticados de esta metodología. Las respuestas de los profesores sobre la adecuación de este criterio, estaban bastante

divididas (Fig. 4, B.2). El 50 % valoró este criterio de forma positiva, mientras que un 37,5 % expresó disconformidad y un 12,5 % no se pronunció. Sin embargo, se observa que un 47,5 % de las respuestas se acumulan en torno a *algo de acuerdo* (25 %)/*algo en desacuerdo* (22,5 %) y sólo un 2,5 % estaba *totalmente en desacuerdo*.

Si el análisis se realiza con respecto al número de alumnos de las asignaturas que imparten los encuestados, se puede ver que aquéllos con un mayor número de alumnos (con más de 160 alumnos) son los que se manifiestaron más a favor de este criterio (estando a favor un 66,6 % y en contra un 25 %), mientras que el profesorado que imparte en asignaturas con menos número de alumnos está muy dividido (42,86 % con respuestas positivas en diferentes grados, la misma cifra con respuestas negativas y un 14,28 % que no se pronuncia).

Si el análisis se realiza por rangos de experiencia docente no hay diferencias significativas. Sí se observa que las respuestas están más polarizadas cuanta menos experiencia tiene el encuestado (de los encuestados con menos de 6 años de experiencia, un 44,4 % estaban *de acuerdo* o *totalmente de acuerdo*, un 22,2 % *en desacuerdo* y un 11,1 % *algo en desacuerdo*) y que tienden más a no posicionarse en los extremos cuantos más años de experiencia se acumulan (un 58,05 % en el medio, un 19,35 % *de acuerdo* y un 12,9 % *en desacuerdo*).

IV-B2. Puesta en marcha y seguimiento: Un 77,5 % se pronunció positivamente a la hora de valorar la utilidad de los cuestionarios de seguimiento como mecanismo para detectar problemas en el equipo, mientras que un 20 % valoró estos cuestionarios de forma negativa (Fig. 4, B.3). Es interesante señalar que si se discrimina por número de alumnos en las asignaturas impartidas, aquellos profesores con un mayor número de alumnos (más de 160) vieron de forma positiva la utilidad de los cuestionarios; los profesores con asignaturas de entre 80 y 160 alumnos y los profesores con menos de 40 alumnos estaban la inmensa mayoría en posiciones favorables también (80 % en los dos casos). Sin embargo, los profesores con un número de alumnos entre 40 y 80 se encontraban totalmente divididos, con sólo la mitad valorando positivamente el uso de los cuestionarios de seguimiento.

IV-C. Resultados sobre las herramientas de desarrollo

La encuesta incluía preguntas acerca de la utilidad de la máquina virtual y el uso de un controlador de versiones. Con respecto al uso de la máquina virtual (Fig. 4, C.1), 3 profesores indicaron que no era aplicable a sus asignaturas. De los 37 restantes, un 86,49 % vio positivo el uso de esta herramienta, un 8,1 % contestó de forma negativa y un 5,4 % no se pronunció. Asimismo, preguntados por la utilidad en las asignaturas que imparten del uso de herramientas de control de versiones (Fig. 4, C.2), 6 indicaron que no era aplicable a su asignatura. De los restantes, un 64,71 % expresó opiniones positivas, un 14,71 % opiniones negativas (de los cuales, el 20 % no impartía asignaturas relacionadas con la programación) y un 8,82 % no se pronunció.

IV-D. Resultados sobre el sistema de evaluación

Con respecto al sistema de evaluación, el punto donde se pueden encontrar opiniones más dispares es el número de pruebas en una asignatura (Fig. 4, D.1): el 45 % valoró positivamente el número de pruebas, el 50 % se pronunció de forma negativa (con un 13 % *en desacuerdo* y un 10 % *totalmente en desacuerdo*) y el 5 % restante no expresó su opinión.

Sin embargo, un 95 % de los docentes preguntados coincidieron de forma positiva en que, en asignaturas donde se trabaje de forma colaborativa, es importante discernir entre la nota individual y la nota de equipo, dándole más peso a la nota individual (Fig. 4, D.2). El 5 % que se manifestó algo en desacuerdo estaba formado por docentes con entre 6 y 10 años de experiencia.

Algo similar ocurre con la importancia de tener una sesión de presentación donde los alumnos presenten de forma clara sus ideas y decisiones (Fig. 4, D.3), donde la mayoría de los docentes se manifestaron a favor (un 97 %), con más de la mitad *totalmente de acuerdo*.

Todos los docentes consideraron que la realimentación a los alumnos, indicándoles sus errores y cómo corregirlos, es una herramienta docente efectiva (Fig. 4, D.4). Además, la mayoría de los encuestados, un 80 %, mostró su acuerdo con que el uso de rúbricas en sus asignaturas pueda ser de utilidad (Fig. 4, D.5), frente a un 16 % que vio la idea de forma negativa. El grupo más entusiasta son los profesores con menos experiencia (menos de 6 años), con un 88,89 % a favor de la utilidad de esta herramienta de corrección, frente a un 77,42 % en el caso de los profesores con más experiencia.

IV-E. Realimentación sobre la metodología

Cuando se pregunta a los docentes por el control de calidad realizado en la asignatura, se puede apreciar una opinión muy favorable acerca de todos los mecanismos implementados en la misma (Fig. 5).

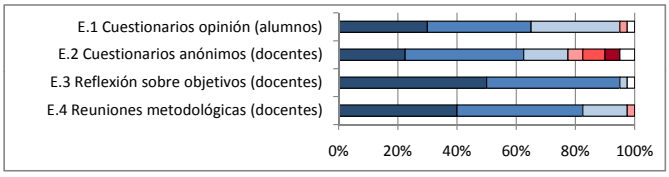


Figura 5. Opiniones acerca de la realimentación sobre la metodología.

IV-E1. Por parte de los alumnos: El 95 % de los profesores consideró que este tipo de cuestionarios en medio del cuatrimestre sobre la marcha de la asignatura pueden ser de utilidad para las asignaturas que imparte (Fig. 5, E.1). Analizando las respuestas tanto por experiencia docente como por número de alumnos en asignaturas, se pudo observar que la distribución de respuestas se mantiene.

IV-E2. Por parte de la plantilla docente: Si bien la inmensa mayoría se mostró favorable con la necesidad de una reflexión por parte de la plantilla acerca de si se han alcanzado los objetivos del curso a su finalización (Fig. 5, E.3), hay diversidad de opiniones acerca de la utilidad del uso de cuestionarios anónimos a la plantilla en las asignaturas que imparten (Fig. 5, E.2). La mayoría consideró que pueden ser útiles (un 77,5 %), aunque un 17,4 % se mostró contrario. Se observa que las respuestas de todos los docentes con menos experiencia (menos de 6 años) fueron favorables al uso de cuestionarios anónimos, mientras que la división de

opiniones se da en el grupo de docentes con más experiencia (predominando la respuesta favorable).

IV-E3. Reuniones metodológicas: prácticamente todos los profesores (97,5 %) han sido positivos al evaluar la necesidad de reuniones metodológicas para la buena marcha de una asignatura (Fig. 5, E.4). Cabe destacar que los profesores con menos experiencia (menos de 6 años) fueron los más entusiastas con la idea, con un 55,5 % *totalmente de acuerdo* y un 44,5 % *de acuerdo*; mientras que entre los profesores más experimentados se podían encontrar valoraciones más variadas (con un 35,5 % *totalmente de acuerdo*, un 38,71 % *de acuerdo*, un 19,35 % *algo de acuerdo* y un 3,2 % *algo en desacuerdo*).

IV-F. Valoración general sobre la metodología aplicada

Como punto final al cuestionario, se les pidió a los docentes valorar la posible utilidad de la metodología en sus asignaturas, así como la capacidad de la misma para aumentar la motivación del alumnado (Fig. 6). Se puede ver que la mayoría consideró que podría ser de utilidad en sus asignaturas así como que podría conseguir aumentar la motivación e implicación del alumnado. Es interesante señalar que tan sólo un caso se mostró desfavorable con ambas afirmaciones y que todos aquéllos que contestaron que estaban *algo en desacuerdo* con que la metodología pudiese aumentar la implicación y motivación de los estudiantes, estaban, a su vez, *algo de acuerdo* con que podría ser de utilidad en las asignaturas que imparten. A su vez, un 66,6 % los que estaban *en desacuerdo* o *algo en desacuerdo* con la utilidad de esta metodología en sus asignaturas, estaban *de acuerdo* con que ésta podía aumentar la motivación de los estudiantes.

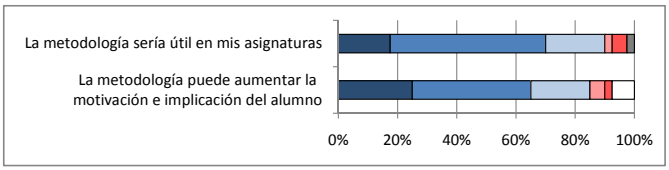


Figura 6. Valoración general sobre la metodología.

V. DISCUSIÓN

En el cuestionario se aprecia que, si bien, la mayoría de los profesores encuestados respaldaron la metodología presentada, hubo tres grandes puntos en los que existían discrepancias: el criterio de formación de los equipos, el número de pruebas de la asignatura y el uso de rúbricas.

Con respecto al criterio de formación de los equipos en la segunda parte de la asignatura, en anteriores ediciones se realizaron pruebas implementado dos criterios distintos. Ambos ordenan a los alumnos según sus notas de mayor a menor:

- Criterio *homogeneización de equipos*: divide la clase en cuatro cuartiles. Cada equipo se forma tomando un individuo de cada cuartil, resultando así grupos homogéneos.
- Criterio *homogeneización de componentes dentro de un equipo*: los equipos se forman con alumnos de notas similares.

La implementación del primer criterio produjo situaciones no deseadas y por ello fue descartado. Por ejemplo, en muchos equipos los alumnos con más conocimientos no dejaban trabajar a aquéllos que, con menos conocimientos, querían aprender, y determinados alumnos fueron a remolque de los miembros del grupo que más conocimientos tenían. Otras consecuencias relevantes que aparecieron como resultado del criterio de formación de grupos se detallan a continuación:

- Al definir equipos homogéneos (primer criterio), todos ellos demandaban aproximadamente la misma cantidad de atención por parte del profesor, no pudiendo atender a todos durante el tiempo de clase. Por el contrario, la implementación del segundo criterio consiguió que los grupos más avanzados demandaran menos tiempo de ayuda durante las clases, pudiendo dedicar el profesor más tiempo a los grupos con problemas.
- La calidad media de los proyectos fue superior cuando se formaron grupos homogéneos entre sí (primer criterio) en comparación con los resultados de los grupos con componentes similares (segundo criterio). Sin embargo, el aprendizaje individual de la asignatura en media fue inferior, tomando como referencia los últimos exámenes individuales de la asignatura.

Por estos motivos, en la asignatura AS se aplica actualmente el segundo criterio en la formación de los equipos, el cual intenta, por una parte, agrupar a alumnos con objetivos comunes y, por otra, maximizar el tiempo de profesor con los equipos con mayor necesidad de supervisión en los laboratorios. Esta decisión se ha corroborado mediante cuestionarios realizados a los alumnos, en los que se muestra que la gran mayoría apoya esta decisión, debido a que en general perciben que un solo profesor en el laboratorio es insuficiente para cubrir las necesidades de todos los alumnos. Entre los comentarios de los alumnos también se valora positivamente el hecho de compartir equipo con alumnos con objetivos similares.

En esta parte del curso, se podría haber implementado un esquema similar al usado por Valero-García y García Zubia en [12], donde una vez formados los equipos, en la primera sesión se ponen en común tanto los objetivos individuales de cada integrante como sus horarios, y si los objetivos no son compatibles, se realizan cambios en los equipos. Se decidió no seguir este esquema para evitar poner en peligro el objetivo principal que es el de aprender a trabajar en grupo con desconocidos y lidiar en un entorno (controlado) con los potenciales conflictos que puedan surgir.

Con respecto al número de pruebas en AS, si bien es cierto que dicho número es elevado, AS ha ido evolucionado a este respecto: de tener 17 pruebas durante todo el curso en las que el peso de la nota estaba uniformemente distribuido, a tener 14 con el peso más cercano hacia el final de la asignatura.

