Teoría de la Señal, Telemática y Comunicaciones:

Una visión del campo a través de trabajos fin de grado y fin de carrera

Curso 2013/2014

Jorge Navarro Ortiz
Luz García Martínez
Eds.

Teoría de la Señal, Telemática y Comunicaciones:

Una visión del campo a través de trabajos fin de grado y fin de carrera

curso 2013 / 2014

Editores:

Jorge Navarro Ortiz

Luz García Martínez

ugr Universidad de Granada

ETSIIT Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

TSTC Departamento de Teoría de la Señal, Telemática y Comunicaciones

ISBN-10: 84-617-3239-1
ISBN-13: 978-84-617-3239-5

Editores: Jorge Navarro Ortiz y Luz García Martínez (Dpto. Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada)

Portada: Pilar Andrés Maldonado
Maquetación: Jorge Navarro Ortiz y Luz García Martínez

Presentación

El campo de las redes y las comunicaciones, la telemática, el procesado de señal e información constituyen un eje primordial de desarrollo de las conocidas *Tecnologías de la Información y las Comunicaciones* (TIC). Esta relevancia queda de manifiesto, de una parte, en la dependencia social actual de las TIC y, de otra parte y derivado de lo anterior, en la enorme demanda actual de formación universitaria relacionada con las telecomunicaciones y la informática.

Si bien es cierto que el área TIC presenta un corpus y fundamentos técnicos bien asentados, no lo es menos que las tecnologías, los sistemas y los servicios evolucionan de forma continua, dando lugar a nuevas posibilidades pero también a nuevas necesidades y retos.

En este contexto, y como colofón al ciclo formativo de las ingenierías universitarias, en particular en lo que respecta a las de *Telecomunicación* e *Informática* en que imparte el *Dpto. de Teoría de la Señal, Telemática y Comunicaciones* (DTSTC), los estudiantes deben desarrollar anualmente un trabajo técnico de cierto empaque que, transcendiendo las materias y contenidos vistos hasta el momento, por una parte evidencie unas capacidades extra de aprendizaje, autonomía y búsqueda de soluciones a problemas complejos, y por otro lado suponga una evolución o mejora en la problemática abordada respecto del estatus actual.

A través del presente libro, y en el marco del *X aniversario* de la creación del DTSTC, se pretende mostrar un ejemplo de lo anteriormente expuesto en base a los desarrollos realizados durante el curso académico 2013/2014 por nuestros alumnos, bajo la dirección y supervisión de nuestros profesores, en algunas de las distintas líneas de investigación, desarrollo e innovación de interés TIC.

Desde aquí quiero evidenciar y agradecer, como responsable en materia docente que soy, la labor y dedicación de todos, alumnos y profesores, en esta tarea tan necesaria socialmente. Ello, junto con el entusiasmo siempre mostrado, son las mejores herramientas de que disponemos para conseguir el avance común y la superación de cualquier obstáculo.

Un saludo,

Pedro García Teodoro
Director del Dpto. de Teoría de la Señal,
Telemática y Comunicaciones
ETS Ingenierías Informática y de Telecomunicación
Universidad Granada

Índice de contribuciones

Área de Ingeniería Telemática

Aplicaciones en dispositivos móviles o de tamaño reducido

Calidad de experiencia

Juegos en red

Proyectos en empresas

Redes móviles e inalámbricas

Seguridad en redes y sistemas

Área de Teoría de la Señal y Comunicaciones

Procesado de la señal en instrumentación científico-técnica

Procesado de señales biomédicas

Procesado de voz y audio

Ingeniería Telemática

Control de una red de sensores ZigBee Home Energy desde dispositivos Android

Tutor: Jesús Esteban Díaz Verdejo; e-mail: jedv@ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

Autor: Juan Vázquez Sánchez, e-mail: juanvs@correo.ugr.es

***Resumen*—Las redes de sensores constituyen en la actualidad un elemento en clara expansión. Estas se componen de un conjunto de dispositivos autónomos distribuidos en un área con la finalidad de monitorizar y medir parámetros a partir de la formación de una red de comunicaciones, inalámbrica en la mayoría de los casos. Los ámbitos de aplicación son numerosos, siendo especialmente relevante en la actualidad su utilización en el contexto de las denominadas *SmartCities*. Otra tecnología de gran impacto en la sociedad actual son los teléfonos inteligentes, que incorporan múltiples capacidades de comunicación y conexión a Internet. En este contexto, en el presente proyecto se plantea el desarrollo de un sistema que permita controlar elementos de una red de sensores, cuya finalidad primaria sea la monitorización del consumo eléctrico de dispositivos en el hogar, desde un dispositivo móvil. Debido a sus múltiples capacidades y posibilidades, se ha elegido la tecnología ZigBee para el despliegue de la red de sensores, mientras que la plataforma móvil seleccionada ha sido Android, por su popularidad y por ser de libre distribución. De esta forma, en el presente proyecto se integran dos tecnologías novedosas y de gran penetración en la actualidad, obteniéndose un producto que resulta interesante para los usuarios finales de cara a controlar su consumo energético. El sistema resultante, además de proporcionar los datos de consumo de los equipos eléctricos monitorizados, permite su desconexión de la red mediante la simple pulsación de una tecla en su dispositivo móvil, gracias a las capacidades que presentan los sensores ZigBee utilizados.**

***Palabras clave*—ZigBee, Android, Smart Energy, redes de sensores.**

I. Introducción

La idea de sostenibilidad y, consecuentemente, el uso óptimo de los recursos disponibles, está muy presente en la actualidad. En el ámbito de las tecnologías de la información y las comunicaciones (TIC), este concepto se ha convertido en motor de múltiples proyectos y tecnologías, entre los que podemos mencionar por relacionada con los objetivos del presente trabajo, la idea de *Smart Cities* [1]. Este es un concepto novedoso aplicado a aquellas ciudades que contemplan la eficiencia energética y sostenibilidad junto con las Tecnologías de la Información y las Comunicaciones (TIC). Además, asociado a este concepto se encuentra el denominado *Smart Grid*. En este último se pretende aplicar las TIC para optimizar el uso de la energía eléctrica. En este sentido, ya es obligatorio en España el uso de contadores inteligentes (*Smart meters*) [2] que pueden ser monitorizados y operados remotamente por la compañía suministradora y que posibilitan el análisis temporal del consumo realizado, consiguiendo de esta forma una mayor rapidez y eficiencia en la relación cliente-proveedor. Las tecnologías disponibles para esta monitorización son varias. Sin embargo, este proyecto se centrará en el uso de ZigBee como elemento central de la solución. Se trata de una tecnología muy interesante, basada en la estandarización de un protocolo para comunicaciones inalámbricas de baja transferencia de datos y dirigida, entre otros, al campo de la domótica, por lo que resulta adecuado para el propósito del presente proyecto.

Como motivación cabe indicar que existen dos elementos principales. En primer lugar, se consideran las tecnologías inalámbricas, cuyo uso se está imponiendo en la actualidad y fruto de las cuales surgen las redes de sensores, que constituyen en la actualidad una tecnología en clara expansión. El segundo elemento son los *smartphones*, sobre los que no hay muchos aspectos que explicitar, ya que actualmente prácticamente todo el mundo dispone de uno de ellos. Las capacidades y servicios que ofrecen, gracias al amplio abanico de aplicaciones de las que disponen, son ampliamente conocidos por los usuarios.

El objetivo principal del proyecto es el control y monitorización remoto del consumo de aparatos electrónicos mediante una red ZigBee, haciendo posible la manipulación de los dispositivos. Para ello se dispondrá de equipos ZigBee con las capacidades necesarias (conmutación y control de consumo de equipos conectados al dispositivo). Dado que lo que se pretende es unir esta tecnología con los *smartphones*, esta manipulación de dispositivos se realizará a través de una aplicación móvil Android.

Este objetivo principal se desglosa en varios puntos. En primer lugar será necesario desplegar y configurar una red ZigBee. A continuación se implementa una aplicación móvil para el control de los elementos de la red ZigBee y su configuración. Finalmente, se precisa del desarrollo de un sistema intermediario para el almacenamiento de los datos de consumo y de configuración de la red que permita su consulta remota y que obtenga los datos necesarios de forma autónoma a partir de la propia red ZigBee.

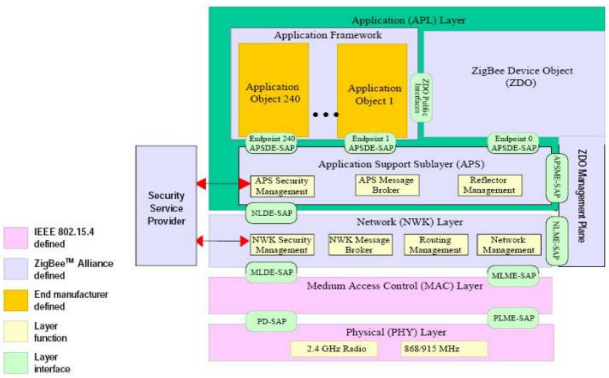


Fig. 1: Arquitectura de ZigBee [3].

II. FUNDAMENTOS TÉCNICOS

Las redes ZigBee incluyen tres tipos de dispositivos, los cuales se disponen en una estructura normalmente jerárquica. Los **coordinadores** se encargan de inicializar y controlar la red, existiendo un único coordinador en cada red ZigBee. El coordinador almacena información sobre la red, la cual incluye términos relativos a la seguridad de la misma. Realiza funciones globales como la gestión del encaminamiento o la incorporación de nuevos dispositivos. Los **routers** permiten extender el área de cobertura de la red, realizando labores de encaminamiento y retransmisión de paquetes hacia otros routers o a los dispositivos finales que depende de él. También pueden operar como dispositivos finales de dicha red. Los **dispositivos finales** son los dispositivos terminales de la red. Tienen la funcionalidad necesaria para comunicarse con el nodo del que depende, denominado nodo padre, que puede ser un router o un coordinador. Pueden transmitir o recibir mensajes, pero no pueden desarrollar ninguna operación de enrutamiento.

La *ZigBee Alliance* [3] proporciona una serie de estándares específicos para las diferentes aplicaciones que se consideran en ZigBee, denominados **perfiles**, tanto para el sector particular como para el sector empresarial, haciendo que los diferentes clientes tengan un mayor control y mejoren sus actividades cotidianas. Estos perfiles especifican cómo deben funcionar/comunicarse los dispositivos ZigBee dentro de un determinado campo/mercado, haciendo posible de este modo que se puedan integrar dispositivos de distintos fabricantes para unas tareas determinadas. Entre los múltiples perfiles existentes, en la realización del presente proyecto se usará principalmente el perfil *ZigBee Smart Energy* [4], el cual facilita el uso de productos interoperables que monitorizan, controlan, informan y automatizan la entrega y uso de la energía y el agua. El objetivo primario de este perfil es el de mejorar la eficiencia en el uso de los recursos.

Las especificaciones de ZigBee se basan en la definición de varios elementos funcionales, entre los que destaca el concepto de *cluster*. Los *clusters* pueden ser entradas o salidas de un dispositivo o un conjunto de ellas. Existe una librería de *clusters* estándar que puede ser usada por cualquier aplicación. Esta librería es la *ZigBee Cluster Library ZCL*, que define un conjunto de *clusters* comunes y los organiza dentro de diferentes dominios funcionales, como pueden ser, a modo de ejemplo, iluminación, calefacción, ventilación, etc. Un *cluster* puede ser reutilizado en varios dominios funcionales, independientemente del perfil considerado.

La pila ZigBee presenta una arquitectura en varias capas (Fig. 1). Las capas inferiores vienen especificadas en el estándar IEEE 802.15.4 (correspondientes a la capa MAC y a la capa física) mientras que las demás capas (capa de red y capa de aplicación) se definen dentro de ZigBee. Además, dentro de la pila de protocolos también se consideran capas *cross-layer*, las cuales se definen como capas auxiliares que proporcionan funcionalidades a varias capas. En el caso de ZigBee hay dos capas de este tipo, que son las denominadas ZDO (*ZigBee Device Object*) y SSP (*Security Service Provider*).

Por otra parte, se usará el sistema operativo Android para realizar una aplicación con su correspondiente estilo de programación. El desarrollo de esta aplicación requiere de una formación específica, ya que se trata de una filosofía de programación que difiere de los lenguajes convencionales orientados a objetos, tales como Java. Una aplicación Android se divide en tres bloques claramente diferenciados. El primer tipo de estos bloques son las clases, las cuales se encargan de desarrollar toda la parte lógica de la aplicación y el funcionamiento de cada una de las pantallas o actividades, así como todos aquellos procesos asociados a la actuación del usuario sobre un elemento de la interfaz y a los procesos que se ejecutan en segundo plano, y que son transparentes para el usuario de la aplicación. Otro bloque lo componen los elementos básicos de una interfaz gráfica, los cuales se encargan de describir todos los aspectos visuales de la aplicación y de recoger toda la información necesaria para describir el aspecto visual de todas las actividades de la aplicación, así como de algunos elementos visuales concretos. El último bloque lo constituye un fichero denominado *Manifest*, el cual incluye propiedades básicas de la aplicación y de los componentes que forman parte de la misma. En la Fig. 2 se muestra la interfaz gráfica de la aplicación implementada.

Además se hará uso de un servicio web y de una base de datos para almacenar la información de gestión de los dispositivos que forman la red ZigBee, así como los datos relativos a las funcionalidades y parámetros de los mismos. Cabe destacar la importancia de esta base de datos en

Fig. 2: Interfaz de la aplicación Android implementada.

relación a la gestión de la información de los dispositivos de la red y la conformación de las tramas necesarias para el control de los mismos.

III. ARQUITECTURA DEL SISTEMA

La arquitectura general del sistema se basa en el paradigma cliente/servidor, en el cual existirá un proveedor de recursos y servicios, y un cliente, el cual se encargará de usar dichos recursos. En la arquitectura propuesta (Fig. 3) se han considerado las funcionalidades necesarias para prescindir del software propietario proporcionado por el fabricante para la gestión de la red ZigBee.

En la arquitectura planteada se pueden diferenciar tres módulos. Un primer módulo se corresponde a la aplicación del dispositivo móvil, en la que se considera una base de datos para almacenar datos de consumo. El segundo módulo se estructura a partir de un servidor, que interacciona con el dispositivo móvil y que accede a una base de datos con información sobre la red. Finalmente, el tercer módulo está compuesto por los dispositivos ZigBee, es decir, de un coordinador y de un router ZigBee.

En el primer módulo se dispone de la aplicación móvil que permite al usuario interactuar con la red ZigBee y realizar operaciones como encender y apagar los dispositivos y obtener el consumo de los dispositivos a lo largo de su tiempo de funcionamiento. Para realizar una gráfica de dicho consumo se precisó de una base de datos para almacenar los datos obtenidos de los dispositivos ZigBee. La idea de implementar esta base de datos en el dispositivo móvil no es otra que evitar sobrecarga de comunicaciones con la aplicación Java en el servidor.

El segundo módulo lo forman una aplicación servidora desarrollada en Java y una base de datos con información relativa a los dispositivos ZigBee que se utiliza para conformar las tramas de comunicación. El servidor Java debe de actuar como una pasarela entre la aplicación móvil y la red ZigBee, en el sentido de interpretar las órdenes enviadas por la aplicación Android y, a partir de ellas, conformar una serie de tramas que realicen las acciones que solicite el usuario mediante el protocolo ZigBee.

El último módulo lo conforma la red ZigBee en cuestión. En este caso concreto se dispone de un coordinador y de varios dispositivos de tipo router (Z-Plug). El coordinador se encargará de comunicar a los diferentes dispositivos las tramas que genera el servidor y, además, de transmitir al servidor de las distintas respuestas de los dispositivos. Los dispositivos Z-Plug se encargarán de medir el consumo de dispositivos electrónicos conectados a ellos y de apagar/encender dichos dispositivos de forma remota.

IV. IMPLEMENTACIÓN DEL SISTEMA

Como se ha comentado, la implementación de este proyecto ha seguido el paradigma cliente/servidor. Esto significa que se tendrá una parte correspondiente al cliente (que engloba todo lo relacionado con la aplicación Android) en la que realizarán modificaciones e interactuará de forma transparente con la red ZigBee, y una parte servidora, que se encargará de gestionar las acciones realizadas en la aplicación por parte del cliente y de traducirlas para que el coordinador sea capaz de enviar la información que necesitan los dispositivos Z-Plug para ejecutar la funcionalidad

Fig. 3 Arquitectura del sistema.

requerida por el usuario. Por lo tanto, en la parte servidora se deben implementar la funcionalidad de pasarela en el sentido de la traducción mencionada desde el dispositivo móvil Android hacia la red ZigBee y viceversa.

Desde el punto de vista de la programación, en cuanto a la estructura de los datos y el formato de los comandos usados, hay que indicar que, para realizar un estudio de las tramas que intervienen en la comunicación de la red ZigBee, se hace necesario el uso y análisis de la API de Texas Instruments denominada "*Z-Stack Monitor and Test API*" [5]. Esta API dispone de varias categorías. Para este proyecto será de vital importancia sobre todo la categoría correspondiente a la capa de aplicación. Esta API permite al usuario interactuar con la capa de aplicación del dispositivo para realizar un control personalizado. Además, será necesaria la gestión del puerto serie, ya que se precisa de un protocolo para que los mensajes puedan ser intercambiados entre el usuario y el objetivo a través del puerto serie RS-232. El propósito de este protocolo es encapsular los mensajes en paquetes para una transmisión y recepción adecuadas para asegurar su integridad.

Las tramas que se intercambian entre el servidor y el dispositivo objetivo contienen un inicio de trama, un *payload* y finalizan con una secuencia de comprobación de trama FCS. Entre el repertorio de comandos ZigBee, existe uno correspondiente a la interfaz de aplicación, denominado *AF_DATA_REQUEST*, cuya finalidad es poder ser usado por el usuario para enviar un mensaje arbitrario a través de la capa AF (*Application Framework*). Este comando tiene atributos de dirección de destino, identificador de *cluster*, dirección de origen, etc. La trama correspondiente se muestra en la Fig. 4, en la que se indican los campos que la constituyen y se presenta un ejemplo real de los utilizados para la implementación del proyecto. Hay que indicar que, aunque esta trama sea especialmente relevante para el proyecto, para obtener los valores necesarios para rellenar sus campos se ha precisado de otro tipo de comandos específicos

Byte: 1		1	1	
Longitud= 0x0A-0x8A		Cmd0=0x24	Cmd1=0x01	
Byte:2	1	1	2	1
DstAddr=0x29A5	DstEndpoint=0x01	SrcEndpoint=0xA	ClusterId=0x6	TransId=0x0
Byte: 1	1	1	0-128	
Options=0x0	Radius=0x0	Len=0x03	Data=0x01,0x01,0x02	

Fig. 4 Trama origen del comando AF_DATA_REQUEST

a partir de la dirección MAC de los dispositivos Z-Plug. En este sentido, el campo de datos se debe rellenar a partir de la información suministrada por la capa inferior, es decir, hay que realizar un estudio de la capa de red del protocolo ZigBee para rellenar correctamente dicha información. Cuando se envía este comando se recibe una respuesta del tipo SRSP (*Syncrhonous Response*). Esta respuesta tiene la finalidad de comunicar en su atributo de estado si la transmisión del mensaje anterior ha sido errónea o, por el contrario, ha sido exitosa. Si además se ha realizado una petición de suscripción con anterioridad, es decir, se ha usado un comando de petición tipo *callback* (el cual consisten en solicitar información por parte del dispositivo de destino) se recibirá una trama *AF_INCOMING_MSG*, la cual incluye información del dispositivo receptor del mensaje original. Tal y como se puede observar en la trama, esta tiene varios valores similares a la trama de envío. Además de estos atributos comunes, también contiene información del nivel de seguridad ofrecido en la comunicación, un atributo de marca temporal para dar robustez a la comunicación y un número de secuencia de respuesta.

Para finalizar este apartado describiremos las pruebas operativas realizadas para la comprobación del correcto funcionamiento de la implementación final. La importancia de este punto para la realización del proyecto el alta, ya que gracias a este conjunto de pruebas se ha hecho posible la justificación de las decisiones tomadas para la implementación final. Se han realizado pruebas diversas que engloban desde pruebas de exploración de variantes y pruebas de verificación. Estas últimas consisten en probar el control de la red ZigBee a través de una herramienta propietaria, como es CleoBee [6], y además usar su sitio web asociado para controlar la red ZigBee desde un navegador. También se han realizado pruebas para la comprobación de la conexión con el servidor a través de Android y se ha hecho uso de las funcionalidades implementadas a través del dispositivo móvil para verificar el correcto funcionamiento y comunicación de la aplicación Android. Adicionalmente se ha efectuado un control de la red ZigBee a través de la aplicación servidora implementada. Además, se ha comprobado la comunicación entre la aplicación Android y la aplicación Java, la cual es de vital importancia, ya que el servidor debe estar bien implementado en el sentido de evitar errores de comunicación y de procesado y gestión de la información proveniente del dispositivo móvil. Se ha comprobado el funcionamiento correcto de la base de datos a partir del análisis de los mensajes en archivos de *log*.

Con respecto a la gráfica del consumo que ofrece la aplicación móvil, se han realizado pruebas sencillas para comprobar que se actualiza correctamente la información de los dispositivos que forman la red ZigBee. Finalmente, una vez implementado todo, se realiza una prueba final y real del funcionamiento definitivo de la solución implementada, con el fin de detectar posibles anomalías en el funcionamiento y corregirlas.

V. CONCLUSIONES

En el presente Trabajo Fin de Grado se ha diseñado un sistema compuesto por diversos bloques que han hecho posible la consecución de los objetivos planteados. En particular, se ha combinado la tecnología ZigBee con los nuevos *smartphones* para conseguir el control y monitorización remotos de dispositivos eléctricos. Entre las contribuciones de este proyecto se pueden destacar las siguientes:

- Se ha desarrollado un conjunto de aplicaciones y sistemas que permiten, de acuerdo al objetivo planteado, el control remoto de dispositivos ZigBee del perfil *Smart Energy*.
- Se ha realizado un análisis de las características y funcionalidades relevantes de ZigBee para la consecución de los objetivos planteados.
- Se ha conseguido la sustitución de una herramienta de carácter propietario para la gestión de la red ZigBee como resultado del proceso de análisis de sus funciones.
- Se ha desarrollado una aplicación destinada a dispositivos móviles Android consistente en el control de la red inalámbrica ZigBee implementada y que ofrece al usuario información sobre dicha red referente al consumo de los dispositivos.

Finalmente, a continuación se presentan algunas sugerencias y nuevas funcionalidades con las que mejorar el sistema obtenido en el presente proyecto con el fin de ofrecer un rendimiento y fiabilidad mayores a las que proporciona actualmente. No obstante, hay que indicar que se han conseguido cumplir los objetivos marcados desde un principio, aunque durante el desarrollo del propio proyecto han surgido de forma natural algunas ideas que podrían dar lugar a algunas mejoras, como son:

- Interfaz gráfica a nivel de desarrollador en la aplicación del aparte servidora. Con esto se conseguirá que, ante cualquier error en la gestión de la red ZigBee, a través de la aplicación Java se fuese capaz de identificar y solucionar el problema de forma más eficiente.
- Ofertar en la aplicación móvil la posibilidad de añadir nuevos dispositivos, en el sentido de ofrecer una lista de dispositivos mediante la pulsación de un botón de la interfaz gráfica de la aplicación.
- Desde el punto de vista de la comunicación, una idea interesante sería la de hacer posible, mediante un dominio IP, la comunicación con la red desde fuera del propio hogar con el fin de que el usuario sea capaz de modificar el estado de un dispositivo sin necesidad de estar en la vivienda.

AGRADECIMIENTOS

La realización del presente Proyecto Fin de Grado ha sido la culminación de un largo y duro proceso que empezó hace cuatro años. En estos momentos, la satisfacción personal y el orgullo de haber llegado al final de este camino son indescriptibles. Este se lo debo sobre todo a Jesús, mi tutor, gracias a la idea que en su día me lanzó y que he tenido la oportunidad de disfrutar y finalizar. También debo de acordarme de mis padres y mi hermano, y en general mi familia, ya que sin su apoyo, esfuerzo y confianza no hubiese sido capaz de llegar a este punto con la madurez con la que he terminado.

REFERENCIAS

[1] "Barcelona, al frente de las 'smart cities'". Disponible en: http://www.domotica365.com/articulos/barcelona-al-frente-de-las-smart-cities.html
[2] *"El contador inteligente",* Disponible en: http://www.endesasmartgrids.com/index.php/es/la-casa-inteligente/el-contador-inteligente
[3] *ZigBee Alliance, "ZigBee Specification", 2008.*
[4] *ZigBee Alliance, "ZigBee Smart Energy Profile Specification", 2008.*
[5] Texas Instruments, "Z-Stack Monitor and Test API", 2011.
[6] Cleode, "ZigBee Network Management User Manual".

Desarrollo de una aplicación móvil para la gestión de un servicio universitario de deportes

Autor: Luis Carlos Casanova Aranda, e-mail: luisccasano88@gmail.com
Tutor: Juan José Ramos Muñoz; e-mail: jjramos.ugr.es
Tutor: Juan Manuel López Soler; e-mail: juanma.ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—En este proyecto se desarrolla una aplicación para smartphone con el sistema operativo Android, destinado a la gestión del servicio de deportes de la Universidad de Granada.**
Esta aplicación se llama DeportesUGR, y su objetivo es dar al usuario un software que permita consultar noticias, las instalaciones y su disponibilidad, los calendarios de todas las competiciones, o solo las de interés del usuario, así como poder consultar la información de contacto o la localización de los campus.
El documento nos ofrece una visión del estado actual del mercado actual de los sistemas operativos existentes, y del mundo de las aplicaciones para smartphone. Además, se incluye el desarrollo de la aplicación, mostrando datos de su análisis, diseño e implementación.

***Palabras clave*—Análisis, Android, aplicación, deportes, diseño, implementación, información, instalaciones, noticias, smartphone.**

HOY en día, los dispositivos móviles nos proporcionan multitud de servicios y funciones a través de aplicaciones, las cuales nos facilitan el día a día.
La Universidad de Granada [1] cuenta con dos campus universitarios deportivos, en cuyas instalaciones se realizan a lo largo del año numerosas competiciones y actividades deportivas, mostrando toda la información en la página web del Centro de Actividades Deportivas (CAD) [2]. Así que, por qué no unir deporte y tecnología y crear una aplicación móvil que nos permita consultar toda la información en nuestro Smartphone con solo unos clics.
El sistema operativo que se ha usado ha sido Android, debido a las numerosas ventajas y facilidades que presenta, así como su carácter de libre distribución y al crecimiento que experimenta día a día.

A. Motivación

Actualmente, a la hora de acceder a la consulta de las diferentes informaciones que presenta la página del CAD, mucha de la información no se puede visualizar correctamente, o directamente no se puede acceder, desde un Smartphone, por lo que se decidió crear una aplicación que nos permitiese, facilitase y agilizase la consulta de noticias, competiciones, instalaciones, información de contacto, disponibilidad de pistas, etc.
Además, la Universidad de Granada, mediante la Convocatoria de ayudas para el desarrollo de aplicaciones para móviles (Apps) de la Universidad de Granada, pretendía que se le desarrollasen diferentes aplicaciones para los diversos servicios que ofertan, entre los que se encuentra el servicio de deportes, por lo que se presentó la candidatura de este proyecto, tras una serie de reuniones con diferente personal del CAD para ver cuáles eran sus necesidades, resultando finalmente elegido nuestro proyecto.

B. Objetivos

Los objetivos de este proyecto eran desarrollar una aplicación móvil que permitiese:

- Mostrar información básica del CAD.
- Mostrar los calendarios de las competiciones en vigor.
- Elegir mis equipos (novedad).
- Consultar la disponibilidad de las instalaciones.

Mostrando siempre la información completamente actualizada, accediendo a ella mediante servicios web.

II. Antecedentes y tecnologías

El que la aplicación se haya optimizado para móviles, aunque también funciona en tablets, se debe al constante crecimiento de las ventas de dispositivos móviles, creciendo un 27% sus ventas en el segundo trimestre de 2014, con respecto a la misma fecha en 2013 [3].
En cuanto a la elección de Android como plataforma de desarrollo, aparte de las numerosas ventajas y facilidades que proporciona a los desarrolladores, es un sistema operativo que está en continua expansión, alcanzando en el segundo trimestre de 2014 una cuota de mercado mundial del 84,6%, y convirtiéndose por primera vez en el sistema operativo que cuenta en su market con el mayor número de aplicaciones disponibles (en torno a 1.300.000 apps), superando incluso a iOS [3].
Para el desarrollo de la aplicación ha sido necesario el uso de algunas tecnologías como son el caso de REST (Representational State Transfer) [4], y de JSON (JavaScript Object Notation) [5].

A. REST (Representational State Transfer)

Para la obtención de la información de nuestro servidor, hicimos uso de servicios web, decantándonos de entre todas las tecnologías disponibles por REST [4], ya que:

- Es un tipo de servicios web, basados en HTTP (HyperText Transfer Protocol) [6].
- Orientado a solicitud-respuesta.
- Más ligero que SOAP (Simple Object Access Protocol) [7].
- Protocolo stateless (sin estado)
- Para su correcto funcionamiento, es necesario el uso correcto de URIs (Uniform Resource Identifier), de HTTP, e implementar hypermedia.

En cuanto al uso correcto de URIs, cada uno de los recursos se codifica mediante URLs, siguiendo la siguiente estructura:

{protocolo}://{dominio o hostname}[:puerto (opcional)]/{ruta del recurso}?{consulta de filtrado}

Las URLs deben cumplir una serie de reglas como:

- Ser únicas y no contener verbos.
- Ser independientes de formato.
- Mantener una jerarquía lógica.

En cuanto al uso correcto de HTTP, para operar sobre los recursos se utilizan métodos HTTP como GET (para consultar y leer recursos), POST (para crear recursos), PUT (para editar recursos), DELETE (para borrar recursos) y PATCH (para editar partes concretas de un recurso).

B. JSON (JavaScript Object Notation)

Para la representación de los datos leídos en el servidor, de entre todas las tecnologías disponibles, se optó por elegir JSON [5], ya que es un formato ligero de intercambio de datos, que permite serializar un objeto, basándose en JavaScript. Está adecuado para entornos web, y presenta una serie de ventajas frente a XML como:

- La sencillez de su formato.
- Escribir un analizador sintáctico mediante JSON es mucho más simple que con XML.
- Se procesa más rápido en cualquier navegador.
- JSON no necesita ser extensible porque es flexible por sí solo.
- JSON permite tiempos de respuesta menores.

III. Diseño

A. Análisis de requisitos

Para la realización del proyecto, se tuvieron en cuenta una serie de requisitos de las diferentes partes implicadas en su desarrollo y posterior uso, como son:

- Requisitos de la convocatoria de la Universidad:
  - La utilización de servicios webs en la comunicación con el servidor.
  - Diseño de la interfaz acorde a los requisitos impuestos por la Universidad de Granada para el desarrollo de sus aplicaciones móviles (splash, launcher, fondo, etc.).
  - Liberación del código fuente de la aplicación.
- Requisitos extraídos de las reuniones con el CAD:
  - Mostrar información básica del CAD, como noticias, competiciones, instalaciones, información de contacto, etc.
  - Mostrar los calendarios de las competiciones en vigor.
- Requisitos extraídos de las encuestas a los usuarios:
  - Poder seleccionar tus equipos de interés, y consultar solamente sus calendarios, sin tener que ver el de todos los equipos inscritos en dicha competición y deporte.
  - Consultar la disponibilidad de las instalaciones para su posible alquiler.

B. Arquitectura general y del cliente

Cumple con el paradigma cliente/servidor, estando el cliente implementado en Android, y el servidor en Java como se puede apreciar en la Fig. 1. La comunicación con el servidor se hace mediante servicios web basados en REST, y la representación de los datos de hace mediante JSON, como se ilustra en la Fig. 2.

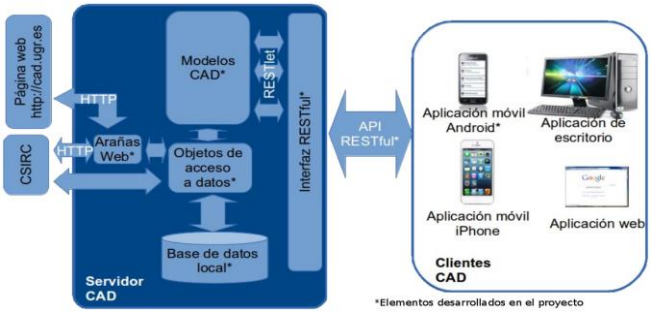


Fig. 1. Arquitectura general del sistema.

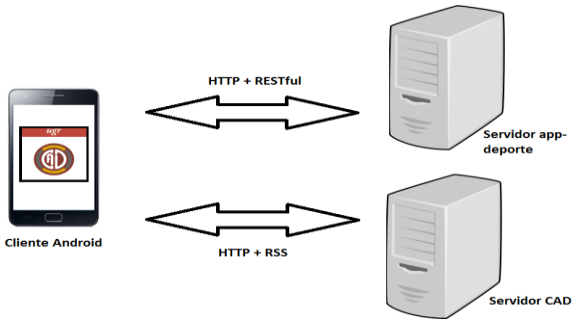


Fig. 2. Protocolos utilizados por el cliente.

C. Diagrama de clases principal

En la Fig. 3, se muestra un ejemplo de un diagrama de clases simplificado, donde se puede apreciar la relación que guarda la activity principal con las diferentes clases que dan acceso a las funcionalidades que presenta la aplicación. En las clases ReservasActivity, TorneosActivity o Noticias, se ve como guardan relación con sus correspondientes clases 'Task', para la ejecución en sugundo plano de sus tareas. También se ve como la clase MisEquipos guarda relación con la clase GestorPreferencias, ya que esta es la que permite almacenar en el móvil los equipos seleccionados.

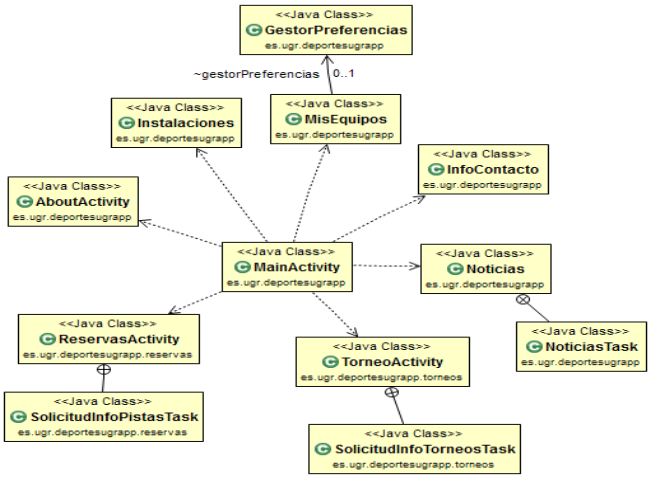


Fig. 3. Diagrama de clases de la Activity principal.

D. *Interfaz gráfica y funcionalidades*

La apariencia de la aplicación está basada en todo momento en la imagen corporativa impuesta por la Universidad de Granada para el desarrollo de sus aplicaciones, permitiendo además el re-escalado de la aplicación para dispositivos de diferentes tamaños.

Por otro lado, la aplicación presenta una interfaz gráfica fácil, sencilla e intuitiva, indicando donde te encuentras en cada momento, permitiéndote avanzar por las diferentes funcionalidades mediante el uso de botones, o listas de botones, y retroceder mediante el uso del botón volver que incorpora el propio terminal móvil.

Las funcionalidades que presenta la aplicación son:

- Consulta de noticias.
- Consulta de competiciones.
- Consulta de instalaciones.
- Consulta de mis equipos.
- Consulta de la disponibilidad de pistas.
- Consulta de la información de contacto.
- Consulta del acerca de.

En la Fig. 4, se muestran algunas capturas de pantalla, mostrando algunas de las diferentes funcionalidades que presenta la aplicación.

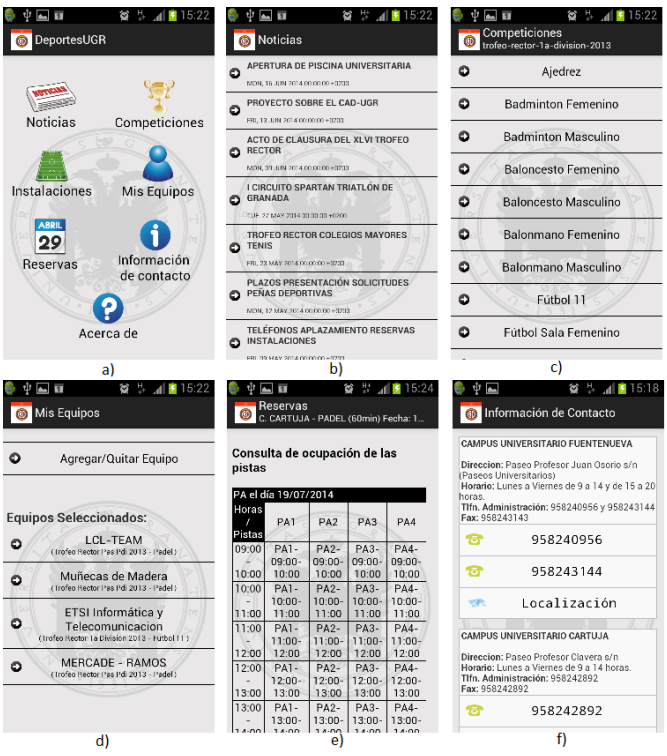


Fig. 4. Capturas de diferentes funcionalidades. a) Activity principal. b) Lista de noticias. c) Lista de deportes. d) Mis Equipos. e) Disponibilidad de pistas. f) Información de contacto.

IV. IMPLEMENTACIÓN

A. *Jackson*

Para la serialización de los objetos que se intercambian mediante los servicios web REST definidos en el sistema, se utiliza el formato de representación JSON. La implementación de la serialización se lleva a cabo mediante la librería Jackson [8]. Jackson, es una librería de utilidad de Java que simplifica el trabajo de serializar y deserializar objetos JSON. Para ello, las clases que se van a pasar a JSON deben contener los getters/setters de las variables que se deseen. A continuación, en la Fig.5, se muestra un ejemplo, donde se aprecia que se le pasa la clase DatosCategoria, que es la que contiene los getters/setters anteriormente mencionados, y donde tras leer la URL del recurso, y mapear la información, se devolverá el resultado.

```
public List<DatosCategoria> obtenerTorneos(String anio) {
    List<DatosCategoria> listaCategorias = null;

    try {

        String respuesta = "";

        // ------------------------------
        // AquÃ- hay que cambiar:
        String url = baseURL + "/torneos/" + anio;

        respuesta = leerURL(url);
        // --------------------------
        // AquÃ- hay que cambiar
        // Intentamos interpertarlo con jackson:
        ObjectMapper mapper = new ObjectMapper();
        mapper.configure(DeserializationFeature.FAIL_ON_UNKNOWN_PROPERTIES,
                false);

        // Ejemplo para recibir una lista de objetos:
        listaCategorias = mapper.readValue(respuesta,
                new TypeReference<List<DatosCategoria>>() {
                });

    } catch (IOException ex) {
        Logger.getLogger(DeporteUGRClient.class.getName()).log(
                Level.SEVERE, null, ex);
    }
    return listaCategorias;
}
```

Fig. 5. Ejemplo de uso de Jackson.

B. *Tareas asíncronas en segundo plano: AsyncTask*

Desde la versión 3.0 de Android, cuando se va a realizar una consulta web, o se va a realizar una tarea que puede tardar bastante o que pueda bloquear la aplicación, es necesario implementar un recurso de Android llamado AsyncTask [9], que permite realizar tareas en segundo plano.

Para su uso, se crearán clases que extiendan de AsyncTask, pasándole una serie de parámetros como se muestra en la Fig. 6.

```
public class SolicitudInfoTorneosTask extends
        AsyncTask<String, Integer, List<DatosCategoria>> {
```

Fig. 6. Ejemplo de creación de una clase AsyncTask.

Dentro de la clase se ejecutarán una serie de métodos, entre los que destacan:

- `onPreExecute()`, que se ejecutará antes de mandar la tarea a segundo plano, mostrando por ejemplo algún mensaje.
- `doInBackground()`, método que lanzará la ejecución de la tarea a segundo plano.
- `onPostExecute()`, que es el método que trae de nuevo la tarea a primer plano, y permite recuperar los resultados obtenidos de la ejecución de la tarea en segundo plano.

C. *Llamadas entre Actividades. Intents*

Las Activities son independientes entre sí, por lo que es necesario utilizar intents, ya que son elementos básicos de comunicación entre los distintos componentes Android. En nuestro proyecto se han usado con diferentes funcionalidades, como:

- Abrir una Activity normal.
- Abrir una Activity pasándole información de la Activity anterior.
- Abrir el navegador web.
- Abrir el correo electrónico para mandar un email.
- Abrir el marcador de teléfono con el número marcado.

Un ejemplo de cómo pasar información de una Activity a otra, puede verse en la Fig. 7, donde se muestra como mediante el método `putExtra(clave,valor)`, se pasa la información que se desea, y en la nueva Activity, dentro del método que crea la Activity (onCreate) gracias al método `getStringExtra(clave)`, se recuperará la información deseada (Fig. 8).

```
public void onClickCalendario(View arg0) {
    // Creamos un Intent para llamar a la activity correspondiente:
    Intent intent = new Intent(EleccionActivity.this,
            CalendariosActivity.class);
    intent.putExtra("com.example.activitydeportes.categoriaId", categoriaId);
    intent.putExtra("com.example.activitydeportes.deporteId", deporteId);

    startActivity(intent);

};
```

Fig. 7. Ejemplo de pasar información a una Activity.

```
Intent intent = getIntent();
categoriaId = intent
        .getStringExtra("com.example.activitydeportes.categoriaId");
deporteId = intent
        .getStringExtra("com.example.activitydeportes.deporteId");
```

Fig. 8. Ejemplo de recuperar información de otra Activity.

D. REST

En la Tabla I se listan algunas de las URL de REST utilizadas en el sistema.

TABLA I
TABLA DE SOLICITUDES

Listado general de deportes	GET /perfiles/deportes
Listado general de equipos	GET /perfiles/equipos
Información de contacto	GET /contactos/
Pistas reservables	GET /reservas/pistas
Disponibilidad	GET /reservas/pistas/{codigoPista}/fecha/{fecha}
Noticia	GET /noticias/{noticiaid}/tablones/{tablon}
Listado de competiciones	GET /torneos/{anio}
Listado de deportes en una competición	GET /categorias/{categoria}/deportes
Listado de calendarios	GET /categorias/{categoria}/deportes/{deporte}/calendarios

Mostrando a continuación, en la Fig. 9, un ejemplo de la respuesta para la obtención de las pistas reservables.

Respuesta:


```
[
    {
        "codigo": "VP",
        "titulo": "C. FUENTENUEVA - VOLEY PLAYA (60min)"
    },
    {
        "codigo": "TE",
        "titulo": "C. FUENTENUEVA - TENIS (60min)"
    },
    {
        "codigo": "PF",
        "titulo": "C. FUENTENUEVA - POLIDEPORTIVAS (60min)"
    },
    {
        "codigo": "P2",
        "titulo": "C. FUENTENUEVA - PABELLON 2 (60min)"
    },
    {
        "codigo": "P1",
        "titulo": "C. FUENTENUEVA - PABELLON 1 (60min)"
    },
    {
        "codigo": "PP",
        "titulo": "C. CARTUJA - POLIDEPORTIVAS (60min)"
    },
    {
        "codigo": "PA",
        "titulo": "C. CARTUJA - PADEL (60min)"
    },
    {
        "codigo": "PC",
        "titulo": "C. CARTUJA - PABELLON (60min)"
    }
]
```


Fig. 9. Ejemplo de respuesta ante la solicitud REST para las pistas reservables.

V. EVALUACIÓN FUNCIONAL

Para comprobar el correcto funcionamiento de la aplicación, se llevaron a cabo una serie de pruebas en diferentes dispositivos como se muestra en la Tabla II, comprobando que todas las funciones principales funcionaban correctamente bajo distintas condiciones, y que en caso de que se produjese algún fallo, se mostrase un mensaje de error, indicando el fallo, para que así el usuario pudiera ser consciente del por qué.

TABLA I I
TABLA DE EVALUACIÓN

Funcionalidad	Situación	Samsung Galaxy SII	Samsung Galaxy SIII	Samsung Galaxy SIV	Samsung Galaxy TAB 2
Noticias	Todo correcto	Ok	Ok	Ok	Ok
	Fallo conexión/servidor	Ok	Ok	Ok	Ok
Competiciones	Todo correcto	Ok	Ok	Ok	Ok
	Fallo conexión/servidor	Ok	Ok	Ok	Ok
	Sin equipos registrados	Ok	Ok	Ok	Ok
Instalaciones	Todo correcto	Ok	Ok	Ok	Ok
	Fallo conexión/servidor	Ok	Ok	Ok	Ok
Mis Equipos	Todo correcto	Ok	Ok	Ok	Ok
	Fallo conexión/servidor	Ok	Ok	Ok	Ok
Añadir/quitar mis equipos	Todo correcto	Ok	Ok	Ok	Ok
	Fallo conexión/servidor	Ok	Ok	Ok	Ok
	Sin equipos registrados	Ok	Ok	Ok	Ok
Disponibilidad	Todo correcto	Ok	Ok	Ok	Ok
	Fallo conexión/servidor	Ok	Ok	Ok	Ok
	Fecha pasada	Ok	Ok	Ok	Ok
	Fecha lejana	Ok	Ok	Ok	Ok
Rotación de pantalla	En cualquier situación	Ok	Ok	Ok	Ok

Tras esto, la aplicación DeportesUGR superó todos los test y controles de calidad de la Comisión de Apps Móviles de la Universidad de Granada.

VI. Conclusiones

Los logros conseguidos en el desarrollo de este proyecto se resumen en:

- Una aplicación con una interfaz fácil, sencilla e intuitiva.
- Publicación de la app en Google Play, a través del canal de la UGR.
- Permite leer las noticias del tablón del CAD.
- Podemos consultar los calendarios y clasificaciones de todas competiciones con las que cuenta la Universidad de Granada.
- Permite ver las instalaciones de las que dispone la Universidad de Granada.
- Se puede consultar la información de contacto.
- Es posible consultar la disponibilidad de una determinada instalación.
- La posibilidad de elegir tus equipos favoritos, o de interés.

VII. Trabajo futuro

Actualmente, al girar el dispositivo, se recarga de nuevo la información, por lo que sería interesante que una vez descargada la información, se almacenase temporalmente en el dispositivo, para que al girarlo no tuviese que cargar de nuevo la información.

Sería interesante añadir la posibilidad de que los capitanes de los equipos pudieran solicitar el aplazamiento de un partido, o confirmar una solicitud de aplazamiento del equipo rival, desde la propia aplicación.

Traducirla a otros idiomas sería algo muy interesante, ya que la Universidad de Granada es el primer destino erasmus, y muchos de sus alumnos en sus primeros meses no dominan el español, por lo que poder hacer uso de ella en otros idiomas sería algo que les facilitaría el trabajo y aumentaría el número de usuarios.

Aunque Android es el sistema operativo más utilizado actualmente, son muchos los usuarios de las instalaciones que disponen de terminales con otros sistemas, por lo que sería muy útil portar la app a otros sistemas operativos.

Añadir la posibilidad de no solo consultar la disponibilidad de una pista, sino también poder reservarla, es una de las mejoras que podría realizarse a la aplicación, una vez la Universidad de Granada permita la reserva de pistas mediante TPV de pago con tarjeta.

Agradecimientos

Dedicado a mis padres, Pedro y Loly, quienes siempre me han apoyado a lo largo de mi vida, y en especial en estos años de carrera, dándome todo y cuanto he necesitado, e inculcándome una serie de valores que me han convertido en quien soy hoy en día, y por todo ello, muchísimas gracias.

A mis hermanos, Pedro e Inma, por estar siempre ahí y preocuparos por mí, apoyándome y dándome un toque de atención cuando ha sido necesario.

A mis tutores, por darme la oportunidad de realizar este proyecto y poder dejar mi huella en la Universidad que tanto aprecio, por atenderme siempre y estar atentos a todas mis dudas y necesidades, sin vosotros no lo hubiera conseguido.

A todos los profesores que han formado parte de mi formación académica, ya que sin sus clases, enseñanzas y consejos no estaría aquí hoy.

Y a todos mis amigos y personas que he conocido a lo largo de mi vida y, en especial, en estos años de Universidad, donde no solo me llevo conocidos, sino grandes amigos que sé que formarán parte de mi vida para siempre.

Referencias

[1] U. d. Granada, «Universidad de Granada,» 2014. [En línea]. Available: http://www.ugr.es/.

[2] U. d. Granada, «Centro de Actividades Deportivas,» 2014. [En línea]. Available: http://cad.ugr.es/.

[3] S. Analytics, «Android Captures Record 85 Percent Share of Global Smartphone Shipments in Q2 2014,» 2014.

[4] A. Marqués, «Conceptos sobre APIs REST,» 2013. [En línea]. Available: http://asiermarques.com/2013/conceptos-sobre-apis-rest/.

[5] JSON, «Introducción a JSON,» 2014. [En línea]. Available: http://json.org/json-es.html.

[6] N. W. Group, «Hypertext Transfer Protocol,» 1999. [En línea]. Available: http://tools.ietf.org/html/rfc2616.

[7] P. W. Group, «Simple Object Access Protocol,» 2000. [En línea]. Available: http://www.w3.org/TR/soap/.

[8] Codehaus, «Jackson,» [En línea]. Available: http://jackson.codehaus.org/.

[9] Android, «Android Developers: AsyncTask,» 2014. [En línea]. Available: http://developer.android.com/reference/android/os/AsyncTask.html.

Luis Carlos Casanova Aranda, 29 de Abril de 1988, Jaén. Ingeniero de Telecomunicaciones.

Servicio de proyección de material docente basado en Raspberry Pi

Autor: Juan Ramón Gutiérrez Martínez; e-mail: juanragutierrez@gmail.com
Tutor: Jorge Navarro Ortiz; e-mail: jorgenavarro@correo.ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—Este proyecto surge con el objetivo de poder hacer uso de los proyectores situados en las aulas docentes sin la tediosa necesidad de tener un equipo conectado a través de un cable VGA. Para ello se conectará un PC de pequeño tamaño (Raspberry Pi [1]) a través del interfaz HDMI del proyector, de forma que el profesor pueda navegar a través de sus transparencias u otros materiales desde cualquier equipo conectado a la red WiFi de la UGR.**
De esta manera, se mejora la usabilidad del servicio de proyección y también la movilidad del docente por el aula, ya que podría utilizar portátil desde cualquier lugar.
Para ello, se ha de diseñar un servidor con autenticación de usuarios para el almacenaje del material docente, así como integrar los diferentes protocolos que sean necesarios para que la Raspberry Pi visualice dicho material a través del proyector y pueda ser controlada de forma inalámbrica.

***Palabras clave*—Raspberry Pi, docencia, material docente, proyección, exposición, diapositivas**

I. Introducción

El auge en las últimas décadas en el uso de la tecnología es una realidad. Actualmente las tecnologías de la información y la comunicación (TICs) están sufriendo un desarrollo vertiginoso, algo que afecta prácticamente a todos los campos de nuestra sociedad, y la educación no es una excepción. Las TIC se han convertido en algo muy arraigado en los centros educativos. Las tecnologías son cada vez más utilizadas en los métodos docentes, por parte sobre todo, de las universidades. Y su uso ha fomentado cambios cualitativos en la forma de enseñanza en cuanto a la presentación de los contenidos.[2][3]

En este punto se han de tener de tener en cuenta varios aspectos. En el sistema utilizado actualmente es condición necesaria que el portátil esté conectado al proyector mediante un cable con conector VGA. Hecho que resulta molesto y que no permite al docente disponer de suficiente movilidad. Por otro lado, también existe la necesidad de transportar constantemente el ordenador personal para poder proyectar el material utilizado.

A esto además, se añade una clara tendencia a la creación de nuevos dispositivos cada vez de menores dimensiones, como la nueva generación de portátiles, *ultrabook*. Lo que está provocando la pérdida o reducción de las posibles conexiones. Esto, además del auge en las nuevas tecnologías portátiles como tabletas o móviles, provoca que los nuevos dispositivos tecnológicos no puedan conectarse a los proyectores que habitualmente hay instalados en las clases mediante un conector VGA. En su lugar, son necesarios adaptadores a partir de una entrada USB o HDMI.

Por tanto, es motivante trabajar sobre un campo que vivimos diariamente y que es muy familiar, con el objetivo de implantar una serie de mejoras sobre el sistema utilizado actualmente, tratando de buscar una solución que proporcione la comodidad de no tener que depender de una conexión mediante cable con el proyector. Algo que, a su vez, facilitaría el movimiento del docente en el aula.

De esta manera, la solución final que se plantee podrá implantarse en las aulas docentes de la propia universidad, algo que es una motivación extra.

II. Estudio del Estado del Arte

A. *Proyectores inalámbricos*

La solución más evidente reside en los proyectores inalámbricos. Este tipo de proyectores utilizan tecnología Wi-Fi o *Bluetooth* para la conexión y comunicación con el ordenador proveedor de imágenes. De esta forma se permite el uso de diferentes dispositivos sin necesidad de conexión cableada, aumentando así la movilidad del docente.

El principal problema de esta solución reside en su precio. El valor mínimo de un proyector de estas características es aproximadamente 1000€ según las principales página de ventas. Algo que aumenta considerablemente el coste de instalación.

B. *Pizarra interactiva y Tablet Monitor*

Esta solución evita los mismos inconvenientes que la anterior gracias al elemento controlador de la pizarra interactiva, *Tablet Monitor*. Aunque también, al igual que los proyectores inalámbricos, presenta un gran inconveniente con respecto a su coste. Será necesario adquirir una pizarra por clase y una *Table Monitor* para cada profesor.

C. *Apple TV y AirPlay*

Applet TV[4] es un dispositivo diseñado para reproducir contenido multimedia en una televisión de alta definición. Y gracias a la tecnología AirPlay[5] se puede utilizar cualquier tipo de dispositivo del fabricante Apple[6] para la reproducción del contenido.

Este dispositivo no solo está destinado al ocio, sino que es una solución que puede ser empleada en el ámbito docente. Esta solución es quizás la que más se asemeja a los objetivos que se quieren cumplir con este proyecto. De hecho, ya se ha realizado un estudio del uso de este dispositivo en el ámbito

TABLA I
RESUMEN

Solución	Ventajas	Inconvenientes
Proyectores inalámbricos	▪ Movilidad ▪ Conexión de diferentes dispositivos	▪ Precio ▪ Desperdicio de los proyectores actuales
Pizarra interactiva	▪ Movilidad ▪ Interacción con la pizarra	▪ Precio por unidad ▪ Necesidad de *Tablet Monitor* por docente
Apple TV	▪ Movilidad ▪ Conexión de diferentes dispositivos ▪ Almacenamiento centralizado (iCloud)	▪ Precio ▪ Necesidad de un dispositivo iOS
Dispositivos Miracast	▪ Movilidad ▪ Económico ▪ Conexión de diferentes dispositivos ▪ *Screen mirroring*	▪ Necesidad de dispositivo *Miracast* ▪ Aún en desarrollo
Chromecast	▪ Movilidad ▪ Solución más económica ▪ Compatibilidad con la mayoría de SO actuales	▪ Sin *screen mirroring* ▪ Aún en desarrollo

académico por la Universidad Rovira i Virgili (URV)[7]. Aunque como principal inconveniente a esta solución se encuentra la total necesidad del docente de disponer de un dispositivo Apple para su uso, algo que causaría demasiados inconvenientes.

D. Wireless Display y Miracast

Como alternativa a la tecnología propuesta por Apple, se encontra *Wireless Display* [8]. Un dispositivo cuya función es básicamente igual que Apple TV, pero utilizando en este caso la tecnología Miracast [9]. Miracast es un estándar creado por la Alianza Wi-Fi y que consiste en una red *peer-to-peer* utilizada para enviar *screencast* de forma inalámbrica formando conexiones *Wi-Fi Direct* de forma similar a como lo hace *Bluetooth*.

Al igual que en el caso anterior, existe la necesidad de un dispositivo compatible con la tecnología Miracast para poder hacer uso de esta solución.

E. Chromecast

Cabe destacar *Chromecast*[10], principal competidor de Apple TV, sobre todo por precio. En cuanto a las características, parecido a los dispositivos comentados anteriormente.

Aunque existen varias diferencias. Este dispositivo es compatible con todas las versiones de los sistemas operativos más utilizados del momento a partir de Android 2.3, iOS 6.0, Windows 7, Mac OS 10.7 y Chrome OS.

Pero este dispositivo no permite *screen mirroring*, simplemente se puede seleccionar el contenido y reproducirlo. Llegando así a otro de sus inconvenientes, la necesidad de tener el contenido almacenado en el dispositivo para poder reproducirlo.

Finalmente, en la Tabla I puede verse un cuadro resumen con las diferentes soluciones estudiadas.

III. ANÁLISIS DE OBJETIVOS

La solución finalmente implementada debe solucionar todos o la mayoría de los problemas planteados en apartados anteriores sobre el actual método docente utilizado en las universidades. Así, se pueden diferenciar una serie de objetivos que se han de cumplir obligatoriamente para que la solución implementada sea la idónea:

- Se deben eliminar las conexiones mediante cable. Permitiendo de esta forma la total movilidad del docente por el aula de enseñanza.
- Debe ser fácilmente portable a diferentes tecnologías y sistemas operativos de forma que en un futuro se pueda utilizar en entornos diferentes.
- Debe existir un sistema de gestión del material centralizado de forma que no sea necesario llevar el material guardado en los dispositivos.
- Debe ser una solución de fácil instalación y transporte, de forma que el sistema no sea una instalación fija en una clase.
- Por supuesto debe ser muy económico, tanto como para que pueda ser instalado sin asumir un gasto elevado por parte de la universidad.

Como se puede intuir, gracias al uso de Raspberry Pi como base del sistema implementado, se podrán cumplir la mayoría de estos objetivos de forma sencilla.

Adicionalmente a estos objetivos, se especifican una serie de objetivos secundarios u opcionales. Dichos objetivos no son obligatorios, pero añaden nuevas funcionalidades al producto final. Estos objetivos son de gran complejidad y suponen una inversión de tiempo mayor. Éstos son los siguientes:

- El material docente debe ser en formato PDF como mínimo, ampliable posteriormente a otros formatos de imágenes o documentos.
- El sistema de seguridad y autenticación de usuarios se debe adaptar al sistema utilizado por la Universidad de Granada. De esta forma se facilitará la tarea de la posterior implantación en las aulas.
- El sistema inicial cuenta con una única Raspberry Pi. Se debe incorporar una base de datos adicional que contenga la información de las localizaciones de los proyectores. Así se podrá elegir en qué aula mostrar el material cuando existan varios sistemas instalados.
- Debe unificar las tecnologías actuales, de forma que sea indiferente el uso de ordenador, tableta o *smartphone* para proyectar el material.
- Debe incorporar un sistema que permita mostrar y visualizar en el proyector la imagen de la pantalla del dispositivos utilizado.

IV. DISEÑO E IMPLEMENTACIÓN

A la hora de realizar el diseño de la solución hay que tener en cuenta los objetivos marcados en el apartado anterior. De esta forma, para que se pueda ser una solución extensible a diferentes plataformas con facilidad se utiliza un servidor web, el cual se configurará de forma que utilice HTTPS en lugar de HTTP por razones de seguridad. Para el almacenamiento centralizado del material docente se utiliza un servidor SFTP.

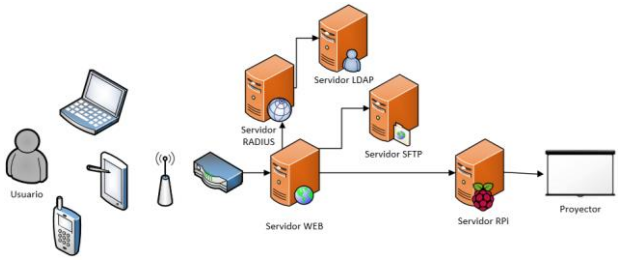


Fig. 1. Diseño global de la implementación

Para adaptar la autenticación de usuarios al utilizado por la Universidad de Granada (UGR) se añade un servidor RADIUS centralizado como servidor de autenticación y un servidor LDAP como gestor de base de datos de usuarios, ya que es el sistema utilizado [11]. De esta forma se consigue mayor facilidad para la implantación del sistema en las aulas docentes. Finalmente, en la Raspberry Pi irá situado un último servidor, que será el encargado de manejar el material a proyectar. Con todas estas indicaciones, el resultado final del diseño puede verse en la Figura 1.

Una vez que se tiene claro el diseño de la solución se han de seleccionar las mejores opciones de configuración o implementación. De esta forma, para facilitar el trabajo se opta por la configuración de todos los servidores en un equipo con sistema operativo Linux (Ubuntu 14.4 [12]). Para el servidor web se utiliza un servidor Apache [13] configurado como HTTPS. Para ello será necesario la creación de un certificado digital. Además, el lenguaje utilizado para la programación del entorno web es PHP [14][15], consiguiente así un entorno muy dinámico y que puede ser utilizado por cualquier dispositivo [16]. Para el servidor de ficheros (SFTP) se utiliza el servidor VSFTPD [17], también configurado con un certificado digital para cifrar la información y aumentar de este modo la seguridad del sistema. Por último, para la autenticación de usuarios se emplearán un servidor FreeRADIUS [18], el cual posee un módulo para LDAP, y un servidor OpenLDAP [19] que estará configurado con dos entradas, una para profesores y otra para alumnos, de igual forma que se ha distinción en los servicios web de la universidad.

El servidor situado en la Raspberry Pi se debe diseñar e implementar de tal forma que se encargue de obtener, mostrar y manejar el material que se proyectará y utilizará el docente. Para ello se utiliza una aplicación cliente-servidor con sockets utilizando el lenguaje de programación JAVA [20]. En lo que respecta al *software* utilizado en la Rapsberry Pi corresponde también a un entorno Linux, RASPBIAN Debian Wheezy [21] en este caso. Además, el *software* utilizado por la Raspberry Pi para el manejo y control del material mostrado es MuPDF [22], el cual permite el manejo total, tanto fichero en formato PDF como otros formatos de imágenes (PNG, JPG, etcétera), mediante consola. Hecho que facilitará la forma en la que se enviarán las órdenes.

Como se ha podido apreciar, todo el *software* utilizado se puede obtener de forma gratuita, contribuyendo así a la reducción de inversión necesaria.

Una vez se tiene claro el software que se va a utilizar, se puede determinar cuál será el funcionamiento general de la solución. Dicho funcionamiento puede verse en la Figura 2.

Un usuario con sus datos accede al entorno web. Para la autenticación se pasa la consulta al servidor FreeRADIUS y este a su vez a la base de datos OpenLDAP. Si los datos son

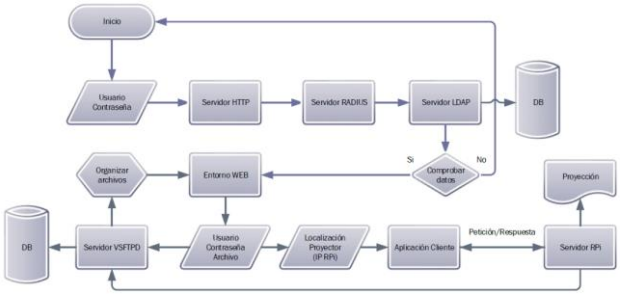


Fig. 2. Diseño general de funcionamiento

correctos el usuario accede finalmente al entorno web. Un entorno muy simple e intuitivo donde se mostrará una lista con los ficheros que el usuario tiene almacenados (véase la Figura 3). Además, desde este entorno se podrá añadir un nuevo fichero, borrar, descargar o renombrar uno antiguo, o enviar dicho fichero al proyector de la clase. Dicho proyector se deberá seleccionar de entre una lista con las clases que tienen este sistema instalado. Esta última acción dará paso a la ejecución de la aplicación cliente, la cual establecerá comunicación con el servidor mediante los anteriormente mencionados *sockets* [23]. Desde esta aplicación se produce una comunicación continua de petición-respuesta donde se enviarán todas las órdenes referentes al manejo del material proyectado, tales como: avanzar o retroceder página, aumentar o disminuir zoom, entre muchas otras.

Dicha aplicación será implementada en JAVA [24], como se mencionó anteriormente. Además, debe ir integrada en el entorno web, para que sea de fácil acceso desde cualquier equipo. De esta forma, la implementación realizada corresponde con un JApplet [25], la herramienta utilizada por JAVA para sus aplicaciones web. La interfaz de usuario varía en función del tipo de material utilizado puesto que las funciones serán diferentes. Un ejemplo de dicha interfaz puede verse en la Figura 4.

Fig. 3. Interfaz web de usuario

Fig. 4. Interfaz de usuario para un fichero PDF

```
Este es el fichero de mensajes logs del Servidor RPi:

[29/06/2014 17:41:51] Iniciado Servidor RPi
[29/06/2014 17:42:36] Conexion con cliente: /192.168.1.10
[29/06/2014 17:42:36] Usuario: admin
[29/06/2014 17:42:38] Conexion con el servidor FTP exitosa
[29/06/2014 17:42:41] Controlando el archivo: CATALOGO COLONIAS.pdf, el usuario: admin
[29/06/2014 17:45:14] Cerrada conexion con el cliene.
[29/06/2014 17:58:56] Iniciado Servidor RPi
```

Fig. 13. Contenido del fichero *log* del ServidorRPi

El diseño e implementación de la aplicación cliente y el servidor JAVA corresponden a los diagramas de estados de las Figuras 5 y 6 respectivamente. En ellas se puede ver cómo el paso de un estado a otro se realiza de igual forma, siguiendo un protocolo de intercambio de mensaje diseñado e implementado especialmente para esta aplicación cliente-servidor. Este protocolo puede verse en la Figura 7.
Por supuesto, como se puede apreciar en las imágenes, ambas implementaciones cuentan con un completo sistema de detección y recuperación frente a errores evitando que el servidor quede bloqueado bajo ninguna circunstancia. Además de un sistema de *debug* que permite al usuario encargado del mantenimiento observar el intercambio de mensajes, y un sistema *log* que permite almacenar los acontecimientos más importantes en el transcurso de su utilización.

V. Evaluación y Pruebas

La fase de evaluación y pruebas es una constante a lo largo de todo el proceso de realización del proyecto. No obstante, en esta fase se realizarán las pruebas correspondientes a un entorno de aplicación real. Escenario que puede verse en la Figura 8. En este entorno, el PC con la dirección 192.168.1.3 corresponde con el entorno Linux que alberga los servidores web, SFTP, RADIUS y LDAP. El PC 192.168.1.10 corresponde al cliente y el servidor 192.168.1.38 al servidor situado en la Raspberry Pi (ServidorRPi).

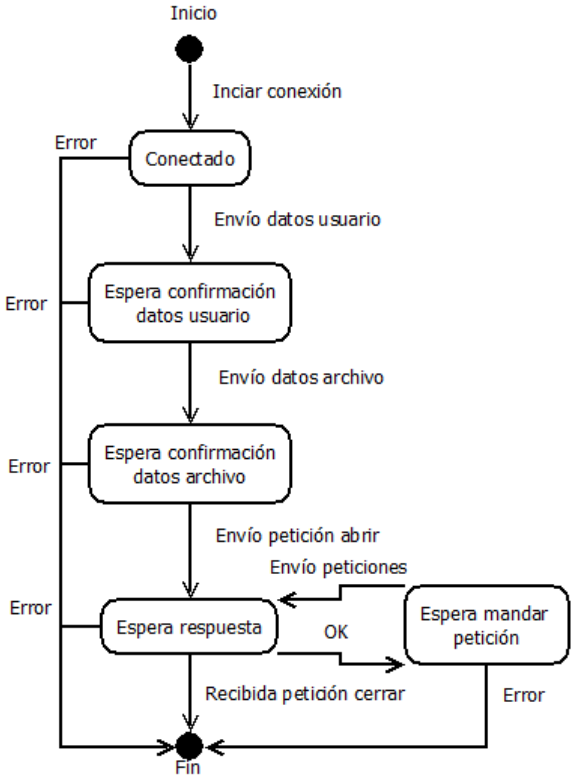


Fig. 5. Diagrama de estados del ClienteRPi

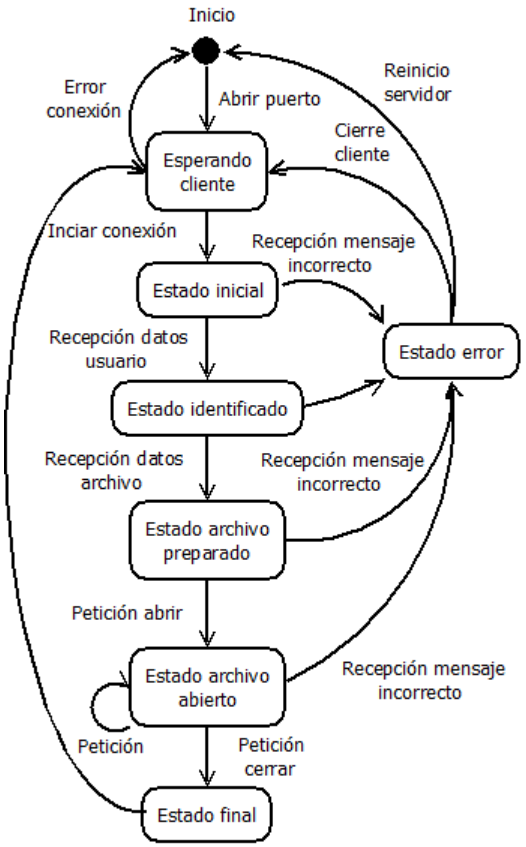


Fig. 6. Diagrama de estados del ServidorRPi

Para la realización de las pruebas se estudiarán todas las alternativas y funcionalidades que ofrece el sistema diseñado para comprobar su total y correcto funcionamiento. Además, paralelamente a esto se realizarán diversas capturas de tramas con la herramienta Wireshark [26], comprobando de esta forma el correcto funcionamiento del sistema.

El resultado obtenido de este proceso se muestra en las Figuras 9-13.

VI. Conclusiones

En este proyecto se ha diseñado e implementado un sistema de proyección de material docente que aporta una solución diferente al sistema utilizado actualmente.

Como se ha visto en el apartado anterior, el resultado final de la fase de evaluación y pruebas ha sido muy satisfactorio. Así, las contribuciones más destacables son las siguientes:

- El sistema implementado permite la proyección de material docente sin la necesidad de utilizar un cable para la conexión con el proyector, haciendo uso de una red inalámbrica. Para el caso, la red Wi-Fi de la Universidad de Granada.
- Como consecuencia del punto anterior, este nuevo sistema permite la total movilidad del docente en toda el aula de enseñanza mientras se proyecta el material.
- El sistema implementa además un gestor de almacenamiento centralizado, donde cada docente podrá guardar el material que quiera utilizar en sus clases. De esta forma, se facilita el trabajo del docente con diferentes equipos, puesto que elimina la necesidad de tener guardado el archivo en el equipo utilizado.
- Para la gestión del sistema de almacenamiento anterior,

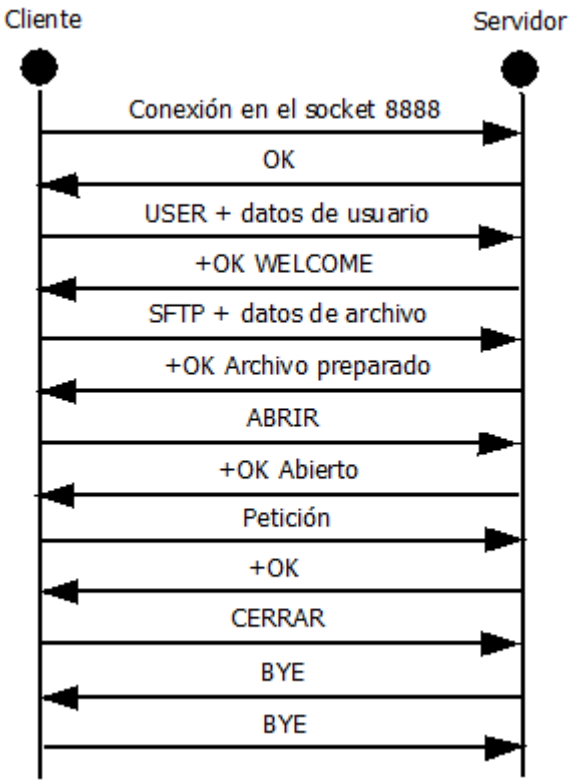


Fig. 7. Intercambio de mensajes ClienteRPi-ServidorRPi

se ha implementado un sistema gestor de base de datos donde se almacenarán todos los datos relevantes a las cuentas de los usuarios.

- Para la autenticación de usuarios, el sistema se ha implementado y adaptado al sistema actualmente utilizado por la Universidad de Granada en sus servicios web. De esta forma se allana el camino de implantación del sistema en el ámbito docente de la universidad.
- El sistema ofrece la posibilidad de trabajar con material docente en formato PDF, o con imágenes en formato JPG y PNG. Además es fácilmente ampliable a otros formatos y tipos de documentos diferentes. También se permite de forma sencilla la ampliación de las funcionalidades de los mismos.
- El sistema implementado permite la reutilización de los proyectores actualmente instalados. Como se viene comentando en capítulos anteriores, se utiliza una Raspberry Pi por clase como único gasto nuevo para la implantación (además del servidor centralizado). Esto supone que el sistema final sea una solución muy económica[27], de forma que se puede considerar seriamente la posibilidad de su implantación en las diferentes aulas de la universidad.
- Además, gracias también a la Raspberry Pi, se consigue que el sistema sea de fácil transporte y de fácil instalación (véase el Anexo II). También permite que el sistema no sea una instalación permanente, aumentando así su usabilidad en diferentes escenarios.
- Finalmente, el sistema no ha conseguido unificar las tecnologías actuales, de forma que sea indiferente el uso de ordenador, tableta o *smartphone* para proyectar el material, que era uno de los objetivos secundarios de este proyecto. Pero sí se ha conseguido un sistema fácilmente portable a diferentes tecnologías y sistemas operativos,

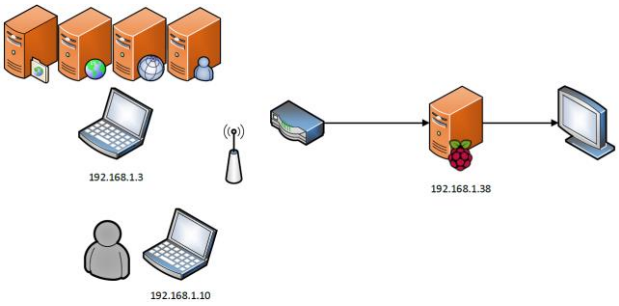


Fig. 8. Escenario típico de aplicación

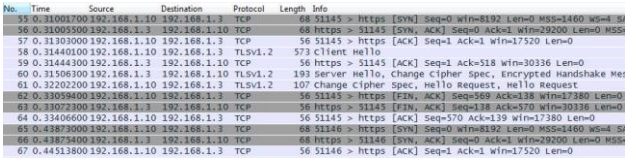


Fig. 9. Tramas inicio de conexión con el servidor web

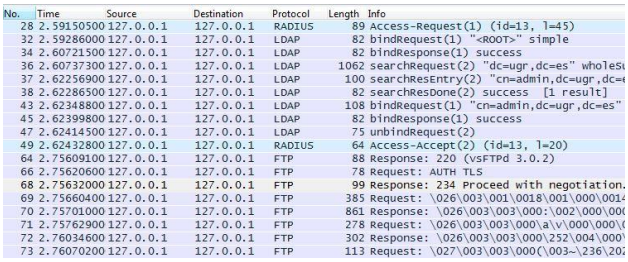


Fig. 10. Tramas de autenticación de usuario en entorno web

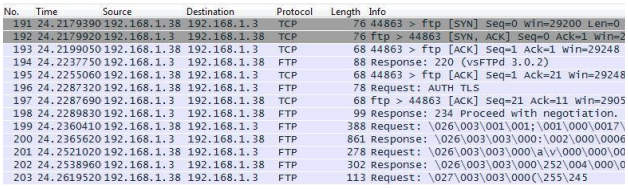


Fig. 11. Tramas de una conexión FTP entre usuario y servidor

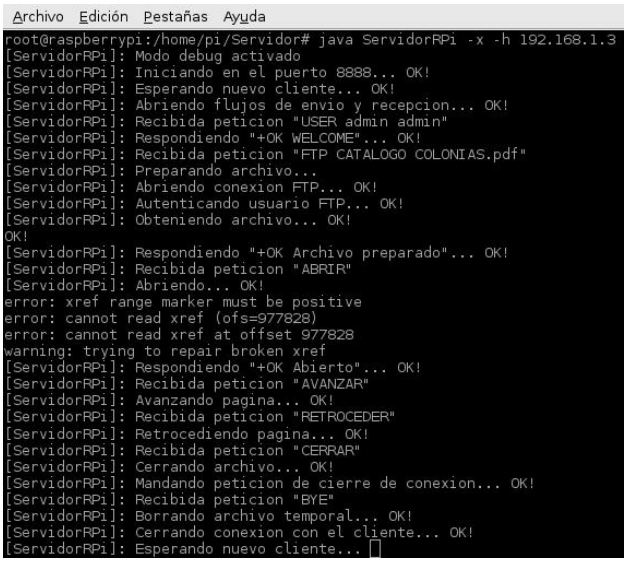


Fig. 12. *Debug* del ServidorRPi

de forma que en un futuro se pueda utilizar en diversos entornos diferentes, que era uno de los objetivos principales.

En definitiva, el sistema implementado aporta una solución real a la problemática actual, y cubre las funcionalidades de un usuario del sistema de proyección docente actualmente utilizado.

Aun habiendo cumplido la gran mayoría de los objetivos establecidos al inicio, aún quedan abiertas las siguientes líneas de trabajo futuras:

- Se ha logrado que el sistema sea fácilmente portable a distintos dispositivos gracias al uso del lenguaje PHP en el entorno web y el lenguaje Java en el entorno de la aplicación cliente–servidor. Por tanto, una línea de trabajo clara es completar la expansión del sistema a los distintos dispositivos que actualmente nos rodean como pueden ser tabletas o *smarthphones*.
- Con las nuevas distribuciones y las nuevas versiones recientes implementadas y optimizados para Raspberry Pi, se pueden estudiar las características de cada una de ellas para lograr mejorar el sistema implementado actualmente. Esto puede ser respecto al rendimiento o respecto al incremento de las funcionalidades del mismo con nuevo *software*.
- Se puede incorporar un sistema que permita mostrar y visualizar en el proyector la imagen de la pantalla del dispositivo utilizado, característica denominada *screen mirroring*. Para ello se puede hacer uso de la tecnología Piracast [28], basada en Miracast [9] pero optimizada para Raspberry Pi. Esta tecnología aún se encuentra en fase beta, por lo que aún queda un tiempo para que esté totalmente terminada y optimizada para poder hacer uso de ella. Por esa razón se descartó la implementación de la misma en este proyecto después de haber realizado un estudio en detalle de ella.

AGRADECIMIENTOS

Ha sido un largo camino hasta llegar a este punto. Me siento orgulloso con el resultado de este proyecto, y esto se lo debo a Jorge, mi tutor, gracias a la oportunidad que en su día me dio.

Por supuesto, debo agradecer a mis padres, y en general a mi familia, su apoyo y total confianza en mí desde el primer momento. Porque solo ellos saben de la dificultad y de todos los obstáculos que he tenido que superar.

Tampoco puedo olvidar a todos mis compañeros, por lo buenos momentos, y en especial a los 6 con los he compartido interrail. Y por su puesto a Miriam.

Gracias a todos.

REFERENCIAS

[1] Web oficial de **Raspberry Pi**: http://www.raspberrypi.org/.
[2] J. Salinas, "Innovación docente y uso de las TIC en la enseñanza universitaria," *Revista Universidad y Sociedad Del Conocimiento*, vol. 1, pp. 1-16, 2004.
[3] R. Palomo López, J. Sánchez Rodríguez and J. Ruiz Palmero, *Enseñanza Con TIC En El Siglo XXI: La Escuela 2.0*. Madrid, 2008.
[4] **Apple TV** sitio web oficial: http://www.apple.com/es/appletv/
[5] **AirPlay** sitio web oficial: http://www.apple.com/es/appletv/airplay/
[6] **Apple** sitio web oficial: http://www.apple.com/es/
[7] S. N. Aznar, "Aumentando la interacción en el aula ordinaria mediante el iPad y demás dispositivos de m-learning," *Revista De Educación y Derecho*, 2014.
[8] **Wireless Display** sitio web oficial: http://www.wirelessdisplay.com/index.html
[9] **Wi-Fi Alliance's** sitio web oficial: http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-miracast/.
[10] **Chromecast** sitio web oficial: http://www.google.es/intl/es/chrome/devices/chromecast/.
[11] Descripción autenticación UGR disponible en: http://csirc.ugr.es/informatica/ServiciosWeb/AutenticacionUsuariosUGR.html.
[12] Sistema operativo **Ubuntu 14.04**. Disponible en: http://www.ubuntu.com/.
[13] Web oficial del servidor web **Apache**: http://www.apache.org/.
[14] Web oficial de **PHP:** http://www.php.net/.
[15] Manual oficial de **PHP** disponible en: http://www.php.net/manual/es/index.php
[16] S. McCracken, "Curso de programación Web con HTML5, CSS, JavaScript, PHP 5 y MySQL," pp. 1148, 2011.
[17] Web oficial del servidor de ficheros **VSFTP**: https://security.appspot.com/vsftpd.html.
[18] Web oficial del servidor RADIUS, **FreeRADIUS**: http://freeradius.org/.
[19] Web oficial del servidor de base de datos **OpenLDAP**: http://www.openldap.org/.
[20] **Java**. Disponible en: http://www.java.com/es/.
[21] Distribución oficial para Raspberry Pi, **RASPBIAN**. Disponible en: http://raspbian.org/
[22] Web oficial de **MuPDF** http://www.mupdf.com/.
[23] K. L. Calvert and M. J. Donahoo, *TCP/IP Sockets in Java*. Amsterdam; Boston: Elsevier/Morgan Kaufmann, 2008.
[24] Documentación oficial de **Java** disponible en: http://www.php.net/manual/es/index.php
[25] Documentación oficial de **JApplet** disponible en: http://docs.oracle.com/javase/7/docs/api/javax/swing/JApplet.html
[26] Herramienta de análisis de red **Wireshark** disponible: http://www.wireshark.org/
[27] C. Albanesius, "Order Limit for $35 Raspberry Pi PC Lifted." *PC Magazine*, pp. 1-1, 2012-07-01.
[28] Tema **Piracast** del foro oficial de **Raspberry Pi** disponible en: http://www.raspberrypi.org/forums/viewtopic.php?t=60636

Juan Ramón Gutiérrez Martínez (10 de Septiembre de 1992, Baeza (Jaén)) es Graduado en Ingeniería de Tecnologías de Telecomunicación con mención en Telemática por la Universidad de Granada en 2014.

Jorge Navarro Ortiz es Profesor Contratado Doctor del área de Ingeniería Telemática de la Universidad de Granada. Tanto su experiencia profesional (en empresas como Nokia Networks, Ericsson y Siemens) como docente e investigadora siempre ha estado vinculada al campo de las comunicaciones móviles e inalámbricas, en el cual ha realizado numerosas contribuciones en forma de capítulos de libros, artículos de revistas, patentes, proyectos y contratos de investigación.

DDSBox: Sistema distribuido de compartición de archivos en tiempo real

Autores: Víctor Cabezas Lucena, e-mail: vclucen@correo.ugr.es
Olmo Jiménez Alaminos, e-mail: olmojial@gmail.com
Tutores: Juan Manuel López Soler, e-mail: juanma@ugr.es
Juan José Ramos Muñoz, e-mail: jjramos@gmail.com
Titulación: Ingeniería Informática
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—La necesidad de almacenamiento de datos en la nube, junto con la compartición de éstos con otros usuarios, es una tendencia en aumento constante. La mayoría de plataformas disponibles ofrecen un enfoque centralizado, por lo que se ha decidido realizar una nueva plataforma de compartición de carpetas entre usuarios de forma distribuida superando los inconvenientes que ofrecen otras plataformas.**

Para ello se ha utilizado el middleware DDS, ya que facilita la tarea de crear un entorno distribuido. Además se han utilizado diversas tecnologías para el cifrado de los datos y también para el almacenamiento de los datos de forma local.

Tras la realización de distintas pruebas para evaluar su funcionamiento podemos concluir que se ha logrado implementar con éxito un sistema de compartición de ficheros entre usuarios de forma distribuida mediante DDS, incluyendo algunas mejoras que no incluyen otras plataformas.

***Palabras clave*—DDS, Middleware, compartición de ficheros, distribución de datos**

I. Introducción

La tendencia actual de transición entre modelos de computación centralizados hacia entornos distribuidos ha hecho florecer una serie de aplicaciones y servicios basados en "la nube" que proporcionan a los usuarios un mayor número de alternativas a la hora de mantener y gestionar su información personal y digital.

En la actualidad existe un gran número de alternativas para la realización de copias de seguridad y compartición de archivos ofreciendo además acceso ubicuo a los datos.

A. DDS

DDS [1] son las siglas de Data Distribution Service for Real-Time Systems o Servicio de Distribución de Datos para sistemas de tiempo real. DDS es un estándar internacional abierto que especifica un modelo de publicación/suscripción para sistemas de tiempo real y empotrados. DDS es un estándar especificado por la Object Management Group (OMG) [2].

En este proyecto se optó por utilizar *RTI Connext DDS* [3], el cual es un middleware de red que implementa el modelo de comunicaciones en tiempo real de publicación/suscripción, permitiendo a un proceso compartir información en un entorno distribuido sin importar su localización física o la arquitectura del resto de procesos.

En la Figura 1 se puede observar el diagrama de una aplicación DDS. Las aplicaciones creadas sobre DDS están formadas por un conjunto de entidades que permiten la interacción entre el *middleware* y la aplicación. Las pricipales son las siguientes:

- **Domain Participant**: En DDS, las entidades se agrupan en torno a dominios. Cada entidad se sitúa y opera en un dominio a través de los *Domain Participant*. Son las entidades de mayor nivel de abstracción.
- **Topic**: Definen los distintos tipos de dato que son transmitidos en DDS. Estos definen la temática de la publicación/suscripción.
- **Subscriber**: Supone un punto intermedio de comunicación entre los *DataReaders* y la aplicación. Se encarga de gestionar las suscripciones a los distintos topics.
- **Publisher**: Es el encargado de publicar *topics* en un dominio.
- **DataReader**: Se trata del punto de acceso de una aplicación al espacio global de datos de DDS para la recepción de información.
- **DataWriter**: Es el punto de acceso de una aplicación al espacio global de datos de DDS para la publicación de información.

B. Antecedentes

En esta sección se revisarán herramientas o plataformas ya existentes que proveen una solución total o parcial para el problema tratado.

- **Dropbox** [4]: Sistema referencia en el desarrollo del proyecto. Sistema centralizado. Espacio limitado.

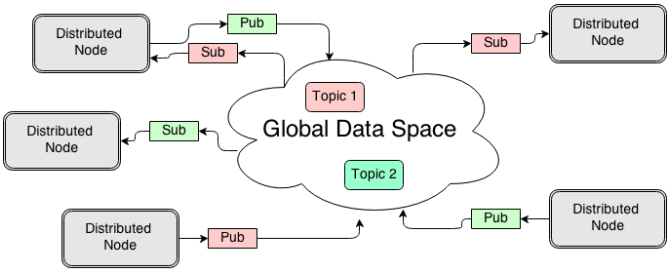


Fig. 1. Arquitectura de una aplicación DDS

- **Owncloud** [5]: Similar a Dropbox. Sistema centralizado. Montaje en servidor propio.
- **Google Drive** [6]: Sistema centralizado con posibilidad de edición de documentos. Espacio limitado.
- **Bittorrent Sync** [7]: Sincronización de archivos mediante P2P [8]. No existe el rol usuario. Se basa en un sistema de clave privada. Sin permisos definidos.
- **Emule** [9]: Compartición de archivos entre un gran número de usuarios vía P2P. Los ficheros se dividen en partes. Sin posibilidad de sincronizar archivos o carpetas.
- **Rsync** [10]: Aplicación y protocolo de sincronización de archivos y carpetas. Utiliza compresión de archivos y versiones incrementales de ellos. Solo permite comunicación uno a uno. Sin control de versiones.

II. Especificación de requisitos

A partir de las plataformas analizadas en la sección de antecedentes se identificaron una serie de requisitos que el sistema a desarrollar debe cumplir:

A. Requisitos funcionales

- Compartición de ficheros y carpetas entre usuarios.
- Realizar una transmisión distribuida de los datos.
- Se comparten carpetas: todos los usuarios con acceso a esa carpeta recibirán todos los ficheros y carpetas que contenga.
- Interfaz de usuario gráfica y por línea de comandos.
- Dos tipos de carpetas compartidas
  - Públicas: cualquier usuario tiene acceso.
  - Privadas: sólo usuarios que hayan sido invitados a dicha carpeta.

  Hay distintos tipos de usuarios para una carpeta compartida, cada uno de ellos con una serie de permisos que se detallan en la Tabla 1.

B. Requisitos no funcionales

- **Portabilidad:** La aplicación debería de ser capaz de ejecutarse en sistemas Windows como Linux, sin tener en cuenta la arquitectura del procesador.
- **Facilidad de instalación:** El proceso de instalación de la aplicación ha de ser lo más sencillo posible, de forma que el usuario no tenga que configurar el entorno en el que ejecutará la aplicación.
- **Transparencia:** El usuario no debe conocer la existencia de entidades DDS, hebras, y demás peculiaridades de la implementación.
- **Rendimiento:** La aplicación ha de ser eficiente tanto en memoria como en tiempo de ejecución, consumiendo sólo los recursos del sistema estrictamente necesarios.

Tabla I
Permisos de usuario

Type	Read	Write	Add user	Add editor
Reader	x			
Collaborator	x	x		
Editor	x	x	x	
Owner	x	x	x	x

III. Diseño

Una vez establecidos los requisitos que debe cumplir el sistema se procede a realizar el diseño del mismo.

A. Arquitectura global del sistema

El sistema a desarrollar consiste en un sistema distribuido en la que la información se intercambia entre distintos clientes de forma directa. Para realizar ese intercambio de información se va a utilizar el *middleware DDS*.

Gracias a este *middleware* la comunicación entre los clientes resulta muy sencilla. En la Figura 2 se ilustra la arquitectura global del sistema. Cada uno de los nodos producirá y recibirá información, por lo que será publicador y suscriptor sobre el *middleware*.

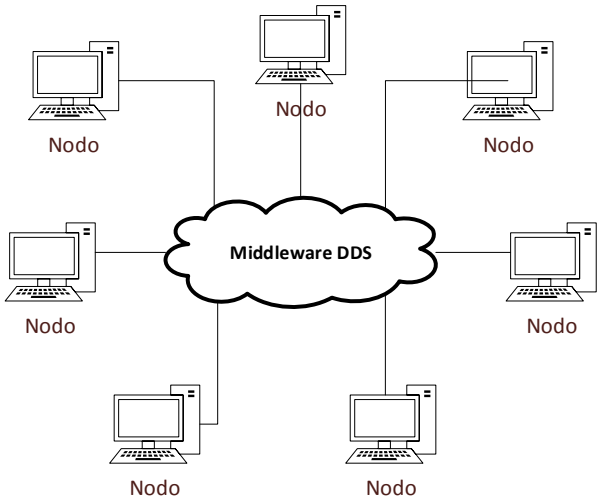


Fig. 2. Arquitectura global

B. Modelo de datos del sistema distribuido

Como se ha explicado en la introducción, la transmisión de la información se va a realizar utilizando diversos tópicos. En esta aplicación va a haber dos tipos de tópicos: globales y por carpeta.

1) Tópicos globales: Se van a utilizar para transmitir información de forma global a todos los usuarios. Son los siguientes:

- **UserInfo**: Se utiliza para transmitir la información correspondiente a un usuario: identificador, nombre de usuario, nombre real, email y clave pública de cifrado.
- **FolderInfo**: Mediante este tópico se transmite la información relativa a una carpeta compartida. Esta información incluye el identificador de la carpeta, su nombre, los usuarios con privilegios y una clave de cifrado en caso de ser una carpeta privada.

2) Tópicos por carpeta: Estos tópicos servirán para transmitir información relativa a cada una de las carpetas compartidas, es decir, cada carpeta compartida tendrá registrado en el *middleware* cada uno de los siguientes tópicos con un identificador único:

- **FileInfo**: Se utiliza para transmitir los metadatos relativos a cada fichero de la carpeta compartida: nombre, tamaño,

fecha de modificación, usuario que lo ha modificado, tipo de modificación.
- **FileSegment**: Sirve para transmitir el contenido binario del fichero por partes.
- **Command**: Mediante este tópico se transmiten comandos propios de la carpeta compartida: si se ha añadido un usuario nuevo y con qué permisos o cuando se elimina un usuario de la carpeta.

C. Diagrama de clases

En la Figura 3 se puede ver un diagrama de clases simplificado para mostrar el diseño de clases de la aplicación.

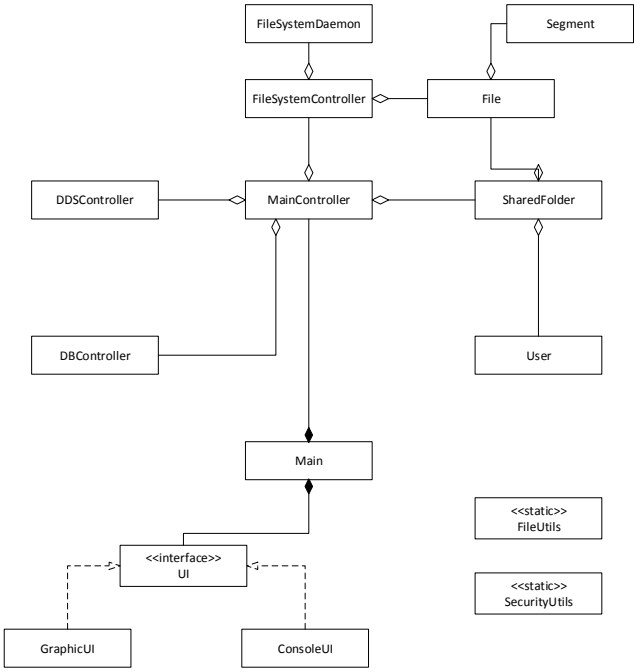


Fig. 3. Diagrama de clases

La clase *MainController* se encarga de toda la lógica general de la aplicación. Por otro lado hay controladores para el sistema de ficheros, para una base de datos local y para gestionar el *middleware DDS*.

También hay un *demonio* encargado de monitorizar el sistema de ficheros e informar al controlador de ficheros de todos los cambios que se produzcan en las carpetas compartidas de la aplicación.

La interfaz de usuario está diseñada de forma que tanto la interfaz gráfica como la interfaz por línea de comandos heredan de una interfaz de java con los métodos que deben implementar ambas interfaces.

D. Cifrado

Uno de los requisitos de la aplicación es la posibilidad de compartir carpetas de forma privada entre usuarios. Por ello surge la necesidad de cifrar dicha información para que un usuario que no tenga acceso a una carpeta compartida no pueda obtener su contenido.

Se van a utilizar dos algoritmos de cifrado: AES (Advanced Encryption Standard) [12] y RSA [11].

- **AES**: Se va a utilizar para transmitir los datos de los tópicos de las carpetas compartidas. Es un tipo de cifrado simétrico, es decir, todos los usuarios con acceso a la carpeta compartida disponen de la misma clave de cifrado, y cada carpeta compartida tendrá una clave de cifrado distinta. Sólo los usuarios que tengan la clave de cifrado de una carpeta compartida concreta podrán acceder a sus datos.
- **RSA**: Se utiliza para transmitir la información sobre una carpeta compartida de usuario a usuario. Es un tipo de cifrado asimétrico, por lo que cada usuario dispone de su propia clave pública y su clave privada.

E. Base de datos local

Surge la necesidad de mantener información localmente en cada nodo de forma que se mantenga una consistencia de la información entre distintas ejecuciones de la aplicación. Para ello se va a utilizar una base de datos local en cada nodo.

La información que se va a almacenar en esta base de datos es la correspondiente a los distintos usuarios, las carpetas compartidas a las que se esté suscrito y los metadatos de cada fichero.

F. Persistencia de los cambios

El *middleware* permite configurar la persistencia de los cambios realizados. Existen tres niveles de persistencia:

- **Volatile**: No se almacena ningún cambio para nodos que se unan posteriormente.
- **Transient**: Los cambios son almacenados mientras la ejecución continúe.
- **Persistent**: Los cambios prevalecen entre ejecuciones.

Para utilizar el nivel *Persistent* es necesario utilizar un *Servicio de persistencia*.

IV. Implementación

A. Lenguaje de programación

La aplicación se ha desarrollado utilizando el lenguaje de programación Java™7 [13]. Se ha elegido por encima de otras opciones porque es multiplataforma y posee un gran conjunto de bibliotecas, de forma que el mismo código sirve para ejecutar la aplicación en distintos sistemas operativos sin la necesidad de realizar modificaciones. Además es uno de los pocos lenguajes soportados por la API de la implementación utilizada del *middleware DDS*.

B. Serialización

Los datos a cifrar para las carpetas privadas son objetos formados por muchos atributos. Por ello se va a proceder a serializarlos. La serialización consiste en pasar un objeto a un array binario. Este conjunto de bits será el que se cifre, de forma que en el destino se puede reconstruir el objeto a partir de dicho array.

C. Identificadores

Al tratarse de un sistema distribuido surge la necesidad de generar identificadores en cada nodo que sean únicos en todo el sistema, de forma que no haya identificadores duplicados para entidades distintas. Por esta razón los identificadores secuenciales no son válidos.

Se han utilizado UUID [14]: son identificadores formados por 32 caracteres hexadecimales que se generan de forma aleatoria según distintas metodologías. En el caso de Java se utiliza una generación de números aleatorios.

La probabilidad de que se genere un duplicado es de $4x10^{-16}$ para 2^{36} claves generadas.

D. Base de datos

Para la base de datos local se ha utilizado el motor *SQLite* [15]. Se ha elegido por ser un motor multiplataforma, ligero y que no requiere ninguna instalación adicional, solo incluir una biblioteca en la aplicación.

V. Evaluación

En esta sección se comentarán las pruebas realizadas y se estudiarán los resultados obtenidos. Las pruebas realizadas se dividen en pruebas *cualitativas* y pruebas *cuantitativas*.

A. Pruebas cualitativas

Este apartado de la *evaluación* se divide a su vez en pruebas *unitarias*, en las cuales se probó el funcionamiento de los distintos módulos que integran el sistema de forma independiente para verificar su correcto funcionamiento, y pruebas de integración, en las cuales se probaron todos los módulos del sistema para comprobar el correcto funcionamiento entre ellos.

Los resultados de ambas pruebas fueron satisfactorios y se verificó el correcto funcionamiento del sistema.

B. Pruebas cuantitativas

En este apartado de pruebas se utilizó una batería de pruebas para medir el rendimiento del sistema implementados y poder compararlo con *Dropbox*, una de las alternativas actuales más conocidas en el mercado.

La batería de pruebas consistía en la transmisión de ficheros de tamaño 1MB, 10MB, 100MB y 500MB desde un nodo emisor a 1, 2 y 3 nodos receptores.

En la Figura 4 se puede observar la arquitectura utilizada para estas pruebas, se trata de un equipo *host* albergando 4 máquinas virtuales representando los nodos descritos anteriormente.

En la Figura 5 se muestran los resultados de las pruebas realizadas para la difusión a 1, 2 y 3 nodos utilizando DDS.

En las Figuras 6, 7 y 8 se comparan los resultados Dropbox y DDS con 1, 2 y 3 nodos respectivamente.

VI. Conclusiones

Una vez presentada la evaluación realizada al sistema desarrollado, se prodece a exponer las conclusiones extraídas.

A. Conclusiones evaluación

Los resultados de las pruebas cualitativas fueron los deseados y se consiguió validar el funcionamiento del sistema desarrollado.

Respecto a las pruebas cuantitativas se concluye lo siguiente:

Como puede observarse, el rendimiento de Dropbox parece inferior al redimiento del sistema implementado, este hecho es debido a que Dropbox inicialmente indexa el contenido del fichero, posteriormente compara dicho índice con su base de

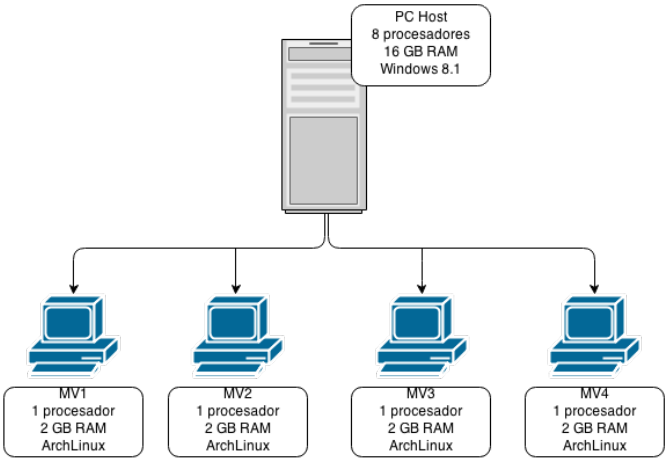


Fig. 4. Arquitectura evaluación cualitativa

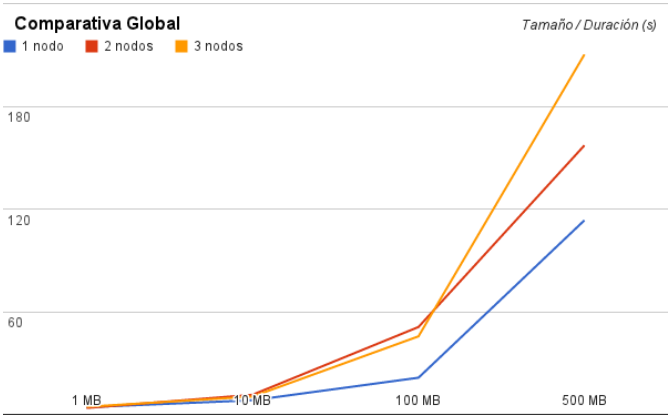


Fig. 5. Resultados pruebas DDS

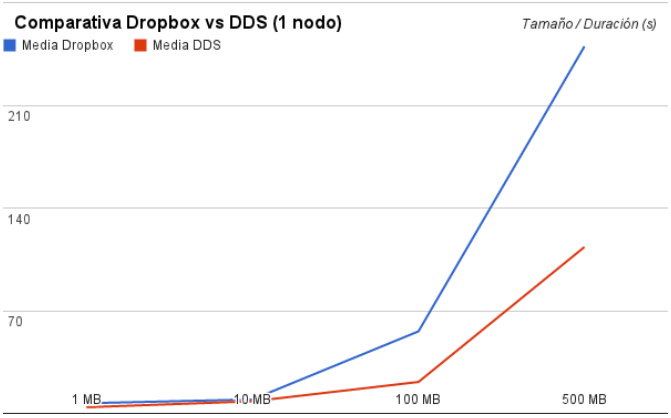


Fig. 6. Resultados pruebas DDS vs Dropbox (1 nodo)

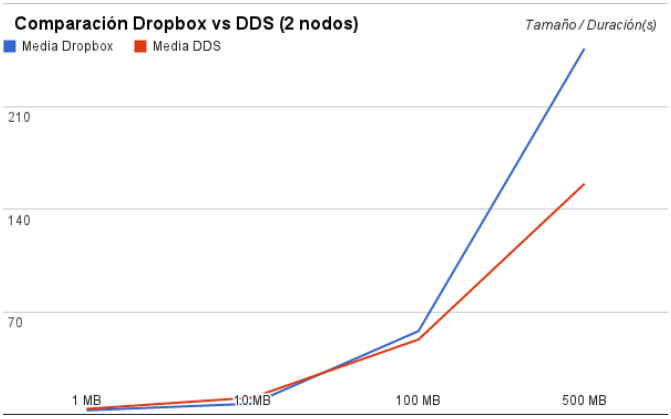


Fig. 7. Resultados pruebas DDS vs Dropbox (2 nodo)

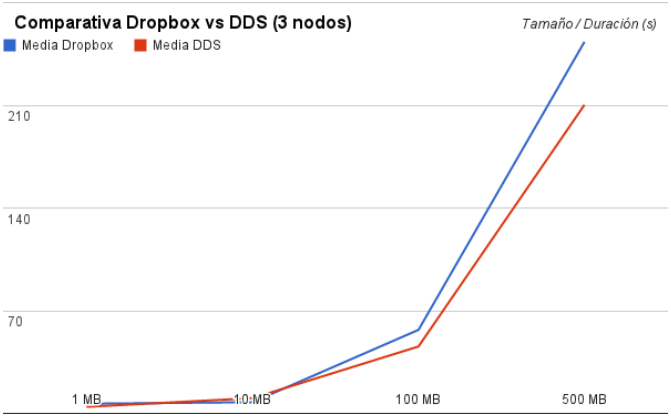


Fig. 8. Resultados pruebas DDS vs Dropbox (3 nodo)

datos, y si lo considera necesario, transmite dicho fichero a su sistema central, por ello, la primera transmisión de cada fichero perjudica el tiempo de transmisión medio para cada escenario.

En general, se observa que el incremento del número de nodos para ambos sistemas implica una reducción del rendimiento a la hora de difundir la información entre estos. A pesar de los datos extraídos durante las pruebas, no se ha conseguido determinar de manera exacta el número máximo de nodos que es capaz de soportar el sistema implementado antes de volverse completamente inestable debido a la escasez de medios para poder realizar dichas pruebas.

En base a los razonamientos realizados anteriormente se puede concluir que la descentralización de la lógica del sistema puede aportar beneficios respecto a un sistema centralizado ya que son los distintos nodos del sistema los que se encargan de tomar las acciones necesarias respecto a un evento, sin tener que esperar respuesta de un nodo central.

B. Conclusiones globales

En general, las conclusiones extraídas son las siguientes:

- Se ha logrado implementar un sistema para la compartición de ficheros mediante DDS cumpliendo los requisitos funcionales establecidos.
- Se han implementado distintos tipos de carpetas (públicas y privadas) y un sistema de privilegios para los usuarios.
- Los ficheros se comparten de forma transparente al usuario, requiriendo una intervención mínima por parte del usuario.
- La aplicación es multiplataforma, funcionando en Windows y Linux.

REFERENCIAS

[1] *Data Distribution Service for Real-time Systems*, OMG formal/2007-01-01, January 2007.
[2] Object Management Group. Disponible en: http://www.omg.org [Último acceso 20 de octubre de 2014]
[3] Real Time Innovations Inc. RTI Connext DDS Professional. Disponible en: http://www.rti.com/products/dds/index.html [Último acceso 20 de octubre de 2014]
[4] Dropbox. Disponible en: http://www.dropbox.com [Último acceso 20 de octubre de 2014]
[5] Owncloud. Disponible en: http://owncloud.org [Último acceso 20 de octubre de 2014]
[6] Google Drive. Disponible en: http://owncloud.org [Último acceso 20 de octubre de 2014]
[7] Bittorrent Sync. Disponible en: http://www.getsync.com [Último acceso 20 de octubre de 2014]
[8] *P2P Architectures*, RFC 5694, November 2009.
[9] Emule. Disponible en: http://www.emule-project.net [Último acceso 20 de octubre de 2014]
[10] Rsync. Disponible en: http://rsync.samba.org [Último acceso 20 de octubre de 2014]
[11] *PKCS #1: RSA Cryptography Specifications*, RFC 3447, February 2003.
[12] *ADVANCED ENCRYPTION STANDARD (AES)*, FIPS 197, November 2001.
[13] Java. Disponible en: https://www.java.com [Último acceso 20 de octubre de 2014]
[14] *A UUID URN Namespace*, RFC 4122, July 2005.
[15] SQLite. Disponible en: http://www.sqlite.org [Último acceso 20 de octubre de 2014]

Desarrollo de una aplicación de Android basada en *crowdsourcing* para la recolección de datos de QoE y QoS sobre vídeos de YouTube

Autor: José Rafael Suárez-Varela Maciá, e-mail: josesvm@correo.ugr.es
Tutor: Jorge Navarro Ortiz; e-mail: jorgenavarro@ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—Este proyecto tiene como fin recopilar información de QoE y QoS sobre vídeos de YouTube reproducidos en dispositivos móviles Android. Para ello se aplicará la filosofía de *crowdsourcing*, obteniendo así información sobre un gran número potencial de usuarios con un coste muy bajo. Toda esta información es almacenada en una base de datos de forma ordenada y será utilizada para la generación de modelos de estimación de QoE así como múltiples análisis estadísticos en los que participen los múltiples datos recogidos.**

***Palabras clave*—*Streaming* de vídeo, Calidad de Experiencia (QoE - *Quality of* Experience), Calidad de Servicio (QoS - *Quality of Service*), *crowdsourcing*, Wi-Fi, redes móviles, Android, YouTube.**

I. Introducción

El servicio de *streaming* es en la actualidad el servicio que cuenta con un mayor volumen de tráfico en Internet. Según un informe de Cisco [1], en el año 2017 se estima que abarcará un total del 69% del tráfico total en Internet, frente al 57% que ya suponía en 2012. Con estas cifras se destaca no sólo la importancia de este servicio en la actualidad, sino también el gran crecimiento que experimentará en un futuro próximo. Dentro de este servicio, el líder indiscutible es YouTube. El éxito de este servicio se atribuye principalmente a la combinación del amplio catálogo de vídeos que ofrece junto con el carácter de red social que permite interactuar entre sus usuarios [2].

Por otro lado, las redes con conectividad inalámbrica han experimentado un crecimiento acusado en los últimos años al mismo tiempo que presentan unas previsiones muy favorables para los próximos años. En concreto, en este proyecto tomarán parte las redes móviles de tipo celular con tecnologías como GSM, UMTS, LTE, etcétera, y las redes inalámbricas que siguen el estándar IEEE 802.11. De estas últimas se considerarán sólo aquellas que cumplen con la certificación Wi-Fi. Según un informe de Cisco [3], en 2012 estas redes en conjunción abarcaban en total un 52% del tráfico total de Internet, mientras que para el año 2017 se estima que supondrán un total del 68%.

Asimismo, se destaca la importancia de los conceptos de calidad de servicio (QoS – *Quality of Service*) y calidad de experiencia (QoE – *Quality of Experience*). La obtención de información de QoE y QoS sobre servicios de *streaming de* vídeo puede dar lugar a la futura creación de modelos de estimación. Estos modelos serán de gran utilidad en tanto que se utilizan a menudo en ingeniería de tráfico. Apoyándose en estos modelos, los proveedores de servicios y los propios servidores de contenidos pueden tratar de buscar una serie de políticas que busquen un punto óptimo en el que se ofrezca un nivel de servicio adecuado con la mayor eficiencia posible. Esto supone grandes reportes económicos puesto que se utilizarán técnicas que conseguirán un aprovechamiento máximo de los recursos. De este modo se evitará llevar a cabo una política de sobredimensionamiento que garantice el correcto funcionamiento de los servicios con su consecuente coste adicional.

Por último, cabe mencionar la importancia del sistema operativo Android dentro del mercado de los dispositivos móviles inteligentes, denominados asiduamente *smartphones*. Se estima que en el último cuatrimestre de 2013, Android se encontraba aproximadamente en el 80% de los *smartphones* existentes a lo largo del mundo [4], frente a su principal competidor IOS, que abarcaba prácticamente un 20%. El principal logro de Android se basa en el amplio número de usuarios con los que cuenta así como en el crecimiento que ha experimentado en los últimos años.

Tomando en consideración lo expuesto hasta el momento, el objetivo principal propuesto en este proyecto ha sido el diseño e implementación de un sistema de recolección de datos de QoE y QoS sobre vídeos de YouTube en dispositivos móviles, en concreto sobre aquellos que utilizan el sistema operativo Android. No obstante, aunque el primer objetivo fue la obtención de datos de QoE y QoS, finalmente se han obtenido otras estadísticas que podrán resultar de interés, tales como datos de carácter demográfico o la obtención de los tópicos relacionados con los vídeos reproducidos.

Tras haber realizado una revisión bibliográfica, no se ha podido encontrar una aplicación que realice las mismas funciones. El trabajo más similar que se ha encontrado ha sido en [5]. Sin embargo según se indica en este artículo, se trata de una aplicación que sólo recopila información sobre la QoE a través del método *OneClick* [6] y relaciona esta información con datos de QoS de nivel de red (velocidad de transmisión, pérdida de paquetes y retardo) medidos en el servidor de *streaming*. Esto indica que el servidor de vídeos debe trabajar de forma colaborativa con el usuario final para combinar la

información recogida. En este caso la herramienta tendría sentido para un administrador de un servidor de *streaming* de vídeo que desease recoger información sobre su propio servicio. Sin embargo, en el sistema desarrollado en el presente proyecto toda la información se recopila en el lado del cliente, desde la aplicación para móviles, lo que posibilitará realizar un estudio sobre el servicio de YouTube sin contar con mediciones realizadas en el lado del servidor. Además, cabe destacar que en la aplicación desarrollada no sólo se recogen parámetros de QoS a nivel de red, sino que también se han monitorizado eventos en la aplicación que permitirán obtener información de la QoS a nivel de aplicación (interrupciones, tiempo de carga inicial del vídeo, etcétera). Con todo ello se tienen datos de QoE (medida mediante el parámetro MOS), datos de QoS a nivel de red y de aplicación, datos demográficos y datos estadísticos sobre los vídeos reproducidos. Todos ellos se podrán utilizar combinadamente para realizar multitud de estudios diferentes.

A lo largo de todo el proceso de diseño se pondrá de manifiesto la filosofía de *crowdsourcing*. De forma resumida, esta corriente se basa en la externalización de pequeñas tareas a diferentes usuarios de forma que contribuirán a la elaboración de un trabajo de grandes dimensiones. En lo que al proyecto se refiere, se pretende obtener a través de la aplicación Android información proveniente de una gran cantidad de usuarios que finalmente permitirán conformar una base de datos importante que pueda dar lugar a la elaboración de futuros trabajos de investigación. Cabe destacar la importancia del sistema operativo Android en la aplicación de esta filosofía, puesto que su amplio mercado facilitará que la aplicación desarrollada pueda potencialmente ser utilizada por un gran número de usuarios que además constituyan una muestra heterogénea.

II. Arquitectura del sistema

Para cumplir con los objetivos y requisitos planteados en este proyecto se ha decidido, después de valorar diferentes opciones, la utilización de la arquitectura representada en la Fig. 1.

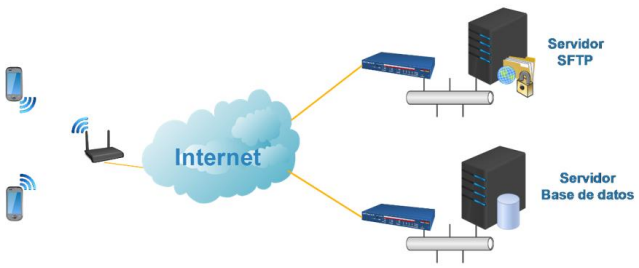


Fig. 1: Arquitectura del sistema diseñado.

Este sistema se compondrá de los siguientes elementos:

- Aplicación Android para el cliente que permita la búsqueda y reproducción de vídeos del servicio de YouTube. A lo largo de la reproducción se irán recogiendo datos relacionados principalmente con la QoS. Además recogerá al término de la reproducción mediante un formulario algunos datos sobre la experiencia percibida por el usuario (QoE).
- Servidor SFTP para la recolección de los datos recibidos desde diferentes dispositivos móviles en cada experimento.
- Servidor de base de datos para almacenar de forma ordenada la información alojada en el servidor SFTP después de un posprocesado de los datos.
- Desarrollo de un programa en Java que llevará a cabo la lectura y posprocesado de la información del servidor SFTP y posteriormente realizará la inserción de ésta en el servidor de base de datos.

El esquema de la Fig. 1 representa la estructura lógica de la red, en la que se pueden observar los dos servidores alojados en diferentes subredes. Esta arquitectura sería factible sobre la implementación final. No obstante, en la implementación real del proyecto, los servicios SFTP y de base de datos han sido alojados en un mismo *host* puesto que se ha considerado la opción más económica y segura y en no se han identificado posibles desventajas.

III. Diseño e implementación de la aplicación Android en el lado del cliente

Para la recolección de datos, se ha desarrollado una aplicación Android que sea lo más intuitiva y atractiva posible para favorecer su uso por parte de usuarios finales.

Esta aplicación supone el elemento principal del diseño de este proyecto ya que en ella se realizarán las principales funciones que permitirán obtener toda la información deseada.

La aplicación constará principalmente de cuatro pantallas o actividades que actuarán como interfaz para el usuario y tendrán diferentes funcionalidades.

La primera de ellas será una interfaz a través de la cual el usuario podrá llevar a cabo una búsqueda de vídeos del servicio de YouTube a partir de unas palabras clave. De este modo el usuario podrá enviar una palabra o frase para que se pueda obtener un listado con los resultados obtenidos. Estas dos actividades se pueden observar en la Fig. 2.

Fig. 2: Actividades de búsqueda y listado de resultados

A partir de la lista de resultados, el usuario podrá elegir uno de ellos para comenzar la reproducción del vídeo. En este momento se ejecutará una actividad en la que se incluye un reproductor de vídeos embebido junto con alguna información descriptiva del vídeo. Se puede considerar esta actividad como la fundamental de la aplicación, ya que en ella es donde se recogen la mayoría de los datos que finalmente se van a enviar

al servidor. Al iniciarse la reproducción se ejecutarán tres hebras que llevarán a cabo diferentes tareas en segundo plano. Las dos primeras se encargarán respectivamente de la recopilación de información de QoS a nivel de red y a nivel de aplicación. La última de ellas recogerá datos descriptivos del vídeo incluyendo los tópicos relacionados con éstos siguiendo el esquema de tópicos identificados de forma unívoca en *FreeBase* [7]. Cabe destacar que todos estos procesos se realizarán de un modo totalmente transparente, tratando así de aproximarse en la medida de lo posible al funcionamiento de una aplicación convencional para la reproducción de vídeos, tal como la aplicación oficial de YouTube. De este modo no supondrá un gran esfuerzo para el usuario la utilización de esta aplicación. En el desarrollo de estas funcionalidades, han resultado de gran utilidad las librerías *YouTube Android Player API* [8] y *YouTube Data API* [9] para la reproducción del vídeo y la detección de eventos que posteriormente darán información sobre la QoS a nivel de aplicación.

Finalmente, cuando el usuario desee finalizar la reproducción del vídeo, se le ofrecerá mediante un diálogo la posibilidad de rellenar un pequeño formulario.

En la Fig. 3 quedan reflejadas las interfaces de reproducción del vídeo y cuando se despliega el diálogo que invita al usuario a realizar la encuesta.

Fig. 3: Actividad de reproducción de vídeos y diálogo al finalizar la reproducción

Finalmente, si el usuario accede a rellenar el formulario, se le presentará una actividad como la de la Fig. 4 en la que se podrá llevar a cabo finalmente el envío de todos los datos recogidos a lo largo del experimento hacia un servidor. Este formulario es breve ya que se pretende que completarlo no suponga un gran esfuerzo para el usuario. Sin embargo contiene datos de gran interés. Como principal información, se obtiene una valoración de entre 1 y 5 sobre la QoE percibida por el usuario, lo que se denomina comúnmente MOS (*Mean Opinion Score*) [10]. Por otro lado se recogen datos de carácter demográfico, como son la edad y el sexo, que a menudo son de interés en estudios estadísticos.

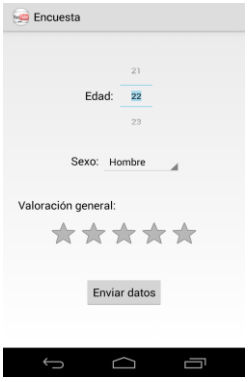


Fig. 4: Actividad de encuesta final al usuario

También cabe destacar que en todo momento se ha tratado de preservar la privacidad del usuario. Con ello, cualquier información que se ha considerado susceptible de identificar al usuario o al dispositivo móvil en el que se realiza el experimento, se ha tratado de evitar o en su defecto se le ha aplicado una función *hash* antes de llevar a cabo el envío de los datos. De este modo se podrán por ejemplo diferenciar los experimentos realizados desde un mismo dispositivo móvil pero no será posible identificar de manera directa el dispositivo que realizó el envío de los datos.

Por último, durante el proceso de implementación se decidió incluir de un modo adicional la posibilidad de reproducir vídeos a partir de un enlace *web* que referenciase a éstos. De este modo se favorecería el uso de la aplicación ya que en la actualidad es muy común la utilización de este tipo de enlaces para la compartición de vídeos a través de redes sociales o aplicaciones de mensajería instantánea.

IV. Diseño e implementación en el lado del servidor

En el lado del servidor se ha implementado por un lado un servidor SFTP, utilizando la distribución de *software* libre openssh [11], y por otro lado un servidor de base de datos utilizando una distribución de mySQL [12]. Estas distribuciones se han elegido en tanto que se trata de servicios ampliamente desplegados en la actualidad y de licencia gratuita.

En el diseño previsto en el presente proyecto se ha decidido utilizar una modalidad de SFTP enjaulado. Esto quiere decir que el usuario SFTP no podrá acceder a todo el contenido del *host* en el que se aloja el servidor, sino que se le ha restringido el acceso a un directorio creado expresamente para éste fin. Con ello se ha pretendido aumentar el nivel de seguridad en el servidor. De este modo, todos los dispositivos móviles podrán enviar al directorio de SFTP los ficheros de datos que se han generado durante el experimento utilizando un nombre de usuario y sus credenciales. Además, SFTP implica la utilización de un canal seguro, por lo que se preservará la confidencialidad de los datos ya que el contenido que viaja a través de Internet estará convenientemente cifrado para evitar que puedan realizarse escuchas en el canal.

En cuanto al servidor de base de datos, se ha contemplado crear una serie de tablas que permitan almacenar todos los datos obtenidos tras un posprocesado. Para ello todos aquellos datos cuyo número de entradas en la tabla puede ser variable en función del experimento (por ejemplo, eventos de interrupción), han motivado la creación de una nueva tabla. De este modo, cada entrada en las tablas contendrá un campo que identificará al experimento al que pertenece con el fin de que se puedan realizar posteriormente consultas selectivas en las que se puedan obtener los datos en conjunto de cada experimento de forma individualizada.

Por último ha sido necesario el desarrollo de un programa utilizando el lenguaje Java para llevar a cabo la actualización de los datos almacenados en el servidor SFTP, procesarlos para obtener nueva información e insertarlos de forma ordenada en la base de datos. Este programa además realizará una comprobación en el inicio de su ejecución en la que, si no

existe la base de datos y las tablas asociadas a ésta, las generará de forma automática para abstraer en la medida de lo posible al administrador del servidor de las tareas iniciales necesarias para la configuración del servidor. En el procesado de los datos se destaca sobre todo que, a partir de la detección de ciertos eventos a nivel de aplicación sobre el reproductor de vídeos, se ha recogido información como el tiempo de *buffering* inicial o el número de interrupciones producidas por agotamiento del *buffer* y su duración. Este programa únicamente añadirá la información que aún no se encuentre en la base de datos y podrá ser ejecutado de forma explícita por parte del administrador del servidor cuando éste desee actualizar la base de datos o podría realizarse un pequeño *script* que lo ejecutase periódicamente. Para la comunicación con el servidor mySQL se ha hecho uso de una API oficial denominada *mySQL connector for Java* [13].

V. Evaluación de los resultados

El producto final que se presenta en este proyecto será la base de datos, que contiene un gran volumen de información relacionada con la QoS y la QoE sobre vídeos de YouTube en dispositivos Android, así como una serie de datos aplicables a diferentes estudios estadísticos.

Esta base de datos sigue un modelo relacional que se compone de seis tablas distintas que contendrán información de diferente naturaleza. Todas ellas contienen un campo que actuará de clave primaria e identificará unívocamente a un experimento concreto. Este campo se compone a partir de la fecha y hora de envío de los datos hacia el servidor y un identificador único del dispositivo móvil, de modo que se podrá recopilar toda la información relativa a un mismo experimento o consultar todos los experimentos realizados desde un mismo dispositivo. Se remarca que no es posible identificar directamente al dispositivo móvil puesto que antes de llevar a cabo el envío de los datos se le aplicó al identificador una función *hash*.

En el diseño de la base de datos existe una tabla principal denominada '*Datos_video*' en la que se incluyen los datos que se recopilan de forma invariante en todos los experimentos. Por otro lado, el resto de tablas incluye un número variable de entradas referentes a cada experimento. Por ejemplo, una de ellas aporta información sobre interrupciones, de modo que cada entrada corresponderá a una interrupción producida en un vídeo. Sin embargo el número de interrupciones para cada vídeo es variable.

A continuación se realiza una descripción de todas las tablas contenidas en la base de datos junto con el significado de cada uno de los campos.

Tabla 'Datos_video':

Se trata de la tabla principal. Contiene una entrada por experimento recibido en el servidor. En ésta se recogen todos los datos recopilados comunes a todos los experimentos.