Como ya se explicó previamente, se mantuvieron una serie de pruebas iniciales con poco peso pues, al hacerlas desaparecer en anteriores ediciones, se detectó que muchos estudiantes no empezaban a preparar la asignatura hasta la primera prueba y, en ese momento, la asignatura estaba lo suficientemente avanzada como para que muchos abandonasen. Por otra parte, si estas pruebas tuviesen mucho peso, también se correría el riesgo de que los alumnos abandonasen, al poder perder muchos puntos.

Como consecuencia de la realimentación de la comunidad docente, se está trabajando para reducir aún más el número de

pruebas sin perder la vertiente positiva asociada a introducir algunas al inicio de la asignatura.

Asimismo, la carga de corrección sobre el profesorado se ha suavizado bastante desde la primera edición de la asignatura, al incluir las rúbricas en el proceso de evaluación, no sólo para el proyecto, sino también de forma interna (aunque después se publica) para cada prueba.

Si bien las rúbricas suponen un trabajo inicial para el autor de la prueba, reduce la carga global de trabajo al proporcionar al profesorado una guía para la corrección y ayudar a la coordinación entre los profesores. Además, contribuye a que los alumnos perciban un criterio de evaluación único y homogéneo, independientemente del profesor que realiza la corrección, mejorando la transparencia de la asignatura y disminuyendo la percepción de arbitrariedad que pudiera tener el alumnado.

VI. CONCLUSIONES

Tras implantar la metodología propuesta en una asignatura real y analizar los resultados de su validación por profesores externos, puede concluirse que una amplia mayoría de los docentes ve positiva su aplicación en asignaturas de programación y equivalentes en ingeniería.

Es interesante destacar que los profesores más receptivos a aplicar esta metodología son aquéllos con menor experiencia en el campo y, aquéllos que imparten asignaturas con características similares a las planteadas en este estudio.

Dos de los puntos más criticados por los profesores son la política de formación de grupos y el uso de rúbricas de evaluación. Como trabajo futuro se plantea incorporar a la metodología nuevos criterios de formación de grupos y mecanismos para sistematizar las rúbricas de corrección y así aliviar la carga del profesorado. Asimismo, se planea reducir aún más el número de pruebas de evaluación para reducir la carga de trabajo del alumnado.

Finalmente, y con el fin de comprobar la aplicabilidad de esta metodología a otros campos se espera colaborar con docentes de otras universidades para su implantación en otras asignaturas de ingeniería. Esto permitiría refinar la metodología analizando qué aspectos son fácilmente extrapolables a otros escenarios y cuáles están más ligados al contexto concreto de cursos de programación.

VII. AGRADECIMIENTOS

Este trabajo ha sido financiado parcialmente por el proyecto nacional del Ministerio de Economía y Competitividad, “Espacios Educativos Especulares” - EEE (TIN2011-28308-C03-01), por el proyecto regional de la Comunidad de Madrid, “eMadrid” (S2009/TIC-1650) y por el programa de estancias postdoctorales Alianza 4 Universidades.

Los autores agradecen al profesor Abelardo Pardo su labor y guía en la asignatura y a todos los profesores que han participado altruistamente en la encuesta objeto de este estudio por su tiempo y aportaciones.

REFERENCIAS

[1] M. Barak, J. Harward, G. Kocur, and S. Lerman, “Transforming an introductory programming course: From lectures to active learning via wireless laptops,” *Journal of Science Education and Technology*, vol. 16, no. 4, pp. 325–226, august 2007.

[2] B. Trilling and C. Fadel, *21st Century Skills: Learning for Life in Our Times*, 1st ed. San Francisco, CA, USA: Jossey-Bass, 2009.

[3] R. M. Felder and R. Brent, “Active learning: An introduction,” *ASQ Higher Education Brief*, vol. 2, no. 4, pp. 1–5, august 2009.

[4] D. Moursund, *Project-Based Learning Using Information Technology*, 1st ed. Eugene, OR, USA: ISTE, 1999.

[5] C. Bouton and R. Y. Garth, “Students in learning groups: Active learning through conversation,” *New Directions for Teaching and Learning*, vol. 1983, no. 14, pp. 73–82, june 1983.

[6] A. Pardo, I. Estévez-Ayres, P. Basanta-Val, and D. Fuentes-Lorenzo, “Programación en C con aprendizaje activo, evaluación continua y trabajo en equipo: caso de estudio,” in *XVI Jornadas de Enseñanza Universitaria de la Informática (JENUI 2010)*, Julio 7-9 2010.

[7] D. R. Woods, *Problem-based learning: How to gain the most from PBL*. Donald R. Woods Waterdown, 1994.

[8] K. Deibel, “Team formation methods for increasing interaction during in-class group work,” *ACM SIGCSE Bulletin*, vol. 37, no. 3, pp. 291–295, Jun. 2005. [Online]. Available: http://doi.acm.org/10.1145/1151954.1067525

[9] B. Oakley, R. M. Felder, R. Brent, and I. Elhajj, “Turning student groups into effective teams,” *Journal of student centered learning*, vol. 2, no. 1, pp. 9–34, 2004.

[10] P. del Canto, I. Gallego, J. M. López, J. Mora, A. Reyes, E. Rodríguez, K. Sanjeevan, E. Santamaría, and M. Valero, “Conflictos en el trabajo en grupo: cuatro casos habituales,” *Revista de Formación e Innovación Educativa Universitaria (REFIEDU)*, vol. 2, no. 4, pp. 211–226, 2009.

[11] A. Pardo, I. Estevez-Ayres, P. Basanta-Val, and D. Fuentes-Lorenzo, “Course quality improvement using mid-semester feedback,” *International Journal on Technology-Enhanced Learning*, vol. 3, no. 4, pp. 366–376, Jul. 2011. [Online]. Available: http://dx.doi.org/10.1504/IJTEL.2011.041280

[12] M. Valero-García and J. García-Zubia, “Cómo empezar fácil con PBL,” in *XVII Jornadas de Enseñanza Universitaria de la Informática (JENUI 2011)*, Julio 5-8 2011.

Herramienta para la mejora del Inglés en vocabularios tecnológicos del ámbito de las Comunicaciones

Luz García Martínez, Jesús Villar Fernández, Isaac Álvarez Ruiz, Carmen Benítez Ortúzar
Dpto. de Teoría de la Señal, Telemática y Comunicaciones
Escuela Técnica Superior de Ingenierías Informática y Telecomunicación
C/ Periodista Daniel Saucedo Aranda, s/n. 18071 Granada.
luzgm@ugr.es, vijefe@gmail.com, isamaru@ugr.es, carmen@ugr.es

***Resumen*—Este trabajo presenta una herramienta individualizada para la mejora de la fonética del Inglés con fines específicos tecnológicos en el campo de las Comunicaciones. Usando reconocimiento y síntesis automática del habla, el estudiante de ingeniería adquiere nuevo vocabulario específico del ámbito científico y profesional al que se va a incorporar cuando se convierta en egresado. La herramienta permite practicar de forma personalizada la fonética y el significado de los términos a través de audiciones, tareas de evaluación automática de la pronunciación y creación de mapas conceptuales. Se presentan vocabularios de diferentes campos semánticos dentro de ámbito de conocimiento deseado, con diferentes niveles de dificultad conceptual que se aumenta de manera individualizada cuando el usuario obtiene evaluaciones satisfactorias. Los vocabularios usados se apoyan en ejemplos de comunicaciones reales del ámbito de la Ingeniería de Telecomunicación, y permiten ser ampliados de manera colaborativa por los diferentes usuarios de la misma.**

***Index Terms*—Inglés con fines específicos, fonética inglesa, Telemática, aprendizaje colaborativo, mapas conceptuales, memoria de aprendizaje, herramientas TIC para el aprendizaje.**

I. INTRODUCCIÓN

El EEES define la siguiente competencia transversal que los Ingenieros de Telecomunicación deben adquirir en su formación [1]: *capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con las telecomunicaciones y la electrónica.*

En este marco, el desarrollo de las habilidades de comunicación es muy importante para conseguir una formación integral y debe ser cubierto en paralelo al aprendizaje de contenidos técnicos. La comunidad científica y profesional del ámbito de las Tecnologías de la Información y las Comunicaciones en la que el egresado va a desarrollar su vida profesional tiene una lengua común incluestionable, que es el inglés. Por esta razón es muy útil que el profesorado aporte metodolgías y herramientas para el estudio del inglés específico del ámbito de la Ingniería de Telecomunicación. Este trabajo presenta una aplicación para la mejora de la fonética inglesa en la adquisición de vocabularios específicos dentro del campo de las Comunicaciones. Para ello se implementa un sistema de reconocimiento y síntesis automática del habla en inglés que permite al usuario aprender vocabularios específicos relacionados con las materias del Grado en Ingeniería de Telecomunicación. El proceso de aprendizaje de los vocabularios comprende el aprendizaje de la fonética y el significado de las palabras, encuadrándolas su marco conceptual. Para que dicho aprendizaje se produza, se evalúa su pronunciación por parte del usuario (mediante el sistema de reconocimiento automático del habla), se ofrece la pronunciación correcta (mediante el sistema de síntesis del habla) y se trabaja el significado de la palabra mediante su definición e inclusión en un mapa conceptual del campo semántico bajo estudio.

La herramienta tiene tres atractivos principales: (i) el aprendizaje individualizado para cada usuario, (ii) la construcción colaborativa entre diversos ususarios que pueden añadir, bajo supervisión del profesor, términos a los campos semáticos ya existentes, y (iii) la especificidad y actualidad de los vocabularios elegidos. El carácter individualizado se consigue mediante un registro histórico de resultados de evaluación fonética del usuario que dan la pauta para aumentar el nivel de dificultad conceptual con nuevos términos de vocabulario que la aplicación le presenta. Los vocabularios elegidos, tanto por el profesor que gestiona y configura la herramienta como por los alumnos usuarios que los pueden ampliar, son extraídos de documentos reales del ámbito profesional y científico dentro del campo semántico bajo estudio (documentos de estandarización, proyectos y especificaciones técnicas, artículos científicos...) y al presentarlos se muestran, por escrito y auditivamente, en extractos de dichos documentos reales.

Con el objetivo de describir la herramienta propuesta, el resto del documento se organiza del modo siguiente. En primer lugar se analizan los fundamentos pedagógicos de la aplicación propuesta en la sección II. A continuación, la sección III hace una descripción detallada de la herramienta y en la sección IV se detallan los criterios de creación de los vocabularios utilizados. Por último, la sección V presenta las conclusiones y los futuros trabajos.

II. PERSPECTIVA PEDAGÓGICA

II-A. Aprendizaje individualizado y colaborativo

El enfoque de esta herramienta combina las ventajas del *aprendizaje individualizado* [2] que se adapta de manera flexible a las necesidades y estilo de aprendizaje particulares del usuario (variantes en tiempo, volumen y contenidos), con las ventajas del *aprendizaje colaborativo* [3] a través de la ampliación colectiva de los vocabularios que la aplicación utiliza. Esta combinación es posible gracias al uso de las Tecnologías de la Información y las Comunicaciones que

permiten llevar un registro histórico individualizado del usuario y configurar la aplicación para sus necesidades y ritmo de aprendizaje. Simultáneamente, gracias a estas TICs los usuarios pueden poner en común su conocimiento personal y añadir términos de vocabulario ampliando de forma colectiva los campos semánticos con los que trabaja la herramienta. Las interacciones que así se generan entre los usuarios de la herramienta son muy positivas ya que permiten al alumno experimentar tanto el proceso personal de aprendizaje como la cooperación grupal y el trabajo en equipo. Se trata por tanto de avanzar en la obtención de la *'capacidad para trabajar de forma efectiva como individuo, organizando y planificando su propio trabajo, forma independiente o como miembro de un equipo'*(competencia transversal de los Ingenieros de Telecomunicación definida en el EEES [1]).

II-B. Teoría de la Profundidad del Procesamiento

El objetivo de la herramienta es que se produzca el aprendizaje de la fonética y significado de las palabras del vocabulario seleccionado. Dicho aprendizaje del vocabulario puede ser sólo memorístico o además significativo. En el caso del aprendizaje significativo el sujeto relacionará la información recibida con la que ya posee, reajustando y reconstruyendo ambas informaciones como resultado de dicho proceso. Este es el tipo de aprendizaje deseable para que los alumnos creen campos semánticos dotados de significado en su aprendizaje de vocabularios de inglés tecnológico especializado.