Esta tabla recoge datos como el tiempo de carga del *buffer* antes de comenzar la reproducción del vídeo, el tiempo total durante el que se ha extendido la reproducción del vídeo, la valoración (MOS) del usuario, edad y sexo de éste, si se ha realizado a través de una red con conectividad Wi-Fi o a través de una red celular para móviles e información asociada a estas redes, datos descriptivos del vídeo tales como el número de reproducciones totales o las valoraciones positivas y negativas por parte de los usuarios de YouTube, etcétera.

Tabla 'Interrupciones':

Esta tabla recoge todas las interrupciones que se producen en cada experimento. Cada entrada de la tabla contiene información sobre una interrupción. Cabe destacar que todas las interrupciones detectadas se deben a que se han agotado los datos en el *buffer*. No se incluyen interrupciones durante la reproducción del vídeo realizadas de forma explícita por parte del usuario. Cada entrada contiene un identificador del experimento en el que se ha producido la interrupción, unas marcas temporales de inicio y fin de ésta y la duración con una precisión de milisegundos.

Tabla 'Niveles_Senal':

Esta tabla recoge medidas de los niveles de señal (RSSI – *Received Signal Strength Indication*) correspondientes a las redes Wi-Fi y móvil. Cada medida incluye la localización del dispositivo móvil cuando se ha realizado la medición y una marca temporal. El nivel de señal de la red Wi-Fi sólo será posible obtenerlo cuando el dispositivo esté conectado a una red de este tipo. Sin embargo, el nivel de señal de la red móvil podrá obtenerse en todo caso puesto que el móvil típicamente está conectado a la red del operador.

Tabla 'Tipo_Conexion_Movil':

Esta tabla representa la tecnología móvil de la celda a la que está conectado el dispositivo móvil. Puesto que el dispositivo puede estar en movimiento durante la reproducción del vídeo, éste puede ir conectándose a diferentes celdas con diferentes tecnologías. Por ello puede haber más de una entrada para cada experimento junto con una marca temporal. Las tecnologías más típicas que pueden registrarse son CDMA, EDGE, GPRS, HSDPA, HSPA, HSPA+, UMTS o LTE.

Tabla 'Topicos'

Esta tabla incluye todos los tópicos relacionados con los diferentes vídeos reproducidos. Al incluir en cada entrada el identificador del experimento, se puede identificar el título del vídeo al que corresponde y el resto de los datos almacenados sobre el mismo experimento.

Tabla 'Errores_Reproduccion'

Esta tabla recoge todos los posibles errores que se pueden producir a lo largo de la reproducción de un vídeo. Estos errores se pueden deber típicamente a la pérdida de conectividad con la red o por fallos producidos en el dispositivo móvil.

Adicionalmente se ha diseñado un proceso por el cual, con el dispositivo móvil conectado a un ordenador personal, se podrán obtener trazas de tráfico pudiendo posteriormente

analizar el patrón de tráfico recibido durante el *streaming* de vídeo. Para ello, se ha utilizado un fichero binario de una distribución de TCPDump [14] que se ha adaptado para dispositivos Android mediante un proceso de *cross-compiling*.

VI. VÍAS FUTURAS

Debe destacarse que este proyecto surge de una beca de colaboración, de modo que el fin último es servir de soporte a la labor de investigación del departamento.

Con la elaboración de la base de datos se pretenderá recoger grandes volúmenes de información que den lugar a la futura creación de estudios estadísticos relacionados principalmente con la QoE y la QoS en servicios de *streaming* de video sobre dispositivos móviles.

Algunos de los trabajos que se consideran de interés a partir de la información recopilada son:

- Realización de modelos de estimación de QoE a partir de diferentes datos de QoS y viceversa.

- La obtención de niveles RSSI asociados a la localización donde se toma la medida permitirá posteriormente trazar un mapa en el que se muestren todas las mediciones de los niveles de cobertura para cada una de las tecnologías móviles (GSM, UMTS, LTE, etcétera) y para las células Wi-Fi.

- Realización de estudios estadísticos en los que se manejen variables tales como el número de reproducciones totales, los tópicos relacionados con los diferentes vídeos o el número de valoraciones positivas (me gusta) y negativas (no me gusta) por parte de los usuarios de YouTube. Asimismo, los datos van asociados al sexo y edad del usuario, por lo que también podrían incluirse en el estudio estadístico dichas variables demográficas.

- Obtención de estadísticas sobre el tiempo de *buffering* antes de iniciar el vídeo o el número de interrupciones y la duración de éstas. Esto permitirá ya no sólo realizar modelos de estimación entre QoS y QoE, sino también realizar algunos estudios que relacionen estas características con el tipo de red que se está utilizando.

- Con la obtención de trazas de tráfico, se podrán realizar estudios futuros sobre la generación de tráfico por parte de los servidores de YouTube. Asimismo, mediante ingeniería inversa podrían descubrirse algunos aspectos del protocolo de comunicación que utiliza este mismo servicio.

No obstante, con la información recogida en la base de datos se estima que se podrían hacer múltiples estudios estadísticos que no han sido contemplados *a priori*.

VII. CONCLUSIONES

En el presente Trabajo de Fin de Grado se ha diseñado un sistema compuesto por diversas herramientas que trabajan de forma colaborativa. Con ello se ha conseguido elaborar una plataforma de monitorización de datos sobre *streaming* de vídeo en dispositivos móviles. Estos datos darán información sobre la Calidad de Servicio (QoS) y la Calidad de Experiencia (QoE) en diversos experimentos en los que se llevan a cabo reproducciones de vídeos del servidor de YouTube. Además se incluyen datos sobre niveles de cobertura de las redes móvil y Wi-Fi, datos demográficos de los usuarios y estadísticas de los vídeos tales como el número de reproducciones, tópicos relacionados, valoración de los usuarios de YouTube, etcétera. Todos estos datos quedarán recogidos en una base de datos centralizada que se utilizará como fuente de información para posibles estudios estadísticos de investigación posteriores.

En el sistema desarrollado, toda la información se recopila en el lado del cliente, a través de una aplicación móvil. Esto ha posibilitado la realización de experimentos sobre el servicio de vídeos de YouTube, que se trata actualmente del líder mundial en el ámbito del *streaming* sobre vídeo, lo que magnifica considerablemente el alcance de este proyecto.

Por último, cabe destacar que la aplicación se basa en la filosofía de *crowdsourcing*, lo que ha reportado una gran eficiencia en costes en lo que se refiere a la obtención de datos y la oportunidad de acceder a una muestra muy amplia y heterogénea conformada por todos los usuarios que utilizan móviles con el sistema operativo Android en la actualidad.

REFERENCIAS

[1] Cisco Corporation. Cisco Visual Networking Index: forecast and methodology, 2012-2017. White paper. [cited 2014 June 6]. Available from: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf

[2] X. Cheng, C. Dale, J. Liu, "Statistics and social network of YouTube videos," *in Proc. IEEE Int. Workshp Quality of Service (IWQoS)*, pp. 229–238, 2008.

[3] Cisco Corporation. Cisco Visual Networking Index Forecast Highlights [cited 2014 June 8]. Available from: http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html

[4] Statista. Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 4th quarter 2013 [cited 2014 June 12]. Available from: http://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

[5] F. Delli Priscoli, V. Suraci, A. Pietrabissa, M. Iannone, "Modelling Quality of Experience in Future Internet networks", *Future Network & Mobile Summit, Berlin*, pp. 1-9, 2012.

[6] C. Kuan-Ta, T. Cheng-Chun, Wei-Cheng X.: OneClick: A Framework for Measuring Network Quality of Experience. *IEEE Conference on Computer Communication, Brazil*, pp. 702–710, 2009.

[7] Freebase website. [cited 2014 July 23]. Available from: https://www.freebase.com

[8] Google Developers. YouTube Player API. [cited 2014 July 22]. Available from: https://developers.google.com/youtube/android/player/

[9] Google Developers. YouTube Data API (v3). [cited 2014 July 23]. Available from: https://developers.google.com/youtube/v3/

[10] ITU-T Recommendation, "ITU-T Rec. P.800.1: Mean Opinion Score (MOS) Terminology", 2003.

[11] OpenSSH website. [cited 2014 July 23]. Available from: http://www.openssh.com

[12] mySQL website. [cited 2014 July 9]. Available from: http://www.mysql.com

[13] mySQL website. mySQL connector Java. [cited 2014 July 20]. Available from: http://dev.mysql.com/downloads/connector/j/

[14] TCPDump website. Documentation. [cited 2014 July 20]. Available from: http://www.tcpdump.org/#documentation

José Rafael Suárez-Varela Maciá (nacido en Granada el 12/03/1992), graduado en Ingeniería de Tecnologías de Telecomunicación (2010-2014) por la Universidad de Granada y alumno del máster oficial de Ingeniería de Telecomunicación en el curso 2014/2015 impartido en la Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación (ETSIIT) de la Universidad de Granada.

Jorge Navarro Ortiz es Profesor Contratado Doctor del área de Ingeniería Telemática de la Universidad de Granada. Tanto su experiencia profesional (en empresas como Nokia Networks, Ericsson y Siemens) como docente e investigadora siempre ha estado vinculada al campo de las comunicaciones móviles e inalámbricas, en el cual ha realizado numerosas contribuciones en forma de capítulos de libros, artículos de revistas, patentes, proyectos y contratos de investigación entre otros.

Diseño de un reproductor de vídeo *streaming* inteligente

Tutor: Juan José Ramon Muñoz; e-mail: jjramos@ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

Autor: Francisco Javier Cuenca Jiménez, e-mail: fjcuencajimenez@gmail.com

En este trabajo se proponen técnicas de reproducción y descarga para la reproducción de vídeo, de forma que ofrezca mejor calidad que el utilizado por el reproductor de YouTube. Para este fin, se han diseñado varios algoritmos que adaptan la frecuencia de solicitudes entre cliente y servidor, así como la velocidad de reproducción, en función de las condiciones del tráfico en la red. Se ha estudiado la relación entre velocidad de reproducción y satisfacción del usuario mediante un test de opinión. El modelo obtenido se ha aplicado en los algoritmos desarrollados.

La evaluación de los algoritmos propuestos mediante un simulador de red demuestran que dan mejores resultados que el reproductor de YouTube móvil en los escenarios de problemas en la red estudiados.

***Palabras clave*— streaming de vídeo, ráfaga inicial, throttling, buffer, parada, umbral, Youtube, Algoritmo, ancho de banda, velocidad de reproducción.**

I. Introducción

El presente proyecto es un trabajo de estudio e investigación sobre la implementación de un reproductor de vídeo Streaming inteligente mediante distintos algoritmos.

En este proyecto profundizaremos especialmente en las estrategias a seguir en distintas condiciones de tráfico en la red que disponemos así como los mensajes que intercambiarán cliente y servidor, al hacer esto podremos ver qué algoritmos son más adecuados para cada uno de los casos y por tanto hacer la simulación en conjunto de nuestro reproductor inteligente.

Con este estudio se pretende mejorar el funcionamiento de los reproductores de vídeo actuales, buscando una mayor eficiencia y otro punto de vista con respecto a las paradas durante la reproducción e intentar que dicha reproducción sea lo más satisfactoria para el usuario.

A. Antecedentes. Descarga de video streaming.

Descarga, reproducción y congestión para YouTube.(1)

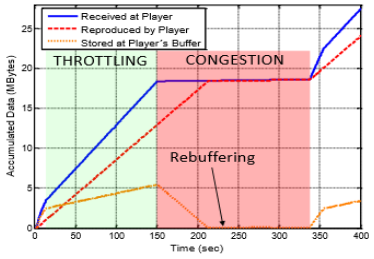
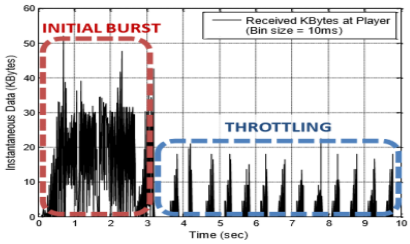


Ilustración de la fase inicial(initial Burst) y la fase de Throttling.(2)

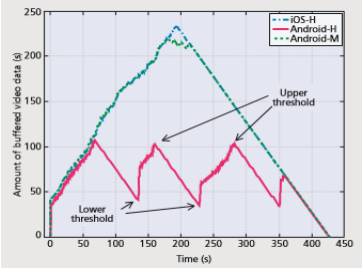


B. Antecedentes. Reproducción de vídeo para Youtube.

Utilización de umbral superior(100-110 segundos) en el buffer de reproducción a partir del cual cerramos conexión.

Utilización de umbral inferior(30-40 segundos) a partir del cual solicitamos nueva conexión.

Android-H usado en dispositivos de alta gama, comportamiento a estudiar.(3)



II. DISEÑO

A. *Estimación del ancho de banda de descarga.*

Utilizamos un Algoritmo para estimar el ancho de banda en cada instante, el resto de algoritmos actuarán cuando detecten un cambio en el valor del ancho de banda:

BW'=(bytesRecibidosAntes-bytesRecibidos)*8/ (tiempoAnterior-tiempoSimulación) (1)

BW=BW'*(1-α)+BW*α, Siendo α=0.99 (2)

B. *Adaptación de umbral superior.*

En nuestro reproductor adaptable buscaremos reducir ese umbral superior para ahorrar memoria cuando sea posible. Por ello descenderemos dicho umbral cuando no haya problemas en la red, y lo aumentaremos al haber problemas, dotando a nuestro reproductor de adaptabilidad en función de las condiciones de la red.

```
if (umbralSuperiorAdaptationMode) {
      if (BW <= (videoSize / videoDuration) * 8 * 1.8
            && BW > (videoSize / videoDuration) * 8 * 1.2)
    {
        umbralSuperior=60;
         }
      else if (BW <= (videoSize / videoDuration) * 8 * 1.2
            && BW > (videoSize / videoDuration) * 8 * 0.6)
    {
        umbralSuperior=70;
      }
       else if (BW <= (videoSize / videoDuration) * 8 * 0.6)
    {
        umbralSuperior=80;
      }
      else if (BW > (videoSize / videoDuration) * 8 * 1.8) {
        umbralSuperior=50;
      }
```

.

C. *Algoritmo de cambio de velocidad. Implementación.*

Nuestro algoritmo será nuevamente adaptable en función de las condiciones de ancho de banda de transmisión:

- Si hay problemas en la red, entonces ralentizaremos el vídeo, disminuyendo los frames/s, para que así de tiempo a que lleguen más datos y el vídeo continúe reproduciéndose sin paradas.
- Si no hay problemas en la red la velocidad de reproducción será la original.
- Es importante notar que tendremos un valor umbral mínimo de calidad que será el 70% de la velocidad de reproducción original, ese será el valor mínimo para la velocidad de reproducción y se ha obtenido mediante tests de opinión como se verá a continuación.

```
if (fpsAdaptationMode) {
    if (BW <= (videoSize / videoDuration) * 8 * 1.8
          && BW > (videoSize / videoDuration) * 8 * 0.6) {
  fps=fpsVideo*BW/(double)((videoSize / videoDuration)
    * 8);
    }
    else if (BW <= (videoSize / videoDuration) * 8 * 0.6) {
      fps = fpsVideo * 0.7;
    }
    else if (BW > (videoSize / videoDuration) * 8 * 1.8) {
      fps = fpsVideo;
    }
    if(fps>fpsVideo){
      fps=fpsVideo;
    }
     if(fps<fpsVideo*0.7){
      fps=fpsVideo*0.7;
    }
  }
```

D. *Algoritmo de cambio de velocidad. Estudio de calidad.*

Vamos a realizar experimentos sobre usuarios para hallar el valor umbral en la velocidad de reproducción a partir del cual la satisfacción del usuario decae hasta valores insostenibles, lo haremos estudiando la calidad del vídeo para cada velocidad de reproducción.

Realizaremos el experimento con dos tipos de vídeo, uno con mayor expectativa de movimiento que otro y nuestras hipótesis serán:

- **Vídeo 1 con mayor expectativa de movimiento:** Su tolerancia a la ralentización será menor que en el vídeo siguiente.
- **Vídeo 2 con menor expectativa de movimiento:** Su tolerancia a la ralentización será mayor que en el primer vídeo.

El experimento se ha realizado siguiendo como modelo la recomendación ITU-T.910.

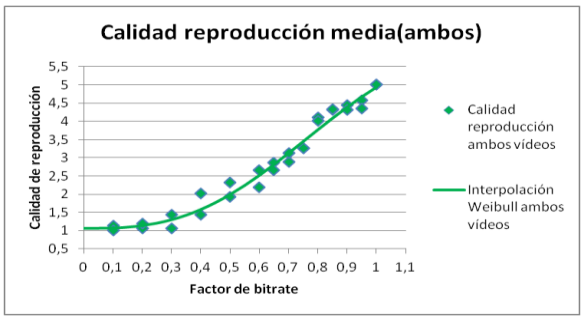
Calidad del vídeo según ITU-T.910:

- **Excelente=5.**
- **Buena=4.**
- **Regular=3.**
- **Mediocre=2.**
- **Mala=1.**

No se han notado diferencias significativas en los resultados dependiendo del tipo de vídeo.

Los resultados son los siguientes:

Calidad en la reproducción, media de todos los usuarios para ambos vídeos.(4)

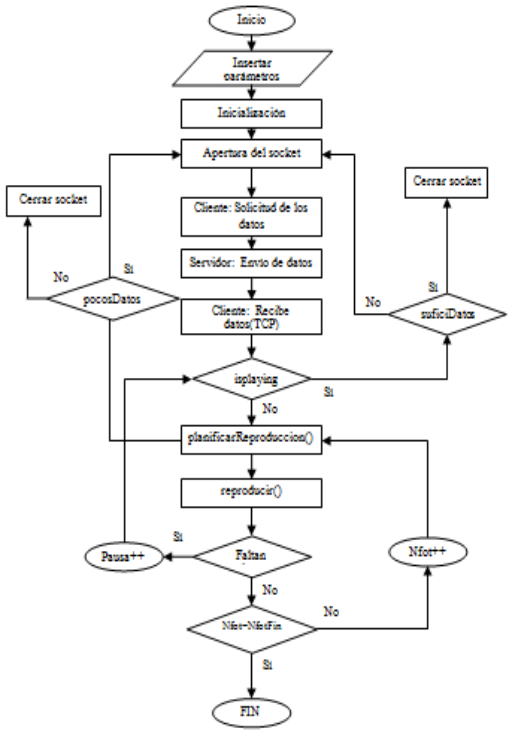


Podemos concluir a partir de la anterior gráfica que consiste en la calidad para ambos vídeos que **si la velocidad de reproducción es mayor o igual al 70% de la velocidad original, la calidad es aceptable para el usuario**, si la velocidad de reproducción es menor entonces no.

III. IMPLEMENTACIÓN

Queremos diseñar un reproductor de vídeo inteligente, para ello definiremos los parámetros necesarios y mostramos explicaremos el funcionamiento general del programa mediante un diagrama de flujo así como los métodos más significativos que implementa nuestros algoritmos inteligentes.

A. Diagrama de flujo de reproductor.



B. planificarReproduccion().

Este método es muy importante, ya que cumplirá tres funciones principalmente:

- Calcular el ancho de banda en cada instante:

```
float alfa = 0.99;  //valor óptimo para evitar fluctuaciones excesivas en el ancho de banda[0,1]
    float Bwprima;
    BWprima = (bytesRcvdAnt - bytesRcvd)*8 / (tiempoAnt - simTime());
  BW = BWprima * (1 - alfa) + BW * alfa;
    bytesRcvdAnt = bytesRcvd;
    tiempoAnt = simTime();
```

- Implementar o no las mejoras introducidas por nuestro reproductor comprobando estas condiciones:

```
    if (umbralSuperiorAdaptationMode)
    if (fpsAdaptationMode)
```

- Llamar al método reproducir() para simular la reproducción del vídeo.

```
    timeoutPlayer = new cMessage("timer1");
    timeoutPlayer->setKind(PLAYERUPDATE);
    scheduleAt(simTime() + delay, timeoutPlayer);
```

C. reproducir().

```
void ClienteYoutube::reproducir() {//método importante que simula nuestro reproductor
  isplaying = true;//estamos en reproducción
      if (segundosRcvd > Nfot / (double) fpsVideo) {
buffer = bytesRcvd - (Nfot*bytesPerFrame); //recalculamos el buffer
segundosBuffer = buffer / (videoSize / videoDuration);//pasamos a segundos los bytes del buffer
bytesPerFrame=(videoSize/(videoDuration*fpsVideo));//bytes que hay en cada frame
videoReproducido = (Nfot*bytesPerFrame)/(videoSize /videoDuration);//video reproducido en segundos
  Nfot = Nfot + 1;//importante pasar al siguiente fotograma una vez terminada la reproducción del fotograma actual
```

Calculamos por primera vez **bytesPerFrame** y lo utilizamos para calcular el buffer, que se irá actualizando al ir cambiando los bytes Recibidos e incrementándose el número de fotograma.

También calculamos el vídeo reproducido y al final una vez reproducido el fotograma actual incrementamos **Nfot**.

```
else {// no tenemos datos suficientes para reproducir, entonces hay una pausa
    isplaying = false;
```

```
    numeroPausas=numeroPausas + 1;
    numeroPausasVector.record(numeroPausas);
}
```

IV. EVALUACIÓN

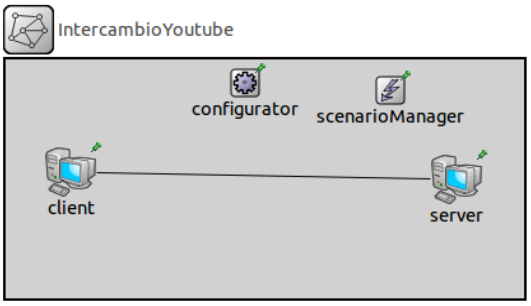
Exponemos los resultados obtenidos tras la simuación del programa implementado en el capítulo anterior, además se describirán los escenarios para los cuales hemos obtenido dichos resultados.

Por último realizaremos un análisis profundo sobre las mejoras aportadas por nuestro reproductor así como analizarlo comparativamente con el reproductor de Youtube.

A. Topología de la red.

Mostramos la topología de la red implementada. Conexión cliente-servidor y el escenario Manager añadido:

Topología de la red.(5)



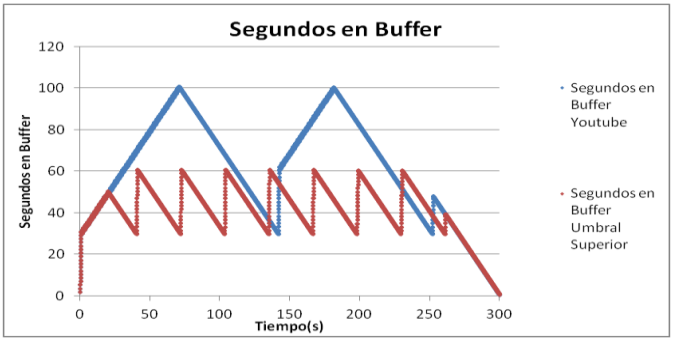
B. Escenario 1 de simulación: umbral superior adaptable.

El escenario 1 de simulación será un escenario sin problemas en la red en cuanto a ancho de banda de transmisión.

Comparativa entre YouTube y nuestro reproductor adaptable una vez activada la mejora en adaptabilidad para el umbral superior.

Ahorro considerable en memoria sin perjuicio en la calidad de reproducción del vídeo a estudiar(300 segundos de duración).

Segundos en buffer en escenario 1 para Youtube y para reproductor adaptable.(6)



Una vez realizado el cálculo de la ocupación media en buffer obtenemos los siguientes resultados:

- **Ocupación media en Buffer para Youtube: 60,427 segundos.**
- **Ocupación media en Buffer para nuestro reproductor: 41,116 segundos.**

Nuestro reproductor para el escenario 1:

- Dota de mayor flexibilidad a la reproducción pudiendo adaptar en cada momento el umbral superior y por tanto la memoria máxima necesaria.
- Produce un ahorro en memoria considerable, reduciendo la ocupación media en buffer considerablemente.
- No produce problemas en cuanto a paradas durante la reproducción del vídeo.

C. Escenario 2 de simulación: velocidad de reproducción adaptable.

El escenario 2 de simulación será un escenario con problemas en la red en cuanto a ancho de banda de transmisión, se simulará una caída en el ancho de banda durante la simulación para ver si nuestro reproductor adaptable es mejor que YouTube en estas condiciones.

Comparativa entre YouTube y nuestro reproductor adaptable una vez activada la mejora en adaptabilidad para la velocidad de reproducción.

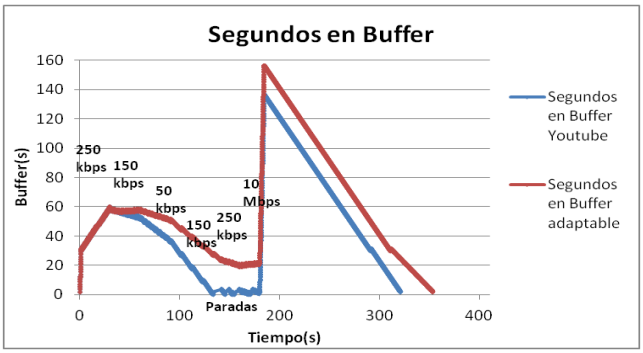
Nuestro objetivo es mejorar la calidad de la reproducción evitando las paradas que tendrá el reproductor de Youtube.

Segundo escenario: hay problemas en la red durante un intervalo grande de tiempo.

- Descenso del ancho de banda hasta alcanzar los **250kbps** en el segundo **30** de la simulación.
- Descenso del ancho de banda hasta alcanzar los **150kbps** en el segundo **60** de la simulación.
- Descenso del ancho de banda hasta alcanzar los **50kbps** en el segundo **90** de la simulación.
- Ascenso del ancho de banda hasta alcanzar los **150kbps** en el segundo **140** de la simulación.
- Ascenso del ancho de banda hasta alcanzar los **250kbps** en el segundo **160** de la simulación.
- Ascenso del ancho de banda hasta alcanzar los **10Mbps** en el segundo **180** de la simulación.

A continuación mostramos el estado del buffer de reproducción para YouTube y para nuestro reproductor adaptable una vez implementada la mejora de ralentización. Se produce agotamiento del buffer para YouTube, para nuestro reproductor no.

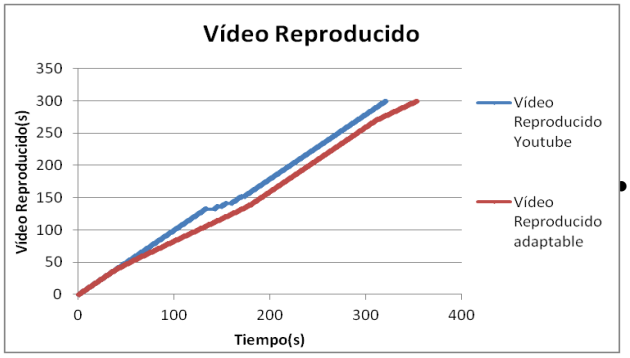
Segundos en buffer en escenario 2 para Youtube y para reproductor adaptable.(7)



- **Número de paradas para YouTube: 4**
- **Número de paradas para reproductor con velocidad adaptable: 0**

Por tanto se muestra que para YouTube el vídeo reproducido tiene paradas durante su reproducción y para nuestro reproductor no se producen estas paradas ya que se adecúa la velocidad de reproducción para evitar el agotamiento del buffer de reproducción.

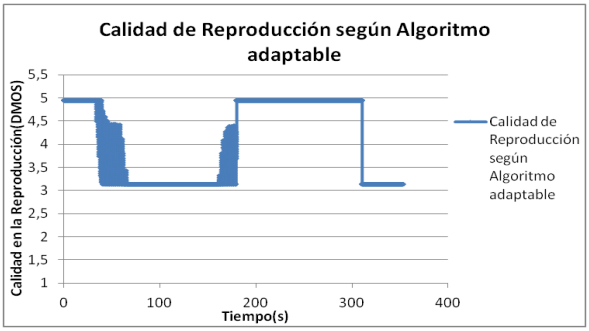
Vídeo reproducido en escenario 2 para Youtube y para reproductor adaptable.(8)



Además vemos como se ralentiza nuestra reproducción cuando empieza a detectar problemas en la transmisión, y gracias a ello evita las paradas.

Si interpolamos los valores de los frames/s obtendremos esta gráfica en cuanto a la calidad de la reproducción:

Calidad de reproducción en escenario 2 para reproductor adaptable.(9)



- Hemos calculado también la calidad media, realizando un promedio y el resultado es de: **4,185.**

Nuestro reproductor para el escenario 2:

- Dota al reproductor de mayor flexibilidad y adaptabilidad según las condiciones de tráfico en la red.
- Reduce el número de paradas, llegando en este caso a evitarlas totalmente mientras YouTube tiene 4 paradas.
- Establece un umbral mínimo del 70% en cuanto a velocidad de reproducción original para asegurarnos una calidad de reproducción aceptable por el usuario.

V. CONCLUSIONES

Se ha propuesto un reproductor alternativo a YouTube implementando mejoras desde el punto de vista de la memoria y la eficiencia en la reproducción de vídeos.

- Hemos diseñado e implementado un reproductor adaptable, flexible y más eficiente que Youtube en términos de memoria, llegando a tener una **ocupación media el buffer de reproducción 40% menor.**
- Hemos implementado un algoritmo que ralentizará la velocidad de reproducción hasta el 70% de la velocidad de reproducción original según las condiciones de tráfico en la red. **Permitiendo un menor agotamiento del buffer de reproducción y reduciendo considerablemente el número de paradas** sin gran perjuicio en la calidad de visualización percibida por el usuario.

Durante el experimento obtuvimos que la mínima velocidad de reproducción necesaria para que el usuario siga con un grado aceptable de satisfacción es el 70% de la velocidad de reproducción original.

- Durante el experimento llegamos a la conclusión que el tipo de vídeo no tiene una influencia significativa en la escala de satisfacción del usuario.

.

A. Trabajo futuro.

Las investigaciones relacionadas con este proyecto pueden seguir realizándose en temas en los que aún no se ha profundizado.

- Seguir buscando mejoras en la reproducción, buscando mayor adaptabilidad en el umbral inferior del buffer de reproducción y otros parámetros.
- Sintonización de los parámetros de adaptación propuestos en nuestro reproductor
- Implementación real del reproductor adaptable.
- Evaluación de la satisfacción de los usuarios en la implementación física del reproductor adaptable con un estudio amplio para varios vídeos, escenarios y diferentes condiciones de adaptabilidad.

AGRADECIMIENTOS

A mi madre Nicol. A mi padre Pepe.

A mi hermano Pepe.

A mis abuelos, Pepe y Dolores.

A mi familia, por estar conmigo cada día, a mis tíos, a mis primos a cada una de las personas que me han ayudado estos años.

A Juanjo por haberme ayudado todos estos meses, por su amabilidad.

A mis amigos, por cada uno de los buenos momentos que me han hecho pasar en estos años de carrera.

.

REFERENCIAS

[1] YouTube, http://www.youtube.com

[2] Rao, A., Lim, Y-s., Barakat, C., Legout, A., Towsley, D., and Dabbous, W.
"Network Characteristics of Video Streaming Traffic" en Proc. ACM, CoNext 2011, Tokyo, Japan, December 2011, p. 25.

[3] Héctor Arturo Aguilera García. "Modelado de tráfico de Youtube Móvil" en ETSIIT, UGR 2013, Granada, España, Septiembre 2013.

[4] Metzger, F., Rafetseder, A., Stezenbach, D. and Tutschku, K.
"Analysis of Web-based Video Delivery" en FITCE Congress (FITCE), 2011 50th, p. 1-6.

[5] Thomas Stockhammer "MPEG's Dynamic Adaptive Streaming over HTTP (DASH) – Enabling Formats for Video Streaming over the Open Internet", 2011.

[6] Global internet phenomena report. Technical report, Sandvine, 2011.

[7] Pablo Ameigeiras, Juan J. Ramos Muñoz, Jorge Navarro Ortiz and Juan M. López Soler. "Analysis and modelling of YouTube traffic" en Transactions on Emerging Telecommunications Technologies, John Wiley & Sons, June 2012. Volume 23, Issue 4, p. 360–377.

[8] Metzger, F., Rafetseder, A., and Tutschku, K. (2012). "A Performance Evaluation Framework for Video Streaming" en Packet Video Workshop (PV), 2012 19th International, p.19.24.

[9] Finamore, A., Mellia, M., Munafò, Torres, R., and Rao, S.G. (2011). "YouTube Everywhere: Impact of Device and Infrastructure Synergies on User Experience" en ECE Technical Reports. Paper 418.

[10] Omnet++, http://www.omnetpp.org/

[11] Deschamps Espinosa, Melissa Elena (2007). Modelado de Mecanismos de Transición a IPv6.
http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/deschamps_e_me/capitulo4.pdf

[12] INET, http://inet.omnetpp.org/

[13] "Subjective video quality assessment methods for multimedia applications".
https://www.itu.int/rec/T-REC-P.910-200804-I/en

[14] Herramienta para interpolación, http://zunzun.com/

[15] Vídeos objeto de estudio.
· A. K. Moorthy, L. K. Choi, A. C. Bovik and G. deVeciana, "Video Quality Assessment on Mobile Devices: Subjective, Behavioral and Objective Studies", IEEE Journal of Selected Topics in Signal Processing, to appear in October 2012.
· A. K. Moorthy, L. K. Choi, G. deVeciana, and A. C. Bovik, "Mobile Video Quality Assessment Database," IEEE ICC Workshop on Realizing Advanced Video Optimized Wireless Networks, Ottawa, Canada, June 10-15, 2012.
· A. K. Moorthy, L. K. Choi, G. deVeciana, and A. C. Bovik, "Subjective Analysis of Video Quality on Mobile Devices," Sixth International Workshop on Video Processing and Quality Metrics for Consumer Electronics (VPQM) (invited article), Scottsdale, Arizona, January 15-16, 2012.

BeeQuizz. Una plataforma en línea para el apoyo a la docencia basado en juegos

Tutor: Juan José Ramos Muñoz; e-mail:jjramos@ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

Autor: Cristina Garrido López, e-mail: cris.garlopez@gmail.com

BeeQuizz es una plataforma para mantener, usar y desarrollar juegos docentes que permitan la mejor asimilación y refuerzo de los contenidos de distintas materias. El sistema ofrece al administrador y a los profesores una interfaz para gestionar bases de datos de preguntas categorizadas por temas y dificultades, que son luego integradas en distintos juegos. Estos juegos pueden ser individuales y multijugador. Los estudiantes pueden acceder a la plataforma desde cualquier dispositivo que disponga de un navegador que soporte HTML5 y conexión a Internet, por lo que se facilita su uso desde cualquier ubicación. Se diseñó una API basada en servicios web que permiten que cualquiera pueda desarrollar sus propios juegos, con acceso a las funcionalidades de la plataforma. Se implementó un juego multijugador y otro de un solo participante para demostrar la funcionalidad del sistema y el uso de las API de BeeQuizz

***Palabras clave*—AJAX, Aplicación, Docencia, HTML5, JQuery, JSON, Juegos, Móvil, Multiplataforma, MVC, Plataforma, Web.**

I. INTRODUCCIÓN

DESDE las últimas décadas del siglo XX estamos viviendo lo que podríamos llamar "Revolución Digital", aunque es a principios del siglo XXI cuando esto se acentúa y cuando podemos hablar de la era de los dispositivos inteligentes. Esto se traduce en la existencia de usuarios conectados las 24 horas del día a la red sin necesidad de estar delante del ordenador, gracias a los *Smartphone y las tablets*. Según un informe realizado por el analista Gartner las ventas de *tablets* crecieron un 69.8% en 2013, mientras que la de ordenadores bajaron un 7.6% respecto al año anterior. [1]

Dado que las instituciones educativas no pueden permanecer al margen de esta evolución se apoyan en ella para ampliar y complementar las actividades realizadas en las aulas, además de usarla igualmente para que el alumno adquiera las habilidades necesarias para sobrevivir en la sociedad actual. Según el informe Horizon 2013 de enseñanza universitaria [2], los juegos y la gamificación son tecnologías que tendrán una gran repercusión en la enseñanza y el aprendizaje universitario en los próximos dos o tres años.

Tras conocer los datos anteriores, se pensó hacer un proyecto que entrelazará el mundo de las TIC (*Tecnologías de la Información y la Comunicación*) y de la educación de una forma lúdica y entretenida, aprovechando todos los aspectos positivos que presentan los juegos en la enseñanza. Además, usando algunas de las tecnologías más demandadas y novedosas de hoy en día, como puede ser el caso de HTML5 y las herramientas asociadas a ella para el desarrollo en aplicaciones móviles.

Los objetivos para este proyecto eran:

- Desarrollar una plataforma Web para la gestión y uso de juegos como herramienta de aprendizaje, que fuese multijugador y multiplataforma: *BeeQuizz.*
- Crear un juego de prueba tanto para un jugador como para varios.
- Disponer de una API (*Application Programming Interface*) para que cualquiera pudiera crear nuevos juegos.

II. ESTADO DEL ARTE

Tal y como se ha comentado anteriormente, el aprendizaje basado en juegos es y será una de las tecnologías más influentes a corto plazo. Desde que en 2003 James Gee [3] describió por primera vez el impacto de los juegos en la enseñanza, este campo ha ido avanzando a pasos agigantados.

Hoy en día el aprendizaje basado en juegos refleja las aptitudes que las instituciones quieren inculcar a sus alumnos, como puede ser la capacidad de resolución de problemas, la comunicación, los conocimientos digitales o la colaboración entre otros.

A. Soluciones existentes

Durante el periodo de investigación sobre el estudio de mercado, se buscaron las diferentes plataformas existentes para el apoyo a la docencia basadas en juegos, identificándose numerosos juegos adaptados al aprendizaje. Sin embargo, no se hallaron tantas plataformas que soportaran el desarrollo y gestión de varios de este tipo de juegos. Los dos ejemplos más representativos de este tipo de plataformas son:

1) Unigenios

Proyecto elaborado por la universidad de Oviedo con otras entidades [4]. Tiene como objetivo acercar la ciencia a los jóvenes de una manera didáctica y entretenida a través del uso de juegos de mesa adaptados a un formato digital.

2) MOODLE [5] (Modular Object-Oriented Dynamic Learning Enviromen)

Entorno de Aprendizaje Virtual que ofrece la creación y gestión de plataformas educativas que van a permitir la comunicación entre el alumno y el profesorado.

Al realizar el estudio de las diferentes aplicaciones comercializadas que responden a las necesidades de este proyecto, se llegó a la conclusión que existían varias carencias que *BeeQuizz* podría subsanar como es la adaptación de la plataforma al entorno móvil y el acceso a la plataforma a cualquier tipo de usuario independientemente de si es alumno de la universidad o no.

B. Tecnologías relacionadas.

A continuación se citan las diferentes tecnologías utilizadas en la realización de *BeeQuizz* y el porqué de su elección.

- HTML5 (**H**yper**T**ext ***M**arkup **L**anguage, versión 5*) [6]: Nuevo estándar propuesto por la W3C (***W**orld**W**ide**W**eb**C**onsortium*) para el desarrollo de documentos basados en etiquetas. Se eligió porque hace posible que las páginas sean compatibles con todos los navegadores incluyendo los de los teléfonos móviles y otros dispositivos, usados para navegar por Internet. Hace que la aplicación sea totalmente multiplataforma.

- *jQuery* [7]: Librería de funciones *JavaScript.* Aporta una compatibilidad robusta entre los navegadores, así como numerosas funcionalidades que permitirán que el recorrido a través de los documentos HTML, el manejo de eventos y las interacciones con AJAX. Fue usado en este proyecto porque es soportado por multitud de navegadores incluidos los navegadores en móviles y *tablets,* y el tiempo de respuesta en los mismos ha mejorado.

- jQuery UI: Librería usada por *jQuery* que presenta una gran variedad de efectos visuales, *widgets* y *plugins.* [8]

- AJAX (*Asynchronous JavaScript + XML*) [9][10]: Conjunto de tecnologías asíncronas que permiten el intercambio de datos con el servidor y la modificación de las páginas web sin necesidad de actualizarlas en su totalidad. Se decidió usarla porque permite una interacción fluida con los clientes, porque da la posibilidad de tratar la información sin que el usuario tenga que esperar el resultado de estos tratamientos para continuar la navegación por la aplicación y porque es válido en cualquier plataforma y navegador.

- JSON (*JavaScript Object Notation*)[11]: Formato de texto, en el que se utiliza la sintaxis Java Script para la descripción de objetos de datos. Estos objetos son utilizados para el almacenamiento y el intercambio de información. Es mucho más pequeño, más rápido y sencillo de analizar que XML. JSON permite la integración sencilla con HTML5 y *jQuery* además de con otras muchas herramientas, por lo que se decidió usarlo. Además, de porque permite intercambiar la información mediante llamadas asíncronas con un formato ligero.

- *Jackson*: Librería de Java que permite serializar y deserializar de una manera sencilla objetos JSON. [12]

- Java [13] [14]: Es un lenguaje de programación orientado a objetos, independiente de la plataforma, que permite el desarrollo de aplicaciones.

- Java Mail: Librería de Java que permite el envío y recepción de correos electrónicos directamente desde la aplicación Java.

- *Spring Framework* [15]: Plataforma Java gratuita que proporciona una infraestructura que actúa de base de las aplicaciones Java a desarrollar.

- *Spring Security* [16]: Framework JAVA que proporciona servicios de seguridad completos (sobre todo autenticación y autorización) para poder gestionar las aplicaciones, que han sido creadas usando el Framework *Spring*.

- *Maven* [17], [18]: Herramienta de software libre para la gestión del ciclo de vida de un proyecto,

- *Apache Tomcat 7*: Contenedor web con soporte de *Servlets* y JSPs (*JavaServer Pages*). En *BeeQuizz* se ha usado de manera totalmente autónoma y será el encargado de contener los *Servlet* de la parte del servidor.

- *PostgreSQL*: sistema de gestión de bases de datos objeto – relacional, de código abierto, de gran potencia y robusto. Se utilizó en *BeeQuizz* gracias a su soporte de distintos tipos de datos y a la herencia entre tablas entre otros.

- *Twitter Bootstrap*: Framework de *Twitter* que permite crear interfaces web con CSS y JavaScript. Adapta la interfaz dependiendo del tamaño del dispositivo sin que el usuario tenga que hacer nada, gracias al diseño adaptativo (*Responsive Design*) que implementa [19]. Fue usado, por su capacidad de adaptarse a cualquier terminal dinámicamente y por su capacidad multiplataforma.

III. TEMPORIZACIÓN Y COSTES

El trabajo realizado a lo largo del proyecto se dividió en una

serie de paquetes de trabajo que a su vez se descompusieron en varias actividades. Haciendo uso de un diagrama de Gantt se hizo una estimación del tiempo a consumir en cada una de estas actividades. La estimación completa del proyecto fue 5 meses.

Las personas que trabajaron en la realización de *BeeQuizz* fueron:

- D. Juan José Ramos Muñoz, profesor del departamento de Teoría de la Señal, Telemática y Comunicaciones de la universidad de Granada como tutor del proyecto.
- Cristina Garrido López, alumna de la Escuela Técnica Superior de Ingenierías Informática y Telecomunicaciones de la universidad de Granada como autora del proyecto.

El coste de los recursos humanos de este proyecto se elevó a 239 días (jornadas de 8 horas) y el coste material es de 10025€.

IV. Diseño de la plataforma

La plataforma *BeeQuizz* es una herramienta que por un lado permite a los usuarios agregar preguntas y respuestas, jugar a los juegos ya existentes y desarrollar otros mediante el uso de API que proporciona *BeeQuizz*. Por otro lado, permite a los administradores realizar actividades extra como la validación, modificación y supresión de las preguntas y respuestas introducidas por los usuarios. Además de la inserción de nuevos juegos.

A. Diseño General

El diseño de la aplicación es de tipo cliente-servidor. El cliente accede a la aplicación, la cual se encuentra alojada en un servidor, a través de la dirección *http://beequizz.es*. En la figura 1 se muestra el esquema del diseño del sistema, cuyos componentes se detallan brevemente a continuación.

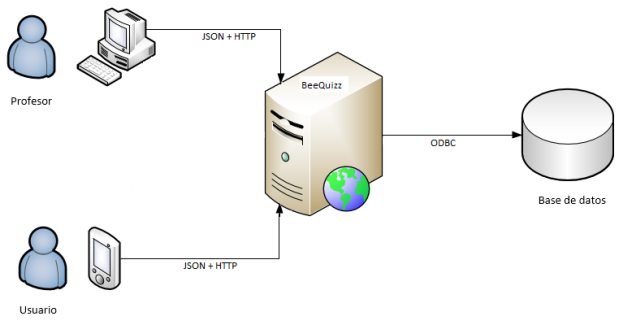


Fig. 1. Diseño general de la aplicación.

1) Dispositivo de usuario

El usuario debe disponer de un dispositivo móvil con conectividad a la red para poder acceder a la aplicación y las características que se le ofrece. También se puede acceder a la aplicación mediante un ordenador de sobremesa o un portátil, con la condición de que tengan acceso a la red.

2) Servidor de alojamiento de la aplicación

Es una pieza clave para la aplicación, ya que aquí se alojan todos los datos de la misma y hace posible su ejecución. Para esto, el equipo consta de la instalación de un software de servidor web, capaz de servir las páginas web y poder atender las solicitudes y respuestas de los usuarios mediante HTTP. También se ha necesitado una base de datos donde almacenar los datos que maneja la aplicación.

3) Base de datos

La información de BeeQuizz se almacenará en una base de datos PostgreSQL alojada en el propio servidor. La plataforma tiene como base tres grandes grupos que son el usuario, la plataforma en sí y las preguntas.

B. Diseño de la arquitectura BeeQuizz

El diseño de BeeQuizz está basado en una arquitectura MVCDAO (*Model View Controller Data Access Object*) o arquitectura de 4 niveles.

Se ha elegido esta arquitectura ya que es bastante clara en cuanto a la estructura, por lo que en caso de modificación o de conflicto en algunas de las capas no hay porqué tocar la estructura y al contenido de las demás capas. La claridad y la organización de la que se habla no hubiesen sido posibles sin la ayuda de Maven y sin las anotaciones de Spring. A continuación se describen cada una de las capas de este patrón de diseño.

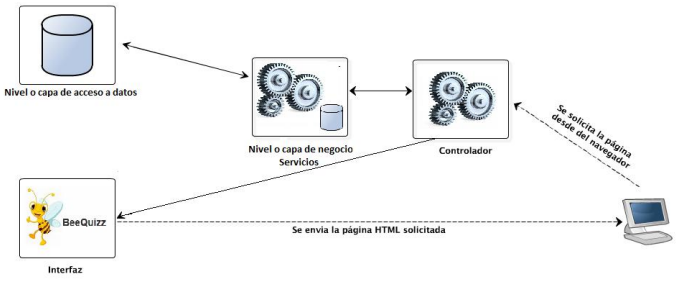


Fig. 2. Esquema de la arquitectura implementada en *BeeQuizz*

1) Capa de acceso a los datos o DAO

Esta es la capa que está en comunicación directa con la base de datos y con la capa negocio. Se encarga de recuperar, registrar o actualizar la información de la base de datos bajo demanda de la capa superior, haciendo uso de las peticiones y demandas SQL, de forma que el tipo de acceso sea transparente al resto de capas.

2) Capa de negocio

En la capa de negocio se encuentra la inteligencia de la aplicación. Es aquí donde se gestiona la lógica de *Beequizz* y se realizan los tratamientos necesarios sobre los objetos recuperados de la base de datos. Esta comunicada con el controlador que es de donde recibe las solicitudes y donde presenta resultados y beequizz.dao a los que solicita o da los datos necesarios para satisfacer la demanda del controlador.

3) Controlador

Se encarga de gestionar el flujo de la aplicación Gracias al envío de datos a través de `HTTP` y a la recepción de peticiones se comunica con el usuario. El controlador va a pasar esta información al servicio que hará las operaciones necesarias y devolverá una información al controlador que será igualmente el encargado de mostrar esta información al usuario.

4) Interfaz

Permite al usuario interactuar con el sistema.

C. Juegos

Uno de los objetivos principales de la plataforma era poder gestionar y usar de forma didáctica. Por lo tanto, se han diseñado dos juegos (uno mono-jugador y otro multi-jugador) que podrían como método de evaluación de los alumnos.

1) Simple Quizz (Juego mono-jugador)

La idea principal era poder utilizar las preguntas que están almacenadas en la plataforma como base de los juegos. Para ello se pensó en realizar un juego del estilo de 50x15, al que se llamará *Simple Quizz* y cuyo diagrama se observa en la figura 3.

Fig. 3. Diagrama de flujo de *Simple Quizz*

El objetivo de este juego es conseguir el mayor número de puntos posibles, contestando a un número determinado de preguntas. Estas preguntas corresponden a un tema y nivel de dificultad elegido por el jugador. Cada una de las preguntas tiene asociadas 4 respuestas, de las cuales tan solo una es correcta. Al acabar la ronda la puntuación obtenida se almacena en la plataforma y sirve al profesor para evaluar los conocimientos sobre el tema elegido.

2) Simple trivial (Modo multi-jugador)

Simple Trivial es un juego que sigue la línea del Simple Quizz pero que difiere con él en algunos detalles. Su diagrama de flujo se puede observar en la figura 4. El más importante de ellos es que este juego es multijugador.

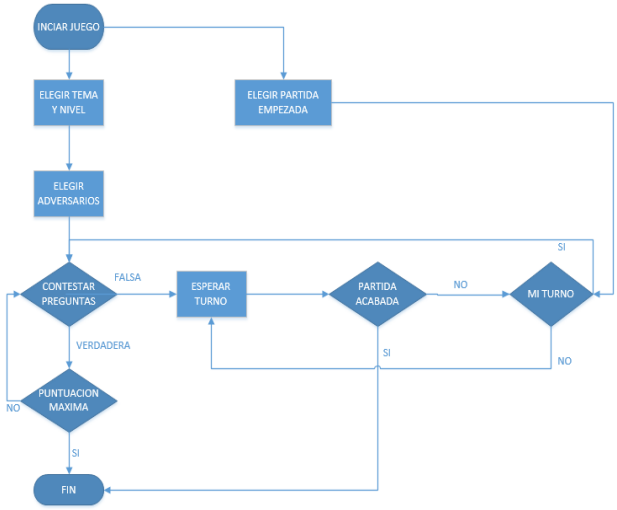


Fig. 4. Diagrama de flujo de *Simple Trivial*

Al igual que *Simple Quizz*, Simple trivial se basa en las preguntas ya almacenadas en la base de datos para su desarrollo. El usuario debe elegir un tema y un nivel de dificultad. A continuación, el usuario debe seleccionar a sus adversarios. La plataforma notifica a dichos adversarios mediante un correo electrónico que alguien quiere jugar contra ellos.

El jugador empieza la partida, una vez que haya elegido a sus adversarios. Al contestar una pregunta de manera incorrecta, el usuario que está jugando cede el turno al siguiente jugador. A diferencia de *Simple Quizz*, este juego no puede ser usado para la evaluación de los alumnos ya que el objetivo es llegar a 100 puntos.

V. Implementación de BeeQuizz

A. Registro, identificación y pagina principal.

Para acceder a la plataforma es necesario estar registrado, por lo que la página de acceso tiene además de la zona de identificación un espacio dedicado al registro de un nuevo usuario (Figura 5). Gracias a *Spring Security* todo usuario que quiera acceder a cualquier página de la plataforma sin estar identificado es enviado a la página de identificación. Una vez que el usuario ha sido registrado e identificado se accede a la página principal de *BeeQuizz* donde se pueden encontrar las distintas categorías que hay en la aplicación: Gestión de preguntas y Respuestas, Administración, Juegos, Estadísticas y Mi perfil.

Fig. 5. Página de registro e identificación de *BeeQuizz*

B. *Gestión de preguntas y respuestas*

En esta sección el usuario va a poder introducir las preguntas y respuestas a la plataforma. Las preguntas están asociadas a un tema y a una dificultad. Para poder introducir respuestas en la base de datos, hay que elegir primero la pregunta para la que se desea introducir la respuesta y a continuación introducir el numero de respuestas deseadas para dicha pregunta.

C. *Administración de la plataforma*

Esta sección es solamente accesible para los usuarios cuyo rol sea Administrador. Además solo estará disponible cuando se esté conectado con un ordenador. Consta de cuatro bloques bien diferenciados que son: validar o modificar preguntas, validar o modificar respuestas, suprimir preguntas o respuestas e incluir juegos.

D. *Mi perfil*

En esta sección el usuario podrá modificar si lo desea, todos los datos relacionados con su perfil.

E. *Estadísticas*

El usuario puede consultar para cada uno de los juegos existentes en la plataforma la clasificación general, así como las partidas ganadas por él.

F. *Juegos*

1) *Simple Quizz*

Este juego está pensado exclusivamente para un jugador. Consiste en contestar de forma correcta el mayor número de preguntas. El número de preguntas lo elige el usuario al principio del juego. También se elegirá el tema o la asignatura y el nivel al principio del juego. Las diferentes etapas que se han seguido en la implementación del juego son las siguientes:

- Se elige el nivel, el tema, la dificultad y el número de preguntas.
- Se crea la partida.
- Se recupera la lista de preguntas que van a ser usadas de manera aleatoria.
- Se carga la página que contiene los check-box.
- Se recupera el contenido de las preguntas como de las respuestas asociadas a ellas.
- Se validan las respuestas.
- Si no hay más preguntas se muestra la puntuación.
- Se termina la partida.

Simple trivial

un juego de prueba multijugador. Consiste en llegar a eguir 100 puntos antes que los adversarios. Desde la ıa principal de este juego se puede empezar una nueva la o acceder a una ya empezada. A continuación se van a lar las diferentes etapas en las que se divide el juego.

- Se elige el nivel, el tema, la dificultad y el número de preguntas.
- Creación de la partida (asociada al jugador que empieza la partida)
- Creación de la lista con todos los usuarios registrados en la plataforma.
- Envío de notificaciones.
- Creación de la partida (asociada a los contrincantes)
- Antes de empezar a jugar se comprueba si es el turno del usuario que va a jugar.
- Después de haber hecho las comprobaciones, de haber verificado que era nuestro turno y que la partida no está acabada se empieza el juego.
- Se recupera la lista de preguntas que van a ser usadas de manera aleatoria.
- Se recupera el contenido tanto de las preguntas como de las respuestas asociadas a ellas.
- Validación de las respuestas.
- Asignación del turno.
- Se verifica si la partida está terminada.
- Se muestran los puntos.

G. *API*

Como se ha indicado anteriormente uno de los objetivos principales de la plataforma era poder usarla como plataforma de juegos. Para esto se implementaron una serie de métodos que van a permitir a cualquier persona que desee desarrollar nuevos juegos poder utilizarlos. Algunos ejemplos son:

- Recuperar la lista de preguntas
- Recuperar el contenido tanto de las preguntas como de las respuestas.
- Guardar la respuesta a una pregunta.
- Recuperar la puntuación global.

VI. Conclusiones y líneas futuras.

A. *Conclusiones y resultados*

Se ha conseguido desarrollar una plataforma, que sigue una sólida arquitectura software, un protocolo extensible y bien definido para la comunicación, y una API que permite

extender el sistema, que facilita el uso de juegos para aprender o reforzar los conocimientos adquiridos. Además de la plataforma, se proporcionan dos juegos de ejemplo, que demuestran el uso de la API diseñada. Todo esto usando en todo momento las tecnologías más demandadas en este momento como es el caso de HTML5, para permitir el desarrollo de interfaces gráficas multiplataforma, y servicios web para permitir el acceso a sus funciones desde cualquier tecnología.

	BeeQuizz	UNIGENIOS	3D GAME	MOODLE
Gratuito	✓	✓	✓	✓
Multiplataforma	✓	✗	✓	✓
Móviles	✓	✗	✓	✓
Juegos multijugador	✓	✗	✗	✗
Libre acceso	✓	✗	✗	✗
Participativo	✓	✗	✗	✓
API	✓	✗	✗	✗

Tabla 1. Comparativa de las funcionalidades

En la tabla 1 se presenta una comparativa de las funcionalidades ofrecidas por las aplicaciones estudiadas en el estado del arte frente a las características que ofrece *BeeQuizz*.

B. *Líneas futuras*

Una de las grandes ventajas que presenta esta plataforma es que es totalmente gratuita y está abierta a todo el mundo. A pesar de todo esto, *BeeQuizz* puede evolucionar todavía un poco más y ganar puestos en su dominio. Para ello se han detectado una serie de servicios o funcionalidades que habría que implementar y que se exponen a continuación.

- Más seguridad: Para evitar los ataques con los que se pueden conseguir información confidencial de la web es necesario configurar el servidor para que obligue a usar el protocolo HTTPS (*Hyper Text Transfer Protocol Secure*).
- Inserción de juegos externos: Agregar la posibilidad de agregar juegos externos, implementados en HTML5
- Inserción de un gran número de preguntas y respuestas mediante la carga por lotes de ficheros XML.
- Implantación y Evaluación. Se podría llevar a cabo la implantación de *BeeQuizz* en algunas de las asignaturas impartidas en la Universidad de Granada.

AGRADECIMIENTOS

Gracias a Juanjo Ramos Muñoz por haberme dado la oportunidad de crear y trabajar en este proyecto, y gracias también al departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada por hacerme participe de este libro.

REFERENCIAS

[1] Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments... (Egham, UK, April 4, 2013)
Disponible: *http://www.gartner.com/newsroom/id/2408515*.
[2] Estudio Horizon año 2013. Disponible:*http://www.nmc.org/pdf/2013-horizon-report-HE.pdf*
[3] Informe eEspaña 2013. Fundación orange. Disponible: *http://fundacionorange.es/fundacionorange/analisis/eespana/e_espana13.html*
[4] UNIGENIOS. http://unigenios.uniovi.es/el-proyecto/
[5] MOODLE. http://docs.moodle.org/all/es/Acerca_de_Moodle
[6] Une réference pour le développeur web. Rodolphe Rimelé. Eyrolles
[7] jQuery, Simplifiez et enrichissez vos développements JavaScript. J. Chaffer et K. Swedberg. PEARSON
[8] jQuery. http://jqueryui.com/demos/
[9] http://www.adaptivepath.com/ideas/ajax-new-approach-web-applications/
[10] Introducción AJAX. *http://librosweb.es/ajax/capitulo_1.html*
[11] JSON. *http://www.w3schools.com/json/*
[12] Utilización JSON. *http://www.json.org/js.html*
[13] Página oficial oracle. *http://www.oracle.com*
[14] Página oficial JAVA. *http://www.java.com/en/download/faq/whatis_java.xml*
[15] Documentación Spring. *http://docs.spring.io/spring/docs/3.1.0.M2/spring-framework-reference/html/overview.html*
[16] Documentación *Spring Security*. *http://docs.spring.io/autorepo/docs/spring-security/3.0.x/reference/introduction.html*
[17] Tutorial Introducción a Maven. Erick Camacho. *http://www.javahispano.org/storage/contenidos/Tutorial_de_Maven_3_Erick_Camacho.pdf*
[18] Tutorial de Maven. *http://docs.codehaus.org/display/MAVENUSER/The+Maven+2+tutorial*
[19] Bootstrap. http://getbootstrap.com/css/

Cristina Garrido López nacida el 8 Octubre de 1987 en Iznalloz (Granada). Cursó los estudios de primaria en el colegio Beato San Juan de Ávila de Iznalloz. Continuó su formación en el instituto Montes Orientales de la misma localidad, donde obtuvo el diploma de Bachillerato en 2005. A continuación, comenzó la carrera de Ingeniería en Telecomunicación en la Universidad de Granada, la cual finalizó en Febrero de 2014.

El curso académico 2009-2010 disfrutó de una beca ERASMUS, por lo que cursó ese año en la escuela de ingenieros ENSEIRB (Burdeos). Entre Febrero y Julio de 2013 realizó unas prácticas ERASMUS en el grupo CAPGEMINI Application Services en Burdeos (Francia). Desde entonces trabaja como ingeniera en CAPGEMINI Application Services en Burdeos.

Diseño de un motor para aventuras gráficas de universo persistente

Autor: Javier Escámez Álvarez e-mail: j.escamez.alvarez@gmail.com
Tutor: Juan José Ramos Muñoz; e-mail: jjramos@ugr.es

Titulación: Grado en Ingeniería en Tecnologías de Telecomunicación

Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*— En este trabajo se ha diseñado, implementado y evaluado un motor de novelas visuales en línea con universo persistente. El motor desarrollado consta de una parte cliente y otra servidora multiplataforma. Para ello, se han diseñado dos esquemas de mantenimiento de la consistencia del estado del juego percibido por los jugadores, el protocolo de comunicación entre cliente y servidor, y un formato de scripting para que otros desarrolladores de juegos puedan definir novelas visuales de este tipo. Además, se ha desarrollado un entorno experimental automatizado para evaluar el rendimiento de las estrategias de mantenimiento de consistencia del estado del juego, y se ha implementado la que ofrece menor latencia.**

El motor ha sido desarrollado en Java con soporte de la librería de videojuegos multiplataforma LibGDX, por lo que puede ser fácilmente portable a móviles y otras plataformas. Además, hasta donde el conocimiento del autor alcanza, no existen en el mercado motores para este tipo de juegos, por lo que este trabajo se puede considerar como una propuesta novedosa.

***Palabras clave*—aventura gráfica, cliente-servidor, java, libgdx, motor, multijugador, novela visual, online, universo persistente, videojuego.**

I. Introducción

En la actualidad, el mercado de los videojuegos ha superado al de cualquier otra forma de ocio, incluyendo el cine, gracias a la interactividad y al gran espectro de clientes potenciales que se expande de forma continua gracias al mercado de las tablets y smartphones, así como de la presencia continua de los ordenadores personales, por lo que se ha considerado una buena vía de trabajo para este TFG.

En las primeras fases de diseño de este trabajo se ha considerado por qué podría ser interesante la propuesta: si bien la narrativa de una aventura gráfica y la interacción del jugador con el entorno es suficiente como para crear un videojuego se busca un elemento diferenciador en el que el mismo entorno sea algo cambiante y persistente, de forma que la experiencia del jugador varíe en función del estado de la entidad que será el servidor.

Para ello, habrá que cumplir con los siguientes objetivos:

- Creación del motor (servidor y cliente)
- Posibilidad de que sea multiplataforma, ya que se quiere cubrir la mayor parte del mercado posible.
- Interfaz clara e intuitiva para facilitar la tarea a los jugadores.
- Sistema sencillo de *scripting* para facilitar a los desarrolladores intermedios
- Que sea ligero en transmisión de datos y de baja latencia.

II. Diseño

Tal y como se diseña nuestro motor, se busca un modelo cliente-servidor con funciones diferenciadas, si bien ambos contarán con una base de datos. En resumidas cuentas, el cliente contará con la interfaz final mientras que el servidor cederá o no los permisos pertinentes para que el cliente avance de una u otra forma por el juego en función de la situación del servidor.

El servidor mantendrá la persistencia del mundo, manteniendo a todos los jugadores en su base de datos así como diversas Flags, que serán las variables de estado. Por su parte, el cliente sólo necesitará conocer lo necesario para ejecutar las acciones pertinentes con el menor intercambio de datos entre ambas entidades posible.

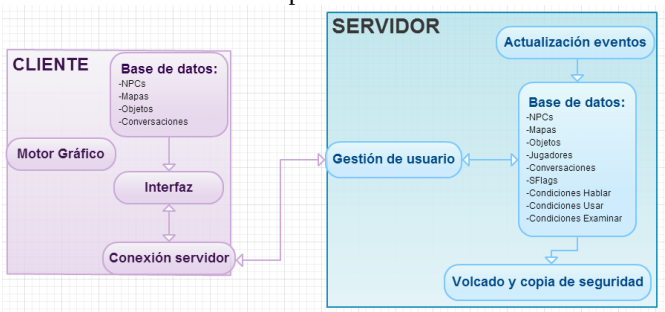


Fig. 1. Diseño básico de la estructura del cliente y el servidor.

Desde un punto de vista general, se considerarán dos grandes bloques en el diseño de nuestro motor: el que toma relación con el cliente y el que hace referencia al servidor. Para ello, se "centralizará" nuestra visión en dos clases básicas: la clase Main (que inicializará MainGDX, la interfaz gráfica de nuestro cliente) y la clase Server, que, como su propio nombre indica, hará las veces de servidor, gestionando mediante hebras las conexiones de los diversos clientes y las actualizaciones de estado de las variables del servidor (como pueden ser la fecha, hora y tiempo atmosférico).

El resto de la infraestructura lógica será compartida, ya que ambos agentes requieren la información de los diversos elementos que participan en el motor.

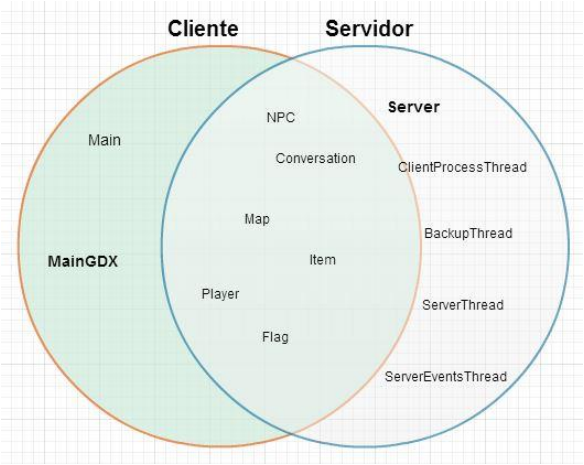


Fig. 2. Diseño básico de clases.

A. *Estructura de clases*

De acuerdo con la Fig. 2, se implementarán las siguientes clases:

- Clases de cliente:
  - o Main: Realiza la inicialización del motor gráfico.
  - o MainGDX: Gestiona todas las peticiones, operaciones de entrada y salida y frontend del usuario, encargándose de todas las interfaces de entrada/salida y motor gráfico.
- Clases de servidor:
  - o Server: Gestiona el servidor, su base de datos y proporciona las herramientas necesarias para operar sobre ella.
  - o ServerThread: Gestiona las conexiones. Abre una hebra ClientProcessThread en cada conexión.
  - o ClientProcessThread: Responde las peticiones de cada uno de los usuarios.
  - o ServerEventsThread: Actualiza de forma periódica las variables del servidor como la fecha, hora y tiempo atmosférico.
  - o BackupThread: Toma una copia de seguridad de la base de datos del servidor. Se trata de una función crítica, ya que en caso de caída del servidor requerimos contar con la última versión de la base de datos para minimizar la pérdida de información
- Clases comunes al cliente y al servidor:
  - o Conversation: Representa cada una de las conversaciones sobre las que se desarrolla el juego en cuestión. El servidor contará con una lista de requisitos para acceder a cada una de las conversaciones.
  - o NPC: Representa a un NPC (Non-Playable Character) que realizará acto de presencia durante una conversación dada. Generalmente tendrá asociado un nombre y un gráfico.
  - o Map: Representa un escenario de la aventura gráfica. Contará con una lista de requisitos (objetos en inventario y flags activadas) para acceder.
  - o Item: Representa un objeto que podrá formar parte del inventario de un jugador. Dicho objeto contará con un nombre y una descripción.
  - o Player: Representa a un jugador, almacenando toda su información, como lista de flags, inventario y datos personales. Contendrá un campo hash que se calculará a partir del resto de sus datos para mantener la coherencia entre la copia del cliente y la que puede tener el servidor
  - o Flag: Representa una variable de estado concreta. Puede tratarse de una variable inherente al jugador o de una global. Existirán variables a nivel de jugador y a nivel global (SFlags)

B. *Mantenimiento de la coherencia*

El mayor problema que puede encontrarse en este modelo es la forma de mantener una coherencia entre la base de datos del cliente con la remota del servidor con el menor tráfico de datos posible, ya que para mantener una mayor sensación de vida en el universo de juego nos interesa que los retardos de debidos a la comunicación sean mínimos (y, en caso de que la conexión del cliente sea limitada, que pueda conectarse sin consumir una gran cantidad de datos).

El problema ha sido afrontado haciendo que todos los cálculos se realicen de forma local y lo único que se transmitan sean las solicitudes y confirmaciones, minimizando así los mensajes y comprobando que el hash de cada jugador sea el mismo tanto en cliente como en servidor en cada transacción de información que pueda inducir a un cambio para garantizar que se mantenga una coherencia.

Inicialmente se consideró hacer que el servidor generara todo para disminuir la carga de procesado del terminal final para hacerlo compatible con dispositivos anteriores pero finalmente se consideró que cargaría mucho al servidor y sería un gran golpe contra la escalabilidad, por lo que se abogó por un procesado compartido.

C. *Diseño de la interfaz de cliente*

La interfaz de un producto creado con este motor tendrá la distribución que se indica en la figura que sigue:

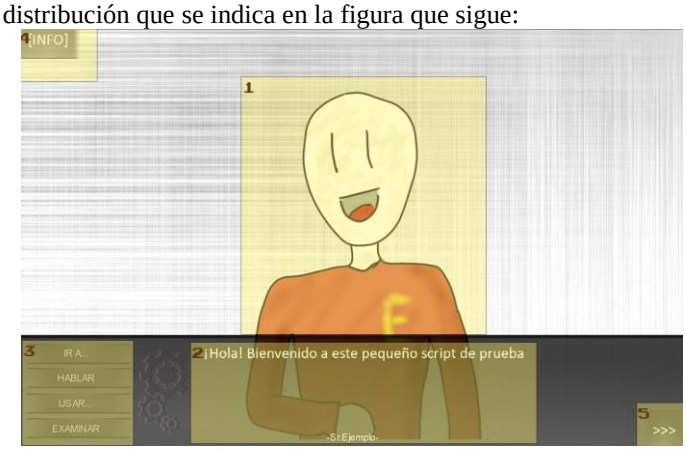


Fig. 3. Interfaz de un juego generado con el motor.

Con los siguientes apartados destacados:

1. Imagen del personaje no jugador (NPC) que nos habla. Puede hallarse vacía si no hay texto en pantalla o el que se nos presenta es fuente de una figura invisible (como el narrador o el propio jugador).
2. Diálogo en pantalla. Incluye, en la parte inferior, el nombre del NPC que nos lo da.
3. Menú del jugador. Incluye:

a. Una opción para desplazarse. Nos abrirá un submenú en el que elegir de entre las opciones disponibles, que a su vez nos proporcionará información y una confirmación. Se ha decidido esta interfaz para ser la más simple, clara e intuitiva, especialmente de cara al usuario de dispositivos móviles gracias a un control plenamente táctil y no invasivo.

b. Una opción para mantener una conversación.

c. Una opción para usar un objeto de nuestro inventario, que funcionará de forma análoga a la de desplazamiento.

d. Una opción para examinar el entorno.

4. Botón de información. Nos proporciona el estado del servidor en una pequeña tabla arriba a la derecha.

5. Botón para avanzar la conversación activa. Al hacerlo, podremos llegar a un menú en el que elegir la opción de diálogo deseada.

Desde el punto de vista del usuario final (véase, el jugador), se ha apostado por una interfaz de la mayor simplicidad posible.

D. Gestión del acceso concurrente

Hemos de garantizar que no haya colisiones a la hora de modificar y leer información de servidor. Como las variables de cada jugador sólo pueden ser modificadas por él mismo y la base de datos de los elementos del mundo como personajes y objetos disponibles sólo podrán ser editadas por el desarrollador de la aplicación final, nos centraremos en un aspecto crítico: las SFlags.

Inicialmente se consideró que, dada la naturaleza de una aventura gráfica no habría que tener excesivo recelo en ese aspecto, ya que hablamos de baja concurrencia y tráfico bajo. No obstante, para garantizar un funcionamiento de mayor calidad, se ideó proteger esa concurrencia mediante semáforos. Antes de hacer una prueba de carga alta se consideró que la gestión del acceso concurrente se podría llevar a nivel global, dado el bajo número de solicitudes en una aplicación de esta naturaleza. Por otro lado, y para cubrir de la forma más correcta posible este diseño, se consideró distribuir el control a cada una de las variables (en lugar de asignar un solo semáforo al conjunto de variables, algo que podría añadir mayores retardos al acceder concurrentemente a varias variables), llevándonos a que las peticiones a distintas variables podrían responderse simultáneamente sin afectar a la coherencia.

E. Protocolo

Desde un punto de vista básico, el protocolo se ha simplificado para que sólo transporte permisos (por ejemplo, si un mapa debería estar accesible o qué conversación ha de tener lugar). Sólo se transportará información de mayor tamaño en el registro de los usuarios y en la secuencia de login.

Eso permite que la transmisión de datos se minimice y el coste computacional del cliente se reduzca en gran medida, algo crítico si se emplea el motor en sistemas de menor capacidad como tablets o netbooks.

Se contará, entonces, con cinco tipos de secuencia:

- Secuencia HELLO: Inicializa la conexión con el servidor.
- Secuencia GETCONVER, USEITEM, EXAMINE: Obtiene el número de la conversación en función de la situación del usuario y el servidor.
- Secuencia ITEMADD, ITEMRM, EDITFLAG: Modifica el inventario o los flags del jugador.
- Secuencia MAPAVAIL: Comprueba si el jugador tiene permisos para acceder a un mapa.
- Secuencia SERVERSTATUS: Pide el estado (fecha, hora, tiempo atmosférico) del servidor.

III. IMPLEMENTACIÓN

La implementación completa del proyecto se ha llevado a cabo empleando el lenguaje de programación Java, con la ayuda de la librería LibGDX, un proyecto de software libre basado en el lenguaje Java que cuenta con la principal ventaja de permitirnos exportar nuestro proyectos a sistemas Android, iOS, HTML5 y sobremesas, lo que la hace candidata perfecta a nuestro proyecto.

Para garantizar la concurrencia y que se acceda de forma correcta a los datos, se empleará un semáforo por cada variable de estado. Inicialmente se consideró usar un semáforo para todo el sistema, pero como se apreciará en el punto IV, atomizar la operación nos proporciona mejores resultados.

IV. EVALUACIÓN

A. Latencia

Para evaluar de una forma fidedigna nuestro sistema, realizaremos nuestras medidas mediante un bot que simula un alto número de usuarios y peticiones (alcanzando varios cientos de miles de peticiones en algo menos de 40 segundos), algo que requeriría una base de usuarios activos de miles de personas para darse en un escenario real.

Aun así, nos puede servir para demostrar que este diseño nos proporciona una alta escalabilidad, ya que el tiempo de respuesta para un número alto de peticiones simultáneas no alcanza el medio segundo de tiempo de procesamiento. También podemos demostrar a partir de esto que tampoco proporciona mucha carga al servidor, ya que el mismo equipo personal (Intel Core i3-2350M @ 2.30GHz, 4GB RAM) ha podido soportar el servidor junto a los clientes automatizados (bots) sin afrontar una carga notable extra.

Para estudiar cómo afecta para el tiempo de acceso en función del número de usuarios activos (para la simulación se mantuvo un número constante de mensajes por usuario). Estos usuarios intentarán competir por la modificación de diez SFlags distintos con probabilidad igual para cada uno de ellos, una prueba que realizamos mediante un pequeño programa que registra a un número (fijado manualmente) de usuarios que envían una serie de peticiones elegidas aleatoriamente entre acceso a diversas flags. Medimos el tiempo medio de acceso para cada una de las flags para una decena de experimentos y obtenemos, de media los la siguiente información:

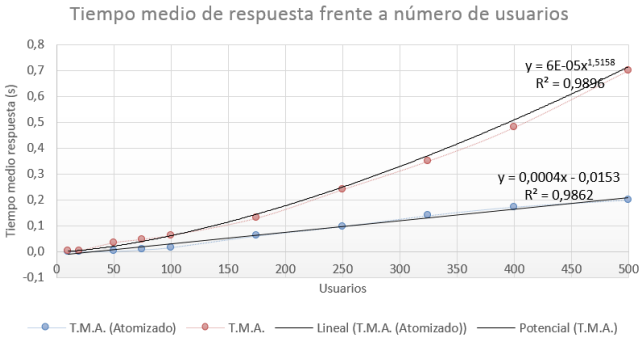


Fig. 4. Medidas de latencia.

Podemos apreciar que, para una misma carga, los valores en el caso en el que se considera atomizar los semáforos son mucho más favorables para nosotros. Eso se debe a que, al

contar con un solo semáforo regulamos todas las peticiones una a una, mientras que en el supuesto de atomizar la operación cada SFlag tendrá su semáforo para regular el acceso. Eso hace que una respuesta que se puede aproximar mediante ajuste lineal a una potencial (gráfica roja) se torne una que se puede aproximar a una lineal (gráfica azul).

B. *Tráfico Generado*

Desde el punto de vista de la conexión de datos, hemos empleado RawCap para obtener las trazas de datos en la interfaz loopback para conocer el tráfico en diversos supuestos. Se ha utilizado en este caso un solo jugador que utiliza una partida de prueba para capturar los datos.

A modo ilustrativo y extrapolando, en el más común de los casos implicaría una tasa de transferencia de subida de 14 bytes al segundo mientras que la bajada será de 4 bytes al segundo, lo que es perfectamente asumible para una conexión de datos de un dispositivo móvil, tanto por la cantidad como por la tasa requerida.

No obstante, es de interés remarcar que estas medidas dependen en gran medida del diseño del juego y del jugador en cuestión. De todas formas, esa variación no será excesivamente significativa porque los tipos de operaciones serán las mismas ya que vienen dictadas por el motor.

V. Conclusiones y trabajo futuro

A lo largo de este proyecto se ha conseguido crear un sistema que permite la generación de forma sencilla de novelas visuales en red a partir de unos ficheros de configuración que gracias a la librería libgdx pueden portarse a sistemas móviles y sobremesa de forma sencilla.

Se ha logrado mantener la consistencia del mundo mediante un protocolo simple y ligero (para minimizar el uso de datos) e implementado de una forma escalable, sencilla y que proporciona una calidad de juego a un número alto de usuarios sin requerir una computadora de gran potencia como servidor.

Finalmente, será de interés tratar unas consideraciones y unas posibles mejoras que podrían ser llevadas a cabo para mejorar la experiencia tanto del desarrollador como del usuario final:

En primer lugar, y de nuevo haciendo referencia a la filosofía eAthena de la que ya se ha hablado, una mejora interesante desde el punto de vista de la funcionalidad y la optimización de recursos sería emplear una base de datos SQL (por ejemplo, haciendo uso de la librería auxiliar gdx-sqlite) en lugar de una en texto plano. Ese cambio también traería consigo una mayor facilidad a la hora de diseñar una API, por ejemplo, para mostrar las estadísticas de un servidor concreto mediante una página web.

También se ha considerado como mejora relevante un sistema de referencias para hacer la experiencia final más personalizada. Por ejemplo que en determinadas líneas de diálogo se mencione al jugador por su nombre registrado o que algunos diálogos varíen en función del sexo del jugador, por ejemplo.

Otra mejora importante sería la integración de efectos gráficos (por ejemplo, fundidos a la entrada o salida de los personajes), así como soporte para efectos sonoros, clips de voces y música de fondo, dando una sensación más fresca y menos mecánica que la apuesta actual. También se ha considerado (y de hecho la estructura está preparada para ello) asociar un gráfico a cada objeto. No obstante, las limitaciones de tiempo han impedido implementar esta funcionalidad.

También, en aras de simplificar la tarea a los desarrolladores sería interesante la creación de un entorno gráfico en el que modificar las bases de datos en tiempo real, así como la generación de eventos programados y el autodisparo de conversaciones en determinadas situaciones para dotar de más potencia al gestor del juego y una experiencia más completa al jugador en última instancia.

Desde el punto de vista del protocolo, una mejora potencialmente interesante consistiría en lugar de comprobar uno por uno los permisos de los mapas se envíe desde el cliente la lista de mapas a la que se intenta acceder y se responda a cuáles de ellos tiene permitido el acceso, lo que reduciría el número de mensajes que hay que enviar y recibir a coste de hacer uno de mayor cantidad de datos.

VI. Referencias

[1] Documentación de la librería LibGDX
http://libgdx.badlogicgames.com/documentation.html
[2] Trabajo de Fin de Grado: Diseño de un motor para aventuras gráficas de universo persistente, Javier Escámez

Javier Escámez Álvarez nacido en 1991, natural de Los Barrios (Cádiz), y formado en Ingeniería de Telecomunicación en la Universidad de Granada.

.

Run Run Bunny

Diseño e implementación de un videojuego multijugador en línea y un mecanismo simple de reparación de pérdidas de paquetes

Autor: Isabel Pérez de la Villa; e-mail: ipvilla@correo.ugr.es
Tutores: Juan José Ramos Muñoz; e-mail: jjramos@ugr.es
Juan Manuel López Soler; e-mail: juanma@ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—En el proyecto se ha llevado a cabo el diseño y la implementación de un videojuego multijugador de plataformas de tipo cliente-servidor, con un máximo de 4 jugadores conectados simultáneamente. Para ello se ha utilizado la plataforma de programación de videojuegos Unity, utilizando el lenguaje C#. Se ofrece también la posibilidad de que el dispositivo donde se ejecuta la aplicación ejerza como servidor o como cliente. Se ha realizado también un estudio de cómo afecta la pérdida de paquetes en la aplicación desarrollada, además de construir un sistema simple para la reparación de pérdidas de paquetes escrito en el lenguaje Java.**

***Palabras clave*— Aplicación, C#, Java, multijugador, proxy, reparación de pérdidas de paquetes, Unity, videojuego de plataformas, Java.**

I. INTRODUCCIÓN

EN los últimos años, videojuegos se han convertido en la principal industria de ocio audiovisual interactivo, superando al cine y a la música. Según los datos registrados por la firma PricewaterhouseCoopers [1], el valor del mercado mundial del videojuego ascendió a 56000 millones de euros en 2010, y se prevé que crecerá hasta los 82000 millones en 2015.

Para los videojuegos en línea se suele exigir una calidad de servicio que en ocasiones las redes IP no son capaces de satisfacer. De esta forma, los jugadores podrían tener una experiencia de juego incómoda, lo que hace que no se disfrute del todo del videojuego.

En el proyecto se ha realizado el diseño e implementación de un videojuego multijugador en línea de plataformas en tiempo real. Este tipo de videojuegos en tiempo real son extremadamente sensible a retardos y a pérdidas, por lo que también se ha diseñado e implementado un mecanismo simple de reparación de pérdidas de paquetes para tratar de solventar este tipo de problemas en redes con entornos ruidosos.

II. REVISIÓN DE ESTADO DEL ARTE

A. Videojuegos similares en el mercado

Existen numerosos videojuegos que responden a las mismas características del juego que se ha implementado durante el desarrollo del proyecto. Entre ellos, encontramos videojuegos como *2 Fast 4 Gnomz* [2], el cual a pesar de tener la misma temática del videojuego *Run Run Bunny*, no tiene funciones de red, y es de un solo jugador. *Sonic Dash* [3] y *Wind Runner* son juegos de velocidad y plataformas con funciones de red, pero sólo para compartir récords con otros usuarios de otras partes del mundo. Encontramos un videojuego llamado *Speed Runners* [4], el cual posibilita la competición entre varios usuarios en línea, con la misma temática de videojuego de plataformas de velocidad.

B. Motores de juego y librerías especializadas

Para el desarrollo e implementación de videojuegos, hoy día existen herramientas que nos facilitan el trabajo. Este es el caso de los motores de juego y las librerías especializadas.

Los motores de juego son entornos de desarrollo con un interfaz relativamente sencillo dedicados a facilitar al usuario el desarrollo de videojuegos completos. Entre los motores de juegos, destacan tres: *GameMaker: Studio* [5], *Unreal Engine* [6] y *Unity* [7]. El primero de ellos está orientado a usuarios que no están habituados a la programación, utilizando un interfaz bastante sencillo basado en una técnica de "arrastrar y soltar". En cuanto a *Unity* y *Unreal Engine*, ambos son motores de juegos más avanzados, y de entre ambos se ha elegido *Unity*, ya que presentaba un tiempo de producción más eficiente.

En cuanto a las librerías especializadas, cabe destacar *LibGDX* [8], una librería escrita en Java especializada en el desarrollo de videojuegos. Con esta librería se hizo el primer intento de programación del videojuego, pero tras varios meses de lento avance, se desechó la idea y se comenzó desde cero la programación definitiva en *Unity*.

C. Técnicas de reparación de pérdidas

Como ya se ha mencionado con anterioridad, en los juegos en línea con requisitos de tiempo real es importante que la comunicación sea consistente. Existen varias técnicas de reparación de pérdidas de paquetes. Este tipo de técnicas pueden dividirse en dos tipos [9]: *técnicas preventivas*, las cuales actúa en previsión de que posteriormente pueda haber pérdidas en la comunicación, y *técnicas reactivas*, las cuales actúan una vez ya ha sido detectada la pérdida de un paquete.

De entre los distintos mecanismos de reparación de pérdidas de paquetes que existen, se destacan a continuación tres de ellos:

- *Retransmisión automática:* Una vez se ha detectado la pérdida, el elemento de la red que detecta la pérdida solicita al emisor que vuelva a reenviar el paquete perdido. Es por tanto una técnica de reparación reactiva.

- *Predicción por el lado del cliente (Dead Reckoning):* Para mitigar el efecto de la latencia, el cliente predice de forma local el estado del juego anticipándose a la respuesta del servidor. Se trata de una técnica preventiva.
- *Corrección de errores hacia delante (FEC):* Se agrega redundancia a la comunicación para hacerla más consistente. Nos encontramos por tanto ante una técnica de reparación preventiva.

III. Temporización y costes

Se expone a la planificación temporal para llevar a cabo las distintas tareas que componen el proyecto, así como una estimación del coste del mismo.

El proyecto se ha dividido en 8 bloques de tareas: **análisis del problema y especificación de los objetivos, revisión del estado del arte, estimación de costes, diseño, implementación, corrección de errores y bugs, estudio del impacto de la pérdida de paquetes y del tráfico generado por Unity**, y **documentación del proyecto**. En la Fig. 1 se muestra el diagrama de Gantt de las distintas tareas citadas anteriormente. El proyecto se ha desarrollado entre el 11 de julio de 2014 y el 12 de septiembre de 2014.

En cuanto al coste estimado del proyecto, éste puede observarse en la Tabla I.

IV. Diseño

Se expone a continuación el diseño propuesto tanto para el videojuego multijugador como para el mecanismo de reparación de pérdidas de paquetes.

A. Historia y funcionamiento del videojuego Run Run Bunny

Run Run Bunny estará protagonizado por uno o más conejos, los cuales deberán huir de un gran camión que se ha adentrado en el bosque, esquivando obstáculos y evitando ser atropellados hasta ponerse a salvo en una cueva en la que dicho camión, por su gran tamaño, no será capaz de entrar. Mientras huyen, podrán coger zanahorias que se encuentran repartidas por el camino.

En la Fig. 3 puede observarse un esquema con el diagrama de estados del videojuego. Al iniciarlo, se mostrará un menú principal, en el que se podrá elegir si ejercer como servidor o como cliente. En caso de elegir iniciar el servidor, el juego entrará en un estado de espera en el que actuará como servidor, haciéndolo todo de forma automática, por lo que el usuario sólo tendrá la opción de desconectar el servidor y volver al menú principal.

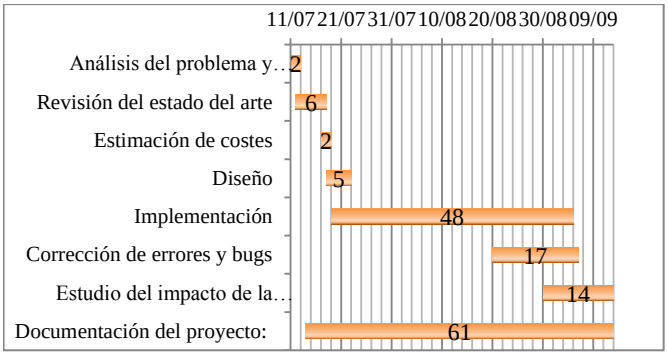


Fig. 1. Diagrama de Gantt del proyecto

Al conectarse a un servidor previamente inicializado, el usuario pasará a una sala de espera donde se mostrará la lista del resto de usuarios conectados al mismo servidor. En el momento en que el primer jugador que entró en la sala de espera haga clic en el botón de comenzar la partida, el juego comenzará para todos los jugadores que estuvieran en la sala de espera.

TABLA I
ESTIMACIÓN DE COSTES

RECURSO	CANTIDAD	COSTE POR UNIDAD(€)
Horas de trabajo	378	25
Ordenador portátil con Windows 7	1	500
Ordenadores portátiles para testeo con Windows 7	2	500
Conexión a internet	(2 meses)	30/mes
Paquete Microsoft Office	1	60
Adobe Photoshop CS5	1	40
Analizador de paquetes Wireshark	1	0
Librería JNetPcap	1	0
Editor Unity3d versión gratuita	1	0
Entorno de desarrollo Eclipse	1	0
COSTE TOTAL:		**11110**

Fig. 2. Pantalla de juego de Run Run Bunny

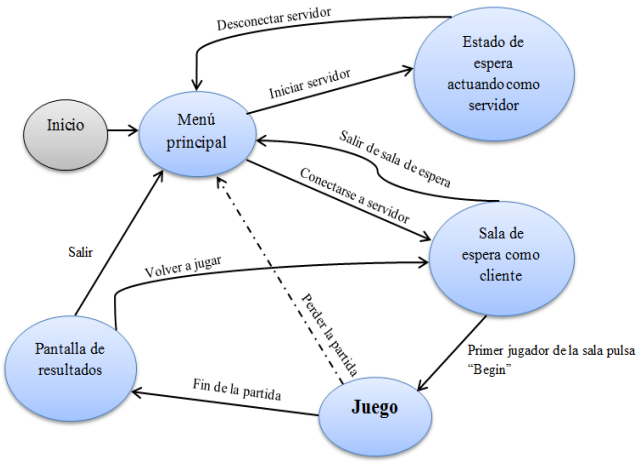


Fig. 3. Diagrama de estados del videojuego Run Run Bunny

Una vez iniciada la partida, el jugador que pierda puede decidir volver al menú principal o permanecer como espectador hasta que ésta termine. Al llegar un jugador a la meta, se mostrará una ventana con un botón que llevará a una ventana de resultados, mostrando las puntuaciones de todos los que han participado en la partida. Desde este punto, el usuario tiene la posibilidad de volver a jugar, en cuyo caso volverá a la sala de espera, o de salir del juego y volver al menú principal.

En caso de que el servidor se desconecte, todos los clientes que estaban conectados a él volverán al menú principal.

B. Métodos de comunicación en Unity

En un videojuego en línea hay dos tipos de aproximaciones: **servidor autorizado** y **servidor no autorizado**. En el caso de servidor autorizado, es el servidor quien controla los movimientos de todos los elementos del juego (un cliente sólo le avisa de qué tecla ha pulsado, y en base a la tecla pulsada, el servidor comprueba cuál es el estado del mundo tras haber pulsado esa tecla), en el servidor no autorizado son los clientes los responsables de sus propios objetos, y se encargan de modificar su estado y enviar la información pertinente al servidor para que éste la retransmita a todos los clientes.

El tener un servidor no autorizado implica que un cliente no sufrirá *lag* o pérdidas en cuanto a sus propias acciones, pero no es seguro ante el hecho de poder hacer trampas. En cambio, teniendo un servidor autorizado, al ser éste el que se encarga de toda la lógica del juego, no hay posibilidad de que los clientes hagan trampas, ya que éstos sólo les dicen al servidor la acción que desean tomar, y el servidor es el que determina qué ha sucedido al realizar tal acción.

Para que los clientes y el servidor se comuniquen entre sí se utilizarán dos métodos de comunicación en Unity: las **llamadas a procedimiento remoto** (RPC) y la **sincronización de estado** (*State Synchronization).* Las primeras se realizarán en casos puntuales del juego: cuando un personaje ha cogido una zanahoria de puntos, al caer un personaje por un barranco, etc.

Por otro lado, la sincronización de estado se aplica a un objeto de juego. Hace que un componente de dicho objeto se sincronice en todos los equipos de la red. Podemos distinguir dos tipos: **sincronización de estado fiable** y **sincronización de estado no fiable**. En el primer tipo, cuando el servidor envía un mensaje con el estado actual de un objeto (en nuestro caso, únicamente la posición, rotación y tamaño del objeto), se asegura que el receptor lo ha recibido. No envía ningún paquete nuevo hasta que no se asegure de ello. Además, sólo se envían los datos que han cambiado con respecto al último estado. Así, por ejemplo, si un objeto ha modificado su posición pero no su rotación desde la última vez que el cliente recibió correctamente un paquete de sincronización de estado, sólo se enviará la nueva posición. De esta forma, se economiza en cuanto a ancho de banda.

En el caso de sincronización no fiable, los paquetes se envían sin confirmar que han llegado correctamente a su destino. Esto agiliza la comunicación, lo que la hace la opción ideal para casos en los que se necesite rapidez (como el caso que nos atañe). En este caso, en los paquetes siempre se envía toda la información del estado del escenario, de tal forma que si un paquete con la posición de los personajes sufre una pérdida, el siguiente paquete que llegue corregirá la posición en el cliente.

Para el videojuego Run Run Bunny, se ha elegido la filosofía de **servidor autorizado**, y se ha optado por la **sincronización de estado no fiable**.

C. Diseño de la técnica de reparación de pérdidas de paquetes

Una vez diseñado el videojuego, se hace el diseño del programa que se ocupará de la reparación de pérdidas de paquetes, con objeto de minimizarlas lo máximo posible. Para este trabajo se hace la suposición de que las pérdidas no se generan por congestión en la red, sino que son debidas a errores o ruido en los enlaces, como ocurre en redes inalámbricas o celulares.

Como técnica de reparación de paquetes se utilizará una técnica basada en la técnica de corrección de errores hacia adelante (FEC): se transmitirá información redundante de forma preventiva. Es decir, los paquetes necesarios para la sincronización de estado del juego se enviarán varias veces, para aumentar la posibilidad de que al menos una copia del mensaje llegue al destino a pesar de encontrarnos en un entorno con pérdidas. Es una técnica sencilla y relativamente poco eficiente, pero dado que necesitamos rapidez al tratarse de una aplicación en tiempo real y que disponemos de recursos y tiempo limitados, puede ser una buena opción. El motivo de que se envíe el mensaje completo es que no conocemos el protocolo que utiliza Unity en la comunicación por lo que, al ser privado, no queda más remedio que enviar el paquete completo.

Se realizó una primera aproximación con *JNetPcap*, una librería de Java. Con esta librería, se pueden utilizar diversos métodos para monitorizar la llegada de paquetes en un interfaz y realizar envíos. La idea era la de monitorizar el interfaz correspondiente, hacer un filtrado de los mensajes que salían del servidor hacia los clientes y enviarlos un número determinado de veces. No obstante, tras varias pruebas, se pudo observar que el método era demasiado lento, inaceptable para una aplicación en tiempo real.

Es por ello que se propuso un diseño alternativo. Para realizar este mecanismo, se creará un *proxy* que sirva de intermediario entre el servidor y los clientes. El *proxy* reenviará los paquetes que le lleguen desde los clientes hacia el servidor, y los paquetes que provengan del servidor hacia un cliente, se lo enviará a éste un número de veces determinado por el usuario.

El usuario podrá seleccionar escribiendo por teclado el puerto donde estará escuchando el *proxy* de cara a los clientes, y tendrá que escribir el puerto por el que está escuchando el servidor y su dirección IP, además del número de veces que deben enviarse los mensajes a los clientes, como ya se ha dicho con anterioridad. Los clientes en este caso deben conectarse al puerto de escucha del *proxy*, y no al del servidor.

La Fig. 5 muestra un ejemplo del esquema de funcionamiento del mecanismo de reparación para 1 cliente. El cliente 1 envía un mensaje de conexión (flecha azul) desde un puerto determinado (en el ejemplo, el puerto 52145) hacia el puerto de escucha del *proxy*. Al recibir dicho paquete,

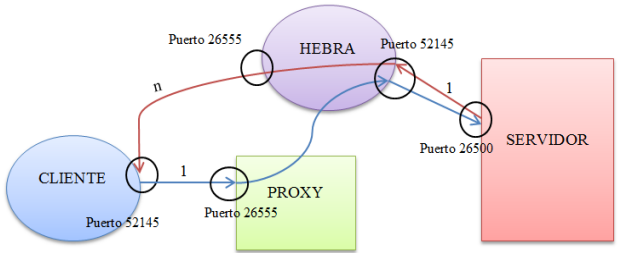


Fig. 4. Esquema de funcionamiento (1 cliente)

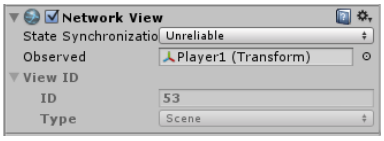


Fig. 5. Componente NetworkView

el *proxy* crea una hebra para atender al cliente, y reenvía el paquete al servidor desde el mismo puerto que el del cliente. Los mensajes de respuesta del servidor se envían hacia el *proxy* por el puerto correspondiente, y la hebra asociada al cliente en cuestión le reenvía el mensaje "n" veces al mismo. El proceso es similar cuando se conectan 2 clientes, sólo que en este caso los puertos de los clientes y del proxy hacia el servidor para cada uno de los clientes son diferentes entre sí, y se lanza una nueva hebra para el segundo cliente, y así con las sucesivas conexiones de clientes que se den.

V. Implementación

Ya se ha mostrado el diseño de las dos aplicaciones que componen el proyecto. Seguidamente, se procede a exponer cómo se ha realizado la implementación de las mismas.

A. *Implementación del videojuego*

El juego se ha desarrollado utilizando el motor de videojuegos Unity en su versión gratuita. Para una mayor organización, el juego se ha dividido en escenas (*scenes*) o niveles, cada una con los elementos necesarios para poder realizar sus funciones: **Menu**, que comprende la parte correspondiente al menú principal del juego, **Game**, la cual corresponde a la partida en sí, y **Results**, donde se muestran los resultados de la partida.

Cada una de estas escenas contiene objetos de juego (*GameObjects)*, los cuales a su vez pueden contener ciertos componentes como gestores de física, animadores, renderizador de *sprites*, etc. Los más importantes son los scripts, escritos en el lenguaje de programación C#. Estos scripts están vinculados al objeto al que pertenecen, y se ejecutan al aparecer el objeto en escena, de forma concurrente. Se pueden decir que conforman "el guion" que debe seguir el objeto una vez que esté en la escena.

Pero en este apartado, destacaremos el componente *Network View* (ver Fig. 5). Este componente es el que da la posibilidad de añadir al objeto la sincronización de estado y realizar llamadas a procedimiento remoto en los scripts. En él se puede elegir el tipo de sincronización de estado que se desea que tenga el objeto. El componente observado (*Observed)* determina qué datos se sincronizarán en todos los puntos de la red. En nuestro caso, sincronizaremos el componente *Transform* (posición, rotación y tamaño del objeto), para el caso de los conejos y el camión. Hay otros objetos que, a pesar de tener el componente *Network View*, no tienen sincronización de estado, sino que sólo lo utilizan para poder hacer uso de RPCs.

B. *Implementación del mecanismo de reparación de pérdidas de paquetes*

Para el programa de reparación de pérdidas, tras varias pruebas fallidas utilizando la librería *JNetPcap* como se comentó con anterioridad, se decidió implementar un *proxy* intermedio entre el servidor y los clientes. Éste actuaría de intermediario de ambos, pero enviando "n" veces los paquetes que provienen del servidor, donde "n" es un número que el usuario le haya determinado por entrada de texto (mínimo 1 vez, máximo 10). El resto de paquetes se envían sólo 1 vez. Para la implementación del programa correspondiente, se ha utilizado el lenguaje Java, usando la plataforma Eclipse. El programa se compone únicamente de dos clases: **ProxyUnity**, la clase con el método principal, y **Hebra**, que incluye los métodos y atributos necesarios para operar con cada una de las hebras asociadas a cada cliente. En la Fig. 7 puede observarse el diagrama UML de clases de la aplicación.

VI. Estudio del tráfico de Unity y evaluación

Tras haber desarrollado el videojuego en una versión *alpha*, y con objeto de poder realizar un diseño del programa de reparación de pérdidas, primero se realizó un pequeño estudio del tráfico generado por el motor de videojuegos Unity, tratando así de diseñar la técnica de reparación adaptada a Unity en lo posible.

Tras el estudio realizado y la implementación de la técnica de reparación, se comprobó la efectividad de la misma en base a las opiniones y calificaciones expuestas por varios sujetos.

A. *Primer estudio del tráfico de Unity*

En un primer estudio se comprobó la diferencia entre utilizar sincronización de estado fiable y sincronización de estado no fiable. Se dispone de un equipo actuando como servidor, donde ejecutamos el analizador de protocolos Wireshark [10]. En el equipo del cliente, ejecutamos el simulador de problemas de red Clumsy [11], el cual nos permite configurarlo con cualquier porcentaje de pérdidas. De esta forma, capturamos los paquetes que salen del servidor y que vienen desde el cliente para 4 casos: sincronización fiable con pérdidas y sin pérdidas y sincronización no fiable con

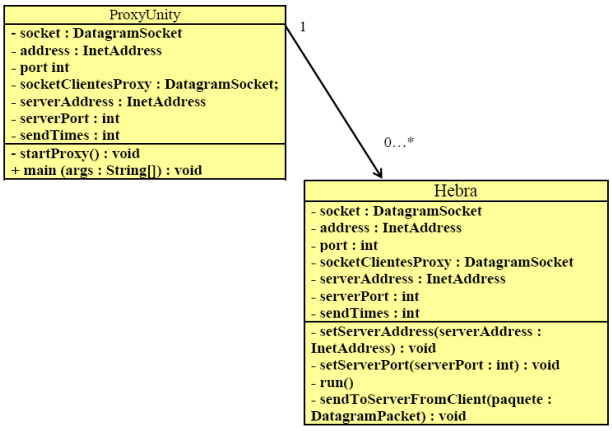


Fig. 6. Diagrama UML del mecanismo de reparación de pérdidas de paquetes

pérdidas y sin pérdidas. Los resultados para el caso del servidor pueden consultarse en las Fig. 7-10, y para el caso del cliente en las Fig. 11-14.

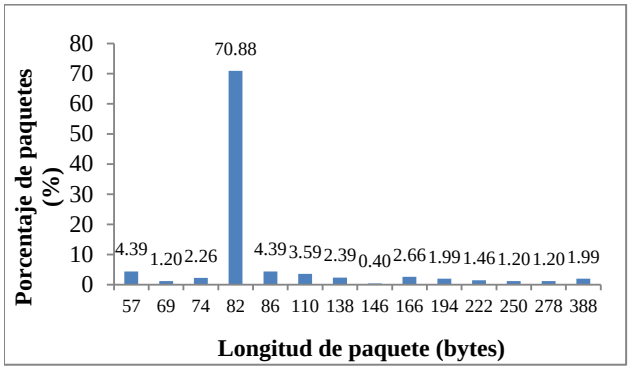


Fig. 7. Paquetes del servidor en sincronización fiable (50% pérdidas)

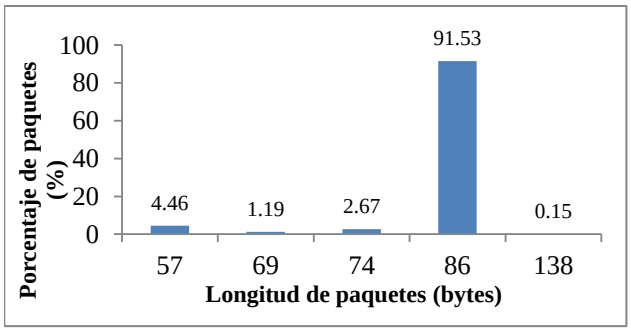


Fig. 8. Paquetes del servidor en sincronización fiable (Sin pérdidas)

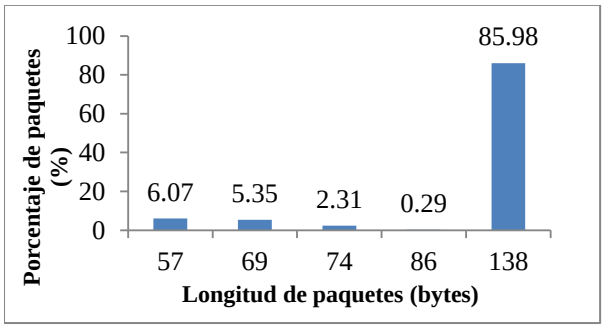


Fig. 9. Paquetes del servidor en sincronización no fiable (50% de pérdidas)

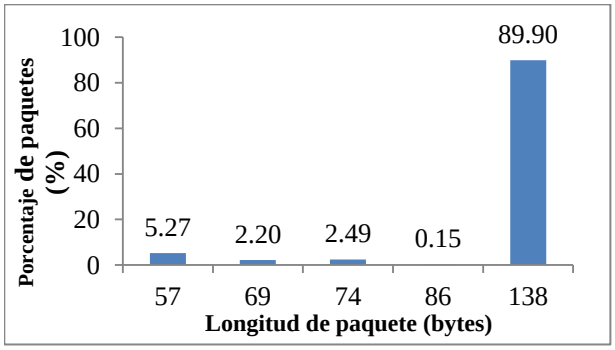


Fig. 10. Paquetes del servidor en sincronización no fiable (Sin pérdidas)

Se observa que los tamaños de paquete por parte del servidor en sincronización no fiable son mayores que en sincronización fiable. Esto es debido a que en la sincronización no fiable en los paquetes siempre se envía toda la información del estado del escenario, y en la fiable sólo el cambio con respecto al último paquete que llegó correctamente. El comportamiento en sincronización de estado no fiable es independiente de las pérdidas que haya en la red.

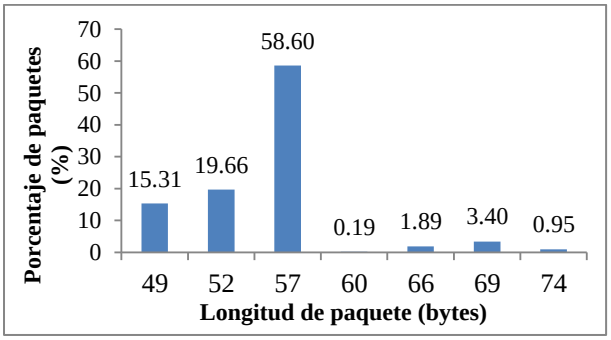


Fig. 11. Paquetes del cliente en sincronización fiable (50% de pérdidas)

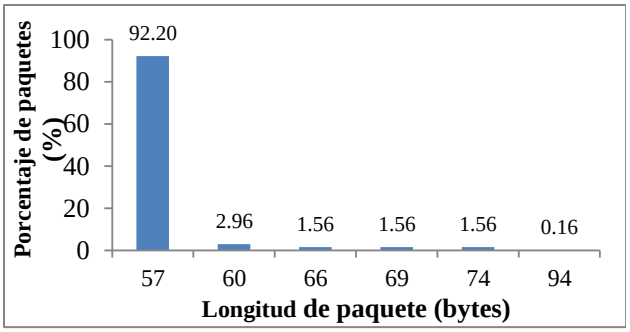


Fig. 12. Paquetes del cliente en sincronización fiable (Sin pérdidas)

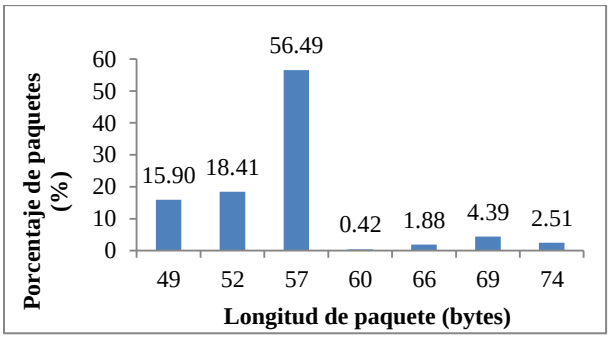


Fig. 13. Paquetes del cliente en sincronización no fiable (50% de

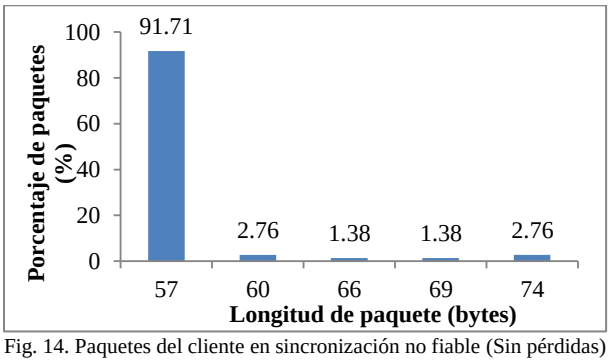


Fig. 14. Paquetes del cliente en sincronización no fiable (Sin pérdidas)

Para el caso de paquetes enviados por el cliente, se puede apreciar que el hecho de que la sincronización de estado sea fiable o no fiable, le es indiferente. Tan sólo afecta el hecho de que haya pérdidas o que no las haya. Ciertos paquetes por parte del cliente sólo se envían cuando hay pérdidas. Comprobándolo con Wireshark, se observa que estos paquetes empiezan por el byte 0xa0. Estos podrían ser paquetes que notificaran al servidor que hay pérdidas.

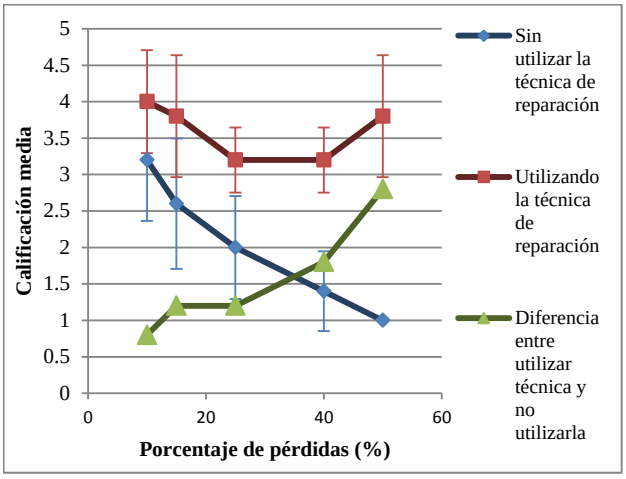


Fig. 15. Mensajes del servidor en sincronización de estado no fiable (50% de pérdidas)

B. *Segundo estudio del tráfico de Unity*

En un segundo estudio, se comprobó la diferencia entre el tamaño de paquetes por parte del servidor en 1 jugador y en 2 jugadores. Para ello, se dispone de un equipo ejerciendo de servidor y ejecutando Wireshark y dos ordenadores que se conectan como clientes. La sincronización de estado era no fiable. Se observó que los paquetes de estado del servidor para partidas de dos jugadores eran mayores que para partidas de un jugador. Esto implica que la sincronización de estado de todos los objetos se envía en un solo paquete, que será mayor cuanto mayor sea el número de objetos a sincronizar

C. *Evaluación de la técnica de reparación*

Para la evaluación de la técnica, se hizo de forma subjetiva. Se les pidió a 5 sujetos que valoraran la experiencia de juego en una escala MOS [12]: 1 (Mala), 2 (Mediocre), 3 (Regular), 4 (Buena) y 5 (Excelente). Las pruebas eran partidas de un jugador con distintos valores de porcentajes de pérdidas, primero sin aplicar la técnica de reparación y luego utilizándola. Los porcentajes de pérdidas que se han tratado son: 10%, 15%, 25%, 40% y 50%. Se utilizaba sincronización de estado no fiable. Las calificaciones medias se muestran en la Fig. 15. En rojo se muestra la calificación utilizando la técnica, en azul sin utilizarla y en verde la diferencia entre ambas calificaciones, es decir, la mejora experimentada al habilitar el proxy en comparación al mismo escenario sin proxy. Nótese que se obtiene 1 punto MOS de mejora al utilizar la técnica de reparación, y que el efecto de la técnica parece ser más notable cuanto mayor es el número de pérdidas.

VII. Conclusiones y trabajos futuros

En el proyecto, se ha diseñado e implementado un videojuego multijugador de hasta 4 jugadores en línea, además de un mecanismo de reparación de pérdidas de paquetes basado en añadir redundancia a la comunicación. A continuación se ha realizado un estudio del tráfico que genera Unity y se ha evaluado la técnica de reparación mediante tests de opinión sobre usuarios reales, y ha mostrado ser eficaz, obteniendo como mínimo un 1 punto MOS de mejora para casi todos los porcentajes de pérdidas estudiados.

En cuanto a trabajos futuros, ambas aplicaciones podrían mejorarse. Por ejemplo, al videojuego se le podría añadir un chat a la sala de espera, agregar habilidades o *Power-Ups* a los personajes y adaptar el juego para su ejecución en móviles o tablets. La técnica de reparación podría mejorarse haciendo un algoritmo dinámico para la adaptación del número de envíos de paquetes en función de las condiciones de red, así como añadir un interfaz gráfico para hacerlo más cómodo de manejar.

Agradecimientos

Agradezco a mi familia por todos estos años de apoyo a lo largo de la carrera.

Gracias a Fran, por ser un pilar fundamental en los momentos en que mis fuerzas parecían empezar a flaquear.

Gracias también a los profesores Juan José Ramos y Juan Manuel López, y al departamento de Teoría de la Señal, Telemática y Comunicaciones por los conocimientos aportados a lo largo de estos años que me dieron la oportunidad de realizar el proyecto.

Referencias

[1] Página de PricewaterhouseCoopers: http://www.pwc.es
[2] Página oficial de 2 Fast 4 Gnomz*:* http://www.qubicgames.com/en/2-fast-4-gnomz
[3] Página oficial de Sonic Dash: http://www.sega.es/sonicdash
[4] Página oficial de Speed Runners: http://tinybuild.com/speedrunners
[5] Página oficial de Sonic Dash: http://www.sega.es/sonicdash
[6] Página oficial de GameMaker: Studio: http://www.gamemaker.nl/
[7] Página oficial de Unreal Engine: https://www.unrealengine.com/
[8] Página oficial de Unity: https://unity3d.com/unity
[9] Ramos Muñoz, J. J. "Mejoras a la transmisión de voz sobre IP considerando criterios de calidad experimentada. Selección automática de protocolos", Tesis Doctoral, DTSTC, Universidad de Granada, España, 2009.
[10] Página oficial de Wireshark: https://www.wireshark.org
[11] Página de Clumsy: http://jagt.github.io/clumsy/index.html
[12] UIT-T Rec. P.800. *Métodos de determinación subjetiva de la calidad de transmisión*, Agosto de 1996

Isabel Pérez de la Villa, nacida en Huelva (España), actualmente Ingeniera de Telecomunicaciones por la Universidad de Granada desde septiembre de 2014.

Rediseño de red privada virtual en una empresa multinacional

Autor: Francisco Andrés Torrecillas Gilabert; e-mail: fatorrecillas@cosentino.com

Tutor: Prof. Dr. Pedro García Teodoro; e-mail: pgteodor@ugr.es

Titulación: Ingeniería Informática

Departamento de Teoría de la Señal, Telemática y Comunicaciones

Universidad de Granada

***Resumen*— Este trabajo consiste en el rediseño parcial del direccionamiento interno de la red privada virtual de la empresa Cosentino. En la fase inicial del proyecto se analiza en detalle la red corporativa, se identifican sus problemas y debilidades, se hace una estimación del crecimiento futuro y se establecen una serie de restricciones. Sobre la base de todo ello se fija una política de direccionamiento que se concreta en un plan de re-numeración de red. La implementación del plan de direccionamiento no solo da solución a los problemas detectados en la red privada objeto de estudio, sino que permite fijar las bases para su crecimiento ordenado futuro.**

***Palabras clave*— Direccionamiento IP, escalabilidad, red privada virtual.**

I. Introducción

ESTE proyecto tiene como objeto de estudio y ámbito de trabajo la red privada virtual de la empresa Cosentino. Dicha empresa es una compañía multinacional con presencia en las principales ciudades de Europa, Estados Unidos, Brasil, Australia y México. En sus orígenes, Cosentino era una pequeña empresa cuya infraestructura creció rápidamente hasta convertirse en la empresa multinacional que es hoy en día. Además, en la actualidad, Cosentino está inmersa en un ambicioso proyecto de expansión para extender su presencia hacia nuevos mercados tales como Oriente Medio y sureste de Asia, así como para afianzarla en aquellas zonas de negocio donde ya está presente. Toda la infraestructura empresarial está soportada por una VPN montada sobre la infraestructura pública de Internet e incluye diversos tipos de instalaciones, tales como centros de distribución, talleres de transformación del producto, *data centers*, oficinas y polígono industrial en Cantoria, donde se ubican sus oficinas centrales y las fábricas de sus principales productos. El rápido crecimiento de la empresa y de su red no ha sido coherente con una política de direccionamiento adecuada. Esta circunstancia ha dado como resultado un diseño de red que, a corto y medio plazo, está dificultando la escalabilidad y la operación de la red.

Así, el presente trabajo tiene como hecho desencadenante el agotamiento del espacio de direcciones IP disponibles en buena parte de las ubicaciones de red VPN de Cosentino. Esta circunstancia imposibilita la conexión de nuevos dispositivos, dejando patente la necesidad de una modificación en la red corporativa que dé solución a este acuciante problema. Un estudio pormenorizado de la red revela la existencia de una serie de problemas adicionales sobre los que también se necesita actuar. Así pues, se plantea la necesidad de acometer un proyecto que tenga como propósito dar una solución total o parcial a los distintos problemas sin afectar la operación de red y que, además, haga posible la introducción de una serie de mejoras que favorezcan el rendimiento de la red en el futuro inmediato.

El desarrollo del presente documento, en coherencia con la labor técnica que describe, parte de la necesaria etapa de análisis para identificar los problemas existentes. Tras ello se discute la fase de diseño, donde se concretan las mejoras específicas a introducir. Finalmente, en la fase de implementación se discuten las actuaciones puestas en marcha para introducir de forma efectiva las mejoras pretendidas sin afectar la operación de la red.

II. Fase de análisis

En la fase inicial del proyecto se realiza un breve estudio del pasado, presente y las perspectivas de futuro de la empresa a fin de entender mejor el diseño actual de la VPN y sus necesidades futuras. Este análisis revela la existencia de una serie de problemas cuya resolución serán los objetivos de proyecto. Dichos problemas son los que se listan a continuación:

1) Uso de direccionamiento público en la red interna

Ciertas secciones de red vinculadas con el área de producción contienen dispositivos configurados con direcciones IP públicas de los rangos 1.0.223.0/24 y 1.0.224.0/24. Esta circunstancia genera una ambigüedad en el enrutamiento que impide el acceso a recursos de Internet (alojados en dichos rangos) desde la red del polígono de Cantoria, al tiempo que complica el acceso remoto para soporte por parte del fabricante de dichos dispositivos.

2) Incorrecto criterio de asignación de números de red

La asignación de los prefijos a las ubicaciones de red es inadecuada puesto que los números de red escogidos son muy cercanos entre sí y cualquier modificación en la longitud de prefijo, a fin de proporcionar mayor espacio de direccionamiento, daría lugar a solapamientos.

3) Agotamiento del espacio de direcciones en sedes remotas

Los prefijos de red asignados en la mayoría de las sedes o delegaciones de Cosentino proporcionan un espacio de direcciones IP disponibles insuficientes para los requisitos

actuales. En consecuencia, es habitual la aparición de problemas de conexión a red en sedes remotas debido a la escasez de direcciones IP.

4) Agotamiento del espacio de direcciones en la red inalámbrica del polígono industrial de Cantoria

El campus donde se ubican las oficinas centrales de Cosentino y sus fábricas, situado en la localidad almeriense de Cantoria, cuenta con una red inalámbrica única. El porcentaje de uso actual del total de direcciones IP disponibles alcanza el 97 % durante horas pico. Así pues, se hace necesario ampliar el espacio de direcciones a fin de garantizar la conectividad WiFi en esta ubicación de red.

Si bien la escasez de direcciones IP disponibles podría solucionarse en base al empleo de IPv6, a fecha de hoy es necesario encontrar una solución IPv4 para el futuro inmediato y para la fase de transición hacia IPv6, proceso este que tomará años, si no décadas.

5) Fragmentación del espacio de direccionamiento

El espacio de direccionamiento privado (10/8) empleado se encuentra fragmentado si se atiende a criterios geográficos. Se da la circunstancia de que una misma red física cuenta con números de red muy distantes entre sí dentro del espacio de direccionamiento. Por otra parte, existen ubicaciones de red situadas en continentes distintos que emplean direcciones de red muy próximas entre sí. En esta circunstancia se hace imposible realizar una adecuada abstracción de información de enrutamiento que naturalmente ha de hacerse en base a criterios geográficos.

III. Fase de diseño

A partir de los problemas/limitaciones antes detectados, la fase de diseño parte de la definición de una política de direccionamiento que se apoya en dos pilares fundamentales:

a) *Enfoque global*. Se tomará el espacio reservado para direccionamiento interno (10.0.0.0/8) y se asignará considerando como ámbito de presencia toda la geografía mundial.

b) Criterios geográficos. La estrategia de asignación empleará criterios geográficos. Se diseñarán bloques de direcciones consecutivas que serán asignados para su concesión a ubicaciones de red según la zona geográfica de adscripción.

La política de direccionamiento se concretará en un plan de numeración que asignará direcciones a las ubicaciones de redes actuales y futuras. La implementación del plan de direccionamiento escogido plantea un reto técnico denominado *renumbering* (re-numeración) recogido en diversos documentos RFC informativos, tales como *RFC 1900 "Renumbering Needs Work"*[4], *RFC 5887 "Renumbering Still Needs Work"*[5], *RFC 1916 "Enterprise renumbering: Experience and Information Solicitation"*[6], *RFC 2071 "Network Renumbering Overview: Why would I want it and what is it anyway?"*[9] y *RFC 2072 "Router Renumbering Guide"*[10]. El *renumbering* o re-numeración es el proceso consistente en la migración de la numeración actual de una red en producción a un nuevo rango de direccionamiento minimizando la interrupción en la operación de dicha red.

Se plantean dos alternativas para el plan de direccionamiento: teórica y práctica. Son como sigue:

1) Plan de direccionamiento teórico. Este plan toma la dirección IPv4 y la divide en una serie de campos:

- *red:* este campo se corresponde con el primer octeto y posee valor constante 10, puesto que se está usando el espacio reservado 10.0.0.0/8.

- *zona:* compuesto por los bits 9 y 10, los diferentes valores de dicho campo permiten codificar cuatro zonas geográficas principales.

- *subzona:* compuesto por los bits 11 y 12, los distintos posibles valores de dicho campo permiten codificar hasta un máximo de cuatro sub-zonas geográficas para cada una de las zonas geográficas principales.

- *delegacion:* compuesto por los bits 13 al 20, este campo permite codificar 256 ubicaciones de red para cada una de las cuatro sub-zonas.

- *host:* compuesto por los bits restante (21 al 32), este último campo definirá la dirección IP de cada dispositivo final conectado a la red en cuestión.

La Figura 1 expone gráficamente la subdivisión en campos realizada para la dirección IPv4 expuesta anteriormente. El valor binario asignado al campo *zona* definirá el prefijo asignado a cada una de las cuatro zonas geográficas principales diseñadas. Por su parte el valor binario asignado al campo *subzona* (conjuntamente con el valor del campo *zona*) definirá el prefijo asignado a cada una de las dieciséis sub-zonas diseñadas. La Tabla I expresa en base decimal los distintos prefijos y su asignación por zonas y subzonas.

Por su parte, En la Figura 2 se muestran gráficamente las cuatro zonas geográficas principales diseñadas, junto con los prefijos asignados a cada una de ellas.

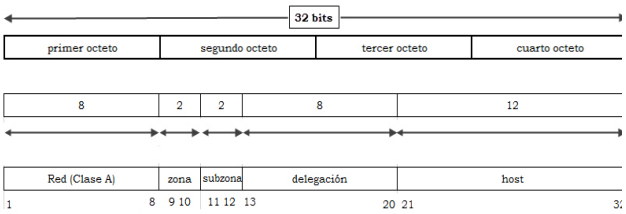


Fig. 1. División en campos de la dirección IPv4 según el plan de direccionamiento teórico.