La Psicología Cognitiva define el proceso de aprendizaje como el procesado activo de la información por parte del sujeto en diferentes etapas [5]. La figura 1 presenta los mecanismos subyacentes responsables del aprendizaje en dicho modelo del aprendizaje [7]:

i. Gracias a la *atención*, la memoria de registro sensorial captura los estímulos (la información se almacena durante menos de un segundo).
ii. Mediante el proceso de *repetición*, dicha información captada se almacena en la memoria a corto plazo. Una vez que la información es almacenada en esta memoria, se ha producido el áprendizaje memorístico'(que hace, por ejemplo, que ciertas cosas se olviden completamente al tiempo de hacer un examen).
iii. El proceso de *codificación* mueve la información desde la memoria a corto plazo hasta la memoria a largo plazo donde se guardará durante cierto tiempo. Consiste en relacionar la información nueva con el conocimiento dotándola así de mayor significado.
iv. La información se puede mover de nuevo desde la memoria a largo plazo hasta la memoria a corto plazo. Dicho proceso recibe el nombre de *recuperación*.

Basada en este modelo de aprendizaje como procesado de la información, La Teoría de la Profundidad del Procesamiento [7] sostiene que cuanto mayor sea el procesamiento cognitivo (de la información tanto fonética como semántica), más posibilidades tiene una información de pasar a la memoria a largo plazo. Es decir, el aprendizaje significativo no depende tanto del número de repeticiones de la información que el usuario haga, sino de que las repeticiones sean lo más creativas y significativas posibles. Se distinguen dos tipos de repeticiones: (i) repeticiones mecánicas de mantenimiento que simplemente mantienen la información activa en la memoria a corto plazo sin consumir recursos cognitivos del usuario; (ii) repeticiones elaboradas de la información y la procesan de algun modo creativo.

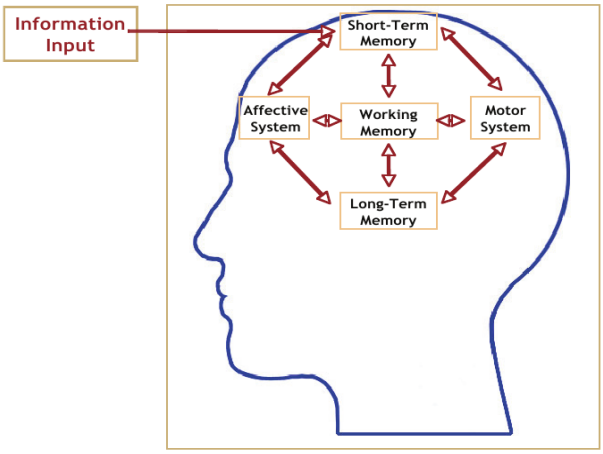


Figura 1. Sistemas de memoria activos durante el aprendizaje [6].

II-C. Mapas conceptuales

La Teoría de la Profundidad del Procesamiento que acabamos de mencionar justifica la organización de los vocabularios que la aplicación presenta al alumno en forma de *Mapas Conceptuales* [6]. Un mapa conceptual es una herramienta gráfica para la organización y representación del conocimiento. Incluye conceptos dentro de círculos o cajas y los relaciona entre sí mediante lineas. Dichas líneas pueden contener términos que explican la relación entre los conceptos que se pueden distribuir de forma jerárquica si su relación lo permite. Es muy frecuente el uso de mapas conceptuales para el aprendizaje de vocabularios [8], [9], [10] ya que su creación por parte del sujeto, implica el establecimiento de relaciones cognitivas que facilitarán un aprendizaje significativo y el almacenamiento de la información aprendida durante un tiempo mayor en la memoria a largo plazo.

La figura 2 muesta un ejemplo de mapa conceptual con términos en inglés del campo semántico de 'Long Term Evolution Technology'

III. DESCRIPCIÓN DE LA HERRAMIENTA

La figura 3 muestra un diagrama funcional de la herramienta. Se ha dividido conceptualmente en tres bloques principales. Hay un primer un bloque de entrenamiento en el que se construye un sistema de reconocimiento automático del habla preparado para reconocer los términos del vocabulario que el usuario va a aprender. Hay un bloque de evaluación en el que se analiza si el usuario pronuncia correctamente las palabras y si conoce su significado. Por último, el resultado de dicha evaluación se analiza en el bloque funcional de análisis de resultados. Si la evaluación es positiva, el usuario termina el aprendizaje incluyendo el término en su mapa conceptual del campo semántico. Si la evaluación es negativa, se le aporta información y se repite el proceso de aprendizaje.

La figura muestra un cuarto bloque funcional en el que actúan tanto el alumno (*usuario ázul'*) como el profesor

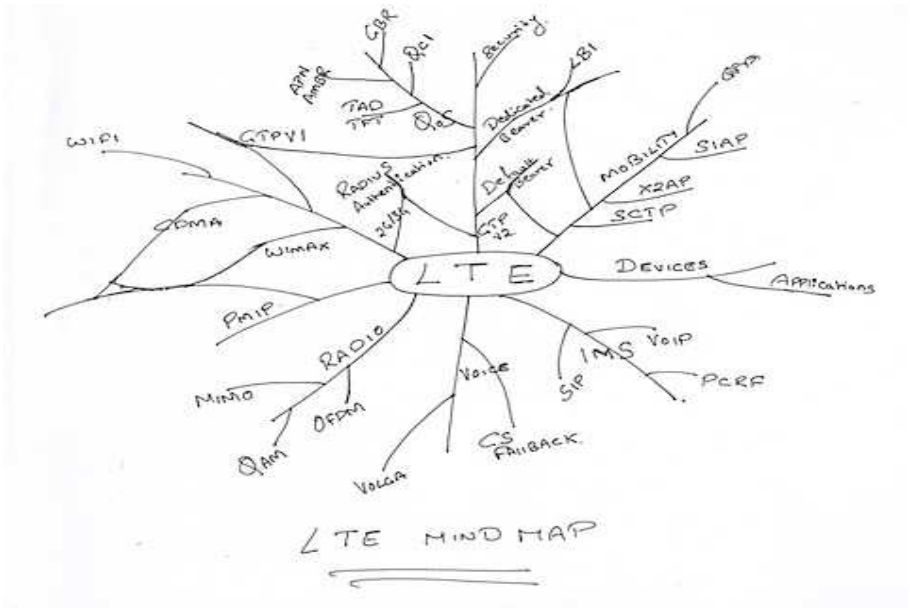


Figura 2. Ejemplo: mapa conceptual sobre LTE [4].

(*usuario 'rojo'*). El objetivo de este bloque es la reconfiguración de los vocabularios con los que cuenta la aplicación. Dichos vocabularios pueden ser reconfigurados por tres tipos de usuarios diferentes:

i. El profesor que apoya el proceso de aprendizaje.
ii. El alumno usuario que al aprender los términos existentes, añada nuevas conexiones cognitivas no contempladas.
iii. Otros usuarios de la herramienta conectados en entornos de aprendizaje colaborativo.

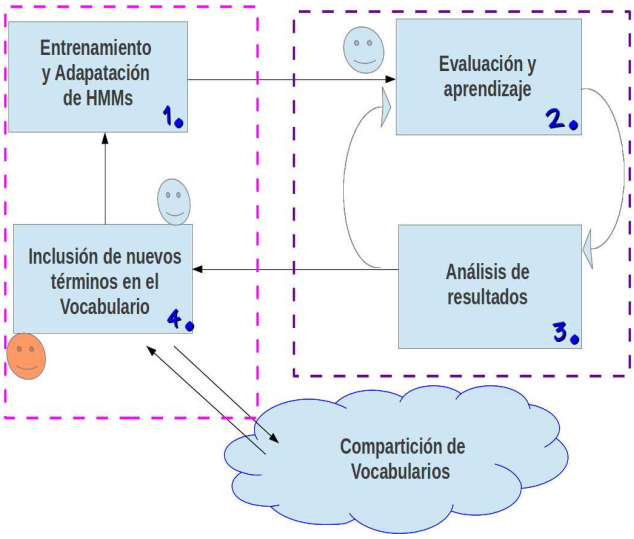


Figura 3. Arquitectura de sistema de la aplicación.

III-A. Entrenamiento del Sistema de Reconocimiento

La figura 4 muestra el diagrama de bloques del reconocedor automático del habla que utiliza la aplicación, basado en Modelos Ocultos de Markov [11], [12]. El reconocedor se entrena con una base de datos en inglés de propósito general fonéticamente balanceada. Con el objetivo de obtener mayor flexibiliad del sistema se utilizan trifonemas (fonemas con información contextual a derecha e izquierda) como unidades básicas de entrenamiento. Para que los Modelos Ocultos de Markov así entrenados tengan representación estadística suficiente de las palabras de los vocabularios tecnológicos específicos con los que se quiere trabajar, se hace un paso posterior de adaptación de los modelos. Para ello, utilizando un sintetizador automático del habla, se generan pequeñas bases de datos con los vocabularios concretos de la herramienta. Es necesario conocer la transcripción fonética del vocabulario con el que se quiere trabajar. Cada uno de los vocabulario específicos sintetizados debe ir acompañado de un diccionario con las transcripciones (en términos de trifonemas) de las palabras que lo componen. Los modelos originales son reentrenados con esos nuevos datos para crear los modelos finales adaptados al propósito específico. Tanto para el entrenamiento original como para la adaptación de modelos se usa la herramienta HTK (*HMM Tool Kit*)[14]. La síntesis automática del habla se ha implementado con la herramienta de síntesis de voz basada en Modelos de Markov HTS (*HMM-based Speech Synthesis Tool*) [15].

III-B. Evaluación y Aprendizaje

III-B1. Evaluación: Como muestra la figura 5 la herramienta evalúa el aprendizaje del significado del término, y su correcta pronunciación.

- La *evaluación semántica* se ha resuelto de un modo simple. Se presentan al usuario tres posibles definiciones de la palabra que se está evaluando y se le pide que elija la correcta. La dificultad es variable graduando la similitud entre las opciones.
- La *evaluación de la pronunciación* es la parte más importante de la herramienta desde la perspectiva del procesado automático del habla. El objetivo es dar un *feedback* de cuánto se parece la pronunciación del usuario a una pronunciación correcta de la palabra. Para ello, usando el Sistema de Reconocmiento de los Modelos de

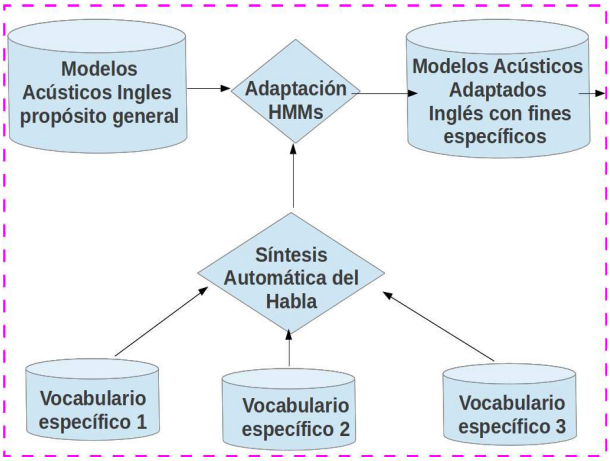


Figura 4. Modulo de entrenamiento y adaptación de modelos.

Markov entrenados y adaptados, hace un alineamiento forzado (o alineamiento de Viterbi [14]) de la señal audio que produce el alumno con la transcripción de la palabra del vocabulario.

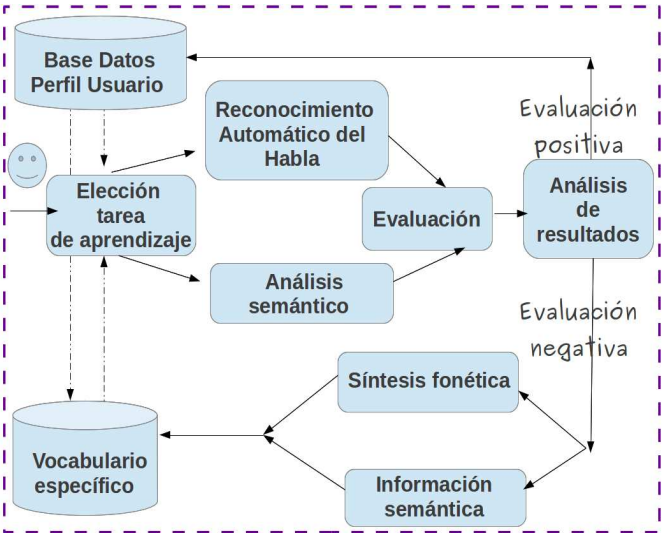


Figura 5. Modulo de Evaluación y Aprendizaje.