TABLA I

POTENCIAL ASIGNACIÓN DE PREFIJOS POR ZONAS Y SUB-ZONAS

Zona	Prefijo	Sub-zona	Prefijo
Europa-África	10.0.0.0/10	Europa Occidental	10.0.0.0/12
		Europa Central	10.16.0.0/12
		Europa del Este	10.32.0.0/12
		África	10.48.0.0/12
Asia-Pacífico	10.64.0.0/10	O. Medio-India	10.64.0.0/12
		Rusia Occidental	10.80.0.0/12
		Sureste	10.96.0.0/12
		Australia.-Indonesia	10.112.0.0/12
América-Norte	10.128.0.0/10	USA Sur	10.128.0.0/12
		USA Norte	10.144.0.0/12
		México	10.160.0.0/12
		Canadá, Alaska	10.176.0.0/12
América-Sur	10.192.0.0/10	Sudamérica Norte	10.192.0.0/12
		Brasil	10.208.0.0/12
		Sudamérica.-Pacífico	10.224.0.0/12
		Sudamérica Sur	10.240.0.0/12

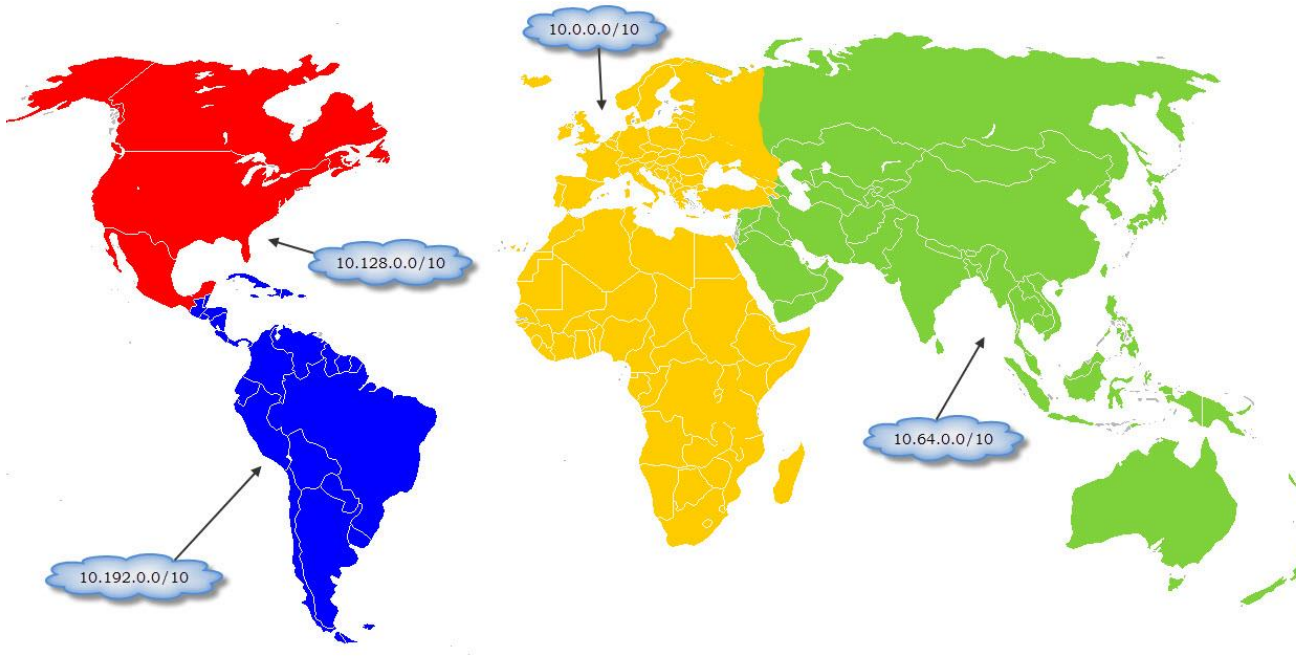


Figura 2. Zonas geográficas principales según el plan de direccionamiento teórico

2) Plan de direccionamiento práctico. Este plan realiza una división del espacio de direccionamiento privado 10.0.0.0/8 en bloques de direcciones contiguos. Dichos bloques serán divisiones binarias limpias para poder ser expresados en términos de prefijos.

La Figura 3 expresa la proporción de los distintos bloques contiguos en los que ha sido dividido el espacio de direccionamiento privado clase A.

La Figura 4 muestra los distintos bloques diseñados, sus tamaños y las zonas geográficas a las que han sido asignados. Destacar que se reservan para uso futuro dos de los bloques diseñados (8 y 9), los cuales no tienen una asignación geográfica. El código de colores empleado facilita la comparación visual con la proporción de cada bloque en relación con el espacio de direccionamiento 10.0.0.0/8 representado en la Figura 3.

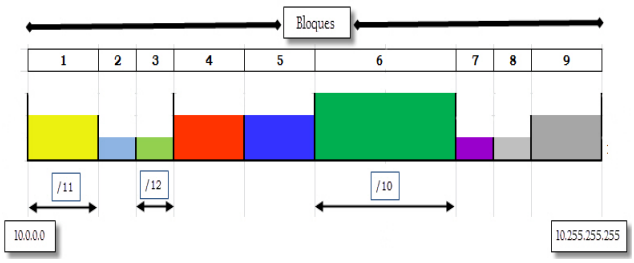


Fig. 3. Diseño de bloques en el espacio de direccionamiento 10.0.0.0/8.

Bloque	Color	Superred	Asignado a
1		10.0.0.0/11	Polígono industrial en Cantoria (Almería)
2		10.32.0.0/12	Sedes Europa
3		10.48.0.0/12	América Norte
4		10.64.0.0/11	Sudamérica
5		10.96.0.0/11	Polígono industrial en Cantoria (Almería)
6		10.128.0.0/10	Asia - Pacífico
7		10.192.0.0/12	África
8		10.208.0.0/12	Reservado para uso futuro
9		10.224.0.0/11	Reservado para uso futuro

Fig. 4. Asignación de bloques por zonas geográficas.

Según este plan de direccionamiento práctico, el diseño de bloques de direcciones permite realizar una abstracción de la información de direccionamiento en base a cinco zonas geográficas principales: Europa, África, Asia-Pacífico, América del Norte y América del Sur. Cada una de esas zonas tiene asignado un único bloque de direcciones con la excepción de la zona europea a la que se asignan tres bloques de direcciones. Dicha circunstancia obedece al cumplimiento de una serie de restricciones de proyecto que se explican más adelante.

La Figura 5 muestra las cinco zonas principales en las que quedaría dividida la geografía mundial según el plan de direccionamiento práctico.

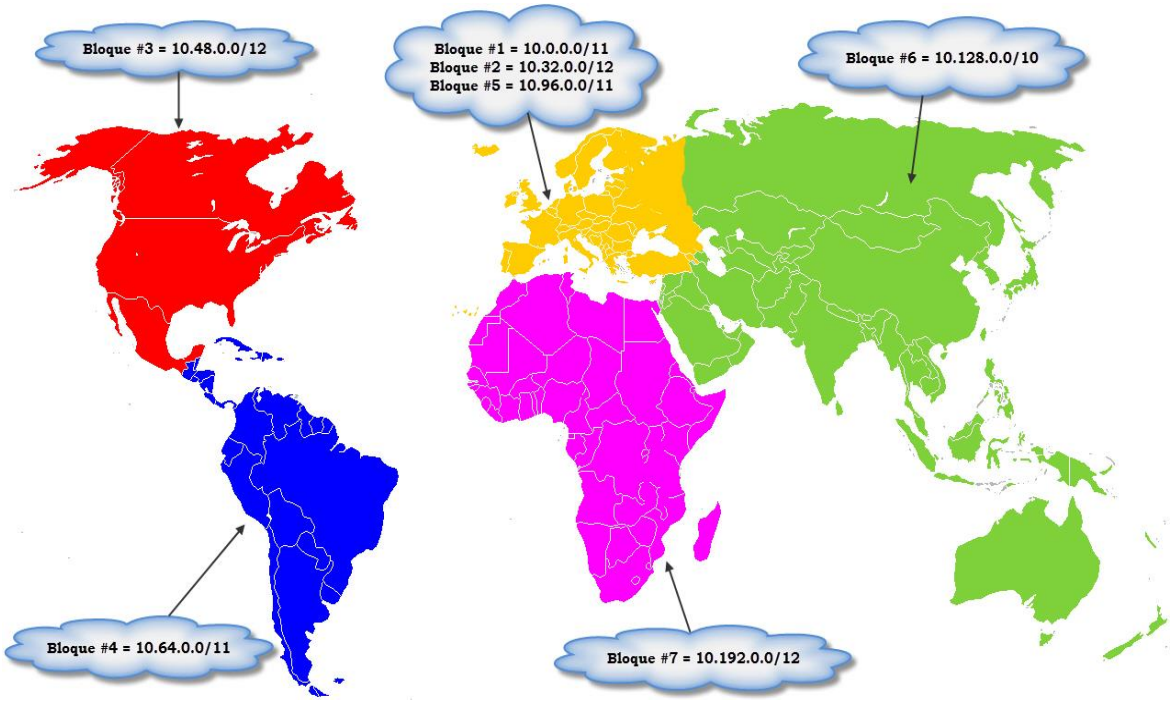


Fig. 5. Zonas geográficas principales según direccionamiento práctico.

La elección del plan de direccionamiento (o numeración) final está condicionada por una serie de restricciones impuestas por la empresa y por la propia actividad del negocio que Cosentino lleva a cabo. Las restricciones de proyecto son tres:

a) No modificar la numeración de red en *data centers.* Los *data centers* cumplen dos funciones fundamentales: proveer interconexión de nodos VPN y dar alojamiento a servicios críticos para la operación de la empresa. La modificación del direccionamiento en dichos *data centers* conlleva un alto riesgo, pudiendo causar el máximo impacto imaginable en la operación de la empresa.

b) No modificar la numeración en las secciones de red vinculadas con producción. La modificación de la numeración de red en las secciones de red que soportan las líneas de producción supone un alto coste de implementación puesto que precisa la intervención de mano de obra especializada y capacitada por el fabricante de la maquinaria. Asimismo, el cambio de direcciones conlleva un alto riesgo de provocar paradas en el proceso productivo. No obstante lo anterior, se hará una excepción en aquellos dispositivos numerados con direcciones IP públicas, los cuales serán migrados a rangos de IP internas.

c) Uso exclusivo de recursos internos a la compañía e implementación remota de las soluciones diseñadas. La empresa impone esta restricción con el fin de reducir los tiempos y costes de implementación del proyecto.

Considerando las restricciones de proyecto, la opción escogida para el plan de numeración que se llevará a la práctica es el plan de direccionamiento práctico. Dicho plan tiene como principales ventajas el hecho de que cumple con las pautas marcadas por la política de direccionamiento, es compatible con las restricciones del proyecto, tiene en consideración el direccionamiento de la red desplegada hasta el momento y da solución a los problemas detectados en la red. Frente a él, el plan de direccionamiento teórico, que sobre el papel es un diseño mucho más óptimo y elegante, no observa las restricciones de proyecto ni tiene en cuenta la numeración de la red actual. En consecuencia, la implantación de dicho plan sería muy traumática y elevaría enormemente los costes de implementación haciendo el proyecto injustificable e inviable.

IV. Fase de implementación

Una vez escogido el plan de direccionamiento a considerar se pasa a la implantación del mismo. Para llevar a la práctica el proyecto serán necesarios dos tipos de recursos: humanos y software:

a) *Recursos humanos*. Es el recurso que mayor coste representa. La mano de obra será necesaria para la ejecución del proyecto es de tres tipos:

- Supervisor de proyecto: técnico encargado de coordinar y dirigir las tareas del proyecto y el trabajo del resto de componentes del equipo.

- Equipo de red: grupo formado por dos técnicos de red con certificación CCNA, los cuales llevarán a cabo la mayor parte del esfuerzo de migración. Se requiere la mencionada certificación puesto que la VPN de Cosentino se compone íntegramente por electrónica de red fabricada por *Cisco Systems.*

- Equipo de *help-desk:* grupo formado por dos técnicos de soporte técnico que prestarán apoyo al equipo de técnicos de red en incidencias menores derivadas del cambio en las direcciones IP, tales como actualización de direcciones IP en aplicaciones que gestionen impresoras, escáneres, unidades de red, etc.

b) *Recursos software*. Para la realización de las diversas tareas en que se divide el proyecto será necesaria la utilización de diversas herramientas software:

- Software escáner de red, que permitirá analizar los equipos conectados a una determinada red antes y después de efectuar la migración de la misma.

- Emulador de terminal y navegador web, posibilitarán cambiar la configuración de red de los equipos conectados tales como *routers*, *switches*, *gateways* de telefonía, impresoras, escáneres y cámaras de seguridad, entre otros.

- Calculadora de subredes IP, que se utilizará para hacer los cálculos de *subnetting* para las distintas redes y subredes.

- Herramienta de soporte remoto, que posibilitará la conexión remota a computadoras de usuarios para la resolución de incidencias derivadas del cambio de direcciones IP.

- Herramientas auxiliares para documentación. La modificación de la red será considerable, por lo que será necesario producir una exhaustiva y detallada documentación que recoja el nuevo direccionamiento. Será necesario elaborar diagramas de red, listados de equipos, planes de implementación, tablas de correspondencia entre los rangos antiguo y nuevo, así como cualquier otro detalle relevante para poder llevar a cabo una adecuada gestión de red en el futuro.

Se establecen tres líneas de trabajo o tareas que darán como resultado la implementación de las soluciones diseñadas. Dichas tareas son las siguientes:

1) Migración de sedes remotas. La aplicación del plan de direccionamiento práctico acarrea la migración de un total de 52 sedes a nuevos rangos de direcciones. Dicha migración es realizada remotamente y requiere un análisis detallado de cada sede y una cuidadosa planificación. La estrategia de migración sin pérdida de gestión remota en los equipos hace necesario representar la topología de red de cada sede en una estructura en árbol donde el nodo raíz es el *router* VPN, los nodos intermedios son los *switches* y los nodos hoja los dispositivos finales (impresoras, teléfonos IP, ordenadores, etc.). Una vez construida la estructura en árbol que representa la red de la sede se procede al cambio en las direcciones IP siguiendo un orden en el cual, antes de migrar un nodo padre, se migrarán todos sus nodos hijos. El último nodo en ser re-numerado será el nodo raíz, esto es, el *router* VPN. Una vez migrado el *router* habrá un breve período de tiempo en que se carece de gestión remota, que se corresponde con el restablecimiento de los túneles VPN. Una vez restablecidos dichos túneles se recupera la gestión remota de los equipos conectados al nuevo rango de red.

2) Segmentación de la red WiFi del polígono industrial de Cantoria. Esta tarea o actuación consiste en modificar la configuración de la red física de dicho polígono generando dos nuevas VLAN de nivel 3 que proporcionarán sendas redes inalámbricas independientes que proveerán de un espacio de direccionamiento mayor. Esta parte del proyecto conlleva tareas de configuración adicionales que quedan fueran del alcance del mismo, siendo planteadas como una de las líneas de trabajo futuras.

3) Eliminación del direccionamiento público en la red interna. Esta última línea de trabajo comprende dos partes. La primera consiste en la modificación de la configuración de la red física del polígono de Cantoria para crear una nueva VLAN de nivel 3 con direccionamiento interno, a la cual serán migrados todos aquellos dispositivos numerados con direcciones IP públicas (rangos 1.0.223.0/24 y 1.0.224.0/24) y será responsabilidad del equipo de técnicos de red encargados del proyecto. La segunda parte del esfuerzo queda fuera del alcance de este proyecto, siendo transferida la responsabilidad de dicha migración al departamento de Automática Industrial, el cual se encarga de operar dichos dispositivos.

V. Conclusiones y líneas futuras

El grado de cumplimiento alcanzado para los objetivos marcados al principio del proyecto puede ser evaluado con total exactitud puesto que dicho proyecto ha sido implementado en su entorno real, es decir, en la red física de Cosentino. Recordemos que los objetivos de proyecto consistían en la resolución de los problemas y debilidades detectados en la etapa inicial del proyecto. El grado de éxito alcanzado en cada uno de ellos ha sido el siguiente:

1) Uso de direccionamiento público en la red interna. Este problema queda totalmente resuelto puesto que, con la cooperación del departamento de Automática Industrial, los dispositivos configurados con direcciones IP públicas han sido migrados a una VLAN de nivel 3 creada al efecto dentro del rango reservado para direccionamiento interno clase A (10.0.0.0/8).

2) Incorrecto criterio de asignación de números de red. Este problema queda totalmente resuelto puesto que la nueva política de direccionamiento y el plan de numeración que la concreta fijan un criterio consistente que permite numerar la red actual y la que se despliegue en el futuro.

3) y *4) Agotamiento del espacio de direcciones en sedes remotas y red WiFi de polígono de Cantoria*. Ambos problemas quedan totalmente resueltos puesto que el nuevo plan de direccionamiento provee prefijos de red con suficiente espacio de direccionamiento para las necesidades actuales y futuras.

5) Fragmentación del espacio de direccionamiento. En este último problema solo se alcanza una resolución parcial. El gran esfuerzo de re-numeración llevado a cabo permite "compactar" el espacio de direccionamiento gracias al diseño de bloques de direcciones consecutivas asignados por zonas geográficas. Sin embargo, aunque el alivio logrado es considerable, la solución total no es alcanzable debido a las restricciones de proyecto que limitan la sección de red susceptible de ser re-numerada.

Más allá de los objetivos alcanzados, seguidamente se esbozan una serie de mejoras futuras que pueden aplicarse en la búsqueda de la excelencia operativa de la red corporativa de Cosentino. Estas líneas de trabajo futuro son tres principales:

a) Mejoras en la interconexión de data centers: Para ello se propone la instalación de *routers* e interfaces virtuales adicionales que provean redundancia física y lógica respecto de la conectividad VPN. Con esta mejora se conseguirá mantener la red operativa de forma transparente en caso de fallo en alguno de los mencionados dispositivos y/o interfaces.

b) Mejoras en la eficiencia del enrutamiento: La re-numeración realizada permite realizar una abstracción de la información de enrutamiento muy potente. Se podrán diseñar distintos dominios de enrutamiento independientes y también podrán aplicarse técnicas de agregación de rutas propagando solo resúmenes de ruta entre los distintos dominios de enrutamiento. Esta medida acarreará una mejora considerable del funcionamiento de la red a nivel global.

c) Mejoras en la red WiFi del polígono de Cantoria: La segmentación de la red inalámbrica original en dos redes independientes (Fábrica, para el área de producción y almacenamiento, y Cosentino, para la zona de oficinas) permitirá distinguir dos grandes grupos de dispositivos con requerimientos de conectividad bien diferenciados. Esta división permitirá aplicar políticas de control de acceso diferenciadas así como posibilitará incrementar el nivel de seguridad al máximo soportado por los dispositivos conectados a cada una de dichas redes.

AGRADECIMIENTOS

A mis padres, Toñi, Antonio y José, por su inquebrantable apoyo.

A Pedro García Teodoro, por su rigor y ayuda como director de proyecto.

A Cosentino y la Universidad de Granada, por las facilidades en la realización del proyecto.

REFERENCIAS

[1] *RFC 791* "*Internet Protocol*": Estándar de Internet definido por el Instituto de Ciencias de la Información de la Universidad de California para el proyecto DARPA. Septiembre, 1981.

[2] *RFC 1219 "On the assignment of the subnet numbers":* RFC informativo escrito por Paul F. Tsuchiya. Abril, 1991.

[3] *RFC 1518 "An Architecture for IP Allocation with CIDR":* RFC histórico escrito por Yakov Rekhter y Toni Li. Septiembre, 1993.

[4] *RFC 1900 "Renumbering Needs Work":* RFC informativo escrito por Brian E. Carpenter y Yakov Rekhter. Febrero, 1996.

[5] *RFC 5887 "Renumbering Still Needs Work":* RFC informativo escrito por IETF (Carpenter, B.; Atkinson, R.; Flinck, H.). Mayo, 2010.

[6] *RFC 1916 "Enterprise renumbering: Experience and Information Solicitation":* RFC informativo escrito por Howard C. Berkowitz, Paul Ferguson, Will E. Leland y Philip J. Nesser II. Febrero, 1996.

[7] *RFC 1918 "Address Allocation for Private Internets":* Documento para descripción de mejor práctica actual escrito por Yakov Rekhter, Robert G. Moskowitz, Daniel Karrenberg, Geert Jan de Groot y Elliot Lear. Febrero, 1996.

[8] *RFC 2131 "Dynamic Host Configuration Protocol":* Documento RFC para seguimiento de estándar escrito por Ralph Droms. Marzo, 1997.

[9] *RFC 2071 "Network Renumbering Overview: Why would I want it and what is it anyway?"*: documento RFC informativo escrito por Paul Ferguson y Howard C. Berkowitz. Enero, 1997.

[10] *RFC 2072 "Router Renumbering Guide":* RFC informativo escrito por Howard C. Berkowitz. Febrero, 1997.

[11] *RFC 2101 "IPv4 Address Behavior Today":* RFC informativo escrito por Brian E. Carpenter, John Crowcroft y Yakov Rekhter. Febrero, 1997.

[12] *RFC 2791 "Scalable Routing Design Principles":* RFC informativo escrito por Jieyun Yu. Julio, 2000.

[13] *RFC 4632 "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan":* Documento para descripción de mejor práctica actual escrito por Vince Fuller y Tony Li. Agosto, 2006.

[14] *CCNA Routing and Switching 200-120 Official Cert Guide Library:* Wendell Odom, Cisco Press, 2013.

[15] *CCNP ROUTE 642-902 Official Certification Guide:* Wendell Odom, Cisco Press, 2013.

[16] *CCNP TSHOOT 642-832 Official Certification Guide:* Kevin Wallace, Cisco Press, 2013.

[17] *CCIE Routing and Switching Certification Guide. 4th Edition: Wendell Odom, Rus Healey y Denise Donohue, Cisco Press, 2012.*

[18] *Designing Cisco Network Service Architectures (ARCH) Foundation Learning Guide (CCDP ARCH 642-874):* John Tiso, Cisco Press, 2011.

[19] *Transmisión de datos y redes de computadores:* García Teodoro, P.; Díaz Verdejo, J.E.; López Soler, J.M. Pearson Educación, S.A. Madrid, 2003.

[20] *Calculadora de subnetting:* Disponible en: http://www.subnet-calculator.com/

[21] *Página web oficial de ICANN:* Disponible en: http://www.icann.org/

[22] *Página web oficial de IANA:* Disponible en: http://www.iana.org/

[23] *Página web oficial de IAB:* Disponible en: http://www.iab.org/

[24] *Página web oficial del Editor de documentos RFC:* Disponible en: http://www.rfc-editor.org/

[25] *Página web del IETF:* Disponible en: http://www.ietf.org/

[26] *Página web oficial de Cisco Systems:* Disponible en: http://www.cisco.com/

Autor Francisco Andrés Torrecillas Gilabert (Arboleas, 15 de Enero de 1978) es Ingeniero Técnico de Sistemas e Ingeniero en Informática (Universidad de Granada), Diplomado en Náutica (Universidad de Cádiz), Ciclo Superior Escuela Oficial de Idiomas (Inglés), Certificado de Aptitud Pedagógica, CCNA Routing & Switching.
A fecha de la realización del presente proyecto ejerce como administrador de redes en Cosentino.

Tutor Pedro García Teodoro es Catedrático de Universidad del área de Ingeniería Telemática de la Universidad de Granada. Tanto su labor docente como su labor investigadora se desarrollan en el campo de las redes de comunicación e Internet, en el cual ha realizado numerosas contribuciones en forma de libros, artículos en revista y ponencias en congresos, tesis y proyectos y contratos.

Identificación de dispositivos en redes inalámbricas mediante su huella RF

Autor: Alexander Quesada López, e-mail: alexql@correo.ugr.es
Tutor: Pablo Padilla de la Torre; e-mail: pablopadilla@ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—Este documento propone el uso de la huella RF de los dispositivos para la identificación de estos en redes inalámbricas. Tal procedimiento consiste en extraer la huella RF del dispositivo y compararla con las existentes en una base de datos con huellas de diferentes equipos, de modo que tras aplicar diferentes técnicas de comparación entre huellas sea posible determinar la identidad del dispositivo concreto. En este trabajo se comentarán los resultados hallados con diversas técnicas de comparación. También se expondrán varias aplicaciones y vías futuras asociadas a esta investigación.**

***Palabras clave*—RF Fingerprint, huella RF, redes inalámbricas, identificación de dispositivos, PLS, PCA, correlación, seguridad.**

I. Introducción

LOS último avances tecnológicos han provocado un gran desarrollo de las comunicaciones inalámbricas. Como consecuencia han surgido diversos sistemas o tecnologías inalámbricas cada vez más asequibles y accesibles a los usuarios ofreciendo grandes ventajas frente a los sistemas cableados. Pero a diferencia de los sistemas tradicionales de cableado, las redes inalámbricas hacen uso de un medio de propagación compartido y fácilmente accesible. Por tanto, este tipo de redes son más propensas a sufrir interferencias o amenazas de seguridad como pueden ser la intercepción de la información, suplantación de la identidad de las entidades de la red, saturación de la red y/o corte de servicio, etc.

Muchos de los ataques o amenazas anteriormente comentados pueden ser prevenidos o tratados con una correcta identificación de los dispositivos presentes en la red. Por ejemplo, los dispositivos sospechosos o detectados como maliciosos pueden ser incluidos en una lista negra que permita controlar, mitigar o prevenir los efectos ocasionados por tales dispositivos. Aunque ya existe una identificación a nivel MAC (Control de Acceso al Medio), esta puede ser fácilmente suplantada. En este contexto cobra mayor relevancia la identificación de dispositivos en la capa física basada en las características físicas en la transmisión de los propios dispositivos.

Al proceso para identificar los dispositivos en una red inalámbrica a través del análisis de las características de su señal RF al comienzo de la transmisión se le conoce como huella RF o *RF fingerprinting.* A través de las características de las señales RF se pueden definir los parámetros que permitan la identificación del dispositivo transmisor, dado que estas señales dependen de muy diversos factores que contribuyen a que sean únicas, como por ejemplo: proceso de fabricación (variación de la frecuencia del oscilador…), factores ambientales (temperatura, humedad…), fatiga o agotamiento del sistema transmisor, software controlador…

El sistema que se propone en este documento está basado en obtener la huella RF a partir de la potencia recibida del dispositivo que se quiere identificar. Como la raíz cuadrada de la envolvente de la señal recibida es proporcional a la señal recibida, analizando la potencia recibida en función del tiempo se pueden apreciar rasgos característicos que permitan la identificación del dispositivo. La potencia medida es la relacionada con la señal que emiten los dispositivos cuando analizan el medio en busca de redes, dado que siempre es la misma. Además esta señal se repite periódicamente aunque se esté conectado a la red.

Este sistema no es un método final que garantice una seguridad absoluta en la red, sino un procedimiento que junto a otros mecanismos de seguridad ya existentes pueda mejorar la seguridad de las redes inalámbricas. Este trabajo no está centrado en la implementación final de un sistema, sino en el análisis de las posibilidades y limitaciones del propio sistema para comprobar su viabilidad y fiabilidad. Se pretende ofrecer al lector una visión de esta tecnología de futuro comentando sus aspectos positivos y negativos.

Este documento se va a dividir en diferentes secciones. En la sección II se analizarán los objetivos propuestos en este estudio y la metodología llevada a cabo para alcanzarlos. En la tercera sección se presentarán y evaluarán los resultados obtenidos. Después, en la sección IV, se proponen varios escenarios de aplicación del sistema de identificación estudiada. En la sección V se exponen algunas vías de futuro para continuar y completar este trabajo. Y por último una sección dedicada a las conclusiones más importantes.

II. Objetivos y Metodología

En este apartado se van a concretar los objetivos que se desean alcanzar con esta investigación. Además se explicarán los métodos y procesos empleados para la obtención de los resultados que permitan alcanzar los objetivos fijados.

A. Análisis de Objetivos

El principal objetivo de la investigación asociada a este documento es proponer un sistema de identificación de dispositivos WiFi en red basado en su huella RF.

Debido a la imposibilidad de implementación del sistema en un entorno real, se ha optado por extraer las huellas RF de los dispositivos y constituir una base de datos en MATLAB. Con esa base de datos se ha simulado el comportamiento del

sistema de identificación con diversas técnicas de comparación y se ha efectuado un análisis del sistema. La finalidad del análisis era determinar las ventajas e inconvenientes de cada una de las técnicas de comparación de señales usadas. Adicionalmente se ha profundizado en el funcionamiento y fiabilidad del sistema, pudiendo detectar varias deficiencias del sistema que se dejan indicadas y se propone su superación en investigaciones futuras, y también algunas propiedades positivas que eran desconocidas.

B. Escenario Experimental

Para obtener las huellas RF de los dispositivos y descargarlas en el PC para trabajar con ellas, se ha hecho uso del despliegue de la Fig 1. Compuesto por el analizador de espectros de R&S al que se conecta una antena monopolo centrada en 2.4GHz y el dispositivo de prueba.

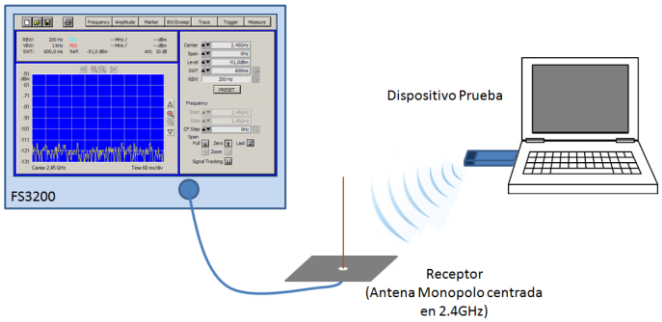


Fig 1. Escenario Experimental para la extracción de la huella RF.

En este caso el analizador de espectros debe de configurarse como analizador en el tiempo, haciendo uso de la opción 'zero-span'. Dicha opción implica una contracción del espectro de frecuencia y una expansión en el tiempo, resultando un analizador temporal de envolvente de señales.

C. Captura y Normalización de la Huella RF

Con la ayuda del montaje anterior es posible extraer la huella RF de los dispositivos y trabajar con ella en MATLAB. Tal procedimiento consta de los siguientes pasos:

1. Visualización en el PC receptor de la señal recogida por la antena.
2. Iniciar la búsqueda de redes en el dispositivo prueba.
3. Al instante se visualizarán los picos de potencia correspondientes a la señal emitida por el dispositivo prueba que constituyen la huella RF. Justo en ese instante se debe de pausar el barrido y descargar las muestras.

Tras este proceso la señal capturada nunca empezará en el mismo instante y por tanto su comparación no será del todo efectiva. Para que todas las señales empiecen en el mismo instante deberán de ser normalizadas, para ello se representa la señal en MATLAB y se fija un umbral. La primera vez que se sobrepase el umbral será la primera muestra de dicha huella RF y los valores anteriores se agregarán al final como ruido.

De este modo se emula el comportamiento del detector en una implementación real. Dicho detector empezará a muestrear la potencia recibida cuando se sobrepase un valor umbral fijado. En las siguientes figuras se muestran la diferencia entre las huellas RF antes y después de ser normalizadas.

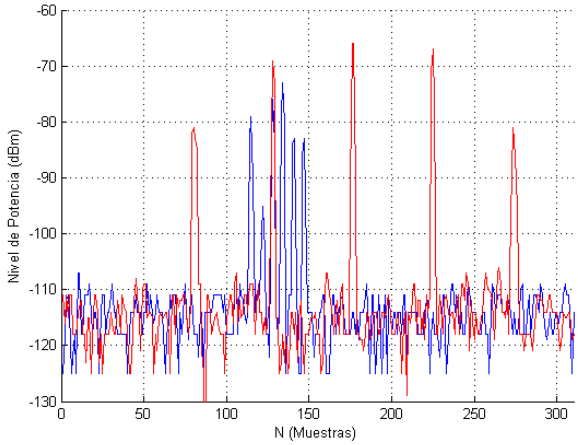


Fig 2. Dos muestras de huellas RF sin normalizar (dispositivos diferentes).

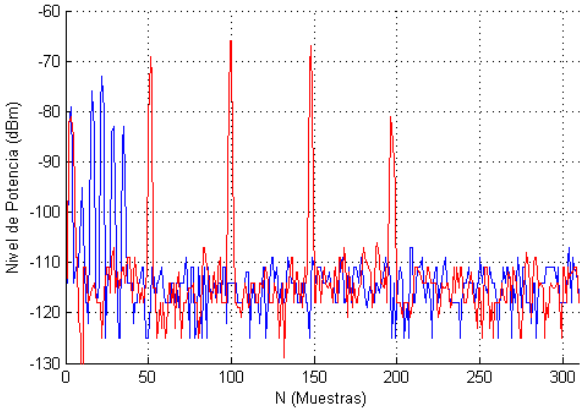


Fig 3. Dos muestras de huellas RF normalizadas (dispositivos diferentes).

Las diferencias entre las huellas RF apreciables en la Fig.8, se pueden usar para identificar al dispositivo. El problema es que al aumentar el número de dispositivos inevitablemente existirán huellas RF muy similares y se cometerán fallos en la identificación.

Otro dato relevante es que los principales patrones de la huella RF son repetitivos, sino sería imposible su identificación con este método. Por eso, aunque la señal recibida nunca será totalmente igual en las 17 veces que se obtiene, sí será muy similar. La duración de las huellas se ha fijado en 1 segundo.

D. Técnicas de Identificación

Tras normalizar las huellas obtenidas, estas se constituyen en una base de datos. La combinación de dicha base de datos y las técnicas de comparación de huellas permite extraer la huella de la BD más similar a una huella prueba (no existente en la BD). De modo que es posible asumir que el propietario de la huella prueba es el propietario de la huella extraída de la BD. Las técnicas empleadas son:

- Distancia entre señales:

$$d(h_{prueba}, h_i) = \sum_{n=1}^{N} \left| h_{prueba}(n) - h_i(n) \right| \qquad (1)$$

- Correlación entre señales:

$$r(h_{prueba}, h_i) = \frac{1}{N} \sum_{n=1}^{N} h_{prueba}(n) \cdot h_i(n) \qquad (2)$$

Para poder efectuar la comparación entre las huellas se debe de emplear la correlación normalizada:

$$\rho(h_{prueba}, h_i) = \frac{r(h_{prueba}, h_i)}{\frac{1}{N}\sqrt{\sum_{n=1}^{N} h_{prueba}(n)^2 \cdot \sum_{n=1}^{N} h_i(n)^2}} \quad (3)$$

De este modo se obtiene un valor entre [-1,1]. Cuando ρ=1 las señales serán iguales, mientras que si ρ=-1 las señales se encuentran fuera de fase. Por tanto la huella que ofrezca una correlación normalizada más cercana a 1 será la que se extraiga de la BD.

- Simplificación de media:

Se trata de reducir el número de señales existentes en la BD. Es decir, si existen 17 huellas por cada dispositivo en la BD, estas se sustituyen por una sola huella que es la media de todas las anteriores. De modo que se habría pasado de 17 huellas por dispositivo a una sola huella por dispositivo. Reduciendo considerablemente el tamaño de la BD. Esta simplificación se aplica combinada con las técnicas anteriores.

- PCA (Principal Components Analysis) y PLS (Partial Least Squares):

Consiste en realizar un cambio de base para que la información más relevante de las señales se encuentre en las primeras muestras. Con su uso se pretende reducir el número de muestras de las huellas maximizando la diferencia entre huellas.

El método PCA es no supervisado dado que no hace uso de ninguna estructura previa y trata de encontrar el subespacio que maximiza la varianza del conjunto de huellas. Mientras que PLS es un método supervisado porque intenta adaptarse lo mejor posible a un patrón dado, es decir, su objetivo es maximizar la diferencia entre las huellas siguiendo un patrón determinado (por ejemplo maximizar la diferencia entre huellas del dispositivos distintos).

III. Análisis de los resultados

Para llevar a cabo esta investigación se han empleado 42 dispositivos compatibles con la tecnología WiFi. Tras extraer 17 huellas de cada uno de ellos se ha constituido una BD, el proceso seguido ha consistido en extraer una huella (huella prueba) y aplicar las técnicas de comparación de señales con el resto de huellas de la BD. Cabe destacar que en el conjunto de dispositivos, se han considerado dos idénticos por fabricante cuando fue posible. Los resultados obtenidos son:

Tabla I
RESUMEN DE LOS RESULTADOS OBTENIDOS

Técnica Comparación	Prob. Ident. Dispositivos	Prob. Ident. Modelo	Prob. Ident. Fabricante	Prob. Ident. Tipo
Distancia sin simplificación	68,49%	70.58%	77,59%	94,60%
Distancia con simplificación	65,13%	78.67%	74,93%	90,06%
Correlación sin simplificación	69,75%	70.95%	82,77%	98,18%
Correlación con simplificación	70,73%	72.80%	82,21%	97,25%
Distancia más PCA	70,59%	72.86%	79,55%	97,78%
Distancia más PLS	74,51%	77.20%	83,33%	98,04%
Correlación más PCA	72,00%	77.20%	82,21%	98,18%
Correlación más PLS	71,85%	78.67%	82,21%	98,20%

A continuación de comentan los resultados obtenidos en cada uno de los casos estudiados: identificación del dispositivo concreto, del modelo del dispositivo, del fabricante del dispositivo, del tipo de dispositivo y otras pruebas efectuadas.

A. *Identificación del dispositivo concreto*

El primer caso de estudio es el más extremo dado que lo que se pretende es determinar la identidad del dispositivo concreto al que pertenece la huella prueba. La probabilidad de acierto total en la mayoría de las técnicas utilizadas es del 70% de éxito tras la identificación. El método de la distancia con simplificación de media es el que peores resultados presenta, esto se debe principalmente a la pérdida de información tras la simplificación con media.

El algoritmo de comparación basado en distancia con reducción PLS es que mejor probabilidad de éxito ha ofrecido (74,51%). Las probabilidades de acierto de las técnicas PCA y PLS dependen en gran medida del conjunto total de huellas y del número de componentes usado. Luego es posible que para otro conjunto de dispositivos y un número de componentes distinto la probabilidad de acierto máxima se obtenga con otra técnica de PLS o PCA.

Para este trabajo se han considerado 25 componentes en las técnicas de reducción (PLS y PCA) como solución de compromiso entre el tiempo de procesamiento (aumenta cuando crece el número de componentes) e información recogida en dichas componentes.

Este caso además de ser es el más extremo es el más interesante ya que es el más útil de todos. Aunque la probabilidad media de acierto se encuentra aproximadamente en el 75% no todos los dispositivos se identifican con la misma facilidad.

- Probabilidad de acierto superior al 90% en el 40% de los casos.
- Probabilidad de acierto inferior al 50% en el 28.5% de los dispositivos.
- Probabilidad de acierto del 70% para el resto de dispositivos.

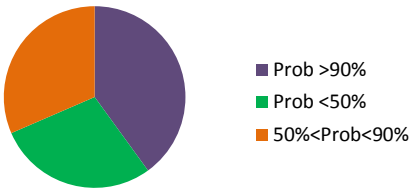


Fig 4. Distribución de probabilidades de acierto considerando el conjunto.

Las probabilidades bajas son debidas en gran parte a la similitud de las huellas de dispositivos dentro de un mismo modelo, fabricante o fabricante del sistema RF. Es decir, en algunos casos la huella entre dos dispositivos es tan similar que son prácticamente iguales y por tanto los errores cometidos son elevados. Esto no es una generalidad, dado que un alto índice de dispositivos del mismo modelo que son identificados muy fiablemente.

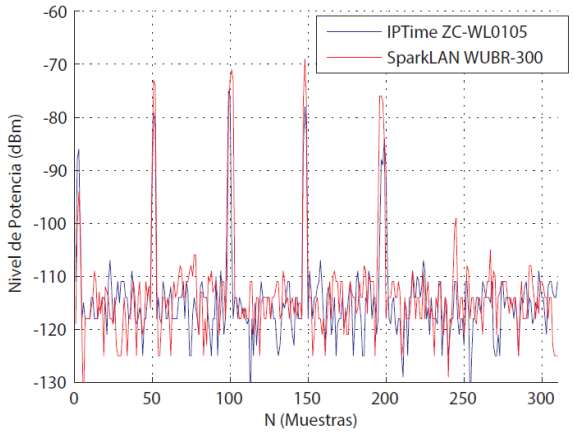


Fig 5. Dos dispositivos distintos con huellas RF muy similares.

B. *Identificación de dispositivos del mismo modelo*

La segunda situación analizada es el nivel de éxito al identificar un dispositivo concreto cuando se tienen varios dispositivos del mismo modelo. Ahora la probabilidad aumenta con respecto al caso anterior, siendo la técnica de distancia con simplificación de media la que mejor resultado muestra. Esto indica que la huella media de los dispositivos puede ser más representativa a la hora de diferenciar dispositivos del mismo modelo.

Por otro lado, los resultados con las técnicas PCA y PLS no son tan representativos ahora ya que estos dependen del conjunto total de dispositivos usados. Esto quiere decir que en ocasiones (para determinados terminales) se ha obtenido una probabilidad de error menor con el total de 42 dispositivos que con sólo dispositivos del mismo modelo.

Para realizar este estudio sólo se han considerado dispositivos de un mismo modelo y concretamente el estudio ha estado compuesto por 16 dispositivos distintos de 8 modelos diferentes. Para el mejor caso posible se ha obtenido:

- Dos modelos (4 dispositivos) con un 100% de éxito.
- Tres modelos (6 dispositivos) con más de un 75% de acierto.
- Tres modelos (6 dispositivos) con más de un 50% de acierto.

Por tanto para estos últimos 6 dispositivos se tiene una fuente de error muy importante debido a dispositivos del mismo modelo. En la mayoría de los casos se supera el 50% de probabilidad de acierto al azar.

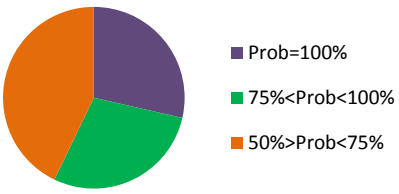


Fig 6. Distribución de probabilidades de acierto sólo con dispositivos del mismo modelo.

C. *Identificación de dispositivos del mismo fabricante y tipo*

También puede resultar interesante la posibilidad de poder averiguar el fabricante de un dispositivo mediante su huella RF. En este caso la probabilidad media de todas las técnicas se encuentra alrededor del 80% de acierto. Esto quiere decir que más de un tercio de los errores de identificación son debidos a la confusión con dispositivos del mismo fabricante.

De nuevo no todos los fabricantes son igual de válidos para aplicar el sistema de identificación, para la técnica con mejores resultados se tiene que:

- El 28.5% de los fabricantes presenta una probabilidad del 100%.
- El 33.5% ofrece una probabilidad comprendida entre el 75% y el 100%.
- El 28% entre el 50% y el 75%.
- El 10% una probabilidad menor al 50%.

En total se han empleado 21 fabricantes diferentes.

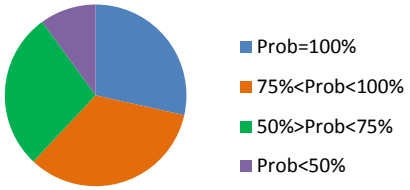


Fig 7. Distribución de probabilidades de acierto de fabricantes.

Por último, se ha estudiado la probabilidad de determinar correctamente el tipo del dispositivo del que se trata obteniendo en la mayoría de los casos una probabilidad de acierto del 98% y por tanto unos resultados bastantes fiables.

D. *Otras Pruebas Realizadas*

Para finalizar con los resultados, se ha efectuado una serie de pruebas para analizar situaciones o casos inicialmente no consideradas, obteniendo las siguientes conclusiones:

1) Si el dispositivo actúa como punto de acceso su huella RF no cambia y además se puede detectar periódicamente por las estaciones base y comprobar la identidad del AP.
2) Si cambia la dirección MAC, que es el principal problema del la identificación con MAC, la huella RF no sufre modificaciones y el dispositivos se sigue reconociendo con la misma probabilidad de acierto.
3) Cuando se modifica el controlador o sistema operativo la huella sufre variaciones (como se ve en la Fig.8) que puede provocar errores de identificación. También es cierto que el cambio de la huella RF no es radical.

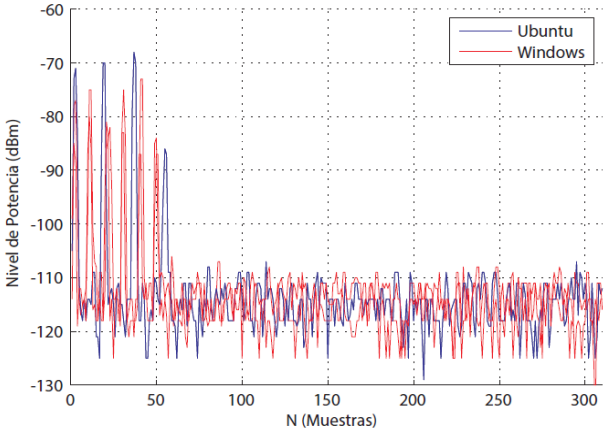


Fig 8. Huellas de un mismo dispositivo con diferentes S.O.

IV. Aplicaciones

La posibilidad de determinar la identidad de un dispositivo en la capa física, sin necesidad de que este se encuentre dentro de la red da lugar a multitud de aplicaciones. Como ejemplo se comentan algunas de las que pueden resultar más interesantes.

A. *Redes Ad-hoc*

En estas redes no hay una entidad o infraestructura que haga de punto de acceso, sino que las estaciones se comunican directamente entre sí. Y por tanto, la aparición de un nodo malicioso en este tipo de redes puede ser crítica, sobretodo porque los protocolos de routing son muy vulnerables. El sistema puede ser una gran herramienta para la detección y aislamiento de estos nodos maliciosos.

Si se detecta que un dispositivo ha provocado un ataque, este se incluye en una lista negra. Entonces el resto de nodos, tras consultar dicha tabla, pueden identificarlo mediante su huella RF y no encaminar paquetes hacia el nodo que ha ocasionado el fallo de seguridad. El administrador de la red debería de fijar los parámetros para que un nodo aparezca en una lista negra.

Otra posible solución, es configurar los nodos para que únicamente se comuniquen con un conjunto cerrado de dispositivos. La aparición de un nuevo dispositivo en la red provocará un fallo de identificación y no podrá formar parte de la red. De este modo se aísla la red frente a la aparición de futuros nodos sospechosos.

En general, se puede emplear como herramienta de seguridad en situaciones en las que sea necesario determinar la identidad de los dispositivos sospechosos.

B. *Operador Inalámbrico*

En la actualidad existen multitud de pequeños operadores que dan servicio de Internet a los clientes de forma inalámbrica con tecnología WiMAX o WiFi. En algunos casos el sistema está compuesto por un modem y un router, y la MAC de dicho router es la que limita el acceso. Además, estas redes no tienen ningún sistema de seguridad WEP, WPA o WPA2 por lo que cambiando la dirección MAC por la de un router de acceso a la red se puede acceder sin problemas y tener servicio de Internet. En este tipo de redes, nuestro sistema puede ayudar a corroborar que las direcciones MAC son las correctas mediante la comprobación de la huella RF de los dispositivos o a través de la identificación del modem. De este modo se evitarán accesos no deseados.

Esta aplicación se puede extender a cualquier red cuyo acceso se encuentre limitado por un filtrado MAC, garantizando que dicho filtrado sea mucho más fiable.

V. Vías Futuras

La identificación mediante la huella RF es una tecnología novedosa y en desarrollo. Luego hay mucho trabajo aún por realizar y concretamente en este sistema aún hay muchos aspectos interesantes y mejoras que deben ser tratados para que el sistema sea más eficaz. A continuación se comentan algunas de las vías futuras de investigación relacionadas con el sistema propuesto.

A. *Aplicación a otras tecnologías*

Una buena forma de continuar la línea propuesta en este documento sería comprobar la posibilidad y eficacia de este sistema de identificación en otras tecnologías inalámbricas, como por ejemplo: Bluetooth, Zigbee, WiMAX, entre otras. A modo ilustrativo se han capturado la huella RF de dos dispositivos Bluetooth y existe una diferencia importante entre ambas que parece indicar que este sistema es extrapolable a dicha tecnología.

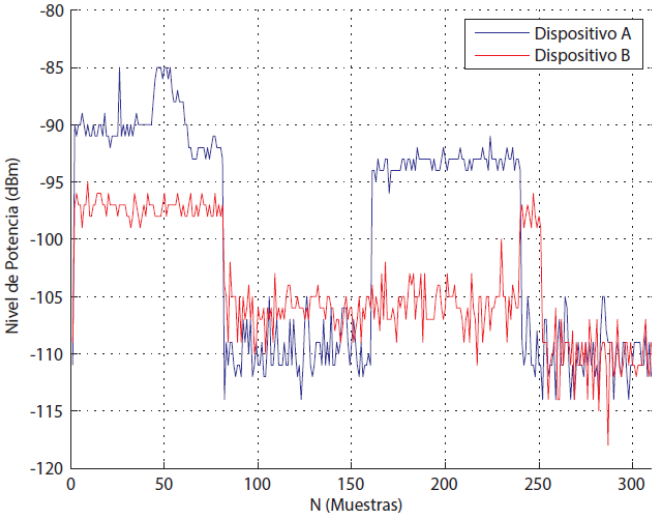


Fig 9. Comparativa huellas RF Bluetooth.

B. *Posibles mejoras*

Otro campo de interés puede ser el estudio de técnicas de comparación de señales que permitan obtener probabilidades de identificación aún mayores. Se proponen las siguientes mejoras:

- Estudio del problema en el ámbito de la frecuencia.
- Incluir sistemas de peso a la hora de decidir la identidad del propietario de la huella. Es decir, no tomar la decisión únicamente en base a la huella que más similitud presente. Por ejemplo, considerar las 5 huellas más cercanas a la huella test y tomar la decisión en base a la identidad de dichas huellas.
- Por diversos factores la huella de un dispositivo puede ser cambiante, como por ejemplo un aumento de la temperatura o la lluvia en entornos de exterior. Por este motivo puede resultar interesante tener una base de datos dinámica. Esto es, que la base de datos se actualice automáticamente dándole un determinado peso a las últimas muestras capturadas. Si se le da demasiado peso, una mala identificación puede dejar inservible nuestra base de datos.
- El conjunto de dispositivos de una red es algo dinámico y que cambia con mucha frecuencia. Luego la situación de tener únicamente los 42 dispositivos no se aproxima a la realidad. Esto quiere decir que haría falta mecanismos para determinar cuando un dispositivo es nuevo y poder almacenar su huella en la base de datos existente.

- La antena empleada y las condiciones de captura de las huellas no son las óptimas. Dado que la antena no ofrece unas prestaciones demasiado elevadas y las medidas se han realizado en la ETSIIT, donde hay un gran número de usuarios haciendo uso de la red WiFi de la UGR y la señal capturada es propensa a sufrir interferencias. Se podría emplear una antena mucho más directiva y con mayores prestaciones en un entorno aislado. Entonces los resultados obtenidos serán mejores. No obstante, el proceso de captura efectuado se aproxima más a una situación real.

- Estudiar la dependencia de la huella RF con el sistema operativo, controlador software y cambio de opciones de configuración para evitar o corregir fallos en el sistema de identificación.

- Reducir el tiempo de procesamiento tan elevado de las técnicas de reducción PCA y PLS aumentaría las prestaciones ofrecidas por nuestro sistema, dado que el tiempo de espera actual es inadmisible.

- Otro aspecto que no ha sido tratado y que es muy importante es la movilidad. Es decir, cómo afecta la localización y movimiento relativo de los dispositivos a la huella capturada por el punto de acceso. Hoy en día la mayoría de las redes inalámbricas se caracterizan por permitir cierta movilidad dentro del alcance de la red. Luego no sería apropiado que nuestro sistema dejará de ser fiable cuando cambia la localización del dispositivo.

VI. Conclusiones

El objetivo de este trabajo era proponer un sistema de identificación para dispositivos en una red WiFi basada en el estudio de señales de RF. La propuesta se ha realizado siguiendo los pasos descritos a continuación.

Inicialmente se puso de manifiesto la necesidad de la identificación de los dispositivos en la capa física. Y como solución a dicho problema se planteó el uso de la huella RF.

Después se hizo un estudio de la situación de esta tecnología que destaca por ser algo novedoso y poco desarrollado.

El sistema concreto consiste en definir la huella RF como el nivel de potencia recibido en el tiempo por el dispositivo a identificar. Las huellas han sido capturadas para formar una base de datos que permita la clasificación de los dispositivos.

Se han aplicado diversas técnicas de comparación de señales para identificar los dispositivos. Obteniendo una probabilidad aproximada de acierto del 70% y que varía en función de la técnica empleada. Para la obtención de estos resultados se ha hecho uso de un conjunto de 42 dispositivos.

Aunque el sistema no es extremadamente fiable, se produce una mejora muy elevada desde un 2.381% a un 70%.

También se ha analizado el rendimiento del sistema a la hora de reconocer correctamente al fabricante y tipo de los dispositivos. Siendo muy significativo que en el 98% de los casos el tipo de dispositivo es determinado con éxito.

Tras estudiar el comportamiento del sistema se han efectuado diversas pruebas con algunos resultados positivos y otros negativos. Por ejemplo se ha probado la invariabilidad de la huella RF al cambiar la dirección MAC y la dependencia de la huella frente al controlador o sistema operativo que gestiona al dispositivo.

Agradecimientos

Este trabajo no hubiese sido posible sin la colaboración del profesor Pablo Padilla de la Torre y todas aquellas personas que han colaborado prestando sus dispositivos.

Referencias

[1] P.Padilla, J.L Padilla, J.F. Valenzuela-Valdés, J. Ramírez y J.M Górriz: “RF Fingerprint Measurements for the Identificaction of Devices in Wireless Communication Networks Based on Feature Reduction and Subspace Transformation”, Measurement Journal, Volume 58, pp.468-475, 2014.

[2] P. Padilla, J.L Padilla and J.F Valenzuela-Valdés, “ Radiofrequency identification of wireless devices base on RF fingerprinting”, Electronics , 24th October 2013, Vol.49, No.22, pp. 1409-1410.

[3] Ureten, O. and Seriken, N., “Wireless security through RF fingerprinting”, Canadian J. of Elect. And Comp. Eng., 32, (1), pp. 27-33, 2007.

[4] Rohde & Schwarz, CH 6:Using the R&S FS300, in: Spectrum Analyzer R&S FS300 Operating Manual, 8th edition,2004.

[5] Mendo, L, “Using the Spectrum Analyzer as an Educational Tool for Mobile Communications”, XXVII URSI National Symposium, 2012.

[6] Yuan, H.L., and Hu, A.Q:,”Preamble-based detection of Wi-Fi transmitter RF fingerprints”, Electron. Lett., 46 (16), pp.1165-1167, 2010.

[7] Aravind Venkataraman, “802.11 Fingerprinting to Detect Wireless Stealth Attacks”.11-20-2008, Georgia State University.

Alexander Quesada López. Nacido el 10 de enero del 1991 en Atarfe (Granada). Graduado en Ingeniería de Tecnologías de Telecomunicaciones por la Universidad de Granada en 2014.

Pablo Padilla de la Torre. Nacido en Jaén en 1982. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid en 2005, Doctor por dicha universidad en 2009, Doctor por la Universidad de Cádiz en 2012. Asistente de laboratorio en la Ecole Polytechnique Fédérale de Lausanne, Suiza, en 2007. Profesor de la Universidad de Granada desde 2009, en la actualidad es Profesor Titular de Universidad. Sus líneas de investigación son variadas, centradas en diseño y caracterización de sistemas de radiofrecuencia y antenas, estudio de rendimiento de redes inalámbricas o procesado avanzado de señal aplicado a distintos ámbitos, entre otros temas de interés.

Desarrollo de un algoritmo de asignación de espectro sobre entornos TVWS

Tutor: Pablo Ameigeiras Gutiérrez; e-mail: pameigeiras@ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

Autor: Manuel González Martín, e-mail: mgmarti@correo.ugr.es

***Resumen*— Uno de los retos para dar cabida al gran volumen de tráfico de datos móviles que se prevé en los próximos años es mejorar la eficiencia de uso actual del espectro electromagnético. Entre las opciones para alcanzar dicho objetivo está aprovechar las bandas de frecuencia que se encuentran sin usar en el espacio destinado a las emisiones de TV, para que puedan ser usadas por usuarios sin licencia. Dicha técnica es conocida como TV White Space (TVWS). El funcionamiento de pequeñas celdas usando canales TVWS sin licencia alguna representa un desafío de coexistencia debido a su despliegue no planificado, sus tecnologías de transmisión heterogéneas, y la escasez de canales TVWS en ciudades muy pobladas. Para gestionar el uso de estas bandas de frecuencia disponibles desarrollamos un algoritmo de planificación de canales, el cual pretende maximizar tanto el rendimiento global de la red como el rendimiento individual de cada uno de los nodos, de manera que se minimice la interferencia producida entre ellos. Además se tendrá en cuenta la posible interferencia producida por estaciones de TV primarias y se intentarán solucionar los problemas de justicia observados cuando dicha interferencia se recibe en los usuarios finales con un nivel de potencia considerable. Para conseguir tales objetivos se propone afrontar el problema mediante el uso de la teoría de juegos, desarrollando una función potencial exacta que capte nuestros objetivos, de manera que el sistema alcance un punto de equilibrio óptimo llamado equilibrio de Nash.**

***Palabras clave*— Asignación de espectro, eficiencia uso de espectro, interferencia electromagnética, teoría de juegos, TV White Space.**

I. INTRODUCCIÓN

SEGÚN estudios realizados, se prevé un gran aumento en el volumen de tráfico de las comunicaciones móviles en los próximos años. Cada vez es mayor el número de usuarios con dispositivos móviles de altas prestaciones, a la vez que aumenta el volumen de tráfico generado por cada uno de ellos [1]. Para poder dar soporte a tal crecimiento se deberá aumentar la cantidad de espectro electromagnético disponible, en lo cual se está trabajando a nivel global para establecer el uso de nuevas bandas de frecuencias destinadas a las comunicaciones móviles, así como conseguir una mejora de la eficiencia de uso del espectro y un aumento de estaciones base. En la actualidad, en la gran mayoría de países, las redes y aplicaciones inalámbricas están reguladas mediante una política de asignación de espectro fija: El espectro está regulado por el Estado, que administra y asigna la utilización de las diferentes bandas de frecuencia a distintas empresas, usuarios y/o servicios mediante autorización, permiso o licencia a largo plazo en amplias regiones geográficas. El espectro es un recurso escaso donde cada vez es más difícil encontrar bandas libres para el despliegue de nuevos sistemas, especialmente en las bandas por debajo de los 3 GHz, particularmente valiosas para los sistemas inalámbricos debido a sus favorables características de propagación. Sin embargo, estudios recientes llevados a cabo por la FCC (Federal Communications Commission de EEUU) han demostrado que gran parte del espectro licenciado asignado está infrautilizado, observándose grandes variaciones temporales y geográficas en su uso, con rangos de utilización desde el 15% al 85% [2]. Además, medidas recientes de utilización de espectro muestran que mientras ciertas partes son altamente utilizadas, otras permanecen prácticamente sin usar, incluso por debajo de los 3GHz. Con el objetivo de aumentar la eficiencia en la utilización del espectro disponible, la FCC propuso la apertura de ciertas bandas de frecuencia asignadas a televisión, para que puedan ser aprovechadas por usuarios no licenciados denominados Usuarios Secundarios. Dichas bandas corresponden a canales no utilizados en determinadas zonas del territorio llamadas TV White Spaces (TVWS). Varios países como EEUU o Reino unido han optado por hacer uso de esta técnica y actualmente se está estudiando la posibilidad de implementarla en el resto de países de la Unión Europea. Es de esperar entonces que el uso de TVWS mejore en gran medida la eficiencia de uso del espectro electromagnético en la banda de TV, ya que se haría un aprovechamiento por parte de usuarios sin licencia de todas las frecuencias que se encuentran sin usar en cada punto concreto del territorio.

Por otro lado, al tratarse de un uso sin licencia cualquier nodo secundario podría emitir en el mismo canal que nodos vecinos, causando graves interferencias que podrían hacer que cayera drásticamente el rendimiento de todos ellos. Debido a esta razón es de esperar que debamos añadir un sistema de asignación de espectro en este tipo de redes de manera que la interferencia provocada entre ellos disminuya lo máximo posible. En la actualidad este problema se intenta abordar de diferentes maneras, desde la creación de grandes bases de datos donde se almacena información referente a los

parámetros de transmisión que podrían usar los nodos secundarios (tales como frecuencia, potencia, esquema de modulación...) en función de su localización, tal y como se muestra en [3], hasta la ejecución de algoritmos de asignación de espectro que basándose en técnicas de escaneo de su propio entorno son capaces de decidir qué canal o canales usar en los distintos nodos.

Varios investigadores han estudiado este problema de coexistencia en TVWS y han propuesto diferentes algoritmos. En [4], Jankuloska propuso un algoritmo de asignación de canales y potencia de manera conjunta para los sistemas Wi-Fi operando en modo TVWS. Su solución se basa en la teoría de juegos y equilibrio de Nash, y su objetivo es maximizar el número de usuarios soportados. En [5], Ye expresó la coexistencia en TVWS como un problema de minimización de la interferencia total. En [6], Peng propuso reducir el problema de asignación de espectro mediante una variante de un problema de grafos de colores. Sin embargo, las soluciones basadas en grafos de colores están optimizadas para una topología fija, y necesitan ser actualizadas con cada cambio en la topología. En [7], Cao propuso un enfoque distribuido para la asignación del espectro en redes con cambios frecuentes en su topología, como las redes ad hoc móviles. Los mismos autores profundizaron en las arquitecturas de gestión de espectro distribuidas en [8], [9]. Aunque las soluciones en [7] - [9] son interesantes, en ellas se supone un modelo de interferencia simplista en el que la interferencia es modelada mediante una métrica binaria geométrica. En [10], se define el algoritmo SSCD cuyo objetivo es maximizar el throughput global de la red, basando su solución en la teoría de juegos alcanzando el equilibrio de Nash.

Se observó que los distintos algoritmos aquí mencionados tienen la peculiaridad de que la asignación de canales realizada con la finalidad de alcanzar sus objetivos hace que pueda existir una gran diferencia entre las capacidades ofrecidas por nodos vecinos de iguales características, haciendo que la asignación de canales realizada no sea justa. En este documento el término de "justicia" hace referencia a la igualdad entre el rendimiento ofrecido por nodos de características similares, y condiciones en su entorno muy parecidas debido a su cercanía. El hecho de tener en cuenta la justicia en este tipo de redes se debe a que en principio, al tratarse de nodos prácticamente idénticos, no debería existir ningún nodo preferente sobre otro. Por lo tanto la diferencia entre las capacidades ofrecidas por cada grupo de nodos situados en una vecindad cercana debería ser muy similar. En casos extremos en lo que existen altos niveles de ruido primario se ha llegado a observar que algunos algoritmos de asignación de canales, como puede ser el caso de SSCD, tienden a anular uno o varios nodos asignándole canales con muy baja SINR, con la finalidad de optimizar algún parámetro de la red prioritario en sus objetivos. Debido a ello, los usuarios situados en la zona de cobertura de dichos nodos prácticamente no tendrían acceso a la red o la capacidad máxima que podrían obtener sería inviable. Para evaluar este hecho se tiene en cuenta el valor de la capacidad obtenida en el "5% outage". Este valor indica la capacidad máxima que puede obtener el 5% de usuarios que se encuentran situados dentro de las zonas de cobertura con las condiciones más desfavorables. De esta manera, si un nodo queda anulado, el valor del outage 5% decae drásticamente.

El algoritmo aquí desarrollado se centra en realizar una asignación de canales en nodos secundarios donde se tenga en cuenta tanto el rendimiento global de la red como el rendimiento individual de cada uno de los nodos que la componen. Además se intentará paliar las deficiencias observadas en los algoritmos de asignación analizados previamente, minimizando la diferencia entre las capacidades ofrecidas por cada uno de los nodos de un vecindario concreto aumentando la justicia obtenida, así como aumentar el valor de la capacidad de 5% outage. Para ello se hará uso de la teoría de juegos y se desarrollará una función potencial exacta de manera que aseguremos que se alcanza el equilibrio de Nash. Finalmente se evaluará el rendimiento del algoritmo propuesto mediante la simulación de distintos escenarios de red con una herramienta destinada a tal fin.