Las figuras 6 y 7 muestra un ejemplo del resultado obtenido al hacer el alineamiento forazado del fichero de voz en el que se pronuncia las palabras '*four seven*'. Las palabra pronunciadas son alineadas con sus transcripciones usando un diccionario y los modelos acústicos de trifonemas e para dar como resultado:

i. La *delimitación temporal* o segmentación óptima de la palabra pronunciada en términos de las unidades acústicas contempladas en el diccionario de transcripciones. Las columnas 1 y 2 de la figura son los instantes de comienzo y final del trifonema en diezmilésimas de segundo. La columna 3 es el trifonema con el que se alinea dicho segmento de señal audio.
ii. Una medida de la probabilidad acústica de que cada uno de dichos segmentos de pronunciación correspondan al modelo estadístico del trifonema con el que se ha alineado (columna 4 de la figura 7).

Una vez obtenida la probabilidad de que los trifonemas pronunciados correspondan a los modelos estadísticos, existen diversos criterios de evaluación de los resultados [16], [17]. En nuestro caso, la probabilidad de cada trifonema pronunciado se ha comparado con la probabilidad media del modelo acústico de dicho trifonema en los datos de entrenamiento. Se han definido unos márgenes aceptables de pronunciación por debajo de ese valor medio y con ese rango de valores se hace la evaluación y se le muestra al usuario los segmentos de palabra correcta e incorrectamente pronunciados, así como una valoración global de su pronunciación.

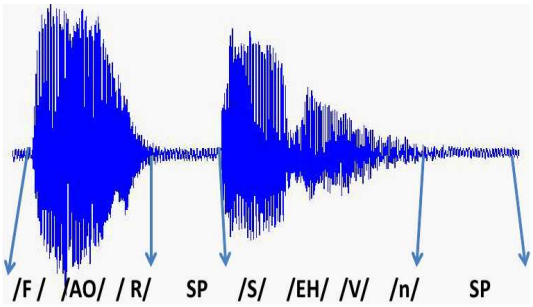


Figura 6. Ejemplo de alineanimiento forzado de la frase '*four seven*'.

```
 7500000  8700000 f   -1081.604736 FOUR
 8700000  9800000 ao   -903.821350
 9800000 10400000 r    -665.931641
10400000 10400000 sp     -0.103585
10400000 11700000 s   -1266.470093 SEVEN
11700000 12500000 eh   -765.568237
12500000 13000000 v    -476.323334
13000000 14400000 n   -1285.369629
14400000 14400000 sp     -0.103585
```

Figura 7. Ejemplo de resultado de un alineamiento forzado.

III-B2. Aprendizaje: Si los resultados obtenidos no son satisfactorios, la herramienta ofrece al usuario la siguiente información para facilitar el proceso de aprendizaje:

i. La definición correcta en inglés del término con el que se trabaja.
ii. La pronunciación correcta del término obtenida con el sintetizador automático del habla.
iii. Tres audiciones (de nuevo con síntesis automática del habla) en las que el término que se estudia aparece en un contexto de uso real del mundo científico o profesional de la Ingeniería de Comunicaciones.

En cambio si los resultados de la evaluación han sido satisfactorios, el siguiente paso es que el usuario integre el término del vocabulario en su mapa conceptual del campo semántico al que pertenezca la palabra, añadiendo si quiere nuevos términos que conecten con el que acaba de aprender.

III-C. Análisis de resultados y reconfiguración de la tarea

El aprendizaje individualizado se lleva a cabo mediante la generación de perfiles de usuario en los que se almacena:

- el historial de tareas realizadas
- los resultados de aprendizaje de las tareas
- los mapas conceptuales que el alumno va creando en cada uno de los campos semánticos con los que trabaja

La lógica de la planificación automática de las tareas para cada usuario se fundamenta en dos condiciones: en primer lugar, los términos que ya se han aprendido pasan de aparecer como *'tareas de aprendizajeá* aparecer como *'tareas de recuerdo o refresco'* que se intercalarán de manera periódica para reforzar su memorización. En segundo lugar, cuando todos los términos de un mismo nivel de dificultad conceptual se dominan, se pasa a un nivel de dificultad conceptual superior.

III-D. Casos de uso y funcionalidad de la herramienta

La aplicación tiene dos tipos de usuario: el profesor y el alumno

- Las tareas que realiza el ***profesor*** son :
  - **TP1.** Crear los campos sémáticos asociados a conceptos técnicos de las Comunicaciones, incluyendo ejemplos reales de uso de los términos.
  - **TP2.** Revisar y validar para su incorporación los términos que el alumno añade al campo sémático por asociación de conceptos.
  - **TP3.** Revisar el proceso de aprendizaje del alumno reflejado en su historial de uso de la aplicación. En particular, los mapas conceptuales que ha creado son un buen indicador de su estructura cognitiva en la materia. Modificar la planificación automática de tareas para el alumno si se considera conveniente.
  - **TP4.** Supervisar el intercambio de términos de los campos semánticos con otros usuarios de la aplicación en redes sociales y comunidades de usuarios.
- Las tareas que realiza el ***alumno*** serán:
  - **TA1.** Realizar las tareas de evaluación con los vocabularios que la aplicación selecciona para él.
  - **TA2.** Aprender la fonética y significado de dichos vocabularios, incorporando los términos a los mapas conceptuales de los campos semánticos
  - **TA3.** Incorporar a los campos semánticos términos afines relacionados con los que la aplicación les plantea.
- Por su parte la ***aplicación*** ofrece las siguiente funcionalidades:
  - **F1.** Evaluación automática del aprendizaje del alumno.
  - **F2.** Registro histórico de la evolución del aprendizaje del alumno y de los mapas conceptuales que genera.
  - **F3.** Planificación automática de las tareas de cada usuario.

IV. DISEÑO DE LOS VOCABULARIOS

El diseño de campos semánticos relacionados con terminología técnica de las Comunicaciones que hace el profesor de la asignatura es una parte clave para que la herramienta sea últil en el proceso de aprendizaje. Se define un campo semántico, red léxica o cadena cohesiva como un conjunto de palabras o elementos significantes con significado relacionado,debido a que comparten un núcleo de significación o rasgo semántico (sema) común y se diferencian por otra serie de rasgos semánticos que permiten hacer distinciones.

Se pueden usar diferentes criterios para la creación de vocabularios de un campo semántico como pueden ser similitud, antagonismo de conceptos, relación jerárquica de términos, uso de tecnologías comunes, etc. Se adaptará a los objetivos de aprendizaje de la materia para la que se utilice la herramienta. Se proponen tres etapas[18]:

- Se detecta la idea central en torno a la cual va a desarrollarse el campo semántico y se le asocia la palabra clave raíz del vocabulario.
- Se establecen categorías secundarias, que corresponden a las partes principales del tema, subapartados destacados... etc. Cada categoría secundaria se asimila con una o más palabras de vocabulario.
- Con los detalles de apoyo o ideas complementarias se crean más niveles del campo semántico identificando las palabras clave con los que se puede asociar. Cuando se establezca la lógica de la tarea de evaluación y aprendizaje, estas categorías más específicas serán las que se utilicen para aumentar la complejidad de la tarea.

V. CONCLUSIONES Y TRABAJO FUTURO

Se propone una herramienta de trabajo individualizado para el aprendizaje de Vocabularios de Inglés tecnológico relacionados con la Ingeniería de Telecomunicaciones que el alumno se va a encontrar en el entorno laboral. Su objetivo es ejercitar la fonética y significado de términos técnicos del Inglés mediante ejercicios de repetición y creación de mapas conceptuales que den una perspectiva global del campo semántico al que pertenencen los términos.

La implementación técnica propuesta para la herramienta utiliza Modelos de Markov para entrenar un Sistema de Reconocimiento Automático del Habla con el que se evalúa la pronunciación de los términos, y un Sistema de Síntesis Automática del Habla con el que se muestra la pronunciación correcta. Con estos dos sistemas y siguiendo un diálogo guiado se definen tareas de aprendizaje cuyo nivel de dificultad conceptual aumenta de manera gradual.

Esta herramienta tiene un amplio potencial de desarrollo y puede ser utilizada en disciplinas muy diferentes, adaptando los Modelos de Markov a los Vocabularios específicos con los que se quiera trabajar. Existen dos vertientes con amplio margen de mejora en la herramienta propuesta:

- En la *vertiente técnica* se puede mejorar el Reconocimiento Automático del Habla. Sería interesante ofrecer al usuario medidas de la correcta entonación y prosodia en frases, para ayudarle en la preparación de exposiciones orales. También sería muy interesante la automatización del proceso de creación de los vocabularios mediante técnicas de búsqueda automática de palabras clave en textos seleccionados.
- En la *vertiente pedagógica*, se pueden diseñar juegos de inteligencia que ayuden al aprendizaje, en vez del diálogo neutro que utiliza esta primera aproximación. Las revisiones por pares iguales de los mapas conceptuales que el alumno genera, también constituirían un valor añadido.

AGRADECIMIENTOS

Este trabajo se ha llevado a cabo con el soporte del Programa de Cooperación India-España de Ciencia y Tecnología, bajo el proyecto ACI2009-0892 del Ministerio de Ciencia e Innovación, y del Proyecto CEI2013-MP-29 del Campus de Excelencia CEI-BioTic Granada.

REFERENCIAS

[1] Orden CIN/352/2009 requisitos de verificación de los títulos universitarios oficiales.

[2] Katherine Sinitsa, 'Learning Individually : a Life-Long Perspective Introduction to the Special Issue', Educational Technology & Society vol. 3, n. 1., 2000 ISSN 1436-4522.

[3] G. Stahl, T. Koschmann, D. Suthers, 'Computer-supported collaborative learning: an historical perspective', R. K. Sawyer (Ed.), Cambridge handbook of the learning sciences (pp. 409-426). Cambridge, UK,2006.

[4] http://wired-n-wireless.blogspot.com.es/

[5] J. Lacher, K. Forster, E. Ruthruff, 'Forty-Five Years After Broadbent (1958):Still No Identification Without Attention'. Psychological Review 2004, Vol. 111, No. 4, 880-913, American Psychological Association. 2004.

[6] J. D. Novak, A.J. Cañas, 'The Theory Underlying Concept Maps and How to Construct and Use Them', Technical Report IHMC CmapTools 2006-01 Rev 01-2008. http://www.ihmc.us

[7] Z. Hongyan, W. Xiaohui, H. Liyang, Énglish Vocabulary Learning System Based on Theory of Depths Processing'. IEEE Computer Society. International Conference on Computer Technology and Development, pp. 491-493. 2009

[8] L. Mei, Y. Kun, C. Hai, Úsing Mind Maps as Strategy for Vocabulary Acquisition in Chinese Universities'. International Conference on Computational Intelligence and Software Engineering (CiSE), 2010.

[9] L. Zhiyi. 'Cooperative Mind Map and Its Application in Meaningful Learning for Junior High School Students'.

[10] Z. Weize, Q. Feiye, 'The Design of a Web 2.0 Based Vocabulary Learning System for EFL Learners'. International Symposium on IT in Medicine and Education (ITME), vol. 1, pp. 485-489. 2011.

[11] L. Rabiner, B. Juang, 'Fundamentals of speech recognition'. Prentice Hall PTR, 1993.

[12] L.R. Rabiner. Á tutorial on hidden markov models and selected applications in speech recognition'. Proc. of IEEE, n. 77, vol. 2, pp. 257-286, 1989.

[13] H.G. Hirsch, Éxperimental framework for the performance evaluation of speech recognition front-ends of large vocabulary task'. STQ AURORA DSR Working Group, 2002.

[14] S. Young et alt., 'The HTK Book', Microsoft Corporation & Cambridge University Engineering Department, 1995.

[15] H. Zen, T. Nose, J. Yamagishi, S. Sako, T. Masuko, A.W. Black, K. Tokuda, 'The HMM-based Speech Synthesis System (HTS) Version 2.0', Proc. of 6th ISCA Workshop on Speech Synthesis (SSW-6), August 2007.

[16] H. Franco, L. Neumeyer, Y. Kim, O. Ronoen, Áutomatic pronunciation scoring for language instruction', Speech Technology and Research Laboratory, SRI International. Proceedings of ICASSP 1997, vol. 2, pp. 1474-1474.

[17] K. L. Srinivas, P. Rao. 'Pronunciation scoring for Language Learners using a Phone Recognition System', Proceedins of the First International Conference on Intellligent Interactive Technologies and Multimedia, pp. 135-139, 2010.

[18] M.K. Åhlberg 'Concept mapping as an empowering method to promote learning, thinking, teaching and research', ISSN 1989 - 9572

Aplicación al Ámbito Académico de un entorno de Simulación/Emulación de Arquitecturas de Red

José Javier Serrano, Julián Fernández-Navajas, José Mª Saldaña
Grupo de Tecnologías de las Comunicaciones – Instituto de Investigación en Ingeniería de Aragón
Dpt. IEC. EINA, Universidad de Zaragoza
Edif. Ada Byron, 50018, Zaragoza
{182482, navajas, jsaldana}@unizar.es

Resumen – **En este artículo se presenta un estudio sobre el empleo de una herramienta de emulación de red para la docencia en Ingeniería Telemática. La posibilidad de integrar, en un mismo escenario, nodos reales disponibles en el laboratorio junto con dispositivos hardware comerciales emulados, presenta muchas ventajas para la formación de los alumnos y la realización de prácticas de laboratorio. En concreto, se ha estudiado el entorno *GNS3/Dynamips*, originalmente diseñado para realizar pruebas de dispositivos de *Cisco* y *Juniper* en entornos telemáticos. En primer lugar, se muestra cómo los dispositivos emulados implementan exactamente las funcionalidades de los dispositivos reales correspondientes. Se han propuesto diferentes escenarios en los que los alumnos pueden realizar pruebas con distintos servicios, integrando máquinas reales con hardware emulado. Se presentan también pruebas encaminadas a caracterizar la escalabilidad del sistema, y las condiciones en las que el emulador se comporta igual que los dispositivos reales. En concreto, se analiza el incremento en el consumo de recursos del sistema emulador (carga de CPU y consumo de memoria RAM) al aumentar el número de nodos emulados. Este consumo puede determinar la escalabilidad de un escenario de trabajo emulado. Además, haciendo uso del protocolo ICMP, se miden las latencias de red que pueden resultar críticas, con el objetivo de comparar los entornos de red reales con los entornos híbridos, en los que el hardware real interopera con el entorno emulado.**

Palabras clave - **telemática, emulación, EEES, red virtual.**

I. INTRODUCCIÓN

El paradigma del aprendizaje centrado en el alumno y el desarrollo de sus competencias nos ayudan a entender la educación como algo más que la enseñanza o la mera adquisición de conocimientos. Este paradigma exige una adaptación de la mentalidad del profesorado y la aplicación de nuevas tecnologías en el diseño de planes de estudios, la preparación de asignaturas, la planificación docente, la conducción de las clases y el seguimiento, tutorización y evaluación de los estudiantes.

Unido a esto, resulta prioritario desde el prisma docente concretar y delimitar aspectos fundamentales, como la consecución y control de los objetivos académicos. También se requiere un reflejo y vinculación directa entre los objetivos académicos y los escenarios de trabajo reales que el alumno, tarde o temprano, deberá afrontar. Por ello, en el contexto de los planes de estudio actuales, para la consecución de estos propósitos resulta deseable poner a disposición del alumno entornos controlados y prácticos de trabajo. De esta manera, se podrán marcar sus pautas del aprendizaje y simultáneamente, será posible delimitar el compromiso entre nivel de exigencia y dificultad asociada a la consecución de los objetivos académicos. Todo ello a través del trabajo práctico continuo del alumno y la supervisión de los objetivos parciales, finalizando en la evaluación global del objetivo final.

En este trabajo se analiza el potencial de un entorno software de simulación/emulación, denominado *GNS3/ Dynamips*[1], para el cumplimiento de los objetivos docentes anteriores. A grandes rasgos, a través de un sencillo e intuitivo interfaz gráfico, este entorno permite implementar topologías asociadas a arquitecturas de amplio espectro tecnológico, abarcando desde los diseños más básicos, hasta tecnologías de uso preferente en la actualidad.

Este entorno está principalmente concebido para emular arquitecturas de red que integran dispositivos de *Cisco Systems* y *Juniper* en entornos corporativos, haciendo uso para ello de las imágenes de los sistemas operativos de los equipos reales. Además, incorpora un considerable abanico de dispositivos de red generales que abarcan desde *switch Ethernet*, *Frame Relay* o ATM, hasta dispositivos *Firewall*, sin olvidar la emulación de terminales Linux. Todo esto permite un amplio rango de posibilidades en el ámbito docente, resultando muy interesante la posibilidad de acotar objetivos parciales y finales de aprendizaje, según los niveles de exigencia que se quieran establecer.

Añadido a esto, se trata de un entorno fundamentalmente práctico (aunque con una carga telemática teórica evidente), dado que el diseño y las configuraciones a implementar son idénticas o muy similares a las que se encontrarán en escenarios de red reales. Por ejemplo, la interacción con los dispositivos se realiza a través de un *prompt* o intérprete de comandos idéntico al de los dispositivos reales. Por ello, la

[1] http://www.gns3.net/dynamips/

asimilación de los contenidos por parte del alumno puede resultar más consistente que la ofrecida por un entorno de trabajo únicamente simulado.

Pero la característica funcional más relevante y decisiva de *GNS3/Dynamips*, y que analizaremos en el presente trabajo, es que permite entornos mixtos, en los que equipos y tráfico de red reales pueden interoperar, en un mismo escenario, con equipos y tráfico de red emulados. Este hecho presenta unas interesantes ventajas prácticas para el diseño y el análisis de los entornos. Por ejemplo, en el ámbito docente, los alumnos podrán lanzar pruebas desde equipos reales, interactuando con un gran abanico de equipos de red, aunque de hecho no se disponga de ellos en el laboratorio.

Además, a través de la herramienta software *Wireshark*, integrada en el entorno, se posibilita la visualización de capturas de tráfico emulado mediante librerías *.cap*, pudiendo analizarse de un modo similar al de una red real. Este tráfico puede tener como origen y/o destino un dispositivo de red real o bien emulado, según sea el propósito del análisis. Esta característica facilita un amplio abanico de arquitecturas, tráficos de red y servicios que pueden ser estudiados desde el ámbito de la docencia en telemática, pero con un claro enfoque hacia el mundo profesional.

La Fig.1 muestra el interfaz gráfico *GNS3,* sobre el que se ha implementado una sencilla estructura de red, que integra un equipo real externo (usando el *ítem* de diseño *cloud* o nube), que interopera con los nodos del escenario emulado.

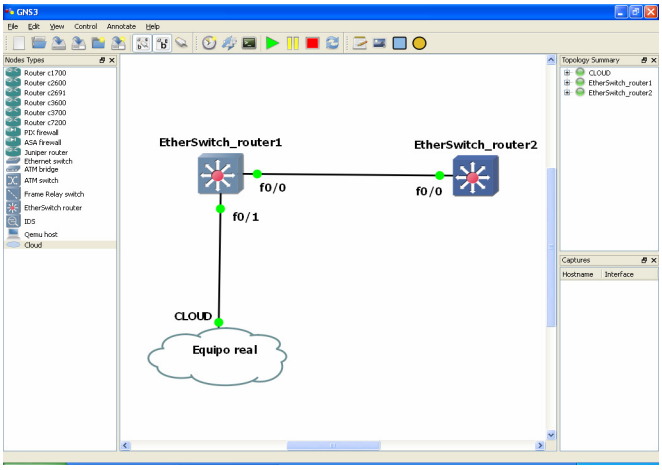


Fig. 1. Panorámica general del entorno *GNS3/Dynamips* con la integración de un equipo real en el entorno emulado.

Por tanto, en este trabajo nos centraremos en el estudio de la capacidad del entorno de emulación *GNS3/Dynamips* como una herramienta de trabajo adecuada para entornos académicos y en su interés para tareas docentes. Expondremos en detalle algunas de las pruebas que permite el sistema, mediante diferentes escenarios, centrándonos en los conceptos que los alumnos pueden aprender. También presentaremos algunas pruebas encaminadas a medir el nivel de realismo del sistema a la hora de emular dispositivos de red. Es importante que el alumno conozca los límites de la emulación, y que compruebe que existen experimentos cuyos resultados no serán idénticos a los que se obtendrían con dispositivos reales.

La estructura del resto del artículo es la siguiente: la sección II detalla los trabajos relacionados. La sección III explica brevemente la solución de emulación utilizada. La siguiente sección detalla las diferentes arquitecturas de red que se han implementado en las pruebas. La sección V presenta las pruebas encaminadas a medir el rendimiento del sistema. Posteriormente, en la sección VI se estudia la influencia del sistema emulador en los parámetros medidos en la red y el artículo se cierra con las conclusiones.

II. Trabajos Relacionados

El interés por el reflejo y traslación de escenarios reales de trabajo hacia entornos virtuales va siendo cada vez mayor, y las propuestas concretas se han ido diversificando. Pueden encontrarse en la literatura especializada estudios de entornos de trabajo telemático que implementan soluciones de virtualización. Por ejemplo, [1] muestra una comparativa de plataformas virtuales, principalmente *Xen* y *VMware*. Estas pueden ser consideradas como las plataformas de virtualización más utilizadas y de mejor rendimiento en los sistemas de producción para la virtualización de servidores. En esencia, se constata comparativamente como la plataforma *Xen* (paravirtualización) presenta un mejor rendimiento que la plataforma *VMware* (virtualización completa).

Así mismo, [2] presenta algunas técnicas de virtualización existentes en el campo docente en la actualidad, incluyendo el análisis de ciertas características funcionales del entorno software *GNS3/Dynamips*. Se plantea en este caso la alternativa de uso de la plataforma XORP (eXtensible Open Router Platform) frente a *GNS3/Dynamips*, con el objetivo principal de minimizar el consumo de recursos del sistema.

Con todo ello, en el presente trabajo nuestro esfuerzo se va a centrar en el análisis del entorno simulador/emulador *GNS3/Dynamips* y en sus potenciales posibilidades.

También los autores de [3] muestran una posible aplicación directa de la utilización de este entorno software en el desarrollo práctico y virtualización de asignaturas de índole telemática, mediante la configuración de escenarios de red. Los escenarios presentados en dicho trabajo abarcan desde unos sencillos y básicos planteamientos iniciales de diseño, como la configuración de enrutamiento estático, hasta la implementación de servicios DHCP y NAT, así como la configuración de *firewall*. Se realizaron igualmente ciertos ensayos para analizar las características y potenciales prestaciones y usos del entorno software *GNS3/Dynamips*.

Estos ensayos, unidos a las referencias anteriores como botón de muestra de estudios y aplicaciones ya realizados, sugieren el empleo de este entorno de virtualización para el desarrollo y consolidación práctica de los contenidos teóricos de asignaturas del área de la Ingeniería Telemática. Unido a esto, la más que contrastada usabilidad del entorno software, facilita enormemente su uso en el ámbito docente.

III. Aplicación y uso de GNS3/DYNAMIPS

Los ensayos realizados en laboratorio van dirigidos, en primer lugar, a que el alumno pueda analizar el diseño y configuración de arquitecturas de red de propósito general, fundamentadas en hardware de red de *Cisco Systems*. En estas arquitecturas, los dispositivos emulados son imagen de elementos de red reales, y funcionan en base a sistemas *Cisco IOS*. Por tanto, estos sistemas operativos deberán ser previamente extraídos del hardware de red, para seguidamente incorporarse en los dispositivos emulados.

En segundo lugar, los análisis se focalizan en la potencial capacidad del entorno simulador/emulador para realizar

pruebas en entornos mixtos, integrando tráfico y equipos reales con escenarios emulados. Esta capacidad puede presentar aplicaciones prácticas interesantes para el alumno, como por ejemplo, segmentar arquitecturas de red en una "parte real" y una "parte emulada", un recurso de diseño que solucionaría problemas logísticos a la hora de implementar topologías extensas con recursos hardware limitados.

Otra aplicación que resulta interesante, especialmente en el entorno docente, es la capacidad de inyectar tráfico real en el entorno emulado para su captura y análisis mediante la herramienta *Wireshark*. Esto permite estudiar las características del tráfico y el efecto de diferentes parámetros de red, como la latencia asociada a una determinada arquitectura de red en un servicio telemático.