II. Modelo Del Sistema

Vamos a considerar una red de pequeñas celdas operando en entornos TVWS. Estas celdas proporcionan acceso inalámbrico a los usuarios situados dentro de su región de cobertura, por lo tanto nos referiremos a estas celdas simplemente como nodos. Denotaremos el conjunto total de nodos en la red como $L=\{1,\ldots,l\}$, los cuales son controlados por un gestor de coexistencia (Coexistence Manager CM) [11] que les proporciona los parámetros de funcionamiento para permitir la coexistencia. Se asume que los nodos operan como dispositivos portátiles modo II, por tanto pueden indicar su geolocalización. Sin embargo, los terminales de usuario operan como dispositivos portátiles modo I, por lo que no tienen la capacidad de geolocalización. El gestor de coexistencia tiene información sobre la localización de cada nodo $i \in L$, pero no tiene ninguna información sobre la localización de los usuarios terminales. Asumiremos que los usuarios terminales están uniformemente distribuidos dentro de los rangos de cobertura de los distintos nodos, y que tanto éstos como los nodos emiten con una potencia de transmisión fija. Se tendrá en cuenta que la máxima potencia de transmisión es de 40mW en canal de TV adyacente y 100mW en canales no adyacentes. El gestor de coexistencia obtiene información sobre la lista de canales TVWS $K=1,\ldots,k$ disponibles en base al contenido de una base de datos TVWS. Representaremos el conjunto de canales usados por cada nodo $i \in L$ mediante un vector $\bar{s}_i=\{c_1,\ldots,c_j,\ldots,c_n\}^T$ donde $\forall j$ $c_j \in K$. Asumiremos también que cada nodo tiene un número determinado de radios disponibles que limita el número máximo de canales que cada nodo puede usar, es decir $\forall i$, $|\bar{s}_i| \leq r_i$ donde r_i es el número de radios disponibles en el nodo i-ésimo. Definimos la función $\delta(\bar{s}_i, c)$ para el nodo i y el canal c como:

$$\delta(\bar{s}_i, c) = \begin{cases} 0, & si\ c \notin \bar{s}_i \\ 1, & si\ c \in \bar{s}_i \end{cases} \quad (1)$$

Adicionalmente definiremos S_i como el conjunto de todas las posibles combinaciones de canales disponibles en el nodo i, y el espacio de combinaciones de canales S como el producto cartesiano del conjunto de posibles combinaciones de canales de cada nodo $S = S_1 \times \ldots \times S_i \times \ldots \times S_l$. Se asume que cada nodo $i \in L$ tiene una región de cobertura R_i, y los usuarios que reciben servicio del nodo i en el canal c localizados en un punto $(x,y) \in R_i$ tienen una relación de señal a interferencia (SINR) γ_i^c:

$$\gamma_i^c(x,y,\overline{s_1},\dots,\overline{s_\iota},\dots,\overline{s_l}) = \frac{g_i(x,y)\cdot P_{ic}}{I_c(x,y)+\sum_{\substack{\forall j\in L \\ j\neq i}} g_j(x,y)\cdot P_{jc}\cdot\delta(\overline{s_\iota},c)} \quad (2)$$

Donde I_c indica la interferencia de primario a secundario en el canal *c* más el ruido térmico, P_{ic} es la potencia de transmisión del nodo *i* en el canal *c*, y $g_i(x,y)$ es la pérdida de propagación desde el nodo *i* hasta la posición *(x,y).* Para simplificar nuestro modelo no se tendrán en cuenta efectos de desvanecimiento rápido en la SINR. La máxima tasa de transferencia de datos de un usuario en el canal *c* puede ser calculada mediante el teorema de Shannon como $W\ log_2\left(1+\gamma_i^c(x,y,\overline{s_1},\dots,\overline{s_\iota},\dots,\overline{s_l})\right)$, donde *W* es el ancho de banda del canal *c*. Definiremos también la función de probabilidad condicional de la SINR de un usuario que obtiene servicios del nodo *i* en el canal *c*, situado dentro de la región de cobertura R_i como $P_{\gamma_i^c}(\gamma_i^c/\overline{s_1},\dots,\overline{s_\iota},\dots,\overline{s_l})$, condicionado por la asignación de canales en el resto de nodos $\overline{s_1},\dots,\overline{s_\iota},\dots,\overline{s_l}$. De esta manera, podemos definir la capacidad meda que ofrece el nodo *i* en su región de cobertura R_i usando el canal *c* como:

$$f(i,c/\overline{s_1},\dots,\overline{s_\iota},\dots,\overline{s_l}) = \int_0^\infty W\log_2(1+\gamma_i^c)\ P_{\gamma_i^c}(\gamma_i^c/\overline{s_1},\dots,\overline{s_\iota},\dots,\overline{s_l})\ d\gamma_i^c \quad (3)$$

Suponemos que el CM tiene información sobre la potencia de transmisión y la localización de cada nodo ϵ *L*. Por tanto, podemos evaluar el nivel de señal recibido procedente de cada nodo en una posición dada. Damos por hecho que el CM puede usar esta información para estimar la capacidad media $f(i,c/\overline{s_1},\dots,\overline{s_\iota},\dots,\overline{s_l})$ mediante la integración de $W\ log_2\left(1+\gamma_i^c(x,y,\overline{s_1},\dots,\overline{s_\iota},\dots,\overline{s_l})\right)$ definida por el teorema de Shannon en la región de cobertura R_i.

III. Formulación Del Problema

En el escenario descrito anteriormente se observan dos fuentes de interferencia principales. En primer lugar encontramos la interferencia provocadas entre los propios nodos situados próximos entre sí, la cual denominaremos interferencia secundario a secundario. Por otro lado tenemos la interferencia provocada por la presencia de estaciones de TV de alta potencia, las cuales emiten parte de su potencia total de transmisión a los posibles canales TVWS adyacentes al de la estación. Esto es debido a la fuga de potencia que se realiza en canales adyacentes al principal, debido la pobre máscara de transmisión que poseen [12]. Este segundo tipo de interferencia lo denominaremos interferencia primario a secundario, y puede resultar especialmente perjudicial ya que en algunos casos pueden dejar a un canal concreto inutilizable. Es en esos casos cuando comienzan a observarse los problemas de justicia en la asignación de canales propuestas por los algoritmos analizados. En determinadas ocasiones con la finalidad de maximizar los objetivos correspondientes del algoritmo evaluado, algunos nodos no reciben ningún canal con una relación señal-interferencia aceptable en la asignación de canales recibida. Este hecho se produce principalmente cuando existe uno o varios canales de entre todos los canales disponibles con un alto nivel de ruido primario, ya que puede darse el caso en el que convenga asignar a un nodo el canal ruidoso con el fin de que no produzca interferencia secundario-secundario a sus vecinos.

El entorno en el que se pretende introducir el algoritmo que desarrollaremos es aquel donde los nodos secundarios a los que nos referimos se trata principalmente de pequeñas celdas destinadas a uso doméstico, haciendo uso de los canales libres TVWS en algún punto del territorio y algún espacio de tiempo concreto. Además al tratarse de un uso personal, los nodos pueden encenderse y apagarse aleatoriamente. Por lo tanto no podemos permitir que algún nodo entre en funcionamiento en la red y su asignación de canales recibida no contenga ningún canal con una buena SINR en comparación con el resto, o que la incorporación de un nuevo vecino cercano haga que decaiga por completo la capacidad de un nodo ya existente, ya que eso equivale a un grupo de usuarios insatisfechos en la red.

IV. Desarrollo Del Algoritmo

Tras una campaña de simulaciones en distintas situaciones y con distintos niveles de ruido primario se observó que podría resultar satisfactorio tener en cuenta la capacidad actual de cada nodo a la hora de realizar la asignación de canales que debería de usar cada uno de ellos, para así un nodo con menor capacidad tener preferencia a la hora de usar un canal sobre un nodo con alta capacidad. Es obvio que esta acción ayudaría a mejorar la justicia de la red, ya que beneficia a nodos con baja capacidad ayudando de esta manera a que ésta aumente. Además aseguraría que la introducción de un nuevo nodo, en cuyo momento no tendría asignado ningún canal y por lo tanto con capacidad actual nula, tenga la máxima preferencia a la hora de elegir los canales a usar.

En primer lugar partiremos de la siguiente función de utilidad, mediante la cual obtenemos una medida del beneficio obtenido con la estrategia de canales $\overline{s_\iota}$ usada por *i*:

$$U_i = \sum_{\forall j\in L}\left[\underbrace{\sum_{\forall c\in\overline{s_j}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l})}_{Cap.\ total\ nodo\ j,\ nodo\ i\ activo} - \underbrace{\sum_{\forall c\in\overline{s_j}} f(j,c|\overline{S_1},..,\emptyset,..,\overline{S_l})}_{Cap.\ total\ nodo\ j,\ nodo\ i\ inactivo}\right] \quad (4)$$

Para favorecer a los nodos con menor capacidad debemos hacer una transformación de la función de utilidad, de manera que un incremento infinitesimal de capacidad en una situación de baja capacidad obtenga un mayor beneficio que ese mismo incremento en una situación de alta capacidad. Es decir, el valor de la derivada de la función de utilidad respecto de la capacidad deberá ser inversamente proporcional al propio valor de la capacidad. Por lo tanto una buena opción sería aplicar la función logaritmo a la capacidad obtenida por cada uno de los nodos:

$$U_i(\overline{S_\iota}) = \sum_{\forall j\in L}\left[\log\left(\sum_{\forall c\in\overline{s_j}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\right) - \log\left(\sum_{\forall c\in\overline{s_j}} f(j,c|\overline{S_1},..,\emptyset,..,\overline{S_l}\right)\right] \quad (5)$$

La anterior expresión tiene el problema de que cuando se evalúe el segundo término de la sumatoria en el nodo *i* la capacidad obtenida es cero, ya que se evalúa teniendo en cuenta que dicho nodo tiene una estrategia con conjunto nulo. Si usamos un argumento nulo en la función logaritmo su resultado es menos infinito lo cual hace que prevalezca sobre el resto de cálculos y el resultado de la función de utilidad sería el mismo para todos los nodos, independientemente de la estrategia usada. Para evitar dicha indeterminación realizamos una transformación en la función de utilidad en la

que se aísle al nodo *i*, quedando de esta manera el problema solucionado:

$$U_i(\overline{S_\iota}) = \log\left(\sum_{\forall c\in\overline{S_\iota}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\right) + \sum_{\substack{\forall j\in L\\ j\neq i}}\left[\begin{array}{l}\log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\right) -\\ \log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\emptyset,..,\overline{S_l}\,)\right)\end{array}\right] \quad (6)$$

Así, la función de utilidad conceptualmente se define como el logaritmo de la capacidad obtenida en el nodo i con la estrategia seleccionada en dicho nodo, menos la degradación producida en el resto de nodos debido a la interferencia co-canal producida por el nodo i, también aplicando la transformación logarítmica. Una vez desarrollada la función de utilidad debemos asegurar que nos encontramos ante un tipo juego no cooperativo que sea potencial exacto. Estos tipos de juegos se caracterizan en que el sistema puede alcanzar un punto de equilibrio óptimo llamado equilibrio de Nash. Para demostrarlo se debe definir una función potencial P exacta que satisfaga: $U_i(\overline{S_\iota},\overline{S_{-\iota}}) - U_i(\overline{S_\iota}',\overline{S_{-\iota}}') = P(\overline{S_\iota},\overline{S_{-\iota}}) - P(\overline{S_\iota}',\overline{S_{-\iota}}')$. Para ello partiremos de la diferencia producida en la función de utilidad suponiendo dos estrategias diferentes, y a partir de entonces comenzar a desarrollar la ecuación hasta lograr la igualdad:

$$\begin{aligned}&U_i(\overline{S_\iota},\overline{S_{-\iota}}) - U_i(\overline{S_\iota}',\overline{S_{-\iota}}') =\\ &\log\left(\sum_{\forall c\in\overline{S_\iota}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\right)\\ &+\sum_{\substack{\forall j\in L\\ j\neq i}}\left[\begin{array}{l}\log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\right)\\ \boxed{-\log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\emptyset,..,\overline{S_l}\,)\right)}\end{array}\right]\\ &-\log\left(\sum_{\forall c\in\overline{S_{\iota'}}} f(j,c|\overline{S_1},..,\overline{S_\iota}',..,\overline{S_l}\,)\right)\\ &-\sum_{\substack{\forall j\in L\\ j\neq i}}\left[\begin{array}{l}\log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\overline{S_\iota}',..,\overline{S_l}\,)\right)\\ \boxed{-\log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\emptyset,..,\overline{S_l}\,)\right)}\end{array}\right] = \end{aligned} \quad (7)$$

$$\underbrace{\begin{aligned}&\log\left(\sum_{\forall c\in\overline{S_\iota}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\right)\\ &+\sum_{\substack{\forall j\in L\\ j\neq i}}\left[\log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\right)\right]\end{aligned}}_{P(\overline{S_\iota},\overline{S_{-\iota}})} -$$

$$\underbrace{\begin{aligned}&\log\left(\sum_{\forall c\in\overline{S_{\iota'}}} f(j,c|\overline{S_1},..,\overline{S_\iota}',..,\overline{S_l}\,)\right)\\ &-\sum_{\substack{\forall j\in L\\ j\neq i}}\left[\log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\overline{S_\iota}',..,\overline{S_l}\,)\right)\right]\end{aligned}}_{P(\overline{S_\iota}',\overline{S_{-\iota}}')} =$$

$$P(\overline{S_\iota},\overline{S_{-\iota}}) - P(\overline{S_\iota}',\overline{S_{-\iota}}')$$

Se ha marcado mediante un recuadro aquellos términos idénticos pero con distinto signo, de manera que pueden omitirse simplificando así la ecuación resultante. Una vez desarrollada la igualdad llegamos a un punto en el que podemos llamar función potencial al término resultante, dada por la siguiente definición:

$$P = \log\left(\sum_{\forall c\in\overline{S_\iota}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\right) + \sum_{\substack{\forall j\in L\\ j\neq i}}\left[\log\left(\sum_{\forall c\in\overline{S_j}} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\right)\right] \quad (8)$$

Reescribiéndola de forma que se evalúen de forma conjunta todos los nodos se puede simplificar aún más la ecuación de manera que la función potencial puede verse como:

$$P = \sum_{\forall j\in L}\left[\log\left(\sum_{\forall c\in K} f(j,c|\overline{S_1},..,\overline{S_\iota},..,\overline{S_l}\,)\cdot\delta(\overline{S_j},c)\right)\right] \quad (9)$$

Con esta función potencial, el modelo de juego maximiza la sumatoria $\sum_{i=1}^{L}\ln(x_i)$, donde x_i el valor de la capacidad obtenida en el nodo *i*. Tal y como se demuestra en [13] el vector de capacidades obtenido es el que optimiza la justicia proporcional en la red.

V. Resultados

Para realizar la evaluación del comportamiento del algoritmo, denominado como algoritmo Log en este apartado, se ha usado una herramienta de red facilitada por el Departamento de Teoría de la Señal, Telemática y Comunicaciones implementada en MatLab.

A. *Escenario de evaluación*

El entorno de despliegue considerado es un cuadrado de tamaño de 200m x 200m con un conjunto de 15 nodos distribuidos al azar sobre el área. El modelo de propagación elegido se basa al presentado en [14] para zonas suburbanas. Los canales disponibles se supone que son canales TVWS adyacentes, por lo que la potencia de transmisión de todos los nodos se establece en 40mW, con un ruido térmico de fondo establecido a -100 dBm para todos los canales considerados. Cada nodo *i* se supone que da servicio a una región circular con radio *Ri*. Esta región está centrada en la ubicación del nodo y tiene radios interior y exterior de 2m y 20m, respectivamente. El área del escenario de implementación se divide en pixeles del tamaño 1m x 1m. El simulador calcula la SINR y la capacidad de Shannon, en los píxeles de la región $Ri\ \forall i$. Con esta información, el simulador calcula la capacidad promedio de cada uno de los nodos, y el rendimiento de la red al 5% outage. Para una mayor generalidad de los resultados se realiza un promediado de 50 simulaciones de red diferentes en los que se varía únicamente la ubicación de los nodos. Se tomará el algoritmo DDSC [15] como referencia para realizar una comparativa de resultados.

B. *Resultados interferencia secundario a secundario*

Para comprobar la interferencia provocada entre secundarios se realizará un barrido en el número de canales disponibles variando el número de radios usados por cada nodo secundario. Se analizaran los casos en los que los nodos secundarios usen un máximo de 1, 2 y 4 radios, variando el número de canales disponibles desde 2 hasta 8.

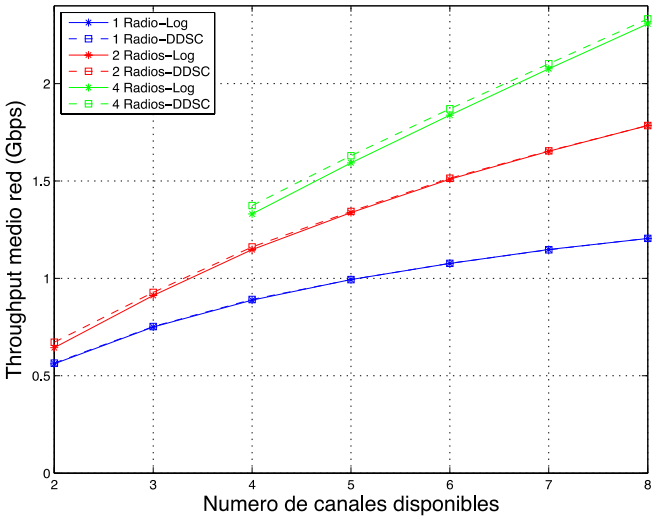


Fig. 1. Throughput medio de la red en función de los canales y radios disponibles en los nodos.

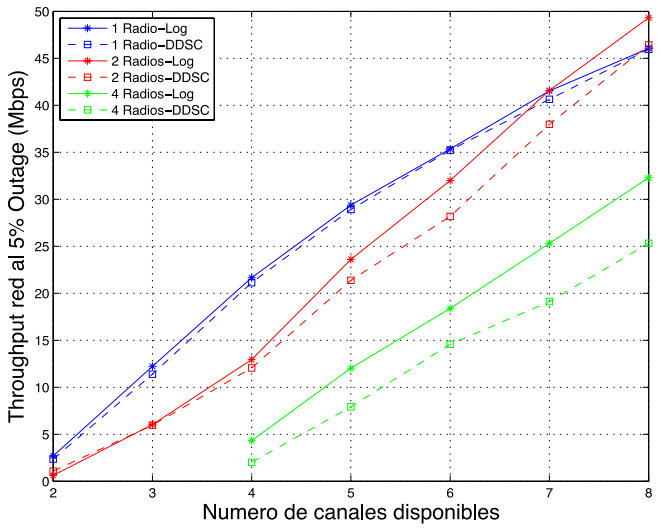


Fig. 2. Throughput 5% Outage en función de los canales y radios disponibles

Se puede observar como el nuevo algoritmo Log obtiene un throughput medio total ligeramente inferior al algoritmo DDSC, aunque la diferencia es mínima y únicamente se hace algo perceptible en el caso en que los nodos usan 4 radios. Sin embargo la mejora del outage al 5% sí que es más notable, especialmente en el caso de 4 radios, ya que en este caso se llega a aumentar hasta en un 100% cuando existen 4 canales disponibles.

C. Resultados interferencia primario a secundario

Para analizar el efecto producido por el ruido primario en el rendimiento de la red se establece un ruido de fondo a todos los canales de un valor de -100 dBm. A continuación el nivel de ruido se irá incrementando gradualmente en 1, 2 ó 3 canales hasta llegar a un valor máximo de -50 dBm, valor que podemos encontrarnos en la realidad en partes del territorio situadas a menos de centenares de metros o algunos kilómetros desde un emisor primario. En primer lugar analizaremos el caso de 4 canales disponibles y un radio máximo en los nodos, ya que los resultados obtenidos son similares al caso de tener 2 canales disponibles pero tenemos la opción de tener un mayor número de canales ruidosos. A continuación se analizará el caso de 6 canales y 2 radios para comprobar el funcionamiento del algoritmo con un mayor espacio de estrategias. Los resultados para 4 canales y 1 radio son los siguientes:

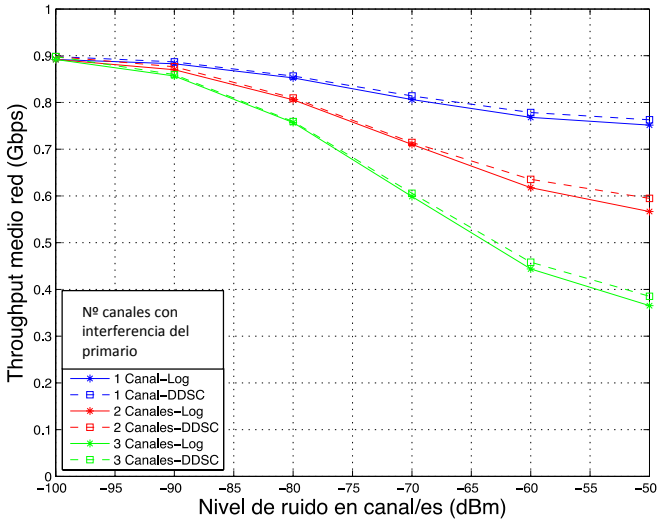


Fig.3. Throughput medio de la red, 4 Canales disponibles, 1 Radio

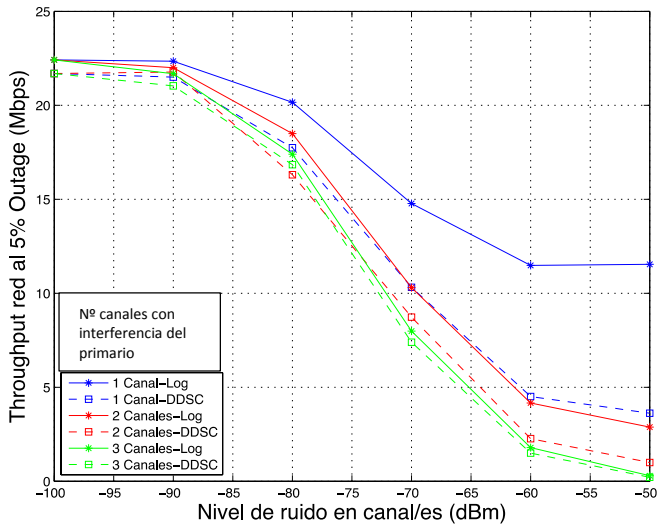


Fig. 4. Throughput 5% Outage, 4 Canales disponibles, 1 Radio

En todos los casos se ha obtenido un outage 5% superior con el nuevo algoritmo, haciéndose especialmente notable en el caso en el que existía un canal ruidoso de los cuatro disponibles. Un hecho interesante es notar que en el caso de usar el algoritmo Log, un sólo radio y un sólo canal ruidoso el outage 5% se estabiliza en un valor concreto (de unos 12 Mbps en este caso) a partir de que el nivel de ruido en dicho canal supere los -60 dBm. Este hecho es bastante interesante ya que nos asegura que a partir de un determinado nivel de ruido el algoritmo descarta absolutamente la posibilidad de asignar este canal ruidoso a ningún nodo, manteniendo una capacidad mínima en todos ellos aunque para ello se perjudique en pequeña medida el throughput total de la red. A continuación se muestran los resultados para 6 canales y 2 radios:

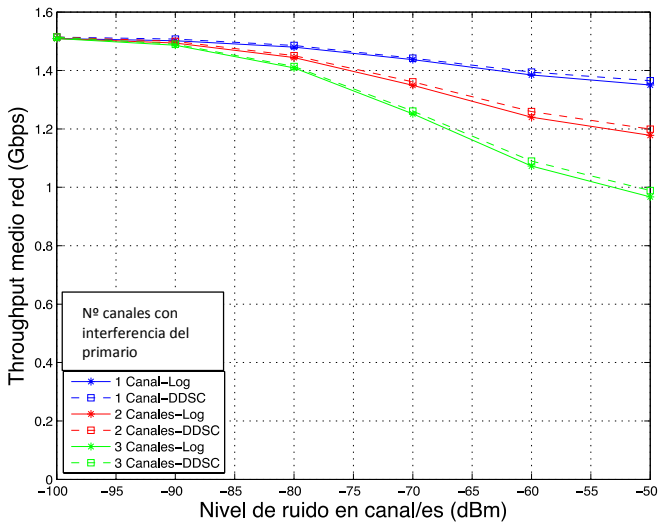


Fig. 5. Throughput medio de la red, 6 Canales disponibles, 2 Radios

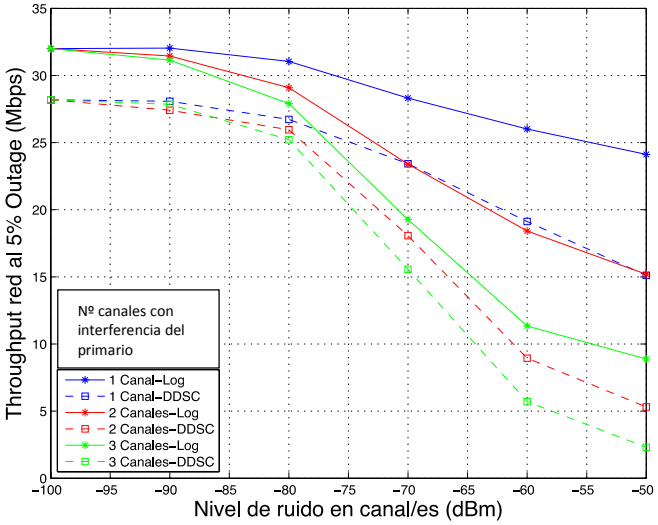


Fig. 6. Throughput 5% Outage, 6 Canales disponibles, 2 Radios

Como se comentó, al tener la posibilidad de usar 2 radios se amplía el espacio de estrategias posibles en los nodos y el efecto del uso de un algoritmo u otro se hace más perceptible en los resultados obtenidos. Como podemos ver el algoritmo Log ofrece un outage 5% muy superior de nuevo al algoritmo DDSC llegando incluso a superar el valor obtenido por éste incluso con un canal ruidoso menos. Cabe destacar que el algoritmo Log es capaz de ofrecer una capacidad de outage 5% aproximadamente igual al outage 5% ofrecido por el algoritmo DDSC con un canal ruidoso menos.

VI. Conclusiones

En este apartado se listan los resultados más relevantes según las campañas de simulaciones realizadas:

- Se ha conseguido maximizar conjuntamente la capacidad ofrecida tanto a nivel global de la red como a nivel de cada nodo individualmente. A pesar de que la capacidad alcanzada a nivel global no es la mayor posible, la diferencia relativa apenas es apreciable.
- El objetivo perseguido de la mejora de justicia ha sido conseguido. El hecho de evaluar la capacidad global de cada nodo en lugar de hacerlo por cada canal nos ha ofrecido la posibilidad de conocer el rendimiento total de cada nodo individualmente. De esta manera nos es posible realizar la asignación de canales en función de la capacidad actual de cada nodo
- El algoritmo aquí desarrollado tiene la capacidad para decidir por sí solo cuando debe ignorar la posibilidad de tener en cuenta un canal en las asignaciones posibles debido al alto nivel de ruido primario encontrado en él. Esta propiedad lo hace realmente interesante ya que facilita la gestión de la red al no tener la necesidad de omitir de la lista de canales disponibles los canales con alto ruido, encargándose el propio algoritmo de ignorar dichos canales.
- La propiedad anterior hace que se eviten las injusticias observadas en otros algoritmos de asignación, donde un nodo situado en una zona con varios nodos bastante próximos pueda quedar aislado usando canales con muy alto ruido primario.
- El hecho de dar preferencia a los nodos con menor capacidad hace que la incorporación de un nuevo nodo tenga la máxima preferencia a la hora de elegir su estrategia a seguir. De esta manera el nuevo nodo elegirá los canales que tengan la mayor SINR en su posición, alcanzado el equilibrio en la red en menor número de iteraciones y afectando su incorporación solamente a los nodos más próximos.
- Ya que la transformación en forma logarítmica realizada penaliza drásticamente la utilidad obtenida conforme la capacidad alcanzada por el nodo tiende a cero, prácticamente la totalidad de nodos obtiene una capacidad mínima bastante mayor al caso del algoritmo DDSC. Debido a ello el valor del outage 5% se ve maximizado en todos los casos.

Por lo tanto podemos considerar este algoritmo de asignación de canales como el adecuado para entornos TVWS donde exista una apreciable densidad de pequeñas celdas de uso personal de características similares, demostrándose que es aquél que alcanza la mayor justicia proporcional y minimiza la posibilidad de encontrarnos ante una situación indeseable.

Referencias

[1] http://www.cisco.com/web/ES/solutions/executive/cin.html

[2] Federal Communications Commission. Disponible: www.fcc.gov

[3] Mark Waddell, Kostas Tsioumparakis y Dave Darlington, "Construction of a TVWS database from DTT Coverage Data", BBC, UK, 2012. Disponible: http://downloads.bbc.co.uk/rd/pubs/whp/whp-pdf-files/WHP227.pdf

[4] B. Jankuloska, V. Atanasovski, y L. Gavrilovska, "Novel spectrum sharing algorithm for maximizing supported WiFi-like secondary user in TV white spaces", en *Proceedings of the 18th European Wireless Conference (EW)*, Abril 2012, págs. 1–7.

[5] B. Ye, M. Nekovee, A. Pervez, y M. Ghavami, "TV white space channel allocation with simulated annealing as meta algorithm", en *Proceedings of the 7th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, Junio 2012, págs. 175 –179.

[6] C. Peng, H. Zheng, y B. Y. Zhao, "Utilization and fairness in spectrum assignment for opportunistic spectrum access", *Mobile Network and Applications*, vol. 11, no. 4, págs. 555–576, Agosto 2006.

[7] L. Cao y H. Zheng, "Distributed spectrum allocation via local bargaining," en *Proceedings of the 2nd IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Network (SECON)*, Septiembre 2005, págs. 475–486.

[8] H. Zheng y L. Cao, "Device-centric spectrum management," en *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Noviembre 2005, págs. 56–65.

[9] L. Cao y H. Zheng, "Distributed rule-regulated spectrum sharing," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, págs. 130–145, Enero 2008.

[10] Pablo Ameigeiras, David M. Gutierrez-Estevez y Jorge Navarro-Ortiz, "Dynamic Deployment of Small Cells in TV White Spaces". Accepted in IEEE Transactions on Vehicular Technology.

[11] T. Baykas, M. Kasslin, M. Cummings, H. Kang, J. Kwak, R. Paine, A. Reznik, R. Saeed y S. Shellhammer, "Developing a standard for TV white space coexistence: technical challenges and solution approaches," *IEEE Wireless Communications*, vol. 19, no. 1, págs. 10–22, Febrero 2012.

[12] Farzad Hessar y Sumit Roy, "Capacity Considerations for Secondary Networks in TV White Space", EE. Department, University of Washington, EEUU, 2013.

[13] Byeong Gi Lee, Daeyoung Park y Hanbyul Seo, "Proportional Fairness Scheduling" en *Wireless communications Resource Management*, 2009.

[14] Y. Z. L. H. H. Villardi, G.P.; Chin-Sean Sum; Chen Sun; Alemseged, "Efficiency of dynamic frequency selection based coexistence mechanisms for tv white space enabled cognitive wireless access points," *Wireless Communications*, IEEE, vol. 19, pp. 69,75, December 2012

Despliegue de femtoceldas en entornos multioperador sobre *TV White Spaces*

Autor: Ana María López Pérez, e-mail: minidor@correo.ugr.es
Tutor: Jorge Navarro Ortiz; e-mail: jorgenavarro@ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—Este proyecto propone el uso de femtoceldas (por ejemplo LTE o LTE-Advanced) para realizar un traspaso/descarga de parte del tráfico de telefonía móvil en la banda de televisión (esquemas *backhaul*), logrando así reducir la sobrecarga existente en estas redes. Para ello se ha diseñado e implementado un simulador extensible y reutilizable que supone una solución completa al problema de reparto y negociación de canales en redes multioperador operando sobre los TVWS: creación del escenario de operación, estimación del modelo de propagación, extracción de parámetros y características, y cálculo de medidas de calidad como la relación señal a ruido más interferencia (SINR) y la tasa de transferencia (*throughput*).**

***Palabras clave*—TV White Space (TVWS), Compartición de Espectro, Teoría de Juegos, Femtocelda, Interferencia Cocanal, Equilibrio de Nash, Negociación.**

I. Introducción

El rápido crecimiento de los servicios de comunicación inalámbricos está provocando que el espectro radioeléctrico sea cada vez más escaso. Este incremento es verdaderamente espectacular para la telefonía móvil pues, según un informe presentado por Ericsson [1], se espera que entre 2011 y 2016 el tráfico de datos mundial en el móvil se multiplique por 10 (véase la fig. 1). Además este informe indica que estos nuevos usuarios se concentrarán en el espacio ya que se estima que el 60% del tráfico total se generará en el 1% del territorio del planeta. Esto puede ser un problema para la calidad de las conexiones y será para las operadoras y los fabricantes de móviles un reto el poder garantizar la calidad del servicio a los usuarios.

Los recursos limitados de espectro y la ineficiencia en su uso, debidos a que en la gran mayoría de países, las redes y aplicaciones inalámbricas están regulados mediante una política de asignación de espectro fija, necesitan un nuevo paradigma de las comunicaciones que explote los recursos radio de manera adecuada. Una propuesta que está tomando cada vez más protagonismo en la comunidad científica es el aprovechamiento de las zonas vacías o sin utilizar del espectro, para dar cabida a otro tipo de servicios que no son los legítimos de la banda de frecuencia.

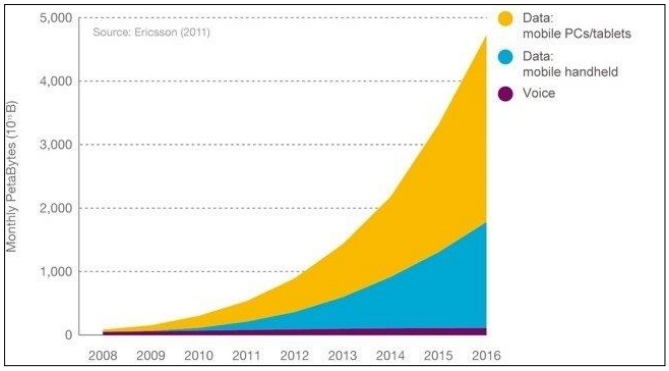


Fig. 1: Evolución en el uso del espectro.

En este sentido, un ejemplo que ya empieza a tomar cuerpo, sobre todo en Estados Unidos (EEUU), es el de los denominados "espacios en blanco" de televisión (*Television White Spaces*, *TVWS*). Éstos tratan de aprovechar aquellas zonas dentro de las zonas teóricas de cobertura del servicio de televisión, donde, por una u otra razón no exista señal, lo que dejaría esas frecuencias disponibles para otros usos o servicios.

En el presente proyecto se han utilizado los espacios en blanco de la banda de televisión, es decir, los TVWS, con objeto de diseñar y desarrollar algoritmos de asignación de frecuencias en entornos de interior para servir en apartamentos, zonas comerciales u oficinas, cobertura móvil mediante el uso de femtoceldas, evitando la posible interferencia entre ellas. Se ha elegido esta banda de frecuencias ya que de esta forma se logra evitar la interferencia con las estaciones celulares base y se aumenta el ancho de banda disponible. Además, el operar sobre los TVWS aporta un beneficio grandísimo, tanto para los operadores como para cualquier usuario, ya que se está adquiriendo una zona del espectro de forma gratuita.

Para lograr la coordinación entre femtoceldas, se ha utilizado una herramienta matemática que intenta resolver problemas de optimización de forma eficiente, la teoría de juegos. Fundamentándonos en esta teoría, se han llevado a cabo cinco modelos de negociación para realizar un reparto de canales entre diferentes operadores, con objeto de mejorar el rendimiento de los usuarios en la red y la calidad de las comunicaciones.

II. TEORÍA DE JUEGOS

El problema del reparto o asignación de canales se modela como una forma normal del juego, que matemáticamente puede ser definido por la tupla $\Gamma = \{N, \{S_i\}_{i \in N}, \{U_i\}_{i \in N}\}$, donde N es un conjunto finito de jugadores (femtoceldas), y S_i son un conjunto de estrategias asociadas con el jugador i (canales TVWS disponibles). Definimos $S = \times S_i,\ i \in N$ como un espacio de estrategia y $U_i : S \rightarrow \mathbf{R}$ como un conjunto de funciones de utilidad asociadas a las estrategias de los jugadores. Para cada jugador i en el juego Γ, la función de utilidad U_i es una función de S_i, la estrategia seleccionada por el jugador i, y el perfil de estrategia de sus oponentes S_{-i}.

Analizando la salida del juego y considerando que los jugadores toman decisiones independientemente y son influenciados por las decisiones de los otros jugadores, se busca definir si existen puntos de convergencia en un algoritmo de selección adaptativa en el que los jugadores no pueden desviarse (ya que bajaría su utilidad), por ejemplo en un equilibrio de Nash. Un perfil de estrategia para los jugadores, $S = [s_1, s_2, ..., s_N]$, es un equilibrio de Nash si y sólo si:

$$U_i(S) \geq U_i(s_i', s_{-i}), \forall_i \in N,\ s_i' \in S_i \quad (1)$$

Si el equilibrio en el perfil de estrategia (1) es determinista, existe una estrategia pura de equilibrio de Nash.

El rendimiento del algoritmo de adaptación depende significativamente de la elección de la función de utilidad que caracteriza la preferencia de los usuarios en un canal particular.

Se ha utilizado la función de utilidad propuesta en **[2]**. Ésta tiene en cuenta tanto la interferencia vista por un usuario al canal particular, como la interferencia creada por los vecinos al elegir un canal particular. Está pensada para utilizarse en escenarios donde los jugares operen de manera cooperativa. Matemáticamente queda definida por:

$$U_i(s_i, s_{-i}) = -\sum_{j \neq i, j=1}^{N} p_j G_{ij} f(s_j, s_i) - \sum_{j \neq i, j=1}^{N} p_i G_{ji} f(s_i, s_j)\ \forall i = 1, 2, ..., N \quad (2)$$

Haciendo uso de esta función potencial, el modelo de juego se basa en definir un orden de encendido aleatorio entre las femtoceldas del escenario, con el que se consigue emular la situación en la que los operadores encienden las femtoceldas en instantes de tiempo distintos y adquieren un canal tan pronto como se encienden. De esta manera establecemos un sistema de turnos, en los que, por cada turno, solo hay una femtocelda seleccionando un canal. Esta femtocelda seleccionará el canal, entre los disponibles, que maximice la función de utilidad y por tanto que minimice la interferencia con el resto de femtoceldas. Este proceso se repetirá hasta alcanzar la convergencia, es decir, aquel punto en el que todas las femtoceldas estén conformes con el canal que tienen asignado. Este reparto de canales se corresponde con la un máximo local (ninguna desviación unilateral mejora la utilidad de un jugador).

III. NEGOCIACIÓN

Suponiendo que los nodos de la red son los puntos de acceso o estaciones base, cuya posición es fija. Asumiendo que hay K canales disponibles para la transmisión, con K<N, y que cada nodo selecciona un único canal para su transmisión/recepción. Para una selección distribuida de la frecuencia de transmisión, el juego es capaz de construir eficazmente el mapa de distribución de canales con una interferencia cocanal reducida.

Un reto para implementar este juego potencial es que el proceso selección de mejor respuesta definido requiere de un coordinador para controlar las órdenes de juego de los usuarios. Con la falta de una infraestructura de control central en nuestro sistema, este proceso se debe implementar de forma distribuida. En nuestro esto lo conseguimos definiendo la toma de decisiones siguiendo el orden de encendido de las femtoceldas en la red. Para poder simular este tipo de situaciones se ha establecido una variable para controlar el orden de encendido, estableciendo éste de manera aleatoria. De esta manera el número esperado de usuarios que toman decisiones concurrentemente en una única iteración es 1, simulando por tanto un proceso de toma de decisiones secuencial. Para decidir que femtocelda es la que tiene permiso para seleccionar un canal en cada iteración se ha supuesto que cada operador dispondrá de entidad coordinadora encargada de gestionar el sistema de turnos.

A continuación vamos a describir cada una de las formas de operar de los operadores y el modo de negociar entre ellos.

NEGOCIACIÓN TIPO 1:

En este tipo de negociación los operadores actúan de forma cooperativa compartiendo toda la información entre sí. De manera que la forma de proceder en el juego es establecer un orden de encendido común para todos los operadores, los cuales irán encendiendo sus femtoceldas y eligiendo un canal entre los disponibles, que maximice la función de utilidad.

NEGOCIACIÓN TIPO 2:

En este tipo de negociación los operadores actúan de forma egoísta no compartiendo ningún tipo de información entre ellos. La forma de proceder será la de realizar negociaciones de tipo 1 de forma independiente por cada operador, disponiendo únicamente de la información de las femtoceldas de las que es propietario.

NEGOCIACIÓN TIPO 3

En este tipo de negociación emulamos situaciones en las que los operadores intercambian información entre ellos bajo ciertas condiciones. La forma de juego parte de situaciones en las que se ha realizado una negociación de tipo 2 y se permite el intercambio de canales entre operadores dentro de un área circular alrededor de una femtocelda. Esta femtocelda se corresponderá con la peor de cada operador considerando únicamente las femtoceldas bajo su control. Dentro de esa área se realizará una negociación de tipo 1, teniendo en cuenta que cada femtocelda tendrá información de las femtoceldas de su mismo operador y las femtoceldas que se encuentren dentro de esa área, que podrán ser de su mismo o de distinto operador. Este procedimiento se repetirá hasta que

se llegue a una situación de equilibrio en la que las femtocelda decidan no cambiar de canal.

NEGOCIACIÓN TIPO 4:

En este tipo de negociación se procede del mismo modo que en la negociación tipo 3, salvo que se establece que dentro del área definida, sólo podrán jugar las femtoceldas propiedad del operador que le toque el turno, si bien conocen la información de femtoceldas de otros operadores dentro de esa área.

NEGOCIACIÓN TIPO 5:

En este tipo de negociación emulamos situaciones en las que una entidad superior, en la que confían todos los operadores, conoce la información de todos ellos y se encarga de gestionar la selección de los canales. La forma de juego parte de situaciones en las que se ha realizado una negociación de tipo 2 y se permite el intercambio de canales entre operadores dentro de un área alrededor de dicha femtocelda. Esta femtocelda se corresponderá con la peor de cada operador considerando todas las femtoceldas del escenario. Dentro de esa área se realizará una negociación de tipo 1 gestionada por la entidad superior.

IV. Entorno de evaluación

En este apartado se va a describir la topología de los dos escenarios confeccionados: modelo *dual stripe* y modelo en *grid*.

1) Modelo dual stripe

Se trata de un sistema propuesto en el informe 3GPP TR 36.814 V9.0.0 **[3]** para modelar escenarios formados por femtoceldas en entornos urbanos de alta densidad. El modelo está formado por dos bandas de apartamentos cada una con dos líneas de *N* apartamentos. Las dimensiones de cada apartamento son 10m x 10m y existe una calle entre las dos bandas con un ancho de 10m. De manera que el escenario completo tendrá un tamaño total de 10(N+2)m x 70m. Un ejemplo de escenario puede verse en la fig. 2, estableciendo *N=10*.

Sobre este escenario se ha definido que es posible colocar una femtocelda en cada apartamento en cualquier posición del mismo. De esta forma resulta un escenario muy interesante para simular redes de aprovisionamiento de servicios celulares en zonas de interior para dar cobertura a un usuario específico, de forma similar a como se proporciona en un hogar cualquiera el servicio de Internet a través de routers inalámbricos WiFi.

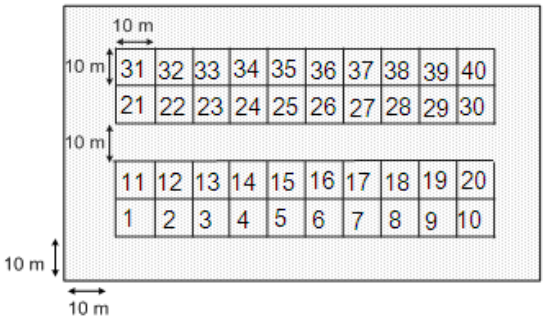


Fig. 2: Ejemplo de escenario 1.

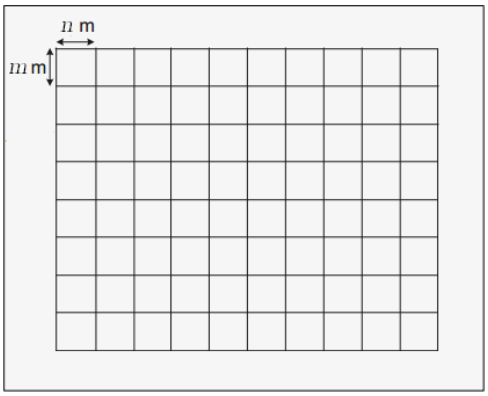


Fig. 3: Ejemplo de escenario 2.

2) Modelo en grid

Un modelo alternativo más sencillo se ha definido de la siguiente manera. Consideramos un espacio constituido por una sola planta sobre la cual se definen zonas de $n \times m$ metros cuadrados en las que está permitido colocar una femtocelda. Un ejemplo de este escenario se muestra en la fig. 3.

Este escenario toma especial transcendencia cuando se quieren simular espacios abiertos, zonas de oficinas o comerciales sobre las cuales se quiera proporcionar cobertura celular a través de femtoceldas.

V. Modelos de propagación

En este apartado realizaremos una breve descripción de los modelos de propagación utilizados a lo largo de todo el estudio. Los modelos de propagación son la herramienta que utilizamos para predecir de manera aproximada las pérdidas que se producen en un ambiente determinado.

Por ello, para cumplir todos los requisitos planteados en el proyecto se han elegido dos modelos de propagación distintos con los cuales se pueden predecir las pérdidas de propagación para escenarios operando sobre TVWS con capacidad para simular entornos urbanos en zonas de interior

1. Modelo dual stripe

Este modelo está asociado al escenario *dual stripe* y, de acuerdo a las características de éste, se establece una formulación diferente dependiendo de la zona del escenario en la que nos encontremos. Ésta viene recogida en la Tabla 1.

Misma banda de apartamentos que la femtocelda	$PL(dB) = 32.44 + 20\log_{10} d(m) + 20\log_{10} f(GHz) + 0.7d_{2d,indoor} + q * L_{iw}$
Fuera de la zona de apartamentos	$PL(dB) = \max(38.8 + 37.6\log_{10} R + 21\log f(GHz), 32.44 + 20\log_{10} d(m) + 20\log_{10} f(GHz)) + 0.7d_{2d,indoor} + q * L_{iw} + L_{ow}$
Distinta banda de apartamentos que la femtocelda	$PL(dB) = \max(38.8 + 37.6\log_{10} R + 21\log f(GHz), 32.44 + 20\log_{10} d(m) + 20\log_{10} f(GHz)) + 0.7d_{2d,indoor} + q * L_{iw} + L_{ow,1} + L_{ow,2}$

Tabla 1: Modelo de propagación *Dual Stripe* adaptado a toda frecuencia

Donde:

- L_{ii} representa las pérdidas por penetración de las paredes de separación entre dos apartamentos, con un valor de 5dB.
- El término $0.7d_{2d,indoor}$ tiene en cuenta las pérdidas por penetración debidas a las paredes interiores de un apartamento.
- L_{Ow} representa las pérdidas por penetración de las paredes externas, con una atenuación de 20dB.
- $L_{ow,1}$ y $L_{ow,2}$ son las pérdidas por penetración de las paredes externas de los dos apartamentos.

Para tener en cuenta las imperfecciones en la implementación de los componentes de RF y evitar un valor alto y no realista de SINR, se introduce un modelo EVM (*Error Vector Magnitude*), que impone un límite suave en el valor de SINR obtenido **[7]**. El EVM constituye una de las figuras de mérito más aceptadas para evaluar la calidad de un sistema de comunicaciones. En términos simples, hace alusión a cómo de lejos están los símbolos de la constelación recibidos de la constelación ideal que hubiera sido enviada por un transmisor ideal. EVM se define como un porcentaje del nivel máximo de SINR y se calcula como:

$$SINR_{max} = -20\log_{10}(EVM/100) \quad (3)$$

Como resultado de ésto, la SINR viene limitada por el EVM:

$$\frac{1}{SINR_{evm}} = \frac{1}{SINR_{\max}} + \frac{1}{SINR_{ideal}} \quad (4)$$

Un aspecto importante a señalar, debido a la inherente deficiencia de los sistemas de RF, es que las mejoras potenciales de SINR no se pueden conseguir completamente. Esto se debe a que, como se ha comentado, existen límites que vienen impuestos por las no idealidades, de los sistemas de trasmisión y recepción.
En la fig. 4 podemos ver un ejemplo de SINR obtenida tras aplicar EVM para todo punto del escenario para dos femtoceldas de las existentes en el escenario.

2. Modelo de propagación en interiores para TVWS

En esta sección se presenta un modelo desarrollado por Gabriel P. Villardi, que permite la estimación rápida y precisa de la interferencia potencial entre dispositivos vecinos que operan sobre los TVWS para realizar simulaciones por ordenador **[4]**.

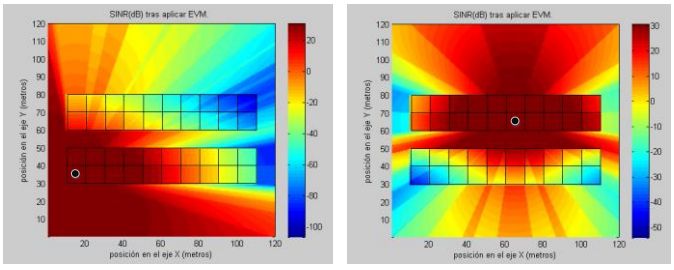


Fig. 4: SINR tras aplicar EVM para todo punto del escenario desde la femtocelda.

El modelo totalmente generalizado teniendo en cuenta la situación en que se encuentran tanto en los puntos de acceso interiores como efectos de sombras, independientemente de la zona suburbana específica, viene dado por:

$$P_r = 10\log_{10}P_t + 10\log_{10}G_t + 10\log_{10}G_r + 20\log_{10}h_r + 20\log_{10}h_t - 43.36\log_{10}d - A - 2B - C \quad (5)$$

Donde:

- B es el valor medio de la atenuación de casa o edifico. Según numerosas mediciones realizadas en **[5]**, se establecen valores de B de 17,7 dB para edificios comerciales (estructura de hormigón con refuerzo de acero) y de 5,4 dB para casas suburbanas (casa de madera estándar con revestimiento de papel y revestimiento de ladrillos en el exterior).
- C es una variable aleatoria gaussiana que tiene en cuenta los efectos de *shadowing* en el receptor en interiores. En **[5]** se establecen valores para C de 9,3 dB y de 6,4 dB, para edificios comerciales y para residencia suburbana, respectivamente.
- $\overline{P}$ y $\overline{\overline{P}}$ representan el nivel de la señal recibida en dB y d es la distancia entre el transmisor y el receptor en metros.
- A es el factor de atenuación suburbana. En **[5]** se establece un valor de 19.26 dB para este factor. Cabe señalar que nuestro objetivo es modelar la interferencia entre los puntos de acceso de radio portátil que operan en los TVWS, por lo que estamos interesados en la PIRE.

VI. Resultados

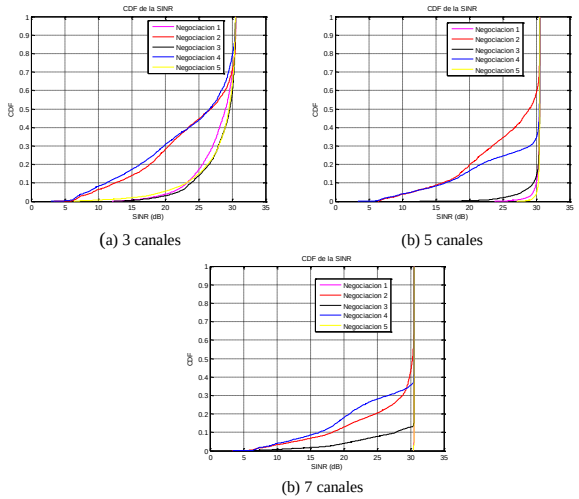
A modo de ejemplo se van a comentar los resultados obtenidos una topología en la que existe una red de femtoceldas constituida por cinco operadores diferentes, se van a mostrar los resultados obtenidos para un escenario en grid en el que existen 5 operadores diferentes con 6 femtoceldas cada uno de ellos.

En las figuras 4 y 5 se muestran, respectivamente, la CDF de la SINR y la CDF del *throughput*, para una de las 50 simulaciones realizas.

Los resultados obtenidos al aplicar las negociaciones de tipo 1, 3 y 5 son muy similares entre sí. De modo que la calidad de servicio media recibida en los apartamentos, al aplicar estos tipos de negociación, será muy similar.

Por otro lado, la diferencia entre el 5 percentil y 95 percentil, es mayor para la negociación de tipo 1 que para las negociaciones de tipo 3 y 5. Se obtienen valores muy próximos para casos en los que existen 3 canales disponibles y aumentando la diferencia hasta el 35% para casos en el que existen 7 canales disponibles. Este efecto es mayor que para la topología en la que existen 3 operadores. Esto implica que en las negociaciones de tipo 1 y 5, la calidad de servicio prestada a todos los usuarios del escenario es muy similar. No obstante, los resultados obtenidos con la negociación de tipo 3 son buenos, puesto que el peor de los casos (3 canales disponibles) tan sólo el 5% de los usuarios dispondrán de un *throughput* inferior a 43,32 Mbps y una SINR inferior a 21,65. Estos valores se corresponden con los obtenidos en las

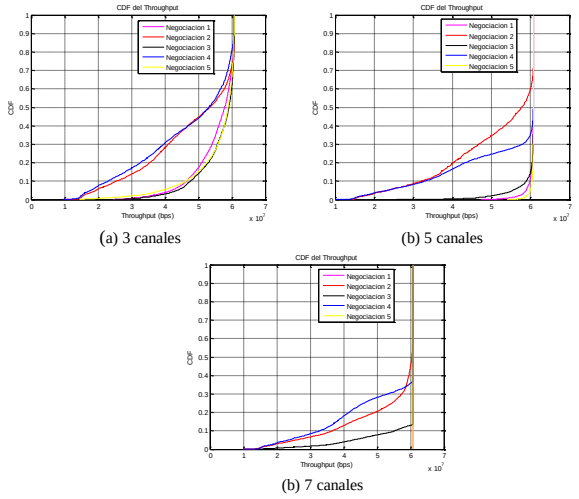
zonas más cercanas a las pareces externas de los apartamentos.



(a) 3 canales (b) 5 canales

(b) 7 canales

Figura 4: CDF de la SINR para la topología 1, en función del número de canales disponibles en el escenario.



(a) 3 canales (b) 5 canales

(b) 7 canales

Figura 5: CDF del *Throughput* para la topología 1, en función del número de canales disponibles en el escenario.

VII. CONCLUSIONES

La motivación e importancia del presente proyecto se basa en que se consigue una solución positiva tanto para operadores como para usuarios a la hora de tratar la escasez de espectro. Desde el punto de vista de los operadores, éstos consiguen reducir la cantidad de tráfico en las macro y micro celdas, mejorando la calidad de los servicios en zonas de exterior. Logrando por tanto abrir un nuevo mercado del que pueden surgir numerosas aplicaciones, relacionadas con la necesidad de introducir nuevos tipos de dispositivos a este fin. Desde el punto de vista de los usuarios finales, se consigue mejorar su experiencia de usuario al disponer de cobertura móvil propia en el hogar o en la oficina. Cabe destacar que la introducción de los sistemas femtocelda no pretende acabar con las redes tradicionales basadas en celdas de gran tamaño, sino que el objetivo es la convivencia de ambas tecnologías a fin de buscar el beneficio global, mejorando los servicios ofrecidos dentro de los edificios a la vez que aumenta la calidad de éstos en la calle.

REFERENCIAS

[1] [11] Ericsson, "Para el año 2016 la cantidad de datos transmitidos desde dispositivos móviles tendrá un aumento de 10 veces," 2011. Disponible en: http://media.ericsson.pl/pr/197861/do-roku-2016-ilosc-danych-przesylanych-za-pomoca-urzadzen-mobilnych-wzrosnie-10-krotnie, 09 de noviembre 2011

[2] [75] N. Nie and C. Comaniciu, "Adaptive channel allocation spectrum etiquette for cognitive radio networks" *New Frontiers in Dynamic Spectrum Access Networks*, pp. 269 – 278, 2005.

[3] [76] 3GPP, "Technical report 3rd generation partnership project; technical specification group radio access network; evolved universal terrestrial radio access (e-Utra); further advancements for e-Utra Physical Layer aspects" vol. 3GPP TR 36.814 V9.0.0 (2010-03) (Release 9), 2010.

[4] [82] G. P. Villardi, C. Sun, Y. D. Alemseged, and H. Harada, "Coexistence of TV White Space enabled Cognitive Wireless Access Points" *Wireless Communications and Networking Conference Workshops*, pp. 18 – 23, 2012.

[5] [85] K. C. Allen, N. DeMinco, J. R. Hoffman, Y. Lo, and P. B. Papazian, "Building penetration loss measurements at 900 Mhz, 11.4 Ghz and 28.8 Ghz," *NTIA Tech. Rep.*, pp. 94–306, 1994.

[6] [83] K. Tsujimura and M. Kuwabara, "Cordless telephone system and its propagation characteristics" *Vehicular Technology, IEEE Transactions*, vol. 26 (4), pp. 367–371, Noviembre 1977.

[7] [95] L. G. U. Garcia, K. I. Pedersen, and P. E. Mogensen, "On open versus closed LTE-Advanced femtocells and dynamic interference coordination" *Wireless Communications and Networking Conference*, pp. 1–10, 2010.

Ana María López Pérez es Ingeniera de Telecomunicación (2007 – 2013) por la Universidad de Granada. Actualmente trabaja como HP GSC IPG Dispatcher en Hewlett-Packard Lisboa. Su función principal es el análisis, gestión y solución de incidencias hardware y software en dispositivos de gama empresarial. Asimismo ha trabajado en Coviran S. Coop. And. Como especialista en Redes y Comunicaciones.

Jorge Navarro Ortiz es Profesor Contratado Doctor del área de Ingeniería Telemática de la Universidad de Granada. Tanto su experiencia profesional (en empresas como Nokia Networks, Ericsson y Siemens) como docente e investigadora siempre ha estado vinculada al campo de las comunicaciones móviles e inalámbricas, en el cual ha realizado numerosas contribuciones en forma de capítulos de libros, artículos de revistas, patentes, proyectos y contratos de investigación entre otros.

Ataques DoS en entornos de red. Análisis y defensas

Tutor: Pedro García Teodoro; e-mail: pgteodor@ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

Autor: Manuel Pablo Fernández Trillini, e-mail: manuft@correo.ugr.es

***Resumen*— En el presente trabajo se lleva a cabo un estudio del impacto que un ataque de denegación de servicio tiene sobre un conjunto de servicios telemáticos convencionales, en un entorno controlado, desde el punto de vista de los clientes legítimos de dichos servicios. Más concretamente, se evalúa el impacto de los ataques *TCP SYN Flood* y *UDP Flood* sobre un servicio web, un servicio de transferencia de ficheros y un servicio de *streaming* de vídeo. Asimismo, se presenta una visión en profundidad de los ataques de denegación de servicio más relevantes en la actualidad. Finalmente, se evalúa la efectividad de la funcionalidad de *SYN Proxy* implementada para el *kernel* de Linux como mecanismo de defensa contra el ataque *TCP SYN Flood*.**

***Palabras clave*—Ataques, DoS, DDoS, seguridad, redes.**

I. Introducción

En los últimos años los ataques a sistemas informáticos han aumentado su complejidad y escala de forma exponencial debido a que los delitos informáticos son cada vez más lucrativos. En este contexto, una de las amenazas más relevantes y que más retos ha presentado –y presenta– a las redes de comunicación son los ataques de denegación de servicio (DoS, *Denial of Service*); y más concretamente su variedad distribuida (DDoS, *Distributed DoS*), los cuales han aumentado en cuestión de unos pocos años su potencia hasta tasas de cientos de Gigabits por segundo, con motivo del uso de las llamadas *botnets* y de *malware* cada vez más sofisticado.

A lo largo de los años han sido propuestas y desarrolladas una gran cantidad de soluciones al problema de la detección y la mitigación de distintos ataques DoS. Sin embargo, lejos de tener una solución definitiva, existen varios motivos que dificultan la tarea del desarrollo de defensas efectivas contra esta amenaza. Por un lado está la enorme variedad de tipos de ataque que hacen uso de tráfico muy diverso y similar al tráfico legítimo. Por otro lado, el incremento del número de dispositivos conectados a Internet ha proporcionado a los atacantes una vía fácil para reclutar un enorme número de agentes o *bots* desde donde lanzar ataques cada vez más potentes.

Este tipo de ataques supone una amenaza constante para muchas organizaciones, ya que en una sociedad como la actual, en la que gran parte de los ingresos de las empresas dependen de los servicios ofrecidos en Internet, la interrupción o la simple degradación de la calidad del servicio puede no solo privar a la empresa de ingresos, sino también mermar la confianza de los clientes.

II. DoS y DDoS

Un ataque DoS ordinario consiste básicamente en el envío masivo de tráfico aparentemente legítimo por parte de un atacante a una red o servidor objetivo (víctima) con el fin de que el enorme volumen de datos exceda la capacidad de procesamiento u otros recursos de la víctima, impidiéndole a esta prestar el servicio, total o parcialmente, a los clientes legítimos.

Por otra parte, un ataque DDoS es una variedad del ataque DoS en el que el atacante no es solo una máquina, sino un gran número de ellas, por lo que el volumen de tráfico y, por consiguiente, el daño causado son significativamente mayores. En este caso el ataque es lanzado de forma indirecta a través de una serie de máquinas comprometidas, las cuales envían flujos de datos a la víctima con el fin de colapsar sus recursos.

La Fig. 1.a muestra un escenario de un ataque DoS en el que, tal y como se ha definido, el origen del tráfico malicioso es una única entidad. Por otro lado, la Fig. 1.b muestra un escenario de un ataque DDoS en el que son varios los equipos involucrados en el ataque y, por lo tanto, el volumen de tráfico malicioso generado es significativamente mayor.

Para llevar a cabo el ataque DDoS, el atacante ha tenido que implantar previamente su código malicioso en una serie de máquinas comprometidas, las cuales pueden organizarse en varios niveles (conocidos como *masters* y *slaves*) [1] de forma que el atacante no interacciona en ningún momento con la víctima, sino que este lanza el ataque a través del envío de instrucciones (coordinación del ataque) a dichas máquinas, los cuales llevan a cabo el ataque en sí contra la víctima, sin ni siquiera tener conocimiento de que están formando parte de un ataque DDoS.