IV. Configuración de Arquitecturas de Red

En base a las consideraciones anteriores, en esta sección describiremos los escenarios que se han implementado con *GNS3/Dynamips*. La idea es que, mediante dos ejemplos de arquitecturas de red, podamos realizar un análisis funcional del entorno emulador. En ambos casos, se realiza la interconexión de dos nodos de red por medio de dos tecnologías distintas. Esta configuración se realiza tanto en un entorno real como en un entorno mixto (real-emulado), para poder comparar así los resultados emulados y los obtenidos con equipos reales. De esta forma, cada nodo emulado representa una determinada ubicación física, correspondiente a una bancada del laboratorio de prácticas, y es imagen de un dispositivo de red real *Cisco Systems*. Para ello, sobre el dispositivo emulado se ha incorporado el sistema *Cisco IOS* extraído de un dispositivo real, según la metodología expuesta en [4].

A. Arquitectura de red WAN ppp

En este caso, se interconectan los nodos emulados *Nodo 1* y *Nodo 2* por medio de un enlace serie WAN *point-to-point* de 1,544 Mbps. Los nodos emulados son dispositivos multilayer de la familia *Cisco 3700 series*, que usan el sistema *Cisco IOS*. La Fig. 2 muestra la topología de esta arquitectura en el entorno mixto, así como las características más relevantes del diseño. Los nodos emulados *Auxiliar 1* y *Auxiliar 2* se utilizarán para funciones complementarias en las pruebas.

A la red emulada se conectan también dos equipos reales externos (PC portátiles) siguiendo las indicaciones de [4]. Su conexión se realiza por medio de un enlace *Fast Ethernet*. Las características de estos equipos no son relevantes en el diseño general de la arquitectura, puesto que sólo se utilizan para inyectar o recibir el tráfico de las pruebas. Del mismo modo, se incorporan en el esquema emulado mediante enlaces *Fast Ehernet* dos *host* virtuales (*QEMU2* y *QEMU3*), que ejecutan el sistema Linux *Microcore*. El entorno de emulación permite también la definición de diferentes VLAN. Haciendo uso de esta funcionalidad, consideramos los equipos reales externos adscritos administrativamente a *VLAN2*, y los *host* virtuales a *VLAN3*.

Por tanto, las configuraciones implementadas en los nodos emulados mediante comandos *Cisco IOS* serán idénticas a las implementadas en el escenario real del laboratorio. Cuando se realizan las configuraciones, el *prompt* o intérprete de comandos es el mismo que si estuviésemos configurando el dispositivo real a través de su puerto consola.

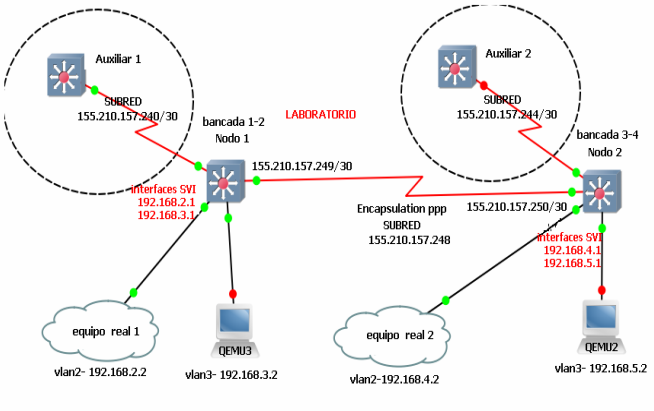


Fig. 2. Topología y características particulares de diseño de la arquitectura de red WAN ppp de estudio.

Cabe destacar que en el entorno emulado, dentro de las características y parámetros de configuración, podemos configurar el *prompt* para que su aspecto visual resulte más familiar para el alumno. En nuestro caso, se ha utilizado la herramienta software *putty*. La Fig. 3 muestra un ejemplo de las configuraciones implementadas en el nodo emulado 1 *(Nodo 1)* de la arquitectura, en este caso la configuración del enlace serie WAN ppp. En este escenario se procede a conferir ciertas características de diseño que permitirían implementar *InterVLAN routing* (conmutación a nivel 3) entre diferentes VLAN, a nivel local en los nodos emulados. Así mismo, no hay que olvidar que la comunicación entre VLAN en nodos diferentes se realiza a nivel de red.

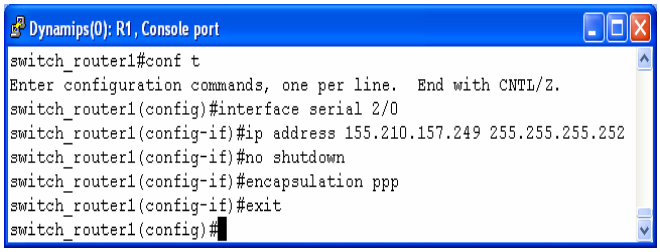


Fig. 3. Configuración del enlace serie WAN ppp en el nodo emulado 1.

Para ello, se configura en nuestra arquitectura el protocolo de enrutamiento dinámico RIPv2, como muestra la Fig. 4. Seguidamente, la Fig. 5 muestra un ejemplo de cómo se implementarían las configuraciones en el nodo emulado 1, a través de los comandos *Cisco IOS* oportunos, mostrando así la asignación física de interfaces a cada VLAN para nuestro ejemplo práctico concreto (Fig. 5a), así como la configuración de los interfaces virtuales SVI, necesarios para implementar *InterVLAN routing* (Fig. 5b).

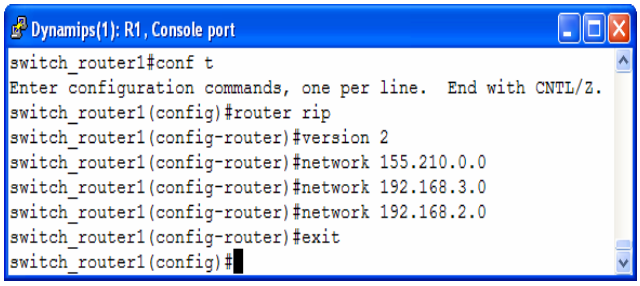
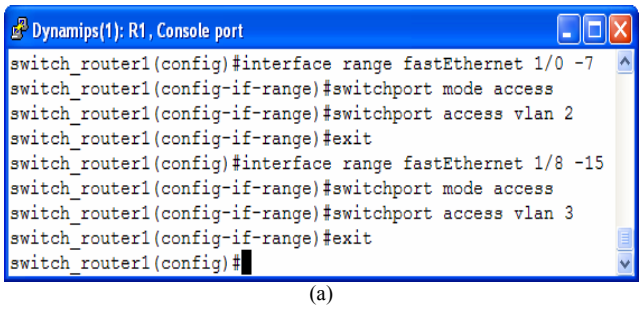
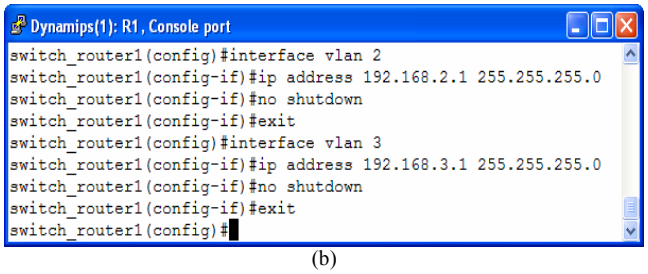


Fig. 4. Configuración del protocolo de enrutamiento dinámico RIP v2 en el escenario emulado.

Una vez implementadas las configuraciones de red, el alumno puede realizar, por ejemplo, un sencillo *test* de la trayectoria del tráfico seguido en la comunicación de equipos pertenecientes a VLAN diferentes en el mismo nodo emulado, como indica la Fig.6. Así se puede comprobar que la arquitectura emulada funciona conforme a nuestros propósitos de diseño, según las configuraciones implementadas, presentando un comportamiento idéntico al de los dispositivos reales.



(a)



(b)

Fig. 5. Configuraciones VLAN en el nodo emulado 1 de la arquitectura WAN ppp.

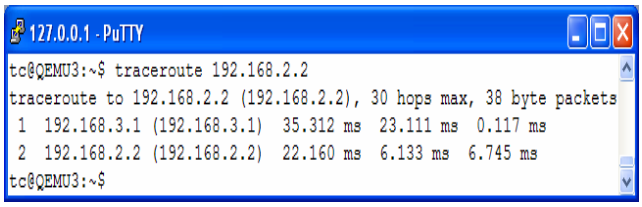


Fig. 6. Trayectoria seguida desde el *host* virtual Linux QEMU3 → equipo real 1, en el nodo emulado 1 (conmutación a nivel 3)

B. Arquitectura de red LAN Ethernet /VTP

En esta arquitectura se configura un entorno conmutado LAN *Ethernet* a nivel 2 y 3, según muestra la Fig. 7. En ella, interconectamos los nodos emulados 1 y 2 por medio de un enlace *Fast Ethernet* que actuará como *trunk-link* (enlace troncal). Por éste circularán, convenientemente identificadas, tramas etiquetadas *(tagged)* y no etiquetadas (*untagged frames)*. Al igual que antes, los nodos *Auxiliar 1* y *Auxiliar 2* se incluyen en el esquema. Los equipos reales externos y los *host* virtuales Linux (*QEMU2* y *QEMU3*) se adscriben a *VLAN2* y *VLAN3*, respectivamente. Al tratarse de un entorno conmutado a nivel 2, no hay intercambio de información a nivel de red entre dispositivos emulados, por lo que no se configuran direcciones IP en los interfaces *Fast Ethernet* asignados al enlace troncal. En consecuencia, no se configura ningún protocolo de enrutamiento dinámico, como sí se hizo en la arquitectura anterior. Recordemos que los nodos emulados son dispositivos *multilayer,* imagen del hardware de red del laboratorio.

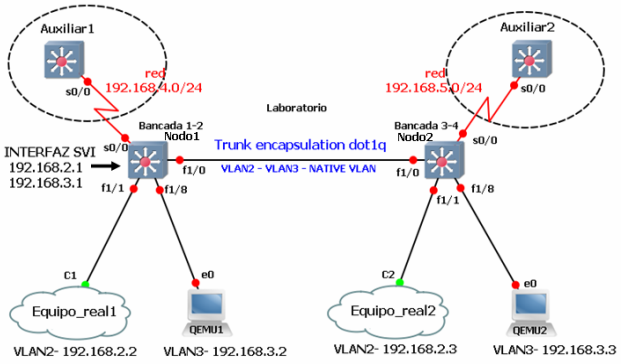


Fig. 7. Topología y características particulares de diseño de la arquitectura de red LAN *Ethernet*/VTP de estudio.

Siendo así, únicamente se confieren características a nivel 3 al nodo emulado 1. Más concretamente, a los interfaces SVI configurados en dicho nodo que nos permitirán implementar *InterVLAN routing* (conmutación a nivel 3 entre VLAN diferentes).

Además, sobre este escenario, se configura el protocolo VTP, propietario de *Cisco Systems,* que permite realizar las tareas de configuración y gestión VLAN de un modo más sencillo. Más información sobre este protocolo y su funcionalidad puede encontrarse en [5]. Aunque la arquitectura implementada aquí es sencilla, la funcionalidad de este protocolo está especialmente indicada en topologías conmutadas más extensas. Así, se configura el rol de servidor VTP en el *nodo 1*. Al *nodo 2* se le asigna la funcionalidad de cliente VTP.

Un ejemplo de estas configuraciones se muestra en la Fig. 8, capturada directamente de *GNS3/Dynamips*. En ella vemos la configuración en el nodo emulado 1 del enlace troncal, en concreto la asignación física particular de diseño de los interfaces *Fast Ethernet* a cada VLAN, así como la configuración del dominio y funcionalidad VTP. Como vemos, el alumno puede, mediante comandos *Cisco IOS,* configurar los parámetros del protocolo del mismo modo que se implementan en el correspondiente hardware de red real.

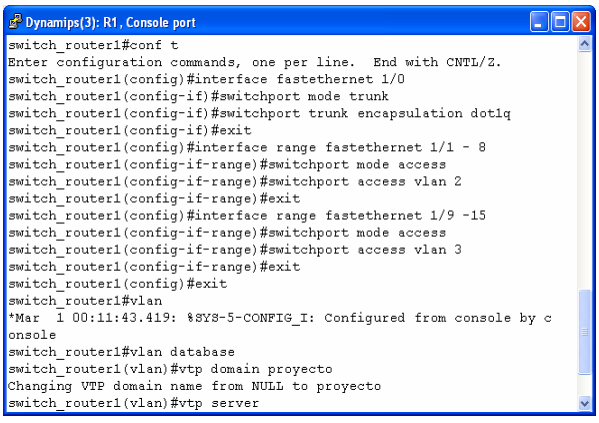


Fig. 8. Configuración implementada en el nodo 1 de la arquitectura LAN Ethernet/VTP.

Como ejemplo del realismo de las pruebas, y de la capacidad del sistema para comportarse de manera idéntica a los equipos reales, mostramos ahora (Fig. 9) el análisis de la trayectoria del tráfico en la comunicación de equipos adscritos a una misma VLAN, pero en nodos diferentes (traza

verde, conmutación a nivel 2 vía enlace troncal), así como la trayectoria usada para comunicar equipos pertenecientes a VLAN diferentes, pero en el mismo nodo emulado (conmutación a nivel 3 vía enlace troncal, traza azul).

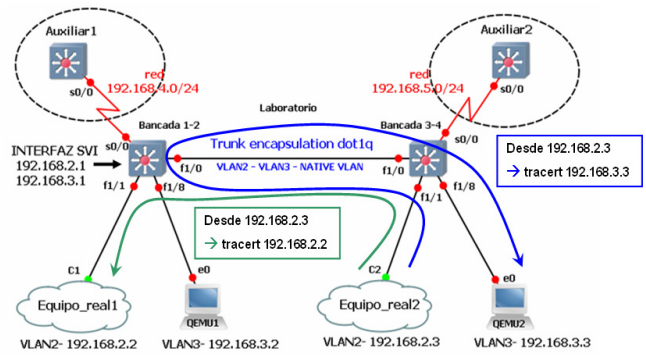


Fig. 9. Análisis de la trayectoria del tráfico de red para distintos tipo de comunicación en la arquitectura LAN *Ethernet*/VTP.

Los resultados de estos ensayos, consecuentes con las configuraciones implementadas, se observan en la Fig. 10. Vemos que la conmutación a nivel 2 entre equipos pertenecientes a la misma VLAN sólo implica un salto, mientras que la conmutación a nivel 3 conlleva dos: el primero para alcanzar el interfaz virtual SVI en el nodo emulado 1, y el segundo para alcanzar el *host* final desde dicho interfaz virtual. En ambos casos se hace uso del enlace troncal. De esta manera, el entorno emulado permite en este caso ayudar al alumno a comprender la diferencia entre la conmutación a nivel 2 y nivel 3, y la funcionalidad de las VLAN.

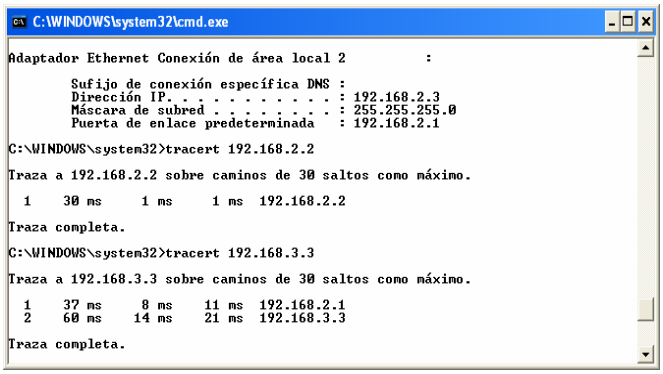


Fig. 10. Resultados de los análisis del rigor funcional de *GNS3/Dynamips*.

C. Ejemplo práctico avanzado de interoperación entre los entornos de red real y emulado

Se plantea, en base a las arquitecturas anteriores, la implementación de un servicio telemático cliente/servidor FTP para la transmisión pasiva y anónima [6] de un fichero de 250 KB. Como muestra la Fig. 11 (por ser la topología similar en las dos pruebas, sólo se muestra la arquitectura LAN Ethernet/VTP), tanto el cliente como el servidor FTP son equipos reales y externos al entorno emulado de *GNS3/Dynamips*, e interoperan con él. El cliente y el servidor se encuentran conectados a nodos emulados diferentes.

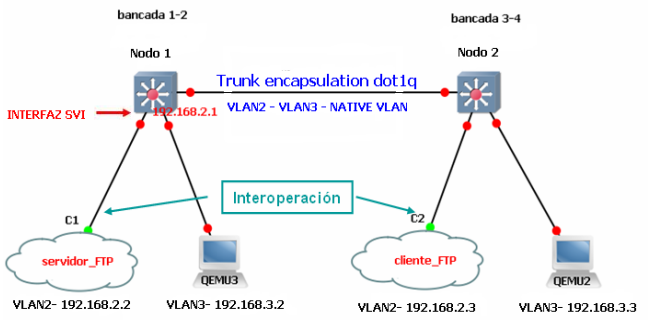


Fig. 11. Esquema de la implementación de un servicio FTP cliente/servidor usando la interoperación del entorno real con el entorno emulado.

Con el objetivo de hacer comprender al alumno la importancia del tamaño de la trama en la transmisión de un fichero, la transmisión se puede realizar con diferentes longitudes de trama Ethernet: 64, 512, 1.024 y 1.514 bytes. En ambas arquitecturas de estudio, la conexión y la transmisión del fichero se puede realizar correctamente, salvo para la longitud de trama de 64 bytes. Esta última es demasiado pequeña como para contener toda la información de las cabeceras añadidas por los protocolos necesarios para el funcionamiento de FTP.

De los resultados obtenidos (Tabla I) se deduce que en este escenario el valor de 1.024 bytes obtiene el menor tiempo de transmisión. El valor de trama de 1.514 bytes parece evidenciar una cierta congestión en el enlace serie ppp, posiblemente relacionada con la diferencia de ancho de banda entre *Fast Ethernet* (en la conexión entre el equipo real y el nodo emulado), y el enlace serie. Para analizar estos resultados se ha realizado la captura del tráfico asociado a la transmisión en el enlace WAN ppp, que el alumno puede visualizar y analizar con *Wireshark*.

TABLA I
RESULTADOS OBTENIDOS EN LA TRANSMISIÓN FTP PASIVA Y ANÓNIMA CLIENTE/SERVIDOR PARA LA ARQUITECTURA WAN PPP.

	trama 64 bytes	trama 512 bytes	trama 1.024 bytes	trama 1.514 bytes
Longitud trama ACK	-	60 bytes	60 bytes	60 bytes
Nº tramas totales en la transmisión (información y control)	-	986	477	361
Nº tramas de información FTP_DATA	-	560 + 1 trama de 419 bytes	257 + 1 trama de 139 bytes	171 + 1 trama de 1.129 bytes
Nº tramas de información FTP_DATA retransmitidas	-	9	10	9
Δ tiempo total en la transmisión (información)	-	13,703 seg.	9,114 seg.	11,36 seg.

En el caso de la arquitectura LAN Ethernet/VTP, la transmisión FTP del fichero se realiza entre equipos reales adscritos a una misma VLAN, pero conectados a nodos emulados distintos. Por consiguiente, la transmisión del

fichero implica en este caso que la conmutación se haga a nivel 2 mediante el enlace troncal *(trunk link)*. Por ello, y como muestra la Tabla II, los tiempos de transmisión son considerablemente más bajos que en la arquitectura anterior.

Del mismo modo, en este caso sí puede considerarse como longitud óptima de trama *Ethernet* 802.3 el valor de 1.514 bytes. Debido a la información añadida por el protocolo IEEE 802.1Q (también llamado *dot1q*), este tamaño se corresponde con un valor de trama Ethernet 802.1Q de 1.518 bytes en el enlace troncal. Estos 4 bytes añaden la información necesaria para identificar *tagged* y *untagged frames* (tramas etiquetadas y no etiquetadas). El protocolo 802.1Q no encapsula la trama original, sino que únicamente añade 4 bytes al encabezado *Ethernet*. El valor del campo *EtherType* cambia a 0x8100, para así señalar el cambio en el formato de la trama. Además, 802.1Q obliga a recalcular el campo FCS [5].

TABLA II
RESULTADOS OBTENIDOS EN LA TRANSMISIÓN FTP PASIVA Y ANÓNIMA CLIENTE/SERVIDOR PARA LA ARQUITECTURA LAN ETHERNET/VTP

	trama 64 bytes	trama 512 bytes	trama 1.024 bytes	trama 1.514 bytes
Longitud trama ACK	-	66 bytes	66 bytes	66 bytes
Nº tramas totales en la transmisión (información y control)	-	966	47	357
Nº tramas de información FTP_DATA	-	561 + 1 trama de 305 bytes	259 + 1 trama de 919 bytes	172 + 1 trama de 453 bytes
Nº tramas de información FTP_DATA retransmitidas	-	24	21	7
Δ tiempo total en la transmisión (información)	-	1,3 seg.	1,03 seg.	0,43 seg.

V. ANÁLISIS DEL RENDIMIENTO DEL SISTEMA

Una característica común a todas las plataformas software de emulación es que el consumo de recursos del sistema emulador puede llegar a ser muy elevado, sobre todo en términos de carga de CPU y memoria RAM. Este hecho puede llegar a condicionar la escalabilidad de las arquitecturas a emular.

Para disminuir el consumo de memoria RAM, *GNS3/Dynamips* dispone de varios optimizadores, entre los que destaca *ghost ios*. Esta utilidad mapea una región de memoria compartida por los dispositivos emulados que ejecutan el mismo sistema *Cisco IOS,* en lugar de copiar el sistema tantas veces como dispositivos se estén emulando. De esta manera se evita que cada dispositivo necesite su propia región de memoria. Por lo tanto, este recurso es óptimo si todos los dispositivos de nuestra arquitectura son similares. Con el uso de *ghost ios,* el consumo de memoria RAM deja de ser crítico para la emulación, siempre que el PC emulador disponga de la suficiente memoria RAM (el mínimo aconsejable son 2 GB).

No ocurre lo mismo con la carga de CPU, que se convierte en el principal límite en la emulación de topologías extensas. A pesar de configurar inicialmente el parámetro *idle PC* [4] al iniciar el diseño de una arquitectura, y así optimizar el rendimiento del procesador en la emulación, la carga de este último aumenta considerablemente conforme se incrementa el número de nodos emulados.

Los ensayos realizados en el laboratorio sobre un PC de gama tecnológica media (procesador de un solo núcleo) emulando las arquitecturas previamente consideradas, se resumen en la Tabla III. Para analizar el consumo de recursos, se consideran activos los nodos *Auxiliar 1* y *2*, que se configuran mediante comandos *Cisco IOS*. Cabe destacar que estos nodos emulados no tienen ningún propósito telemático especial de diseño: su objetivo es solamente evaluar la repercusión del número de nodos emulados activos sobre el rendimiento y el consumo de recursos del sistema emulador. Así podremos evaluar, de un modo aproximado, la potencial escalabilidad del diseño de la arquitectura emulada.

Se ha observado que los resultados se estabilizan tras un pequeño transitorio inicial, una vez iniciamos los equipos que participan en el escenario. Este tiempo es necesario para el inicio del sistema operativo *Cisco IOS* y las configuraciones asociadas a las arquitecturas de red. En los resultados de la Tabla III, las expresiones "XX→XX" deben interpretarse como el descenso en el consumo de recursos en el PC emulador, cuando los recursos optimizadores (principalmente *ghost ios*) se activan.

TABLA III
CONSUMO DE RECURSOS DEL SISTEMA EMULADOR OBTENIDO

Nodos activos	Carga de CPU (*offmode*)	RAM en uso en MB (*offmode*)	Carga media de CPU (*pseudo-activo)*	RAM en uso en MB (*pseudo-activo*)
1 nodo	1% max.	318	1-2 %	780 → 540
2 nodos	1% max.	318	4 % → 2-3%	940 → 720
2 nodos + 1 QEMU	1% max.	318	16 % →14%	950 → 750
2 nodos + 2QEMU	1% max.	318	17 % →15%	960 → 760
2 nodos + 1 Aux (noQEMU)	1% max.	318	6 % → 4-5%	970 → 760
2 nodos + 2 Aux (noQEMU)	1% max.	318	11 % →10%	980 → 790

No debe confundirse el descenso en la carga de CPU en este caso con el descenso debido a la configuración del parámetro *idle PC* (parámetro a configurar en los nodos emulados al iniciar el diseño de una arquitectura). El descenso es atribuible a que el sistema se estabiliza tras varios minutos, una vez se han cargado completamente los sistemas *Cisco IOS* y las configuraciones de los dispositivos, y posteriormente los recursos optimizadores de memoria RAM están activos y se ha configurado la región de memoria compartida para los dispositivos. El estado *offmode* es el estado del PC antes de iniciar el software emulador.