Estas máquinas comprometidas suelen recibir el nombre de agentes o *bots*, y se organizan en redes conocidas como *botnets*, las cuales se utilizan para realizar todo tipo de acciones maliciosas en Internet: desde el lanzamiento de

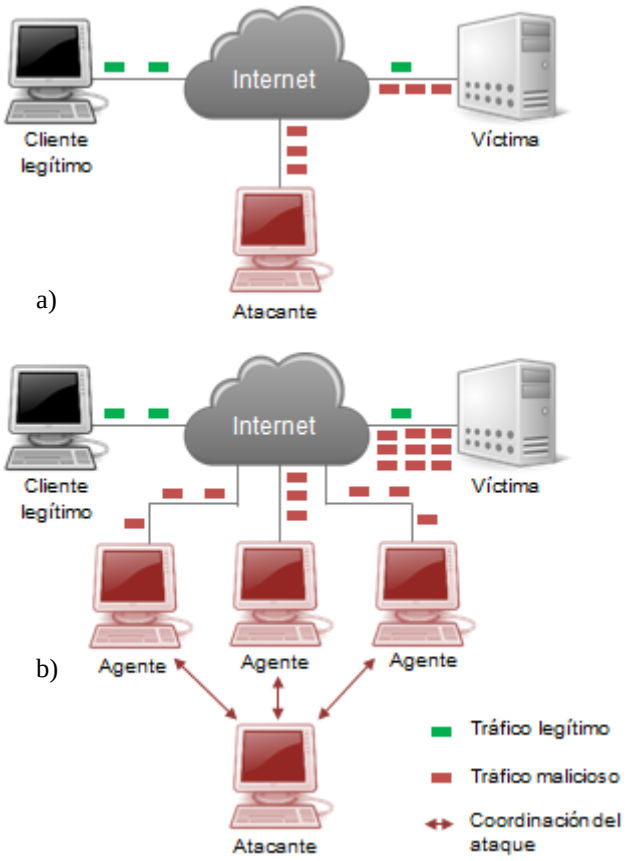


Fig. 1. (a) Escenario de un ataque DoS. (b) Escenario de un ataque DDoS en el que un atacante controla a tres agentes.

ataques DDoS hasta la suplantación de identidad, el envío de *spam* o la realización de todo tipo de fraudes.

Existen dos métodos básicos para llevar a cabo un ataque de denegación de servicio: la explotación de una vulnerabilidad descubierta en un protocolo o aplicación de la víctima o el envío de un flujo masivo de paquetes de apariencia legítima con el fin de colapsar los recursos de esta. El primer tipo se conoce como *ataque de vulnerabilidad*, mientras que el segundo se conoce como *ataque de inundación* (*flooding*).

Por otra parte, si se atiende a la tasa del ataque, estos pueden ser clasificados en *ataques de fuerza bruta* o *ataques de baja tasa* (*low rate*). Estos últimos buscan degradar o denegar completamente un servicio con la mínima tasa de tráfico posible, eludiendo a la vez a los posibles sistemas de detección de la víctima.

A continuación se describen algunos de los ataques DoS más relevantes. [1]

A. *TCP SYN Flood*

En la actualidad, la inmensa mayoría de los sistemas de red están basados en el protocolo de transporte TCP y, por lo tanto, son susceptibles a sufrir este tipo de ataque.

TCP es un protocolo orientado a conexión y, como tal, requiere una fase de establecimiento de conexión. Esta fase consiste en una negociación de tres pasos que, como se esquematiza en la Fig. 2.a, inicia el cliente enviando un paquete TCP con el *flag* SYN activado. Tras recibir esta petición de establecimiento de conexión, el servidor responde con un SYN-ACK y reserva los recursos para esta conexión, creando lo que se conoce como una conexión semi-abierta. Finalmente, para confirmar el establecimiento de la conexión el cliente debe responder con un ACK.

El ataque *TCP SYN Flood* se basa en aprovechar esta reserva de recursos producida en el servidor enviando una gran cantidad de paquetes SYN, los cuales son paquetes *a priori* legítimos y por lo tanto muy difíciles de detectar como maliciosos.

Normalmente, estas peticiones de conexión utilizan direcciones IP origen falsificadas (lo que se conoce como *IP spoofing*) por lo que, como se muestra en la Fig. 2.b, los SYN-ACK del servidor se "perderán", permaneciendo el servidor a la espera de recibir el ACK que complete la negociación, habiendo reservado los recursos para esa conexión.

Este ataque agota rápidamente los recursos del servidor, el cual no puede aceptar más conexiones entrantes.

Otros ataques DoS basados en el protocolo TCP son los ataques de inundación *SYN-ACK Flood*, *ACK Flood* y el conocido como *TCP Reset*.

B. *Naptha*

Una variante de *TCP SYN Flood* es el conocido como *Naptha*. En este caso, el atacante completará la negociación de tres pasos, establecerá un gran número de conexiones con la víctima e intentará mantenerlas el mayor tiempo posible, respondiendo a los mensajes *keep-alive*. [2]

Con esto el atacante pretende impedir que se puedan llevar a cabo nuevas conexiones con el servidor de la víctima.

C. *UDP Flood*

El atacante inunda a la víctima con datagramas UDP a puertos aleatorios con el objetivo principal de consumir su ancho de banda. Para conseguir esto, los paquetes enviados suelen ser de gran tamaño.

Para llevar a cabo este ataque, el atacante no requiere ninguna información de la víctima, aunque sí necesita un número adecuado de *bots* para asegurar el éxito del ataque.

D. *ICMP Flood*

Es un ataque muy simple basado en el envío masivo de paquetes *ICMP Echo Request* (*ping*) a la víctima con el objetivo de colapsar su ancho de banda, provocando además el envío de paquetes *ICMP Echo Reply*, consumiendo gran parte de los recursos del servidor.

Otros ataques conocidos basados en el protocolo ICMP son *Smurf* y el ya obsoleto *Ping of death*.

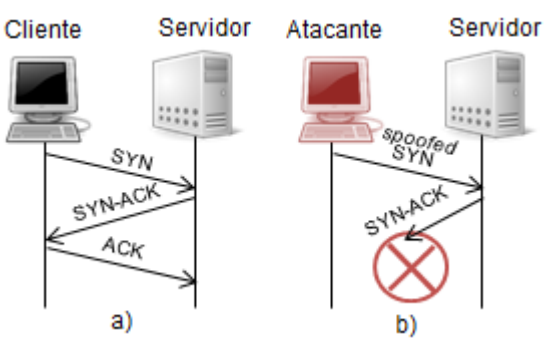


Fig. 2. Establecimiento de conexión TCP: (a) normal y (b) en un ataque *TCP SYN Flood*.

E. *Ataque de amplificación DNS*

Se trata de un ataque de reflexión en el que el atacante envía peticiones *DNS Request* (sobre UDP) a uno o varios servidores de nombre realizando *spoofing* de forma que la IP origen de las peticiones coincida con la IP de la víctima. Así, como se muestra en la Fig. 3, el servidor DNS responderá a la víctima con paquetes UDP de un tamaño significativamente mayor que el de las peticiones, multiplicando la escala del ataque y consumiendo un gran ancho de banda de la víctima.

A partir de una petición DNS de aproximadamente 60 bytes, es posible obtener unas respuestas de unos 4.000 bytes, esto es, un factor de amplificación ×65.

Por este motivo, este ataque entra dentro de una categoría llamada *ataques de amplificación*, los cuales son uno de los mecanismos más utilizados para lanzar ataques a gran escala en Internet y han sido utilizados en algunos de los ataques DDoS que más volumen de tráfico han implicado.

Si bien este ataque es el de amplificación por excelencia, en los últimos tiempos han surgido nuevos ataques basados en otros protocolos cuyo funcionamiento es similar al de amplificación DNS, entre los que destacan los basados en los protocolos NTP (*Network Time Protocol)* y SNMP (*Simple Network Management Protocol*).

NTP es un protocolo que opera sobre UDP y cuya finalidad es sincronizar la hora entre cliente y servidor. Este protocolo dispone de un comando llamado *monlist*, el cual hace que el servidor devuelva las direcciones de los últimos *hosts* con los que ha interactuado y, por lo tanto, la respuesta es significativamente mayor que la petición, consiguiendo una amplificación de aproximadamente ×206 en el ancho de banda y una tasa de ataque 10 veces mayor. [3]

Por otra parte, una petición *getBulkRequest* del protocolo de gestión de redes SNMP de unos 87 bytes puede generar respuestas de decenas de Kbytes fragmentadas en varios datagramas UDP.

La principal ventaja de estos ataques es que el atacante puede prescindir de utilizar un gran número de equipos para realizar el ataque.

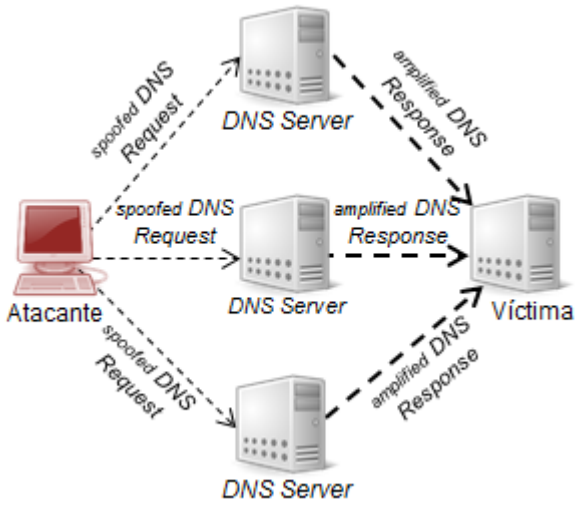


Fig. 3. Esquema del funcionamiento de un ataque de amplificación DNS.

F. *HTTP Flood*

La mayoría de los ataques DoS se llevan a cabo contra servidores web, y es por ello que muchos de estos ataques utilizan el protocolo HTTP para saturar los recursos de la víctima.

El ataque *HTTP Flood* se suele basar en el envío masivo de peticiones HTTP (ya sea de tipo GET, PUT, POST, o cualquier otro método) con el fin de consumir recursos computacionales y de red en la víctima.

Una variante de este ataque, conocida como *Slowloris*, consiste en enviar peticiones HTTP incompletas, lo que provoca un daño aún mayor, ya que la víctima esperará a que se reciban las siguientes partes de la petición, manteniendo la conexión activa mucho más tiempo.

Dentro de este grupo también se encuentra el ataque conocido como *CGI Request Attack*, el cual consiste en inundar a la víctima con peticiones CGI con el fin de agotar sus recursos computacionales.

G. *Teardrop*

Este ataque explota una vulnerabilidad en el reensamblado de paquetes a nivel de red. Consiste en inundar a la víctima con fragmentos IP inválidos, ya sea porque estén solapados o porque su tamaño sea mayor que el especificado. [1]

A pesar de ser una vulnerabilidad conocida y reparada en los sistemas operativos modernos, este tipo de ataques puede causar comportamientos inesperados e incluso reinicios en algunos equipos.

H. *Ataques de baja tasa*

Una de las variedades de los ataques DoS más interesantes son los conocidos como ataques de baja tasa (*low rate*). En ellos el atacante no precisa enviar una tasa elevada de paquetes a la víctima, sino que aprovecha cierta información para construir el ataque de forma inteligente, con el objetivo de producir una degradación o una denegación total en el servicio de la víctima eludiendo posibles sistemas de detección.

En esta categoría, el más conocido es el ataque de baja tasa contra el protocolo TCP [4], el cual estructura su funcionamiento en torno a una vulnerabilidad presente en el mecanismo de control de flujo del protocolo TCP. El objetivo es enviar ráfagas de paquetes maliciosamente separadas en el tiempo con el fin de que la víctima entre en zona de congestión y reduzca su tasa efectiva a prácticamente cero.

Por otra parte, en [5] se describe el ataque *LoRDAS* (*Low-Rate DoS Attack against Server*). En él, el atacante busca evitar la disponibilidad del servidor, haciendo que el tiempo libre de las colas de servicio tienda a cero. Para ello, el atacante debe ser capaz de predecir la aparición de un espacio libre e insertar en ella una nueva petición suya. De este modo, la probabilidad de que los clientes realicen una conexión en ese breve espacio de tiempo es mínima. El atacante estará consiguiendo así que el servidor únicamente sirva sus peticiones y logrará, como consecuencia de esto, denegar el servicio a todos los demás clientes.

Otro ataque DoS de baja tasa mencionable es el conocido como *RoQ* (*Reduction of Quality*). [6]

III. Entorno de evaluación del impacto de ataques DoS

Una vez descritos los ataques de denegación de servicio más relevantes se procede a estudiar el impacto que algunos de estos tienen sobre una serie de servicios de red convencionales desde el punto de vista de la calidad de servicio (QoS) percibida por los clientes legítimos.

Para llevar a cabo este estudio se ha implantado una topología de red sencilla como la que se muestra en la Fig. 4. Dicha red consta de cinco equipos, cada uno de ellos implantado mediante una máquina virtual en *VirtualBox*, utilizando el sistema operativo Ubuntu.

Además del *router*, los equipos involucrados son los siguientes:

A. Servidor

Es la máquina que ofrece los servicios sobre los que se van a desarrollar los ataques DoS.

Se tienen un total de tres escenarios de trabajo, y en cada uno de ellos el servidor ofrece un servicio de red distinto, cada uno de ellos con distintas características. Estos servicios son:

- Servicio web (HTTP)
- Servicio de transferencia de ficheros (FTP)
- Servicio de *streaming* de video en tiempo real (RTSP)

B. Atacantes

Es la máquina desde donde se lanzan los ataques DoS. Los ataques que se llevan a cabo son dos de los vistos en el apartado anterior:

- *TCP SYN Flood*
- *UDP Flood*

Con el estudio de estos ataques se pretende observar el impacto de un ataque de vulnerabilidad como es el ataque *TCP SYN Flood*, ya que la gran mayoría de los servicios de red actuales son susceptibles a sufrir este ataque. Por otro lado, mediante el estudio del ataque *UDP Flood* se busca observar el impacto que tienen este y otros ataques basados en el consumo de ancho de banda de red, como pueden ser los ataques de amplificación.

Los ataques se realizan a distintas tasas de paquetes por segundo y hacen uso de *IP spoofing*.

C. Clientes

Se trata del equipo que simula a los clientes legítimos de los servicios, es decir, quienes acceden a los servicios ofrecidos por el servidor y quienes obtienen los distintos parámetros de QoS de interés.

D. Sumidero

Este equipo únicamente se encarga de recibir las respuestas del servidor a los paquetes procedentes del atacante y descartarlos con el fin de evitar inundar la red con paquetes *ICMP Destination Unreachable* que puedan distorsionar los resultados.

Para observar la degradación en las prestaciones de los distintos servicios se han medido una serie de parámetros de interés en cada uno de los servicios.

En el caso del servicio web se ha obtenido el tiempo medio transcurrido desde que se solicita una página web hasta que esta es recibida completamente, parámetro que denominamos *tiempo de respuesta*.

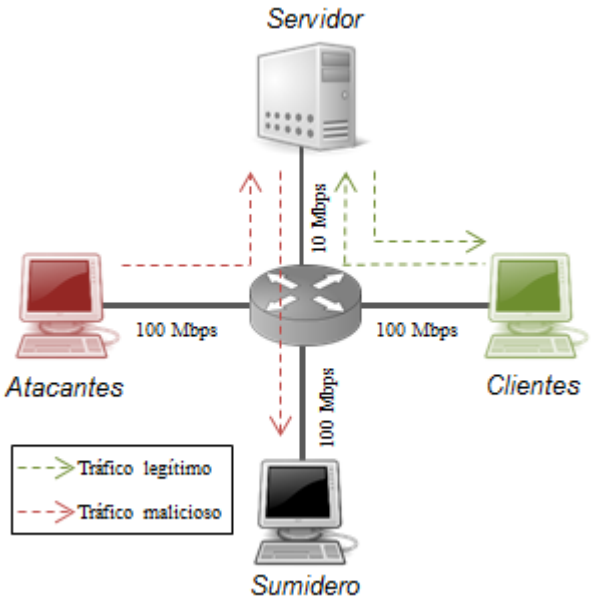


Fig. 4. Topología de la red utilizada para el estudio del impacto de ataques DoS.

Las prestaciones de un servicio de transferencia de ficheros están determinadas por el tiempo transcurrido desde que se solicita establecer la conexión TCP con el servidor hasta que el fichero se transfiere por completo. A este parámetro lo denominamos *latencia* de transferencia.

Finalmente, para observar las prestaciones del servicio de *streaming* se han obtenido una serie de parámetros de QoS del *stream* tales como el *porcentaje de paquetes perdidos*, el *bit-rate medio* y el *tiempo entre paquetes*.

IV. Análisis de resultados

En las Fig. 5 y 6 se representan gráficamente los resultados obtenidos bajo los dos ataques DoS realizados para cada uno de los tres servicios evaluados. En ella se representan los distintos parámetros de interés medidos en función de la tasa del ataque realizado en paquetes por segundo (pps).

En el caso del ataque *TCP SYN Flood* (Fig. 5) se puede observar que en los tres escenarios el servidor trabaja a un rendimiento normal hasta unas tasas de ataque de entre 400 y 500 pps, mientras que la degradación de las prestaciones de los servicios empieza a ser importante a partir de una tasa de ataque de aproximadamente 800-900 pps. Es decir, el servidor se ve desbordado a partir de la recepción de unas 800 peticiones de conexión TCP por segundo.

A partir de una tasa de ataque de entre 1.200 y 1.400 pps la degradación es tal que no se consigue establecer una conexión con el servidor y, por lo tanto, no es posible obtener los parámetros deseados. En este punto se considera que se produce una denegación de servicio total.

Es importante mencionar que, tal y como era de esperar, la degradación de las prestaciones se produce a la hora de establecer la conexión TCP con el servidor, es decir, los clientes deben esperar más tiempo para establecer esta conexión, transcurriendo el posterior intercambio de datos en condiciones normales.

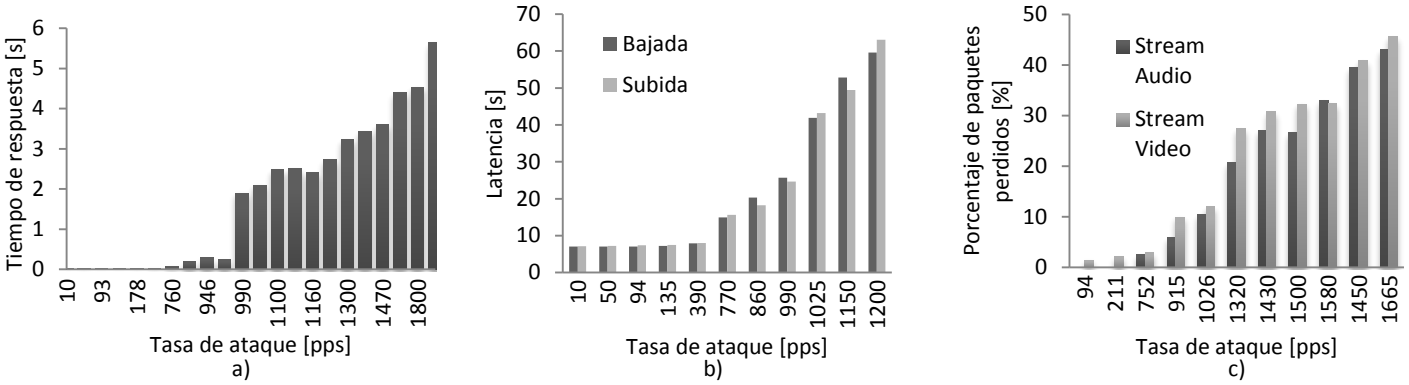


Fig. 5. Evolución de las prestaciones de los servicios (a) web, (b) transferencia de ficheros y (c) *streaming* de video en función de la tasa el ataque *TCP SYN Flood.*

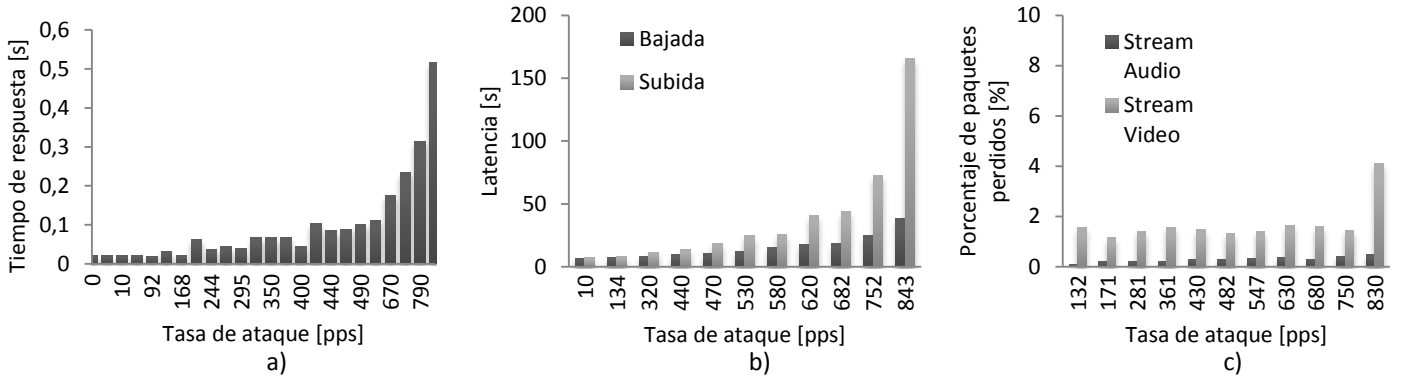


Fig. 6. Evolución de las prestaciones de los servicios (a) web, (b) transferencia de ficheros y (c) *streaming* de video en función de la tasa del ataque *UDP Flood.*

Por otra parte, aunque los parámetros de QoS utilizados para evaluar las prestaciones del servicio de *streaming* se obtienen después de que se establezca la conexión TCP, se observa un incremento notable en el porcentaje de paquetes perdidos del *stream* de video. Esto nos permite comprobar que el ataque *TCP SYN Flood* está consumiendo importantes recursos del servidor.

Para finalizar con el análisis del impacto del ataque de *TCP SYN Flood* hay que destacar el hecho de que para producir una degradación importante (e incluso una denegación de servicio total) no se ha requerido un gran consumo de ancho banda. Como ejemplo de esto se puede mencionar que una tasa de ataque de 900 pps (suficiente para atenuar notablemente el rendimiento del servidor) se corresponde con una tasa de 513 kbps; esto es, solo un 5% de la capacidad del enlace del servidor.

Los ataques *UDP Flood*, cuyos resultados se muestran en la Fig. 6, se han llevado a cabo en tasas que van desde 10 hasta unos 820 pps, que se corresponde con una tasa de ataque de 10 Mbps; esto es, el equivalente a la capacidad del enlace *router*↔servidor.

En este caso, la degradación en las prestaciones del servicio web se refleja en un incremento en el tiempo de respuesta, aunque esta atenuación en el rendimiento no es tan severa como ocurría bajo el ataque *TCP SYN Flood*. Es cierto, no obstante, que el tiempo de respuesta dependerá del tamaño de las páginas web solicitadas que, en este caso, no es excesivamente grande.

Por el contrario, en el servicio de transferencia de ficheros sí que es más notable la degradación de las prestaciones, y esto se refleja en un incremento en la latencia de transferencia.

En este caso, la subida y la descarga de ficheros presentan latencias diferentes. Este comportamiento responde al hecho de que el ataque consume ancho de banda en el enlace de subida (*router*→servidor) y a su vez, las respuestas del servidor consumen ancho de banda de bajada (servidor→*router*). Concretamente, los resultados muestran que la relación entre la tasa de ataque y las respuestas del servidor, esto es, la relación entre el ancho de banda de subida y el ancho de banda de bajada del enlace, es de aproximadamente 2,3:1.

Esto último se refleja en que, para tasas de ataque importantes, la latencia de transferencia en la subida sea aproximadamente 2,3 veces mayor que en la descarga para ficheros del mismo tamaño, ya que la capacidad disponible del enlace es menor.

Como ejemplo se puede mencionar que frente a los 7 segundos de latencia de subida que se tiene en condiciones normales, para un ataque cercano a los 10 Mbps, la latencia se incrementa hasta los 168 segundos.

Finalmente, y como cabía esperar, el servicio *streaming* no sufre una degradación en la QoS ya que el vídeo utilizado requiere un *bit-rate* de unos 700 kbps, un ancho de banda que en todo momento está disponible en el enlace servidor→*router*.

Es importante mencionar que los ataques se han realizado hasta tasas nunca superiores a 10 Mbps. Si se superase este valor, el *router* se vería obligado a encolar paquetes y, llegado a un punto, descartarlos si estos desbordan las colas, llegándose a perder paquetes de los clientes legítimos y, por tanto, produciendo una degradación aún mayor.

V. Evaluación de SYN Proxy

A pesar de los esfuerzos invertidos en la investigación y el desarrollo de defensas eficientes, los ataques DoS continúan siendo un problema que está lejos de tener una solución definitiva.

El objetivo principal de una defensa es proporcionar un buen servicio a los clientes legítimos incluso durante el ataque, de forma que estos no perciban una degradación en las prestaciones del servicio.

El objetivo secundario es mitigar el efecto del ataque en los recursos de la víctima, de forma que estos puedan ser dedicados enteramente a los clientes legítimos.

En [1] el autor clasifica los mecanismos de defensa en mecanismos de prevención, detección, respuesta y tolerancia y mitigación.

Especial atención ha acaparado a lo largo de los años la propuesta de defensa ante el ataque *TCP SYN Flood*. Entre los principales mecanismos que intentan solventar la vulnerabilidad que permite la realización de estos ataques se encuentran los conocidos como *SYN Cache*, *SYN Cookies* y *SYN Proxy*. [7]

Las *SYN Cookies* llevan años implementadas para Linux, con escasa efectividad. Por otra parte, la funcionalidad de *SYN Proxy* ha sido implementada recientemente, a partir de la versión 3.12 del *kernel*. Esta defensa consiste básicamente en dividir la conexión cliente-servidor en dos conexiones: cliente-*proxy* y *proxy*-servidor, de forma que el cliente solo interactúe con el servidor una vez se haya comprobado que se trata de un cliente legítimo.

Naturalmente, sigue existiendo un agotamiento en los recursos del *proxy*.

Lo que se ha hecho ha sido comparar el rendimiento de un servidor web, por un lado sin ninguna defensa y por otro con un *SYN Proxy* implementado según se describe en [8] en un S.O. Debian Wheezy.

Los resultados obtenidos se muestran en la Fig. 7. En ella se puede apreciar que mediante la implementación del *proxy*, el número de conexiones que puede manejar el servidor es algo superior: mientras que sin defensa soporta unas 1.600 peticiones de conexión por segundo antes de que se produzca una denegación de servicio total, la defensa implementada permite elevar este número hasta aproximadamente 2.500 paquetes SYN por segundo.

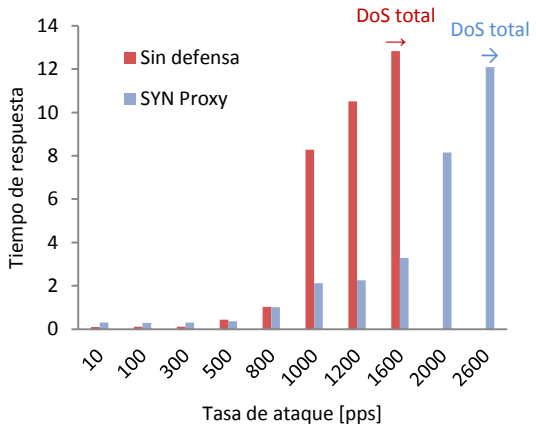


Fig. 7. Tiempo de respuesta HTTP en función de la tasa del ataque *TCP SYN Flood* sin defensas implementadas y con *SYN Proxy* de Linux.

VI. Conclusiones

Con la realización de este trabajo se ha pretendido estudiar los ataques de denegación de servicio en las redes telemáticas con el fin de poner de manifiesto la gravedad que supone esta amenaza. Para ello se ha llevado a cabo un estudio teórico de los ataques DoS más relevantes y se han lanzado una serie de ataques en un entorno de máquinas virtuales que nos han permitido observar el comportamiento y la degradación que sufren ciertos servicios telemáticos convencionales bajo estos ataques.

Finalmente se ha puesto a prueba la funcionalidad de *SYN Proxy* de Linux para hacer frente los ataques *TCP SYN Flood* y se ha comprobado que, aunque lejos de solucionar el problema, permite hacer frente a unas tasas de ataque algo mayores.

Agradecimientos

A Pedro García Teodoro, tutor de este Trabajo de Fin de Grado, por dedicar su tiempo a ayudarme y poder realizarlo, y al Departamento de Teoría de la Señal, Telemática y Comunicaciones de la ETSIIT de la Universidad de Granada, por darme la oportunidad de publicarlo.

Referencias

[1] B. Gupta, R. Joshi, M. Misra (2009). "Defending against Distributed Denial of Service: Issues and Challenges", *Information Security Journal: A Global Perspective*.

[2] SANS Institute (2000), "NAPTHA: A new type of Denial of Service Attack"

[3] J. Graham-Cumming, «CloudFlare» (2014). "Understanding and mitigation NTP-based DDoS Attacks". Disponible en http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks.

[4] Aleksandar Kuzmanovic, Edward W. Knightly (2003). "*Low-Rate TCP-Targeted Denial of Service Attacks (The shrew vs. the mice and elephants*)". SIGCOMM'03.

[5] G. Maciá Fernández. "Ataques de denegación de servicio a baja tasa contra servidores", Tesis doctoral, DTSTC, UGR, Granada, España, 2007.

[6] M. Guirguis, A. Vros Ibrahim, M. Yuting Zhang (2005). "*Reduction of Quality (RoQ) Attacks on Internet End-Systems*". SIGCOMM'05.

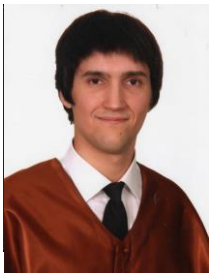
[7] W. M. Eddy (2006). "*Defenses Against TCP SYN Flooding Attacks*". The Internet Protocol Journal – Vol. 9.

[8] "*Homemade DDoS Protection Using IPTables SYNPROXY*". [En línea]. Disponible en: https://r00t-services.net/knowledgebase/14/Homemade-DDoS-Protection-Using-IPTables-SYNPROXY.html.

[9] G. Maciá Fernández, J. E. Díaz-Verdejo, P. García Teodoro y F. de Todo Negro (2008). "*Evaluation of a Low-Rate DoS Attack against Application Servers*". Computers & Security, Vol. 27.

[10] J. C. Gallardo, *Seguridad en Redes Telemáticas*, Mc Graw-Hill, 2004.

[11] D. Dittrich, Mirkivic, Reiher, *Internet Denial of Service: Attack and Defense Mechanisms*, Pearson Education, 2004.



Manuel Pablo Fernández Trillini nació en 1991 en Rosario (Argentina). En 2014 obtuvo el título de Grado en Ingeniería de Tecnologías de Telecomunicación en la Universidad de Granada (España) y actualmente cursa un Master en Ingeniería de Telecomunicación en la Universidad de Granada.

Detección de ataques en OMNeT++
Dropping en redes MANET

Autor: Pablo Garrido Sánchez, e-mail: pablogs9@correo.ugr.es
Tutor: Prof. Dr. Pedro García Teodoro, e-mail: pgteodor@ugr.es
Tutor: Dr. Leovigildo Sánchez Casado, e-mail: sancale@ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—El presente proyecto implementa un mecanismo propuesto en la bibliografía para la detección de comportamientos maliciosos en nodos de una red MANET. El esquema de detección se centra en los ataques de tipo *dropping*, una forma concreta de los conocidos como ataques de denegación de servicio.**

Se presentan dos implementaciones del un mecanismo de detección de dichos ataques: un esquema de detección aislado y otro distribuido. La base sobre la que se desarrolla todo el trabajo es el simulador de eventos discretos OMNeT++, sobre el se incorpora el simulador de redes INET y el *framework* de seguridad en redes NETA.

Los resultados de las simulaciones finales corroboran que el modelo distribuido de detección de ataques *dropping* permite detectar comportamientos maliciosos en los nodos de la red con una tasa aceptable de falsos positivos, mientras que el sistema aislado permite corroborrar los fundamentos teóricos del mecanismo propuesto.

***Palabras clave*—Ataque de *dropping*, IDS, MANET, OMNeT++**

I. Introducción

La seguridad informática y de redes es un campo de estudio de gran relevancia actualmente, en gran medida debido al auge de las tecnologías digitales y a su inmersión casi total en todos los aspectos de la sociedad actual. De entre las distintas tecnologías, arquitecturas y aplicaciones existentes en la actualidad, las redes ad hoc, y en particular las redes MANET (*Mobile Adhoc Network*), son las que presentan una mayor proyección de futuro. Un ejemplo de red MANET se presenta en la Figura 1. En ella se observa un conjunto de nodos con movilidad y cierto rango de cobertura, que pueden comunicarse entre ellos de forma no centralizada y basando su comunicación en la retransmisión multi-salto de información entre nodos. En esta figura se observa un conjunto de nodos retransmisores (marcados como N) sobre los que se sustenta la comunicación entre emisor y receptor (E y R respectivamente).

La detección de ataques a la seguridad en un sistema de este tipo constituye un aspecto clave para la necesaria solución de los mismos y, con ello, permitir la continuidad de los servicios y prestaciones del entorno. Con este objetivo central, el presente documento presenta el desarrollo de un sistema de detección de ataques *dropping* en redes MANET.

Las redes MANET son un tipo de redes formadas por nodos móviles. Su naturaleza es ad hoc, de manera que no hay gestión centralizada o infraestructura fija. En ellas, para poder alcanzar la conectividad entre todos los nodos se ha de adoptar una filosofía de *routing* adaptativo multi-salto. Los nodos actúan como *routers* y precisamente en esto es en lo que se basa este tipo de redes para el envio de información: en la confianza en que el resto de nodos retransmitan el mensaje hacia su destino. En relación a este hecho surgen los ataques de *dropping*.

El ataque de *dropping* en redes MANET consiste en la no retransmisión de paquetes por parte de un nodo malicioso, impidiendo así que lleguen a su destino último. El nodo que lleva a cabo este tipo de ataque es denominado *dropper* y se presenta (marcado con la letra A) en la Figura 2. El descarte de paquetes por parte del *dropper* puede ser total o selectivo, dejando en este último caso de retransmitir únicamente paquetes con ciertas características. Las principales motivaciones de este comportamiento pueden ser propósitos puramente maliciosos o actitudes egoístas, cuyo fin es preservar recursos energéticos.

II. Herramientas

En el marco antes referido, este trabajo pretende implementar en un entorno de simulación el mecanismo de detección de *droppers* propuesto por Sanchez-Casado *et al.* [1]. Para ello se propone utilizar uno de los simuladores de redes más aceptados y utilizados en los sectores académicos: OMNeT++ junto con el *framework* de simulación de redes INET.

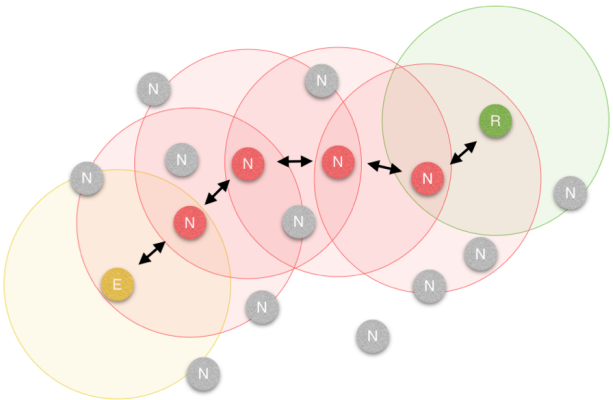


Fig. 1. Ejemplo de red MANET.

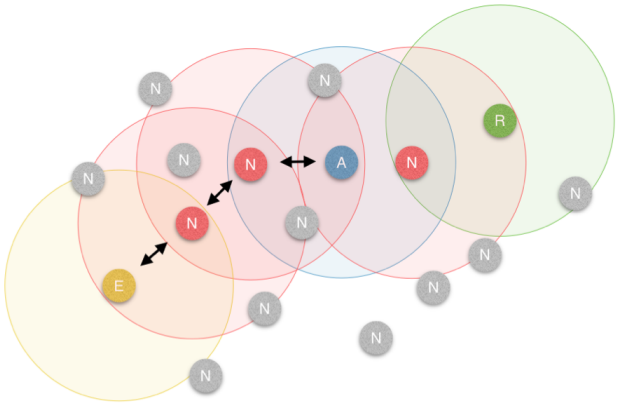


Fig. 2. Ejemplo de red MANET con un nodo malicioso.

OMNeT++ [3] es un simulador de eventos discretos basado en C++. Proporciona un motor de simulación y un entorno de trabajo basado en Eclipse. Separa además los contextos de simulación y diseño de sistemas, es decir, permite definir los sistemas como clases de C++ y realizar simulaciones en escenarios creados mediante lenguajes propios.

Dentro de OMNeT++ se encuentra INET a modo de simulador de redes. El *framework* INET define prácticamente todos los aspectos de las redes de comunicación actuales. En él se encuentran definidas todas las capas de la pila OSI, desde los niveles físcos descritos por 802.11 hasta aplicaciones UDP, pasando por la descripción de medios de transmisión (medios inalámbricos, soportes cableados...), protocolos de enrrutamiento o herramientas para dotar a los nodos de movilidad.

Sobre INET, el grupo NESG (*Network Engineering & Security Group*) de la Universidad de Granada desarrolla NETA (*NETwork Attacks*) [4], un *framework* para la simulación de ataques de red. En NETA se presentan nodos de red con protocolos *hackeados*, de manera que estos nodos puedan llevar a cabo ciertos ataques. Más allá de ello, NETA propone una arquitectura organizada donde poder desarrollar nuevos ataques de red, es decir, unicamente redefiniendo el comportamiento del protocolo que nos interese se podría implementar un nuevo ataque y realizar simulaciones en entornos de red para ejecutar dichos ataques.

Este desarrollo trata de completar la arquitecura de NETA, facilitando el desarrollo posterior de detectores de ataques a la seguridad de redes y demás soluciones defensivas que tienen cabida dentro del concepto de *supervivencia en redes* [2]. Para ello se generará una arquitectura similar a la existente en cuanto a ataques. Además, se implementan dos detectores de eventos contra la seguridad de sistemas de red tipo MANET, ambos relacionados con el ataque de *dropping*.

III. Seguridad en redes MANET: *dropping*

Tal y como se introdujo, un ataque de *dropping* es una forma de denegación de servicio que sucede en una red de comunicación basada en retransmisiones entre nodos como pueden ser las redes MANET. En ellas, que un nodo tome una actitud atacante (*dropper*) supone que rompa la cadena de retransmisión, llevando a cabo por tanto una denegación del servicio de retransmisión que se espera que ofrezca al resto de los nodos de la red e impidiendo la comunicación entre los nodos origen y destino. Como se apuntó anteriormente, este descarte de paquetes puede ser total o parcial según la estrategia adoptada, es decir, el atacante podría no retransmitir ningún paquete o podría decidir qué paquetes concretos no va a retransmitir.

Dentro de esta segunda opción encontramos el descarte selectivo y el descarte probabilístico. En el primero de ellos el nodo decide qué paquetes descartar en base a cierto criterio como podría ser el origen, el destino, el tipo de mensaje, etc. El segundo tipo de descarte, que será con el que se trabaje en este proyecto, implica que el nodo malicioso descartará los paquetes que deba retransmitir con cierta probabilidad. En las simulaciones que se exponen más adelante, por ejemplo, el *dropper* descartará 20 de cada 100 paquetes que reciba.

A. *Mecanismo de detección del ataque de dropping*

El algoritmo de detección que se va a implementar es el expuesto en la bibliografía antes mencionada [1].

En un primer momento se podría pensar que un comportamiento malicioso de tipo *dropping* en un nodo dado sería facilmente detectable con solo tener en cuenta el número de paquetes que recibe (destinados a ser retransmitidos) y el número final de paquetes que verdaderamente retransmite. Sin embargo, esta aproximación tan sencilla obvia multitud de aspectos que no solo son trascendentes en el contexto de una red con nodos móviles inalámbricos como es una MANET, sino que son claramente vitales para el correcto funcionamiento de un mecanismo de detección de comportamientos maliciosos. Estos aspectos están relacionados con los errores de transmisión en los que, debido al ruido del canal o a posibles colisiones entre paquetes, un paquete es imposible de retransmitir (condición de red inalámbrica) o situaciones en las que el nodo hacia el cual se habría de retransmitir cierto paquete no se encuentra dentro del rango de cobertura del nodo de retransmisión (condición de red de nodos móviles).

La heurística de detección que se va a implementar considera ambas condiciones de forma nativa[5], ya que fue diseñado para ser utilizado en el contexto de las redes MANET que utilizan AODV[1]. Su funcionamiento es multicapa ya que toma como parámetros de entrada información de diversas capas de la pila OSI. A modo de resumen (una explicación más detallada se puede encontrar en el documento extendido referente a este proyecto), tomará como datos de entrada:

- De la capa IP, los datagramas a retransmitir[2] y los retransmitidos. De esta manera, se obtiene una noción porcentual de la fiabilidad de retransmisión del nodo. Este parámetro se conoce como probabilidad de retransmisión o P_{FWD}.
- De la capa MAC, se obtienen las tramas RTS enviadas y las tramas CTS recibidas. Ambas tramas forman parte del

[1]AODV (*Ad hoc On-demand Distance Vector*) es uno de los protocolos de encaminamiento reactivos más conocidos y empleados en redes MANET. AODV permite desarrollar una estrategia de comunicación multisalto, adaptándose a los cambios de topología producidos como consecuencia de la movilidad de los nodos.

[2]Un datagrama se considera como datagrama a retransmitir siempre que no tenga como destino el propio nodo que lo recibe, y siempre que el nodo que lo recibe tenga una ruta válida hacia el destino del datagrama.

mecanismo de sondeo de portadora virtual del estándar inalámbrico 802.11. Mediante ellas se puede obtener una aproximación del estado de congestión del canal inalámbrico conocida como probabilidad de colisión o P_{COL}.

- Del protocolo AODV, se obtiene el número de mensajes RREQ generados por el nodo en situaciones de movilidad. Un nodo genera este tipo de paquetes cuando necesita buscar una nueva ruta hacia un destino concreto en la topología. Bajo ciertas circunstacias de movilidad, estos mensajes se generan para tratar de reparar un enlace que se ha roto dentro de una cadena de transmisión. En esta situación, el mecanismo ha de percatarse que el nodo no está descartando paquetes, sino que ha comenzado un proceso de reparación local de ruta y está esperando una respuesta. Este parámetro se conoce como probabilidad de movilidad o P_{MOB}.

Una vez obtenidos estos parámetros, se estima la probabilidad de que un nodo concreto tenga un comportamiento malicioso de tipo *dropper*, o P_{DROP}, tal y como indica (1):

$$P_{DROP} = \begin{cases} 0 & \text{si } P_{MOB} = 1 \\ 1 - \frac{P_{FWD}}{1-P_{COL}} & \text{en otro caso} \end{cases} \quad (1)$$

Sobre este valor se centra todo el proceso de detección, ya que la clasificación de un nodo como malicioso o legítimo se realiza comparando P_{DROP} con un valor umbral o *Thr* previamente fijado por el algoritmo. De esta manera, se clasifica al nodo de forma sencilla mediante la lógica expuesta en (2):

$$clase(nodo) = \begin{cases} malicioso & \text{si } P_{DROP} \geq Thr \\ legítimo & \text{en otro caso} \end{cases} \quad (2)$$

B. Estructuras del sistema de detección del ataque de dropping

A continuación se discute la arquitectura sobre la que se implementará el algoritmo de detección descrito. Para ello se proponen dos modelos, uno aislado y otro distribuido.

En primer lugar, el modelo aislado consiste en una arquitectura en la cual cada nodo accede a sus propios módulos IP, MAC y AODV para obtener los datos de entrada del mecanismo. Para ello, como se muestra en la Figura 3, se incorpora un controlador de detección aislada de *dropping* en cada nodo, que será el encargado de obtener los datos de las distintas capas, procesarlos, y tomar una decisión acerca de su propio comportamiento en base a la ecuación (2). En caso de (auto)detectarse un comportamiento de *dropping*, el nodo procedería a activar un procedimiento de respuesta para alertar de dicho comportamiento al resto de nodos de la red.

La validez de esta estructura se pone en entredicho en el momento en que se plantea la implementación del sistema de detección de ataques de *dropping* en un entorno real. Un nodo que pretenda actuar de forma maliciosa para deteriorar las prestaciones de una red de comunicación bajo ningún concepto advertiría al resto de nodos de sus propias acciones o intenciones maliciosas. A pesar de ello, intuitivamente se entiende que la ejecución del algoritmo dentro de un nodo habría de proporcionar una clasificación completamente fiable del comportamiento del nodo ya que se dispone de primera mano de los parámetros requeridos por el mecanismo de detección. Este hecho se observará en los resultados más adelante.

Por esta razón es por la que se propone como alternativa una solución basada en un sistema distribuido. En este, la resposibilidad de detectar los comportamientos maliciosos recae sobre un nodo central que tiene acceso al estado de todos lo nodos a partir de la información proporcionada por sus respectivos vecinos. Para esta arquitectura se introduce el concepto de *nodo monitor*. Un nodo monitor es aquel que activa su tarjeta de red inalámbrica en modo promiscuo, es decir, que procesa todas las tramas inalámbricas que reciba del medio aunque no sea el destinatario. De esta manera, podemos hacer que estos nodos monitores extraigan la información relevante para el mecanismo de detección de ataques de *dropping* de cada paquete que monitoricen e informen al nodo central o controlador.

Así, el controlador de detección podrá actualizar una base de datos con información acerca de cada nodo de la topología. Con estos datos calculará la heurística de clasificación de comportamientos para cada nodo y alertará al sistema de qué nodos están teniendo un comportamiento malicioso. La Figura 4 muestra este esquema de detección en el cual los nodos usuarios (y potencialmente malicisos) no intervienen en el proceso de detección de comportamientos maliciosos.

Bajo este nuevo paradigma de implementación nos encon-

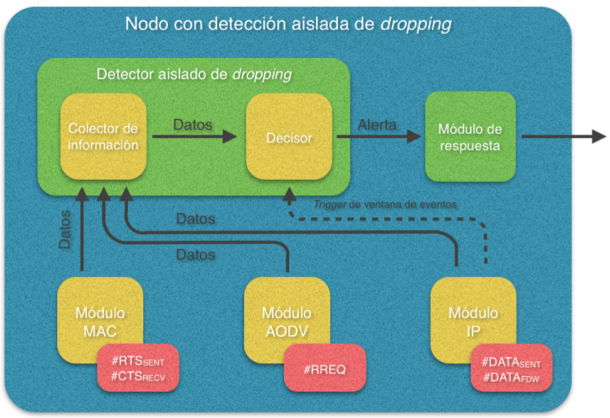


Fig. 3. Estructura del sistema aislado de detección de *dropping*

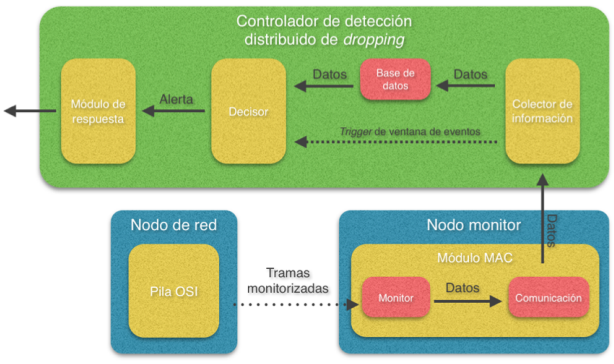


Fig. 4. Estructura del sistema distribuido de detección de *dropping*

tramos que, al no estar tratando con los mensajes que manejan las propias tarjetas de red de los nodos monitorizados, no se puede determinar qué mensajes se reciben correctamente en dichos nodos. Por tanto, para implementar el sistema distribuido de detección de ataques de *dropping* se han de sustituir los parámetros de entrada del algoritmo de detección relacionados con los paquetes recibidos en un nodo (CTS recibidos y datagramas IP a retransmitir) por los paquetes dirigidos al nodo según los nodos monitores (esto es, paquetes CTS y datagramas IP enviados al nodo; al margen de que estos pudieran recibirse incorrectamente).

Un aspecto a tener en cuenta en ambos esquemas de detección es que dicha detección, aislada y distribuida, no se realiza de forma continua en el tiempo, sino que ha de ser discretizada. Tal y como propone la bibliografía, la forma óptima de discretizar la detección es mediante una ventana de eventos en lugar de una temporal. De esta manera se evita la detección "parcial" de sucesos; por ejemplo, la emisión de un RTS pero no la recepción del CTS correspondiente.

IV. Implementación

Para la implementación de ambos sistemas dentro del contexto de NETA se ha adaptado la filosofía ya utilizada para la descripción de ataques de red y nodos atacantes a la descripción de detectores, ya sean aislados o distribuidos.

En primer lugar, se implementará un controlador de detección que estará presente en la topología de simulación. Este controlador genérico será el armazón sobre el que se llevará a cabo el diseño de un detector de cierto tipo de ataques de seguridad y tendrá la funcionalidad básica, es decir, iniciar y finalizar el proceso de detección en el momento que se precise y comunicarse con los nodos que intervengan en el proceso de detección.

Por otra parte, en el caso del detector del ataque de *dropping* se habrán de reescribir las clases C++ que corresponden con los protocolos IP, MAC y AODV de la pila OSI descrita en INET. Estas nuevas implementaciones permitirán obtener los parámetros de entrada del mecanismo de detección concreto implementado en este proyecto.

Por último, las implementaciónes concretas propuestas aquí extienden las funcionalidades del controlador genérico de detección. El controlador aislado de detección de *dropping* implementa la comunicación con el controlador interno de cada nodo. De esta manera, es capaz de acceder directamente a los niveles OSI mencionados y ejecutar el procedimiento de catalogación del comportamiento del nodo para, posteriormente, activar la interfaz hacia las rutinas de respuesta que alertarán al resto de nodos de la topología de un comportamiento malicioso por parte de cierto nodo. Esta última consideración acerca del protocolo de notificación de ataques y respuesta se escapa del propósito del presente trabajo, si bien es de mencionar que en esta dirección existen líneas activas de investigación [6].

Tomando como base todo lo anterior, la implementación distribuida implementa el modo promiscuo en cada nodo. Esta implementación captura cada paquete monitorizado, lo analiza e informa al controlador distribuido de detección de ataques *dropping*. Para realizar este análisis, se extraen las cabeceras de los niveles de la pila OSI que corresponden a los parámetros de entrada del algoritmo de detección. Una vez se dispone de estos datos, se envia un mensaje hacia el controlador que actualizará la base de datos de información, no sin antes comprobar las duplicidades, ya que es muy probable que un mismo paquete sea monitorizado por varios nodos monitores al mismo tiempo.

En ambos casos, el controlador (ya sea el del modelo distribuido o el aislado de cada nodo) al detectar el evento final de la ventana de eventos comenzará el proceso de análisis y detección. Durante la implementación del proyecto se proponen algunas definiciones de mensajes utilizados por el sistema. Entre ellos se encuentra el mensaje de comunicación entre los nodos monitores y el controlador distribuido, mensaje que contiene campos para cada una de las cabeceras relevantes en el proceso de detección. También es de citar el mensaje que el propio controlador dirige hacia el sistema de respuesta, en el que, entre otros parámetros, se incluyen el tipo de ataque detectado, el nodo detectado como atacante, la referencia al nodo que ha realizado la detección, la severidad del ataque y la precisión o fiabilidad de la detección realizada.

V. Simulaciones

Para validar el sistema implementado se diseñan una serie de simulaciones a modo de banco de pruebas. Estas simulaciones tratarán de ajustarse lo más posible a un escenario de comunicación entre nodos de una red MANET, entre los que se encuentra un nodo malicioso que lleva a cabo un ataque de *dropping*.

Estas simulaciones se repetirán 75 veces (con distinta semilla) para diferentes valores del umbral de detección o *Thr*. Cada repetición supone un escenario en el que los nodos se comunican entre sí durante 500 segundos. De esta manera, se obtendrán resultados estadísticamente válidos para diferentes configuraciones del sistema.

El hecho de realizar las simulaciones para diferentes valores del umbral de detección pone de manifiesto que para el correcto funcionamiento del sistema de detección de ataques de *dropping* es necesario ajustar dicho umbral a un valor igual o superior a P_{DROP} de los nodos maliciosos, tal y como se observará en el apartado de resultados.

Tabla I
Especificación de los parámetros de simulación

Parámetro	Valor
Topología	1000m x 1000m
Nodos legítimos	24
Nodos maliciosos	1
Probabilidad de *dropping*	20%
Tamaño de mensajes UDP	512 Bytes
Periodo de mensajes UDP	0.25 s
Capa MAC	802.11g
Bitrate	24/54 Mbps
Slot Time	9 us
SRL	7
Potencia TX	2 mW
Frecuencia portadora	2.4 GHz
Pathloss	2
Umbral SNR	4 dB
Potencia de ruido	-110 dBm
Sensibilidad RX	-85 dBm
Movilidad de nodos	*Random Waypoint*
Velocidad máx. de nodos	10 m/s
Tamaño de la ventana de eventos	100 datagramas IP

Los parámetros más importantes de la simulación se reflejan en la Tabla I, siendo los más relevantes el número de nodos legítimos y maliciosos, 24 y 1 respectivamente, y la probabilidad de *dropping* del nodo malicioso, fijada al 20% para todas las simulaciones.

La efectividad del sistema se mide en tasa de aciertos y fallos. Para ello, en cada una de la repeticiones se considerará como acierto cada vez que se detecte al nodo malicioso o *dropper* al menos una vez y se considerará fallo cada vez que se catalogue un nodo legítimo como malicioso al menos una vez. De esta manera, es posible extraer las tasas de aciertos y errores del sistema a las que denominaremos *True Positive Ratio*, o tasa de verdaderos positivos, y *False Positive Ratio*, o tasa de falsos positivos. respectivamente.

Para la generación de estas estadísticas se utiliza el lenguaje de programación Python. Con unos *scripts* simples se analizan todos los vectores de salida de las simulaciones y se realizan los cálculos estadísticos para obtener las tasas de verdaderos y falsos positivos.

VI. Resultados y conclusiones

Los resultados de las simulaciones muestran un correcto funciomiento del sistema acorde con las previsiones y consideraciones expuestas anteriormente.

En primer lugar, la Figura 5 muestra la curva ROC de verdaderos y falsos positivos para cada valor del umbral en el sistema de detección de ataques *dropping* aislado. Tal y como se puede observar, el sistema funciona correctamente para valores del umbral iguales o inferiores a la probabilidad de *dropping* del atacante, presentando en estos casos tasas de verdaderos positivos superiores al 75% en el peor de los casos. Para valores del umbral superiores a la probabilidad de *dropping* de los atacantes, el rendimiento del sistema se ve gravemente deteriorado (valores del ratio de verdaderos positivos inferiores al 30%).

Por otra parte, el hecho de que los resultados de sistema aislado presenten una tasa de falsos positivos prácticamente nula se debe a que, al realizarse el proceso de detección y catalogación del comportamiento de los nodos dentro de los propios nodos y con datos fidedignos acerca del número de paquetes que estos manejan, la probabilidad de fallo es casi inexistente.

Respecto a los resultados de las simulaciones con el sistema distribuido de detección de ataques de *dropping* propuesto, podemos observar, basándonos en la Figura 6, un rendimiento ligeramente inferior. La justificación de este peor rendimiento reside en las aproximaciones realizadas en el sistema distribuido, así como en la filosofía de monitorización de paquetes que este sistema utiliza para obtener los datos necesarios para la detección.

De la misma manera que en el modelo de detección aislado, se observa una diferencia entre valores del umbral fijados por encima de la probabilidad de *dropping* de los nodos maliciosos. En este segundo caso observamos tasas de verdaderos positivos inferiores al 30% para valores no ajustados del umbral de detección y valores superiores al 70% para valores ajustados del mismo umbral. Obsérvese en este segundo caso el ligero decaimiento del rendimiento del sistema.

La tasa de falsos positivos empieza a considerarse en este modelo distribuido por las razones ya comentadas. Para los valores óptimos del umbral de detección esta tasa de error se encuentra entre el 8% y el 10%.

Una vez analizados los resultados de las simulaciones del proyecto se puede concluir que, partiendo de un proceso de estudio acerca del funcionamiento y la seguridad de las redes MANET, así como un análisis de los diferentes tipos de ataque de *dropping* en las mismas, y continuando con las implementaciones descritas, se ha cubierto el propósito perseguido.

A modo de resumen, se han diseñado e implementado dos versiones de un sistema basado en un mecanismo de detección de ataques *dropping*. Ambas versiones son funcionales; sin embargo, solo la modalidad de detección distribuida es plausible para su implementación en escenarios reales.

Como objetivo secundario, se ha completado el *framework* de simulación de eventos de seguridad NETA del grupo NESG de la UGR con una estructura preparada para la futura implementación de sistemas de detección de ataques a la seguridad de sistemas en redes ad hoc.

Por último, se dejan abiertas posibles líneas de mejora en diversos aspectos. Entre ellos se encuentra la optimización de las comunicaciones entre los nodos que componen el sistema de detección para evitar la sobrecarga de la red, o

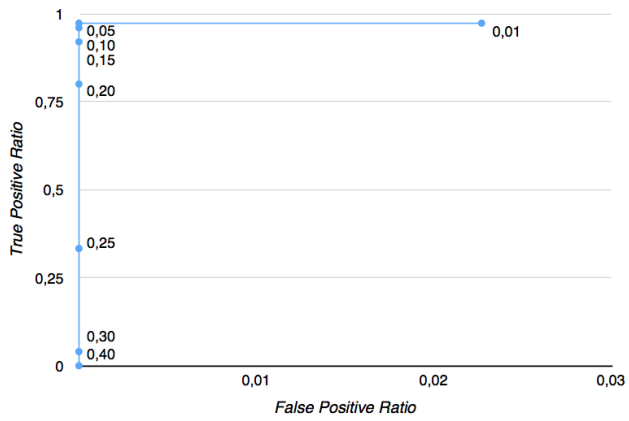


Fig. 5. Resultados de las simulaciones del sistema aislado

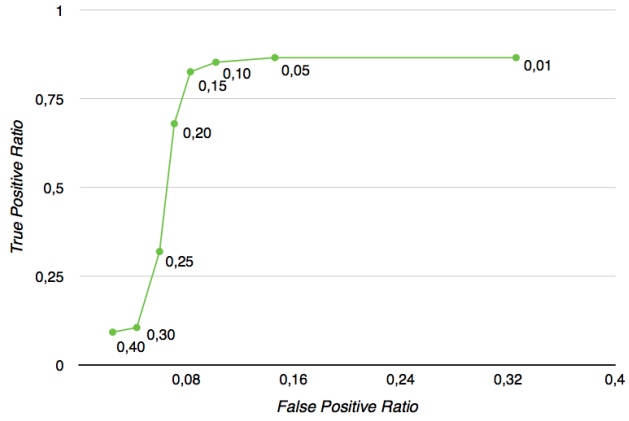


Fig. 6. Resultados de las simulaciones del sistema distribuido

la securización del propio sistema de detección de ataques de *dropping*, vulnerable en este primero estadio a eventos que compromentan su integridad, confidencialidad o disponibilidad.

AGRADECIMIENTOS

El trabajo descrito en este documento no habría sido posible sin el inestimable consejo y la ayuda de ambos tutores: Pedro y Leo. Gracias por las oportunidades.

REFERENCIAS

[1] L. Sánchez-Casado, G. Maciá-Fernández y P. García-Teodoro. *"Multi-Layer Information for Detecting Malicious Packet Dropping Behaviors in MANETs."* NESG, 2012.

[2] Proyecto SuMA (*Survivability of MANETs against security threats*): http://nesg.ugr.es/suma/ – Acceso: 2014-10-07

[3] Manual oficial de OMNeT++: http://www.omnetpp.org/doc/omnetpp/Manual.pdf – Acceso: 2014-10-07

[4] NETwork Attacks (NETA): http://nesg.ugr.es/index.php/en/neta – Acceso: 2014-06-07

[5] L.Sánchez-Casado, G. Maciá-Fernández y P.García-Teodoro. *Data Forwarding in MANETs: An Analytical Model to Detect Malicious Packet Dropping Behaviors.* NESG, 2014.

[6] L. Sánchez-Casado, R. Magán-Carrión, P. Garrido-Sánchez y P. García-Teodoro. *Protocolo para la Notificación y Alerta de Eventos de seguridad en Redes Ad-hoc*. RECSI (Reunión Española sobre Criptología y Seguridad de la Información), 2014.

Pablo Garrido Sánchez nació en Cádiz, España, en mayo de 1992. Actualmente estudia el Máster en Ingeniería de Telecomunicación de la Universidad de Granada tras haber terminado satisfactoriamente el Grado de Ingeniería de las Tecnologias de Telecomunicación con mención en Telemática en junio de 2014 en la misma universidad. Además de la telemática y la seguridad en redes, sus principales intereses incluyen ciertas ramas de la electrónica como son los sistemas empotrados o la automatización y robotica.

Herramientas Big Data de detección de intrusiones para entorno docente y de investigación en Seguridad en Redes de Computadores

Autor: Anabel Reyes Maldonado; e-mail: anreyes@correo.ugr.es
Tutor: José Camacho Páez; e-mail: josecamacho@ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—Gracias a la alta disponibilidad de información de distintas fuentes que ha hecho posible el desarrollo de Internet, uno de los conceptos más importantes es el tratamiento y análisis de grandes conjuntos de datos: el llamado Big Data. La experiencia sobre estas técnicas se acepta como una de las capacidades más interesantes para la contratación de nuevo personal técnico en las grandes multinacionales, junto con el uso de herramientas como Splunk y Afterglow. Actualmente, los laboratorios docentes de la Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación (ETSIIT) de la Universidad de Granada no poseen la flexibilidad requerida para el estudio de la seguridad en red con herramientas Big Data. Dicha limitación es la razón por la cual se plantea el uso de la emulación por virtualización de sistemas para la realización de este trabajo. Mediante este proyecto se han podido comprobar las ventajas e inconvenientes que tiene cada una de estas herramientas, así como la facilidad de detección de anomalías en red gracias a ellas.**

***Palabras clave*—Afterglow, Big Data, Firewall, Seguridad, Sistema Detector de Intrusos, Splunk.**

I. PROBLEMÁTICA

DEBIDO al gran aumento del número y sofisticación de las amenazas de seguridad se necesitan de habilidades y herramientas para tratar el problema, como es el análisis de grandes cantidades de datos (Big Data).

La empresa RSA señala al Big Data como una solución transformadora para los retos de seguridad, donde el análisis de Big Data permitirá que los profesionales de seguridad recuperen las ventajas de la vigilancia en tiempo real con respecto a los ataques sofisticados [2].