Una vez iniciado *GNS3/Dynamips*, el estado *pseudo-activo* se refiere al tiempo en que los nodos sólo intercambian información de los protocolos a nivel 2 y 3. Igualmente es apreciable cómo el uso de *host* virtuales Linux QEMU eleva significativamente la carga de CPU, respecto a escenarios que no los incluyen (para ello, comparamos las filas 2 y 3 de la Tabla III). Sin embargo, conforme incorporamos más *host* virtuales QEMU, el consumo crece, pero en mucha menor medida (resultado comparativo de las filas 3 y 4).

Finalmente, y centrando la atención únicamente en los nodos emulados *switch-router* de nuestras arquitecturas anteriores (quedan por tanto excluidas las filas 3 y 4 de la Tabla III), podemos "aproximar" la tendencia del consumo de CPU a partir de dos nodos emulados con una progresión geométrica de razón dos (incidimos en la connotación de cálculo aproximado), que nos permitiría implementar arquitecturas de hasta 7 nodos emulados. Esta cota máxima de potencial *escalabilidad* implicaría una carga de CPU entre el 70% y el 90 %. Acerca de este consumo, no debe olvidarse la circunstancia de que nuestro sistema emulador es un PC de gama tecnológica media. Sobre PC emuladores de gama tecnológica alta es esperable una mayor capacidad de incluir máquinas emuladas.

VI. Análisis de Parámetros de Red en la Interoperación entre los Entornos Real y Emulado

En la sección anterior se ha contrastado mediante pruebas de laboratorio que la funcionalidad a nivel 2 y 3 del emulador es rigurosa. Vemos confirmado, por tanto, que los nodos emulados dentro de *GNS3/Dynamips* pueden interoperar con equipos reales en la red, a través de interfaces *Ethernet* disponibles en el PC emulador [4]. Este hecho da la posibilidad de que el alumno pueda utilizar hardware emulado sin la necesidad de disponer realmente del equipo.

En esa sección analizaremos la capacidad del entorno para emular con realismo ciertos parámetros de red que pueden ser críticos en la prestación de servicios telemáticos. Aunque la funcionalidad del hardware emulado sea idéntica al del real, existirán de hecho algunas diferencias en el comportamiento, como por ejemplo, valores diferentes en los retardos añadidos por los dispositivos. No olvidemos que existen servicios en los que el retardo es crítico (por ejemplo, Voz sobre IP, VoIP), y para los que la ITU-T define unos valores máximos [7].

Estas particularidades deben ser adecuadamente interpretadas por el alumno, que deberá distinguir los retardos asociados al hardware real de los que se deriven de utilizar un entorno emulado. Se han realizado en el laboratorio, y utilizando las arquitecturas previamente presentadas, dos tipos de análisis para medir las diferencias entre un entorno real y uno mixto incluyendo máquinas reales y emuladas. En ambos se han implementado peticiones de eco desde el *equipo real 1* de los diseños (ver Fig. 2 y Fig.7), evaluándose el retardo de ida y vuelta (*Round Trip Time, RTT)* a través del protocolo ICMP (instrucción *ping*).

Los análisis se han realizado para diferentes cargas de trabajo del PC emulador, utilizando para ello los nodos *Auxiliar 1* y *2* de las arquitecturas. En consecuencia, el valor del *Round Trip Time* reflejará la latencia mínima a considerar en el escenario real-emulado de trabajo, ya que el protocolo ICMP no implementa control de errores en la transmisión.

Para el primero de los análisis, la petición de eco tiene como destino el interfaz virtual SVI configurado en el *nodo emulado 1* (recordemos que este interfaz sirve para implementar *InterVLAN routing*). El segundo de los análisis tiene como destino el *equipo real 2*, que interopera con el *nodo emulado 2*. En este segundo análisis deberemos "atravesar", por lo tanto, la arquitectura emulada, y recibir la petición de eco en el *equipo real 2*. Estos ensayos se reflejan en la Fig. 12, para la arquitectura LAN *Ethernet*/VTP (el esquema sería similar para la arquitectura WAN ppp). Así mismo, los análisis se han realizado para las longitudes de trama Ethernet consideradas en apartados anteriores: 64, 512, 1.024 y 1.514 bytes.

Los valores de la latencia para el primero de los experimentos son muy elevados, y similares para las dos arquitecturas. Estos valores se muestran en la Tabla IV.

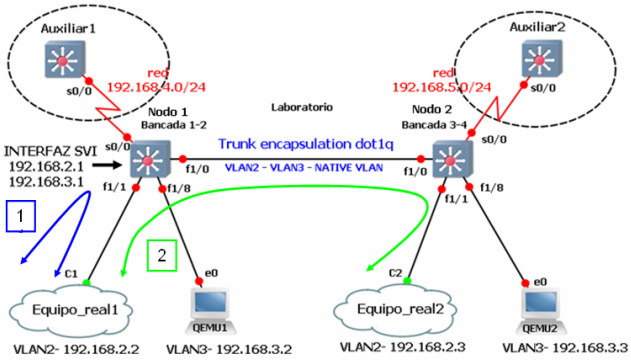


Fig. 12. Detalle de los ensayos implementados en el análisis de la latencia de red en la interoperación entre los entornos de red real y emulado.

TABLA IV
VALORES OBTENIDOS EN EL PRIMER EXPERIMENTO DE LA LATENCIA DE RED

RTT promedio (milisegundos)	1 nodo activo	2 nodos activos	3 nodos activos	4 nodos activos
Trama de 64 bytes	32 → 30	40 → 34	47 → 40	61→ 49
Trama de 512 bytes	34 → 31	41 → 35	48 → 42	62→ 51
Trama de 1.024 bytes	37 → 32	44 → 37	51 → 45	67→ 54
Trama de 1.514 bytes	39 → 33	45 → 39	52 → 46	67→ 55

Para el segundo de los experimentos, en el caso de la arquitectura WAN ppp los resultados son igualmente elevados, debido a que existe una comunicación a nivel 3 entre los equipos reales a través de la arquitectura emulada.

Y aunque estos valores cumplen de hecho las recomendaciones de retardo máximo de la ITU-T [7], no son directamente trasladables a un escenario de red real similar, ya que nuestra conexión *extremo-a-extremo* sólo incluye dos nodos emulados.

En el caso de la arquitectura LAN Ethernet/VTP los resultados son más acordes a lo esperable en un entorno real análogo, como muestra la Tabla V. En este caso, la petición de eco sólo requiere conmutación a nivel 2 entre los equipos

reales, por estar adscritos a la misma VLAN en nodos emulados diferentes.

TABLA V
VALORES DE LATENCIA OBTENIDOS EN EL SEGUNDO EXPERIMENTO PARA LA ARQUITECTURA DE RED LAN ETHERNET/VTP.

RTT promedio (milisegundos)	1nodo activo	2 nodos activos	3 nodos activos	4 nodos activos
Trama de 64 bytes	-	2 → 1-2	3 → 2	3 → 2
Trama de 512 bytes	-	2 → 1-2	3 → 2	4 → 3
Trama de 1.024 bytes	-	2 → 1-2	3 → 2	5→ 4
Trama de 1.514 bytes	-	3 → 2-3	4 → 3	6 → 5

A partir de los resultados obtenidos, podemos interpretar que se da un comportamiento correcto de la latencia a nivel 2, pero un comportamiento poco realista cuando se ejecutan en *GNS3/Dynamips* procesos de conmutación a nivel 3. Estos límites en el realismo del entorno emulador deberán ser tenidos en cuenta por el alumno, sabiendo que la conmutación a nivel 3 añade unos retardos adicionales, que estarán en función de la capacidad de proceso de la máquina en la que se ejecute el entorno.

Tal como se mencionó con anterioridad, focalizando el uso de *GNS3/Dynamips* como herramienta académica, el comportamiento de la latencia no resulta decisivo ni condiciona el análisis de arquitecturas de red y la funcionalidad de los protocolos a nivel 2 y 3. Pero puede resultar interesante, bajo el prisma docente, aprovechar los ensayos anteriores como base para incidir en la importancia del análisis, comportamiento y restricciones de la latencia y de otros parámetros de red.

VII. CONCLUSIONES

En este trabajo se han presentado una serie de análisis sobre el uso de entornos de pruebas mixtos, integrando máquinas reales y emuladas, en el ámbito de la docencia en Ingeniería Telemática. En concreto, se han realizado diferentes pruebas con el entorno software *GNS3/Dynamips,* como una herramienta adecuada en el ámbito académico, con un claro enfoque hacia el mundo profesional.

Se ha contrastado la adecuada usabilidad del software, a través de su intuitivo interfaz gráfico. A pesar de que actualmente este emulador se circunscribe a entornos corporativos con hardware de *Cisco Systems* y *Juniper*, esto no es inconveniente para diseñar y analizar arquitecturas de red más generales. Las configuraciones de estos dispositivos emulados se realizan de forma idéntica a como se implementarían mediante el puerto consola del hardware real correspondiente. Esta ventaja permite al alumno realizar pruebas con escenarios de red reales sin necesidad de disponer de los dispositivos físicos, cuya disponibilidad puede ser limitada. Igualmente, esta circunstancia es una ventaja manifiesta a la hora de plantear posibles escenarios de estudio.

Añadidas a las ventajas anteriores, la capacidad del entorno emulador de interoperar con escenarios de red reales amplía enormemente las posibilidades docentes para el análisis de escenarios y servicios telemáticos, teniendo en cuenta que las capturas de tráfico emuladas se pueden analizar mediante *Wireshark*.

Se han presentado pruebas, mostrando que la funcionalidad a nivel 2 y 3 del emulador es correcta y rigurosa con análogos escenarios de red reales. También se ha detectado que el sistema añade retardos diferentes de los que se obtendrían en un entorno real, especialmente si el número de nodos es elevado y se usa conmutación a nivel 3.

Como trabajo futuro se considera el uso de recursos optimizadores más complejos de *GNS3/Dynamips*, que pueden aumentar su escalabilidad. Tal es el caso del recurso *Hypervisors*, que permiten repartir la carga de los procesos de emulación entre varias máquinas, aumentando así las posibilidades de diseño y la escalabilidad de las arquitecturas de estudio.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente subvencionado por el Fondo Social Europeo en colaboración con el Gobierno de Aragón, el proyecto CPUFLIPI (MICINN TIN2010-17298) del Gobierno de España así como por la Cátedra Telefónica-Universidad de Zaragoza.

REFERENCIAS

[1] S. Gimeno Martínez. "Evaluación de plataformas virtuales: Estudio comparativo". Tesis de Máster. Universidad Politécnica de Valencia. Escuela Técnica Superior de Informática Aplicada. Valencia, Diciembre de 2008.

[2] J. Martínez, J.J. Ortega, J.A. Fernández. "Laboratorios virtuales de redes: sí, inténtelo en casa". JENUI 2011. Sevilla. Julio de 2010.

[3] J. M. Ribadeneyra Sicilia. "Prácticas de redes en entorno real en laboratorios de propósito general". XVI Jornadas de Enseñanza Universitaria de la Informática. Santiago de Compostela: Universidade de Santiago de Compostela. Escola Técnica Superior d'Enxeñaría, p. 155-160, 2010.

[4] Graphical Network Simulation – GNS3- Documentation (n.d). Recuperado en octubre de 2012 de http://www.gns3.net/documentation

[5] Cisco Systems, Inc. (2006). *Cisco Networking Academy program, CCNP: Building Multilayer Switching Networks v.5.0*, San Jose, USA: Americas Headquarters.

[6] File Transfer Protocol (n.d.). En *Wikipedia*. Recuperado en Diciembre de 2012 de http://es.wikipedia.org/wiki/File_Transfer_Protocol

[7] Unión Internacional de Telecomunicaciones (n.d.). *Normalización UIT-T.* Recuperado en Febrero de 2013 de http://www.itu.int/ITU-T/sitemap/index.asp

Índice de autores