FICO prueba la importancia que está teniendo el Big Data sobre todo en los últimos años [3], afirmando que:

- La venta de soluciones de analítica pasó de 11.000 millones de dólares en 2000 a 35.000 millones de dólares en 2012.
- Que el número de puestos de trabajo relacionados con el Big Data creció un 15% entre 2011 y 2012.
- Y que cada día se crean 2,5 trillones de bytes relacionados con Big Data, por lo que la analítica es cada vez más necesaria para tomar decisiones predictivas precisas.

La *Figura 1* representa un estudio según Cisco, donde muestra la cantidad de datos de tráfico IP que se van a generar mensualmente hasta 2016 en el mundo. Este crecimiento va a estar influido por los distintos factores como el creciente número de dispositivos conectados, un mayor número de usuarios en Internet, una mayor velocidad de ancho de banda, más vídeos, crecimiento del uso del WiFi, entre otros.

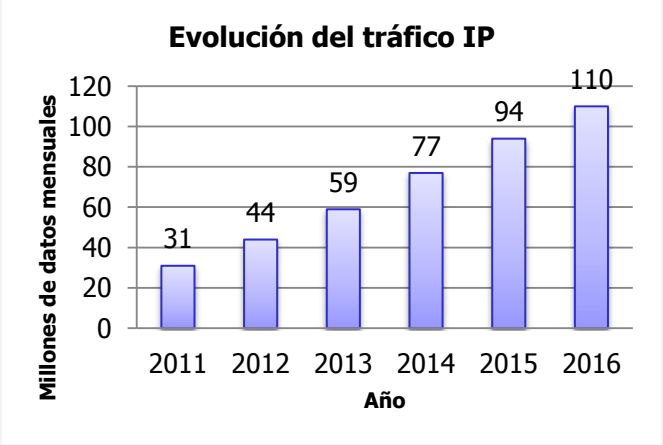


Figura 1. Datos mensuales previstos para el 2016

Esto es un reflejo del interés en ofertar contenidos docentes sobre seguridad en red con herramientas Big Data.

Los laboratorios de la Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación presentan severas limitaciones para el diseño flexible y realista de prácticas de seguridad en red. Por lo que se plantearon dos objetivos principales para la realización del mismo:

- Objetivo I: Un primer objetivo de este proyecto es el diseño una metodología para instaurar un laboratorio virtual de seguridad en redes de comunicación. Dicha metodología se enmarca dentro de una propuesta del Proyecto de Innovación Docente.
- Objetivo II: Para poder realizar todo lo mencionado, es necesario disponer de sistemas de detección como sistemas detectores de intrusos (IDS) o firewalls,

que permitan detectar accesos no autorizados a la red y almacenarlos en un archivo de registro de eventos (.log) para su posterior análisis mediante las herramientas Big Data de detección de intrusiones. Además se realizó un test de penetración y la creación de una *botnet*, en conjunto con las herramientas de detección, para estudiar ambas vertientes de la seguridad, es decir se comprobó cómo de preventivo puede llegar a ser un estudio de seguridad, o cómo trabaja una de las mayores técnicas de infección, así como la reacción por parte de una Organización que incluye métodos proactivos de seguridad.

II. SOLUCIÓN PROPUESTA

La limitación de los entornos docentes es la razón principal por la cual se ha realizado un estudio de las diversas aproximaciones a una red real con las que se podría solventar el problema. De forma que se han analizado sus fortalezas y sus debilidades y elegido posteriormente la más completa y realista.

En un primer lugar se pensó en la utilización de la virtualización, con ella se puede utilizar más de un sistema operativo en un mismo ordenador, de forma simultánea y persistente, de esta forma nos acercamos más a una aproximación de una red real [3]. Uno de los inconvenientes de las máquinas virtuales es su coste computacional, que lleva a que la ejecución de un gran número máquinas pueda saturar fácilmente los recursos de la máquina anfitriona.

En segundo lugar, y por el contrario que la virtualización, la emulación no permite ni la simultaneidad entre sistemas operativos, ni ejecutar directamente el código del sistema huésped [4]. La principal diferencia con la virtualización reside en que los emuladores hacen una translación de las instrucciones de la maquina emulada, en lugar de ejecutar directamente el código en el *guest.* Por este motivo, los virtualizadores tienen un funcionamiento menos problemático y más rápido que el tradicional emulador.

En cuanto a la simulación la elaboración de un modelo de simulación realista puede conllevar horas y horas tanto de trabajo como de espera de resultados. Por este motivo, la simulación no parece la estrategia más adecuada para el estudio de la seguridad en red.

De modo que analizadas las circunstancias, decidimos elegir la virtualización ya que es la única herramienta que nos posibilita la simultaneidad entre sistemas operativos, siendo esta crucial para el desarrollo de los experimentos de seguridad.

Ya que se ha optado por la virtualización, se debía elegir también la plataforma de virtualización. Se ha analizado VirtualBox, VMware y KVM. Entre ellas aunque la que mejor rapidez, estabilidad y rendimiento ofrece es VMware, se ha seleccionado VirtualBox por ser gratuito y multiplatafoma, además de ofrecer prestaciones aceptables.

III. HERRAMIENTAS BIG DATA DE DETECCIÓN DE INTRUSIONES

En la realización de este proyecto se han hecho uso de las siguientes herramientas de detección de intrusiones.

A. Firewalls

Un firewall o cortafuegos es un dispositivo de hardware o un software que permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una red. Protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet) [5].

En concreto se ha hecho uso de Iptables, que es componente más popular construido sobre Netfilter. Iptables una herramienta de cortafuegos que permite, no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log.

B. Sistemas Detectores de Intrusos

Un Sistema Detector de Intrusos o IDS es un sistema que intenta detectar y alertar sobre las intrusiones intentadas en un sistema o en una red, considerando intrusión a toda actividad no autorizada o no que no debería ocurrir en ese sistema.

En concreto se ha hecho uso del IDS Snort. Snort es un sniffer de paquetes y un detector de intrusos basado en red. Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL [6]. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

C. Sistemas de monitorización

Se ha hecho uso del Sistema de Monitorización *Splunk* que es un software que captura, indexa y correla en tiempo real los datos generados por máquinas de aplicaciones, almacenándolo todo en un repositorio donde busca para generar gráficos, alertas y paneles muy fáciles de definir [7]. Además, ayuda a visualizar una gran cantidad de datos mediante la realización de pequeñas gráficas. Se puede descargar Splunk gratis, obteniendo una licencia Enterprise de Splunk por 60 días y donde podremos indexar hasta 500 megabytes por día. Se puede convertir a una licencia gratuita perpetua o comprar una licencia Enterprise.

D. Sistemas de visualización

Se ha hecho uso del Sistema de visualización Afterglow. Afterglow es una colección de scripts que facilitan el proceso de generación de enlaces gráficos [8]. AfterGlow está destinado para ser utilizado en la línea de comandos ya que no dispone de ninguna interfaz gráfica de usuario, aunque también puede ser incorporado a otras aplicaciones (como es nuestro caso, incluida dentro de Splunk). AfterGlow espera un archivo CSV, como entrada y genera un archivo de lenguaje gráfico de puntos atribuido.

IV. PRUEBAS

Una vez analizadas las opciones para la reproducción de un estudio de seguridad en un entorno virtualizado, para su posterior uso docente en los laboratorios de la Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación (ETSII) de la Universidad de Granada, se realizaron una serie de experimentos para evaluar la respuesta de Splunk en el análisis de grandes cantidades de datos, recogidos por un firewall y un sistema detector de intrusos (IDS), y la visualización de lo obtenido mediante la herramienta Afterglow.

La red física de la que se partirá es la mostrada en la *Figura 2*. En cada una de las dos máquinas físicas implicadas se virtualizaron los sistemas operativos necesarios para cada experimento y en los que cada una contiene la instalación y configuración de las herramientas necesarias.

Figura 2. Red física

La máquina uno es propiedad de Mónica Leyva [9], y con ella se ha realizado el test de penetración y la creación de una botnet. Mientras que la máquina 2 es de mi propiedad, y en ella se incluyen las herramientas de detección de intrusos y visualización de resultados, así como de la red privada objeto de penetración e infección. La interconexión se ha hecho mediante un router físico y cables de red.

Se realizaron dos experimentos, haciendo uso de virtualización mediante Oracle VM VirtualBox, lo que da flexibilidad para, con dos máquinas, poder modelar redes de alto realismo y formadas por un gran conjunto de máquinas.

Ambos experimentos han contado con ataques a la seguridad estudiados estudiados por Mónica Leyva García en su proyecto "Herramientas de test de penetración y ataques en red para entorno docente y de investigación en Seguridad en Redes de Computadores" dirigido por el profesor José Camacho Páez [9].

V. EXPERIMENTO I: TEST DE PENETRACIÓN

En este primer experimento se ha realizado un escaneo de puertos mediante el software Nmap desde una máquina situada fuera de la red interna privada. En segundo lugar se ha realizado un escaneo de vulnerabilidades mediante Nessus de la máquina a atacar (en este caso un equipo con sistema operativo Windows XP vulnerable), de forma que escaneará los puertos para buscar puertos abiertos y después intentará varios exploits para atacarlo. Por último, ha realizado la explotación mediante Metasploit y, una vez dentro del equipo se eliminó y creó archivos. Todos estos ataques han sido realizados por Mónica Leyva García en su proyecto [9].

El setup escogido para la realización de este caso de estudio es el de la *Figura 3*.

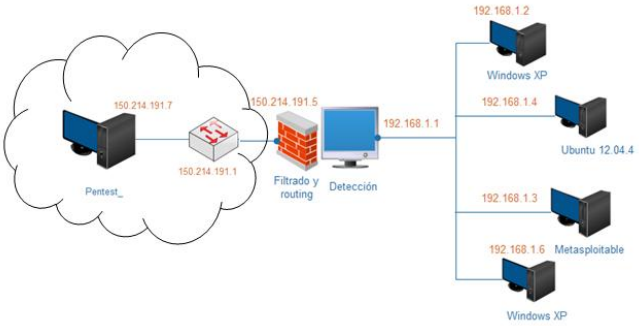


Figura 3. Diagrama de red "Teste de Penetración"

A. *Fase de exploración*

Una vez recogidos los datos registrados por los sensores (snort e iptables) se indexan en Splunk para su monitorización. Al recibir eventos que contienen las palabras claves "nmap" y "scan" se activa una de las alertas gestionadas. Para ver mejor la cantidad de eventos de alerta sobre escaneos mediante el software Nmap, se realiza mediante Splunk una visualización, como se puede ver en la *Figura 4*. En ella se puede ver un resumen de todos los eventos recogidos por la alerta en función del tiempo en el que se dieron.

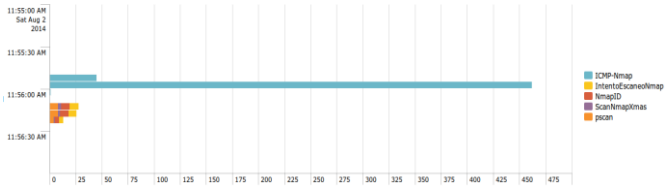


Figura 4. Cantidad de eventos Nmap

Cabe destacar que en los primeros intervalos de tiempo se han recibido una gran cantidad de mensajes ping enviados para descubrir los host que están activos. Una vez descubierto el host a atacar se procede a la realización del escaneo de puertos.

B. *Fase de penetración*

Al recibir eventos pertenecientes al software Nessus, Splunk activa una de las alertas gestionadas (Nessus). Si se accede a los datos recogidos por esta se observa que Splunk obtiene datos recogidos por Snort con una referencia externa a sistemas de identificación de ataques soportados por Snort. Si se accede a cada una de las referencias Web que se indican, se da información adicional sobre el plugin de nessus específico.

Por otro lado, Iptables sigue recibiendo mensajes de Nmap, ya que Nessus realiza un escaneo de puertos mediante el uso del software Nmap.

C. *Fase de mantenimiento del acceso*

Snort da dos mensajes de alerta clasificados como débiles cuando Metasploit está accediendo a la máquina, generalmente considerados como falsos positivos, y que en el caso de estudio concreto no indican que se esté realizando una explotación de las vulnerabilidades de un equipo mediante Metasploit.

¿Porqué Snort no detecta a Metasploit una vez dentro? Esto es debido a que Metasploit usa la carga útil Meterpreter la cual reside en la memoria [10]. Por este motivo nuestro sistema detector de intrusos no es capaz de detectar a Metasploit.

VI. EXPERIMENTO II: BOTNET

En este segundo experimento se ha realizado un proceso de infección y robo de información por una *botnet*, todo ello realizado por Mónica Leyva García en su proyecto [9]. En primer lugar, un usuario accede a una página web (http://150.214.191.4/segred) y descarga el troyano Zeus. Una vez infectado el equipo, se accede a otra página web (http://150.214.191.4/segred/ExpII) mediante usuario y contraseña. Así, el Botmaster se hará con estos datos.

El setup escogido para la realización de este caso de estudio es el de la *Figura 5*.

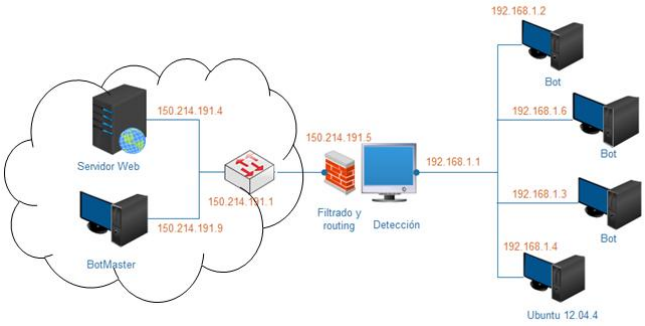


Figura 5. Diagrama de red "Botnet"

Por desgracia para Snort bloquear las peticiones que realiza esta botnet no es un proceso simple debido a la aleatoriedad de las rutas URL que se solicitan para introducir el archivo que contiene el bot [11]. Según referencias consultadas en Internet no hay una regla específica en Snort para detectar al troyano Zeus. En la mayoría de los casos se especifican reglas en Snort para determinadas blacklist de páginas web (páginas web que contienen malware, spam o phishing y están en una "lista negra").

Por lo tanto, para este caso de estudio se ha configurado Snort de manera que detecte y alerte sobre peticiones GET, POST, descarga de un ejecutable (.exe) y M-SEARCH. Splunk es el responsable de alertar en el caso de recibir todas estas alertas de forma consecutiva, de forma que esta se active cuando se reciban eventos en un rango de tiempo corto (3 minutos) y que además la suma de la cantidad de eventos recibidos (GET+POST+M-SEARCH+ejecutable) sea un número igual o superior a 7, ya que cuando se produce una infección con Zeus se va a recibir: GET, POST, GET, descarga ejecutable .exe, M-SEARCH, M-SEARCH, M-SEARCH.

A. *Fase de reclutamiento*

Cuando se accede a una página web, se envía una solicitud HTTP GET para obtener información referente al servidor. Una vez se accede a la descarga del ejecutable se envía una solicitud HTTP POST y se procede a la descarga del archivo que contiene el bot (bot.exe). Por último, una vez realizada la infección, se envían las 3 solicitudes M-SEARCH desde la Botmaster.

B. *Fase de ejecución del ataque*

Al acceder a una página web, se envía una solicitud GET hacia el servidor. Una vez nos identificamos en la página con usuario y contraseña, se envía un HTTP POST hacia el servidor web y otro hacia la Botmaster para enviar la información recogida a la base de datos. Estas peticiones se realizan mediante solicitudes GET y POST, por lo que en una situación normal esto no podría ser considerado como robo de información, ya que estas son las mismas que las enviadas en una comunicación normal entre un cliente y el servidor web correspondiente, es decir, no podemos detectar el robo de información que realiza la Botmaster.

C. *Ataque satisfactorio*

Una vez llevada a cabo la infección, Splunk genera alertas sobre la detección de varias solicitudes GET, POST, ejecutable .EXE y M-SEARCH. Por desgracia, hay que observar detenidamente cada una de estas alertas ya que pueden dar lugar a falsos positivos. Para ello, se accede a la alerta, Splunk notifica sobre los eventos producidos que cumplan con la condición de la misma en determinados intervalos de tiempo donde ocurrió el problema. Se deben revisar cada una de estas alertas para ver si ha ocurrido un posible caso de infección mediante el troyano Zeus.

En la *Figura 6* se puede ver un caso de éxito de infección de un equipo mediante el uso de la botnet Zeus, ya que cumple con los requisitos mínimos establecidos para considerar que se ha producido una infección mediante el uso de esta botnet.

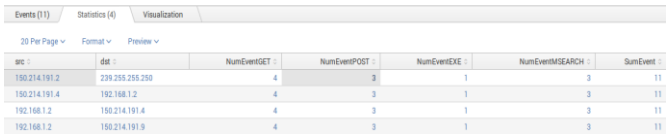


Figura 6. Detección de infección mediante la botnet Zeus

En la *Figura 7* se puede observar una representación mediante Afterglow de una infección mediante la botnet Zeus y su posterior robo de información.

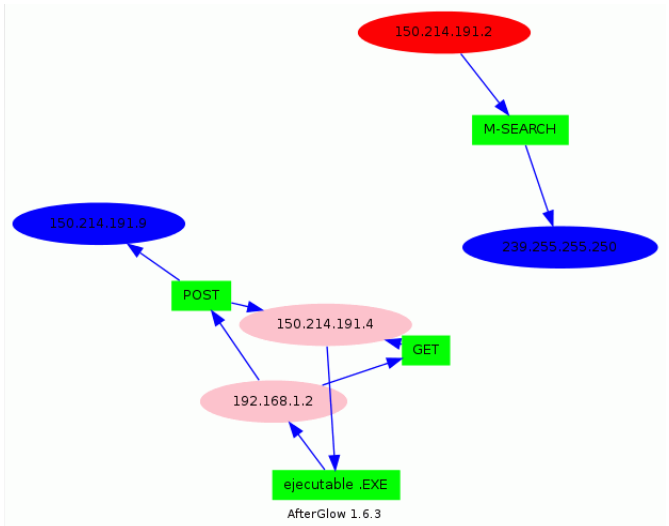


Figura 7. Visualización de la infección mediante Zeus

VII. CONCLUSIONES

Para finalizar, destacar como ventaja principal de Splunk su facilidad a la hora de configurar una alerta tanto para la detección de escaneos como de una intrusión, además de una vista rápida y cómoda de los resultados para poder analizar el problema de una forma más sencilla.

Afterglow, al estar incorporado dentro de Splunk, nos ofrece la ventaja de una visualización fácil y rápida del problema, sin necesidad de tener conocimientos adicionales sobre la configuración del mismo.

Como desventaja, cabe destacar las deficiencias que presentan tanto los sensores en cuanto a la detección de Metasploit o en la configuración para la detección de una infección por parte de una botnet, como de Splunk para una detección 100 % segura de la botnet específica estudiada.

Finalmente, se puede concluir que el material generado en el presente proyecto para ser utilizado en un laboratorio de seguridad cumple totalmente con los objetivos iniciales. En este sentido, se establece un punto de inicio para la consecución de dicho laboratorio virtual de seguridad en redes de comunicación, aportando el realismo propio de una red real y la flexibilidad necesaria para que con tan solo dos ordenadores, una pareja de alumnos pueda simular todas las partes de una red.

AGRADECIMIENTOS

En primer lugar agradecer a mi tutor del proyecto, José Camacho, por darme la oportunidad de trabajar con él. En segundo lugar a mis padres, porque sin su cariño, su apoyo y dedicación en los momentos duros nunca hubiera llegado hasta aquí.

REFERENCIAS

[1] http://argentina.emc.com/about/news/press/2013/20130226-02.htm
[2] http://www.puromarketing.com/53/18070/experto-data-profesion-futuro.html
[3] http://es.wikipedia.org/wiki/Virtualizaci%C3%B3n
[4] http://centrodeartigos.com/articulos-noticias-consejos/article_126283.html
[5] http://elsoftwarelibre.wordpress.com/2009/07/19/iptables-el-firewall-de-linux/
[6] http://www.linux-magazine.es/issue/46/060-066SnortLM46.pdf
[7] http://es.splunk.com/web_assets/pdfs/secure/Splunk_Product_Datasheet_es.pdf
[8] http://afterglow.sourceforge.net/manual.html#6
[9] Proyecto Final de Carrera “Herramientas de test de penetración y ataques en red para entorno docente y de investigación en Seguridad en Redes de Computadores”, realizado por Mónica Leyva García y supervisado por el Profesor José Camacho Páez.
[10] http://es.scribd.com/doc/212177504/Curso-Metasploit
[11] http://www.fortiguard.com/legacy/analysis/zeusanalysis.html

Herramientas de test de penetración y ataques en red para entorno docente y de investigación en Seguridad en Redes de Computadores

Autor: Mónica Leyva García, e-mail: monilg@correo.ugr.es

Tutor: José Camacho Páez, e-mail: josecamacho@ugr.es

Titulación: Ingeniería de Telecomunicación

Departamento de Teoría de la Señal, Telemática y Comunicaciones

Universidad de Granada

***Resumen*—La seguridad en redes de computadores se ha convertido en una de las principales preocupaciones de toda aquella Organización que posea sistemas de información y tecnologías potencialmente vulnerables. Es por ello que es necesario proteger los activos adecuadamente contra amenazas e intrusiones. El método preventivo con mejores resultados es el test de penetración, por ser tan intrusivo como un ataque real, permitiendo corregir los agujeros de seguridad encontrados.**

Actualmente, los laboratorios docentes de la Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación (ETSIIT) de la Universidad de Granada no poseen la flexibilidad requerida para reproducir condiciones realistas para el estudio de la seguridad en red, por tanto, el presente proyecto establece un punto de inicio para la consecución de un laboratorio virtual de seguridad, combinando la virtualización con los laboratorios de la ETSIIT, incrementando la capacidad de reproducción de un entorno real con la flexibilidad necesaria para el diseño de prácticas de seguridad de gran calidad.

***Palabras clave*— Ataque, *botnet,* ciber-delincuencia, intrusión, seguridad, test de penetración, virtualización, vulnerabilidad.**

.

I. INTRODUCCIÓN

ESTE trabajo presenta un estudio de las técnicas de evaluación de seguridad en una red, apoyado en los llamados tests de penetración. Se evalúan algunas de las principales herramientas necesarias para dichos tests, así como para realizar ataques a una red de computadores. La motivación para abordar este tema reside en que la seguridad TIC es uno de los principales retos de la actualidad debido al aumento de incidencias de seguridad en este ámbito.

El presente proyecto se ha realizado de forma coordinada con el proyecto titulado 'Herramientas BIG DATA de detección de intrusiones para entorno docente y de investigación en Seguridad en Redes de Computadores', realizado por Anabel Reyes Maldonado [1] y dirigido por el profesor José Camacho Páez. En dicho proyecto se evalúan herramientas de monitorización y visualización de la seguridad en red. La combinación de ambos proyectos está enfocada al posterior uso en un entorno docente, para prevenir, detectar y mitigar amenazas haciendo uso de la emulación por virtualización de sistemas.

De modo que, un primer objetivo para este proyecto consiste en diseñar una metodología para crear un laboratorio virtual de seguridad en la ETSIIT, enmarcado dentro del Proyecto de Innovación Docente con código 14-54. Y el segundo de los objetivos consiste en realizar un estudio de ambas vertientes de la seguridad, mediante la realización de un test de penetración y la creación de una *botnet*, en conjunto con las herramientas de detección, es decir se podrá comprobar cómo de preventivo puede llegar a ser un estudio de seguridad, o cómo trabaja una de las mayores técnicas de infección, así como la reacción por parte de una Organización que incluye métodos proactivos de seguridad.

II. REVISIÓN DEL ESTADO DEL ARTE

La limitación de los entornos docentes es la razón por la cual se ha realizado un estudio de las diversas aproximaciones a una red real con las que se podría solventar el problema. De forma que se han analizado sus fortalezas y sus debilidades y elegido posteriormente la más completa y realista.

A. Virtualización

La primera aproximación a red real estudiada ha sido la virtualización, con ella se puede utilizar más de un sistema operativo en un mismo ordenador, de forma simultánea y persistente [2]. Es decir, la virtualización es un proceso que se basa principalmente en montar un sistema operativo, denominado máquina virtual, mediante la instalación de un *software* por encima del SO que usamos normalmente, llamado anfitrión.

Uno de los inconvenientes de las máquinas virtuales es su coste computacional, que lleva a que la ejecución de un gran número máquinas pueda saturar fácilmente los recursos de la máquina anfitriona.

Actualmente las plataformas de virtualización más importantes para el uso de máquinas virtuales son las siguientes:

- VMWare [3]. Es el estándar del mercado ya que es el más rápido, estable y seguro, principalmente en sus versiones de pago. Actualmente ofrece dos versiones gratuitas, VMware Player y VMwareESXi, pero con ciertas limitaciones. Es multiplataforma.

- Virtual Box [4]. Única solución profesional gratuita y disponible como software de código abierto GNU (GPL). Tiene soporte multiplataforma incluyendo Solaris y una lista creciente de características como instalar el software con privilegios adicionales a la máquina física, tareas como compartir, archivos, unidades, periféricos, etc.
- KVM [5]. Solución para implementar virtualización completa con Linux. Utiliza una versión modificada de QEMU (emulador de procesadores), que permite obtener un rendimiento espectacular cuando no se trata de Microsoft Windows como guest. No tiene un soporte completo para controladores.

.

B. *Emulación*

La emulación, por el contrario, no permite ni la simultaneidad entre sistemas operativos, ni ejecutar directamente el código del sistema huésped.

La principal diferencia con la virtualización reside en que los emuladores hacen una translación de las instrucciones de la maquina emulada, en lugar de ejecutar directamente el código en el *guest*. Por este motivo, los virtualizadores tienen un funcionamiento menos problemático y más rápido que el tradicional emulador.

C. *Simulación*

Según Shannon, la simulación es el proceso de diseñar un modelo de un sistema real y llevar a término experiencias con él, con la finalidad de comprender el comportamiento del sistema o evaluar nuevas estrategias -dentro de los límites impuestos por un cierto criterio o un conjunto de ellos - para el funcionamiento del sistema [6]. Por tanto un simulador, en este caso, tendría como fin probar la seguridad de una red sin comprometer la máquina donde se simula.

Por desgracia, la construcción de un modelo de gran envergadura no es trivial, ni tampoco la interpretación de los resultados. Además, la elaboración de un modelo de simulación realista puede conllevar horas y horas tanto de trabajo como de espera de resultados. Por este motivo, la simulación no parece la estrategia más adecuada para el estudio de la seguridad en red.

Analizadas las circunstancias, se opta por la virtualización ya que es la única herramienta que posibilita la simultaneidad entre sistemas operativos, siendo esta crucial para el desarrollo de los experimentos de seguridad.

III. SOLUCIÓN PROPUESTA

Teniendo en cuenta los objetivos especificados para este proyecto, la disponibilidad de *hardware* real de interconexión de red en los laboratorios de la ETSIIT, y analizando todas las posibilidades disponibles, la opción más adecuada pasa por combinar el uso del virtualizador VirtualBox, por ser gratuito, multiplatafoma y ofrecer prestaciones aceptables, junto con un dispositivo de interconexión real, aportando mayor realismos y menor gasto computacional que una simulación del dispositivo.

IV. DISEÑO DEL ENTORNO

Se ha seleccionado la configuración detallada, por ser considerada la idónea para la posterior extrapolación de la misma a los laboratorios docentes de la ETSIIT, así como para realizar el test de penetración y la creación de una *botnet*. En la Fig..1, se observa la red física a partir de la cual se inician los experimentos. En la máquina 1 se virtualizan todos aquellos sistemas operativos necesarios para el *pentest* y el despliegue de la *botnet*, mientras que la máquina 2, propiedad de [1], se encarga de la detección de intrusos en la red, es decir, en ella se encuentran tanto las máquinas virtualizadas vulnerables como las de detección y visualización. El *router* interconecta ambas subredes. Además se ha configurado VirtualBox de forma que simule una red física real y soporte que cada una de las máquinas virtuales tenga una IP diferente.

El primero de los casos de estudio es un test de penetración. Un test de penetración es un análisis de seguridad autorizado por la Organización solicitante, éste se trata del método preventivo con mejores resultados, por ser tan intrusivo como un ataque real, permitiendo corregir los agujeros de seguridad encontrados.

El test de penetración no se debe confundir con la auditoría ya que el primero amplía los esfuerzos realizados para la evaluación de vulnerabilidades, es más intrusivo y requiere un nivel de habilidad más alto del que se necesita para la auditoría de red ya que emula acciones de los ciber-criminales. Pero tampoco se debe confundir con el *hacking* a pesar de que los métodos y herramientas empleados sean los mismos. Tras realizar el test de penetración se podrá saber si las estrategias de mitigación empleadas están trabajando como se esperaba y a continuación actuar en consecuencia, tomando medidas preventivas y correctivas.

Un test de penetración debe estar cuidadosamente planificado, de forma que en primer lugar se realizará un análisis del entorno (alcance, IPs…), posteriormente se decidirá el tipo de test de penetración que se realizará y completará el análisis preparatorio mediante un análisis de puertos. A continuación se confecciona una lista detallada de vulnerabilidades encontradas, para que en la etapa de mantenimiento del acceso el *pentester* emule al ciber-criminal y explote éstas vulnerabilidades. Finalmente se deberían eliminar rastros, aunque en el presente proyecto no se ha realizado dado que se está colaborando con [1] y ella podría necesitar esos rastros para determinar mi intrusión.

Además de la correcta planificación, se debe conocer qué herramientas hay disponibles para desempeñar el análisis correctamente, de forma que se ha realizado un estudio de las posibilidades y elegido aquellas herramientas mejor

Fig. 1.- Esquema de red real

posicionadas en su categoría según el *ranking* "Top 100 Network Security Tools" [7] , además de ser gratuitas.

Por tanto, como escáner de puertos se ha seleccionado Nmap [8], para la búsqueda de vulnerabilidades se usará Nessus [9] y finalmente para explotar las mismas se empleara Metasploit [10].

El segundo de los casos de estudio, es un ataque de red, para ello se ha creado una *botnet*, grave amenaza de seguridad, que ha multiplicado su presencia en la red en los últimos años. El principal motivo que lleva a los ciberdelincuentes a usar *botnets* es el económico, es decir, enriquecerse a costa de empresas.

En una *botnet*, aquellas máquinas que son infectadas reciben el nombre de *bots*, término derivado de la palabra 'robot', dichas máquinas están controladas por un agente humano conocido como *botmaster*.

La comunicación entre *bots* y *botmaster* se realiza por mensajes de órdenes y control (C&C).Las posibilidades de los *bots* son mayúsculas ya que pueden realizar ataques de DoS, son capaces de distribuir *malware* y *spam*, realizar fraudes y un largo etc.

Aunque una *botnet* pueda usarse como herramienta de *pentest*, su uso en ataques de ciberseguridad es mucho más extendido. Por este motivo, a continuación se seguirá una organización en apartados más acorde con el ciclo de generación de la *botnet* que con las etapas de un test de penetración. Cada una de las etapas del ciclo de vida completo de éstas hasta conseguir el ataque exitoso ilustrará claramente durante el experimento dos.

De entre las *botnet*s estudiadas, se ha seleccionado Zeus [11], que corresponde a una *botnet* HTTP, la cual es controlada remotamente desde un sitio web por el *botmaster*. Zeus se ha especializado en robar credenciales bancarias equipos con versiones de Microsoft Windows.

V. TEST DE PENETRACIÓN

El *setup* elegido para la realización de este caso de estudio se muestra en la Fig. 2 en la Máquina 1, se ha creado una máquina virtual denominada *Pentest_* con la imagen de un Ubuntu e IP 150.214.191.7 a partir de la cual se realizara el test de penetración. Para ello se ha incluido Nmap, Nessus y Metasploit.

La IP ha sido fijada en base al rango de direcciones que mediante DHCP provee el *router*. Este realmente no ejerce de *router* en la red diseñada sino de *switch*. El direccionamiento hacia la red privada se hará desde el *firewall*, Iptables. Tanto el *router* como la máquina virtual, en un caso real serían considerados como Internet.

La Máquina 2, con la imagen Ubuntu, contiene el *firewall* Iptables, u sistema detector de intrusos (IDS), Snort, un *software* de monitorización, Splunk, junto con el *software* de visualización, Afterglow. Este equipo dispone de dos interfaces, una con dirección IP pública (150.214.191.5) y otra con dirección IP privada (192.168.1.1). La red privada incluida contiene distintos sistemas operativos para dotar de realismo a la red.

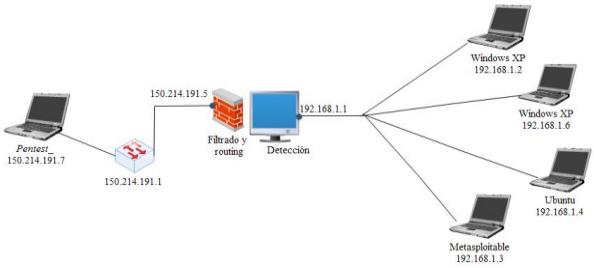


Fig. 2. Mapa de red. Objetivo: test de penetración

Teniendo claro el esquema de red y la finalidad del test de penetración, a continuación se muestra su desarrollo.

El test de penetración se ha realizado en el rango de direcciones privadas de la subred controlada por [1] tratando de conseguir una intrusión obteniendo los más altos privilegios y realizando modificaciones en el mismo.

Se ha procedido al test de penetración mediante una 'Prueba a Ciegas' la cual se lleva a cabo sin el conocimiento del administrador, en este caso [1], para así evaluar la vigilancia y respuesta de éste así como de la propia red. Para ello se conoce el rango de direcciones IP tanto públicas asignadas por el *router* que actúa como servidor DHCP, como privadas establecidas para la red interna.

A continuación, se ha sondeado el sistema mediante un escaneo de puertos. La herramienta con la que se ha desempeñado este propósito es Nmap que manda paquetes IP, TCP y UDP al sistema remoto y analiza las respuestas comparando con su base de datos, para determinar qué *hosts* están disponibles en la red, qué servicios están ofreciendo los anfitriones (nombre de la aplicación y versión) y qué sistemas operativos se están ejecutando.

En esta Fig. 3 se muestra parte del resultado de escanear todo el rango de direcciones privadas. Que tal y como se observa se ha conseguido saber que la máquina cuya IP es la 192.168.1.2 usa un sistema operativo de Microsoft Windows, ya sea XP o 2003. Además se muestran los puertos que están abiertos y el tipo de servicios que ofrecen. Con esta información acerca del SO y los servicios ya se pueden conocer algunas vulnerabilidades del sistema.

Queda completado por tanto el trabajo preparatorio, Tras la evaluación, se usa un *scanner* para confeccionar una lista con las vulnerabilidades y su nivel de riesgo. El *scanner* elegido es Nessus.

```
monica@monica-VirtualBox:~$ sudo nmap -O 192.168.1.0-255

Starting Nmap 6.00 ( http://nmap.org ) at 2014-06-12 12:20 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.0045s latency).
All 1000 scanned ports on 192.168.1.1 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.2
Host is up (0.0082s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_s
erver_2003
OS details: Microsoft Windows XP Professional SP2, Microsoft Windows XP SP2 or S
P3, or Windows Server 2003, Microsoft Windows XP SP2 or Windows Server 2003 SP2
```

Fig.3. Resultado escaneo de puertos

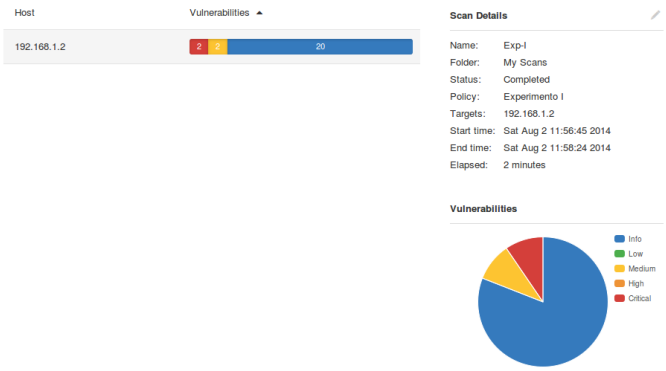


Fig. 4. Resultado del escaneo realizado por Nessus

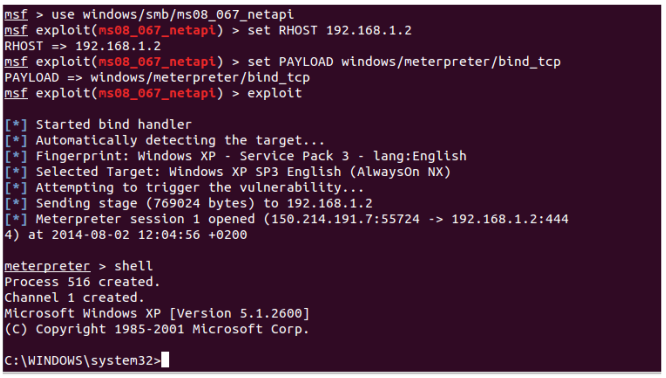


Fig. 5. Acceso conseguido

Tras finalizar el escaneo a la dirección 192.168.1.2, se reporta el número de vulnerabilidades de la máquina y el riesgo asociado a las mismas, como se observa en la Fig. 4.

De entre las dos vulnerabilidades que mayor riesgo tienen asociado, las características que presenta la vulnerabilidad *MS08-067* son más afines a la finalidad de este test de penetración, por lo que será la usada para el mantenimiento del acceso.

MS08-067 es una vulnerabilidad en el servicio 'Server' que un atacante puede aprovechar para ejecutar código arbitrario sin autenticación y con los mismos privilegios que el usuario que haya iniciado la sesión. Si dicho usuario posee derechos de administrador, se tendrá control completo del sistema para crear, modificar o borrar archivos, instalar programas, crear nuevas cuentas de usuario, etc.

Tras detectar la vulnerabilidad el *pentester* debe comportarse tal y como un ciber-delincuente y explotar las debilidades del sistema. De los tres *exploiters* válidos para la vulnerabilidad *MS08-067*, se usará Metasploit por ser gratuita.

Para explotar la vulnerabilidad, Fig. 5, en primer lugar se hace uso del protocolo de red SMB usado para compartir archivos entre nodos de una red, pero cuya finalidad, en este caso, es acceder remotamente a un Windows XP aprovechando el *bug* mediante el cual se realiza la explotación.

A continuación se configuran los parámetros del módulo con el que se trabaja, en este caso *MS08_067_netapi*, y se establece la dirección del equipo poseedor de la vulnerabilidad. Finalmente, se ejecuta la carga útil, es decir, la parte del *exploit* que realiza la acción maliciosa en la máquina víctima.

Como la finalidad es entrar en el sistema de la víctima, el tipo de carga útil usado es el *bind_ tcp* de Meterpreter. Meterpreter se trata de carga útil avanzada, que opera a través de la inyección de DLL. El Meterpreter reside completamente en la memoria de la máquina remota y no deja rastros en el disco duro, por lo que es muy difícil de detectar con las técnicas forenses convencionales. Por último, si se lanza un *shell*, obtenemos el acceso al sistema con privilegios de administrador.

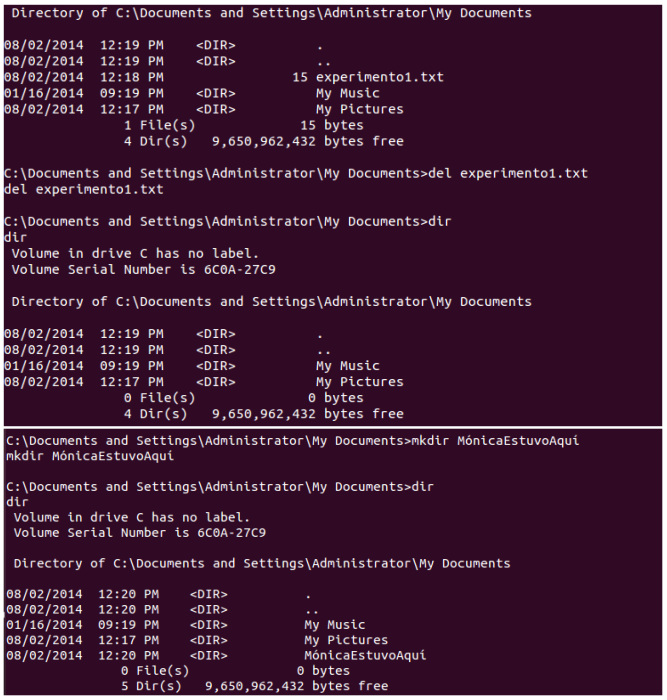


Fig. 6. Modificaciones en el sistema remoto

Una vez que se ha conseguido el acceso, las posibilidades son múltiples… En el test de penetración con conseguir modificar, crear o eliminar algún archivo es suficiente para demostrar que el sistema es potencialmente vulnerable. En la Fig. 6 se muestra cómo se ha eliminado el documento *'experimento1.txt'* y cómo se ha creado una nueva carpeta denominada *'MónicaEstuvoAquí'* sin ningún tipo de impedimento.

VI. BOTNET

En la fig. 7 se puede ver en detalle la arquitectura de red planteada para el segundo caso de estudio, tratándose éste de la creación de una *botnet Zeus*. El segmento de la red que a este proyecto corresponde difiere al anterior y se conforma de *botmaster* (150.214.191.9) *y servidor web* (150.214.191.4).

El *botmaster* se ha realizado a partir de un SO Windows XP y cuenta con herramientas para crear, mantener y controlar la botnet.

Por otra parte en un Ubuntu se ha incluido un servidor web en el cual se aloja la página web desde la que los usuarios descargarán el ejecutable del Zbot. También incluye una

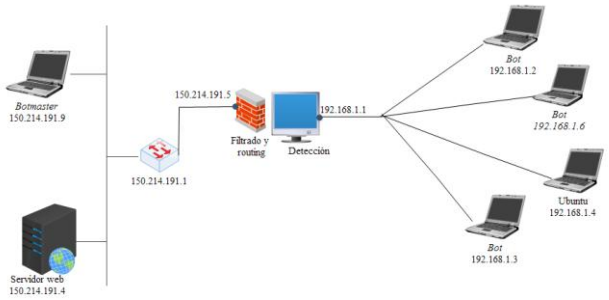


Fig 7. Mapa de red. Objetivo: creación de botnet

página web con un formulario a rellenar por los clientes, de forma que a aquellos que sean *bots*, le puedan ser robados los credenciales.

El direccionamiento se hace tal y como en el experimento anterior y las herramientas usadas para la detección por parte de [1]son las mismas. Aquellas máquinas de la red privada cuyo sistema operativo sea Microsoft Windows que ejecuten el Zbot, se convertirán automáticamente en *bots* de la red.

El ciclo de vida de la botnet comienza con la concepción. En esta etapa, el fichero relevante para la confección del *bot.exe* el cual desencadenará la infección es el config.txt

El archivo de configuración se divide en dos secciones; *staticConfig y dynamicConfig. StaticConfig c*ontiene los parámetros que son codificados en el *bot* y a los que obedece el mismo y d*ynamicConfig incluye* parámetros que pueden ser cambiados tras la creación del *Zbot,* ya que no son codificados por el *builder*, sino que son guardados como una configuración encriptada a la que el *bot* tiene acceso a ellos en todo momento, como es el caso de la URL del *script* php que acepta las descargas de los datos, archivos etc. de los *bots.*

Una vez que el archivo de configuración ha sido editado en base al fin buscado, es momento de crear el troyano. Para ello se emplea la herramienta *Zeus Builder.* Tras cargar el *config.txt* se crean los archivos *.bin y .exe*, siempre y cuando el *builder* no encuentre errores en el archivo de configuración. Ambos archivos obtienen su nombre a través del *config.txt*.

Una vez que se ha creado el troyano, es momento de considerar qué método de infección es el adecuado. En este proyecto se ha creado un servidor web que aloja la página web a partir de la cual cada usuario que acceda descargará el ejecutable del *bot.*

En el momento en el que este cliente se identifique correctamente y trate de acceder al contenido que hay tras ella, según el navegador que use pedirá confirmación para que el *bot.exe* sea almacenado o se descargará automáticamente. En todos los casos el usuario posteriormente deberá ejecutarlo.

Tras la ejecución, se inician dos procesos casi simultáneos. Por una parte, el ejecutable descargado y usado en la instalación se elimina de forma automática, se copia a sí mismo en el PC, aumenta sus privilegios e inyecta código de modo que intercepta la API de Windows en cada proceso.

Tras completarse todo este proceso, el *bot* envía tres consultas "M-SEARCH *" a la dirección *multicast* 239.255.255.250, a través del puerto UDP 1900 (SSDP)

Esta consulta UPnP se utiliza para detectar dispositivos UPnP en la red, y determinar así si el ordenador infectado tiene una IP pública.

Por otra parte, el *botmaster* en su servidor a partir de este instante registrará al equipo, y por tanto comienza el ciclo de interacción donde el cliente se convierte en un *robot* de la *botnet*. Con la infección de la víctima ya se tiene una infraestructura C&C (Comand & Control), y para controlarla el *botmaster* dispone del panel de control.

La página inicial se muestra información sobre cuántos equipos hay infectados, cuánto tiempo están activos, versión del *bot* etc.

Tras la infección, cuando el *bot* acceda a determinada página web, los credenciales serán robados. En la Fig. 8 se ve cómo la máquina cuya IP es 192.168.1.2. trata de acceder a la página http://150.214.191.4/segred/login_sucessII.php introduciendo su pareja de *usser-pass* correctamente en http:// 150.214.191.4/segred/ExpII.php , Tras ser comprobado por el servidor que los datos son correctos y redireccionar a la página deseada http://150.214.191.4/segred/login_sucessII.php, el *bot* envía la información robada al servidor de comando y control, mediante una solicitud POST al *url_server*, URL especificada en el archivo de configuración.

El servidor de comando y control usa una base de datos MySQL llamada 'bssnet' para almacenar información acerca de la *botnet*, es por ello por lo que se pueden mostrar los reportes en cualquier momento desde el panel de control.

Esto se puede se puede ver en la Fig.9, donde se muestran los resultados del robo de credenciales detallado en este experimento (observar *user*, *pass*, URL inicial y redirección).

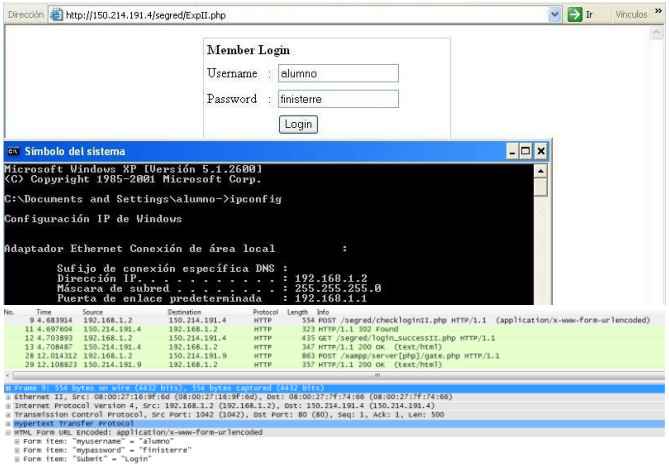


Fig. 8.- Robo de credenciales

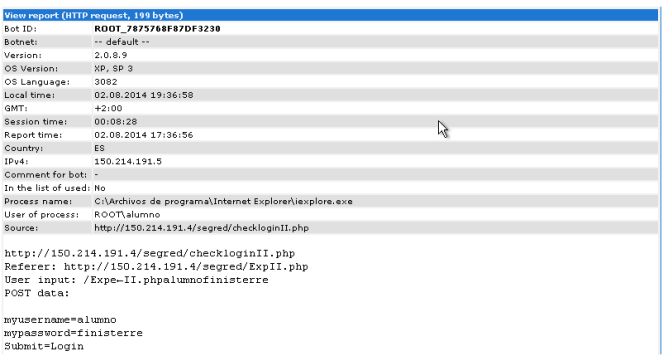


Fig. 9. Reporte de credenciales robados

Queda constatado que Zeus posee una potente capacidad de intrusión y de robo ya que aunque en el presente proyecto, las credenciales robados no son más que una identificación de acceso a una página web, en el caso en que la máquina infectada efectuase una compra *online*, la importancia del robo aumentaría enormemente ya que a partir de dicho instante, el *botmaster* podría usar esa cuenta bancaria como si se tratase de la suya propia.

VII. ANÁLISIS DE LOS RESULTADOS

Este proyecto ha sido orientado a diseñar un entorno docente y de experimentación de seguridad en red, y ofrecer un par de casos de estudio en el mismo. Se puede concluir que el material generado en el presente proyecto para ser utilizado en un laboratorio de seguridad cumple totalmente con los objetivos iniciales.

Inicialmente se ha realizado un estudio de las técnicas de evaluación de seguridad en una red para realizar un test de penetración y mediante las herramientas seleccionadas se ha conseguido detectar que en la red había máquinas vulnerables a las cuales se ha podido acceder y modificar archivos con permisos de administrador, y lo que es más, todo ello sin dejar huella una vez que se ha accedido. De forma similar, se ha conseguido satisfactoriamente crear una *botnet* y recopilar credenciales de las máquinas infectadas.

Si penetración o ataque se realizan en una Organización reglas de detección defectuosas, o inexistentes, las alertas no serán registradas, como se ha podido comprobar con algunas de las pruebas realizadas.

REFERENCIAS

[1] Reyes Maldonado, Anabel. “Herramientas BIG DATA de detección de intrusiones para entorno docente y de investigación en Seguridad en Redes de Computadores”. Proyecto Fin de Carrera, TSTC, UGR, Granada, España 2014

[2] VIRTUALIZACIÓN http://www.microsoft.com/spain/virtualizacion/products/server/default.mspx

[3] MÁQUINA VIRTUAL, VMWARE *http://www.vmware.com/es*

[4] MÁQUINA VIRTUAL, VIRTUALBOX https://www.virtualbox.org/

[5] MÁQUINA VIRTUAL, KVM *http://www.linux-kvm.org/page/Main_Page*

[6] SIMULACIÓN *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4309432*

[7] TOP 100 NETWORK SECURITY TOOLS *http://sectools.org/*

[8] *NMAP http://nmap.org/*

[9] NESSUS *http://es.wikipedia.org/wiki/Nessus*

[10] PROYECTO METASPLOIT *http://en.wikipedia.org/wiki/Metasploit_Project*

[11] ZEUS- BOTNET *http://www.antisource.com/article.php/zeus-botnet-summary*

Herramienta para la detección de *botnets* parásitas P2P

Autor: Juan Rafael Villén Pulido, e-mail: juanry_5@hotmail.com
Tutor: Gabriel Maciá Fernández; e-mail: gmacia@ugr.
Tutor: Rafael Alejandro Rodríguez Gómez; e-mail: rodgom@ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*— El principal potencial de las redes *botnets* reside en su infraestructura distribuida, de forma que numerosos equipos controlados por un solo atacante son capaces de cometer actividades ilegítimas, En concreto, una de las preocupaciones de la actualidad es el negocio ilegal que subyace bajo ellas, el cual mueve cifras económicas alarmantes.**

De todos los tipos de *botnets* existentes, el presente Trabajo está centrado en las *botnets* parásitas P2P. Este tipo de *botnets* utilizan redes legales y legítimas para ocultarse y comunicarse.

El propósito de este Trabajo es la implementación de una herramienta de detección de *botnets* parásitas que funcione de forma unificada aprovechando distintos módulos ya implementados. Sus objetivos principales son llevar a cabo una monitorización constante de los recursos de una zona de la red de Mainline y descargar de forma automática aquellos recursos identificados como anómalos por el algoritmo de detección de *botnets* parásitas. Así, la herramienta a desarrollar permitirá, la visualización de los resultados obtenidos en una interfaz gráfica.

***Palabras clave*— detección de botnets parásitas, Kademlia, Mainline, monitorización, P2P, preprocesado, recursos anómalos.**

I. INTRODUCCIÓN

ACTUALMENTE, la detección de *botnets* es una temática bastante popular en la literatura de investigación. Una gran mayoría de las propuestas para la detección de *botnets* están basadas en mecanismos de detección a través de los cuales se pueda extraer la actividad *Command and Control* (C&C) de la *botnet.* En [1] se describen diferentes técnicas de detección de botnets basadas en la extracción de la actividad C&C de la *botnet.* Entre ellas podemos encontrar técnicas de detección estructurada y técnicas basadas en el comportamiento. Estas técnicas necesitan un análisis de una gran cantidad de tráfico de la red de la cual extraer modelos de comportamiento para aplicar a la hora de detectar anomalías en la red. El problema principal de este tipo de técnicas, es que suelen ser técnicas particulares para cada una de las *botnets* a detectar, debido principalmente a que el tráfico de red C&C es muy variable de unas *botnets* a otras.

Este trabajo está centrado en un tipo de *botnets,* en concreto está centrado en las *botnets* parásitas P2P. La particularidad de este tipo de *botnets* son las siguientes:

1. Este tipo de redes construyen canales C&C de acuerdo al protocolo de comunicación de una red P2P como puede ser el caso de BitTorrent.
2. Los paquetes con los comandos de la *botnet,* son enviados periódicamente a través de la red de BitTorrent hacia los miembros de la *botnet* que serán los encargados de ejecutarlos.

Es decir, este tipo de *botnets* difieren de las *botnets* P2P tradicionales en que utilizan en su fase de interacción redes legítimas para comunicarse.

Dentro del campo de la detección de *botnets*, la detección de las *botnets* parásitas está considerada como uno de los problemas más complejos [2]. Esto es debido principalmente a que en las *botnets* P2P, no tienen un sistema estructurado si no que son de tipo distribuido y los recursos son compartidos por diferentes nodos de la red, de esta forma, estas *botnets* no pueden ser eliminadas atacando al servidor central. Por otro lado, en las redes P2P la compartición de un recurso, que contiene las ordenes para los miembros de la *botnet*, no tiene porqué diferir sustancialmente de lo que podría ser la compartición normal de un recurso en la red P2P legítima.

Por este motivo principal, no es útil llevar a cabo un sistema de detección basado en el estudio del tráfico de la red a través del cual se puede detectar que lo que se está compartiendo es un recurso que contiene comandos pertenecientes a un *botmaster*.

En [3] se presenta hasta ahora, el único esquema de detección de *botnets* parásitas, basado en el modelado de la evolución del número de nodos que comparten un recurso en una red P2P durante el tiempo. Este sistema de detección está basado en la monitorización del número de nodos que comparten un recurso determinado. En base a este número de nodos y a un modelo teórico del comportamiento esperado en la compartición de un recurso por parte de una *botnet*, esta aproximación es capaz detectar la compartición de recursos pertenecientes a posibles *botnets* parásitas.

Haciendo uso de este esquema de detección, en este Trabajo se ha implementado una herramienta de detección de *botnets* parásitas que funciona de forma unificada aprovechando distintos módulos ya implementados**.**

II. Conceptos Fundamentales De Bittorrent

A continuación para la comprensión general del presente trabajo, se explican los conceptos fundamentales de Bittorrent.

BitTorrent es una red de compartición de archivos P2P en Internet. Sobre dicha red se comparten muchos archivos con diferentes formatos y contenido. El objetivo principal de BitTorrent es llevar a cabo una compartición distribuida de archivos por un número elevado de clientes, motivando a su vez que aquellos que hayan descargado los archivos, los compartan con posterioridad. Los archivos que se comparten en la red de BitTorrent son llamados recursos, mientras que los clientes son llamados pares (*peers*) o nodos.

El presente trabajo, trabajo realiza la monitorización de los recursos de la red de Mainline. Esta red es una implementación de Kademlia usada por clientes de BitTorrent. Al ser una implementación de Kademlia, utiliza el protocolo DHT, el cual hace que la red consiga un carácter distribuido, evitando la utilización de *tracker* centralizado que era uno de los problemas principales de la red de Bittorrent. Por otro lado, en esta red, tanto los recursos como los nodos son identificados con un identificador único de 160 bits.

De todos los mensajes que se intercambian en la red de Mainline, en este proyecto interesa la monitorización de los mensajes del tipo *announce_peer* de una zona concreta de la red de Mainline. Así, se va a permitir conocer qué nodos comparten qué recurso en cada instante de tiempo.

III. Estructura De La Herramienta De Detección De Botnets Parásitas P2P

Una vez descrito los conceptos fundamentales de Bittorrent, ahora se presenta el sistema de detección de *botnets* parásitas del que hace uso la herramienta desarrollada.

En este sistema de detección se supone e intuye que los recursos que sean compartidos por usuarios legítimos en redes P2P van a tener un comportamiento diferente aquellos recursos que sean pertenecientes a una *botnet* parásita P2P.

De esta forma el sistema de detección está basado en 2 tipos de modelos de comportamiento:

- Modelo de comportamiento asociado a un recurso legítimo.
- Modelo de comportamiento asociado a un recurso *botnet*.

Los modelos de compartición de recursos van a venir determinados por la evolución temporal del número de nodos P2P que comparten un recurso concreto (*nr(k)*). En este Trabajo se está interesado en aquellos recursos que son populares, es decir que durante un cierto periodo de tiempo son compartidos por un gran número de nodos ya que se considera que los recursos *botnets* van a pertenecer a este grupo.

En todo recurso popular se encuentran dos fases fundamentales:

- Fase de compartición: Al comienzo de la compartición el recurso cuenta con pocos nodos que lo estén compartiendo. Poco a poco, la popularidad del recurso va aumentando hasta que llega un periodo en el cual el recurso es compartido por un número elevado de nodos. Una vez pasa este periodo, el interés de los clientes por este recurso decrece rápidamente hasta alcanzar un punto desde el que la disminución del número de nodos se hace más suave.
- Fase de desaparición: Esta fase abarca el periodo desde el punto en el cual la disminución del número de nodos es más suave, hasta que el recurso desaparece, es decir, hasta que no es compartido por ningún cliente desapareciendo de esta forma de la red.

Conociendo las distintas fases de la evolución de *nr()* para un recursos popular, y asumiendo que un recurso *botnet* se comporta de forma diferente a un recurso legítimo. Este sistema de detección está basado en 2 principios:

- La primera característica es que un recurso *botnet* debe ser un recurso popular. Estos recursos van a estar compartidos por un gran número de nodos, es decir van a ser recursos populares. Cuando un *botmaster* actualiza el código del *bot* o envía comandos, todos los *bots* deben descargar el recurso *botnet*. Esto implicará un gran número de descargas.
- Por otro lado la segunda característica a tener en cuenta es que los recursos *botnets* deben presentar un tiempo de vida breve, ya que este recurso apunta directamente al *botmaster* y a los nodos que forman la *botnet*. Esto hace que en comparación con un recurso legítimo, en la fase de desaparición, nr(k) va a sufrir una caída bastante abrupta y así se establece un umbral de caída.

En el siguiente esquema, se muestra el sistema de detección propuesto. En él, se aprecia que una vez realizada la monitorización de la red de Mainline durante un periodo de monitorización de una hora, se lleva a cabo el procesado de los mensajes de tipo *announce_peer* que se han recolectado. Durante la fase de entrenamiento, se filtran aquellos recursos que son legítimos y posteriormente se establecen los umbrales de popularidad y caída que determinan en la fase de detección si un recurso va a ser anómalo o no. Así, si durante la monitorización de un recurso, este recurso es popular y además sufre una caída abrupta en nr(k) que supera el umbral de caída establecido , este recurso será marcado como anómalo.

IV. Diseño E Implementación De La Herramienta

A continuación, una vez conocido el sistema de detección en el cual se basa esta herramienta, se lleva a cabo la explicación del diseño y la implementación de la misma. En esta imagen se observa los 3 módulos principales de los que consta la herramienta:

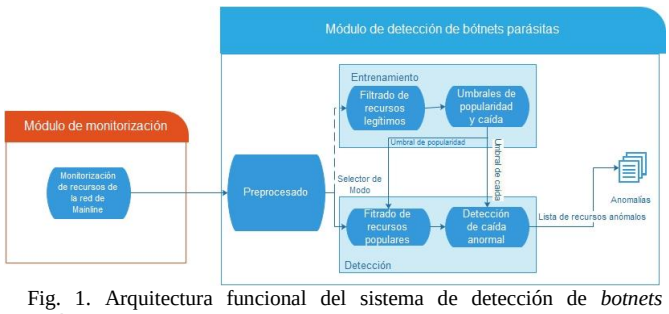


Fig. 1. Arquitectura funcional del sistema de detección de *botnets* parásitas P2P.

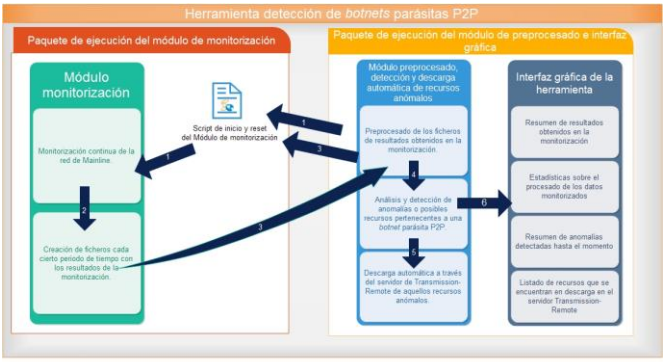


Fig. 2. Diseño e implementación de la herramienta de detección de *botnets* parásitas P2P.

- Modulo de monitorización.
- Modulo de detección preprocesado y descarga automática de recursos anómalos.
- Interfaz gráfica de la herramienta.

Una vez iniciada la herramienta, el módulo de monitorización comienza la monitorización de una zona de la red de Mainline y cada periodo de monitorización genera un fichero con los resultados de la monitorización. En concreto, genera un fichero con información acerca de los mensajes *announce_peer* que se han compartido.

Posteriormente, para cada periodo de monitorización el modulo de detección lleva a cabo el procesado de estos ficheros para posteriormente detectar aquellos recursos que son anómalos en base al sistema de detección de [2]. Por último, aquellos recursos que son detectados como anómalos, son puestos en descarga en servidor de Transmission-Remote, cumpliendo de esta forma la automatización de la descarga de aquellos recursos que son anómalos.

Por otro lado, a través del módulo de la interfaz gráfica, vamos a tener información en cuanto a:

- Los resultados obtenidos durante la monitorización.
- Estadísticas sobre el procesado de los datos.
- Resumen de anomalías detectadas.
- Listado y evolución de los recursos que están en descarga en el servidor de Transmission-Remote.

Esta interfaz gráfica está formada por 2 ventanas principales:

- Ventana de configuración de preferencias: permite al usuario el establecimiento de los parámetros necesarios para llevar a cabo la monitorización, la detección y la descarga de recursos anómalos.
- Ventana del programa: Recoge los resultados obtenidos durante el procedimiento de monitorización, detección y descarga de recursos anómalos. En concreto, esta interfaz está formada por 3 pestañas distintas:
  - Estadísticas generales: muestra información relativa al procedimiento de monitorización de recursos anómalos y al procesado de dicha información. Dispone de una gráfica en la que se puede visualizar la evolución temporal del número de mensajes que se han enviado y recibido a lo largo del tiempo, así como la evolución temporal del número de *peers* vecinos con los que la herramienta cuenta en cada momento.

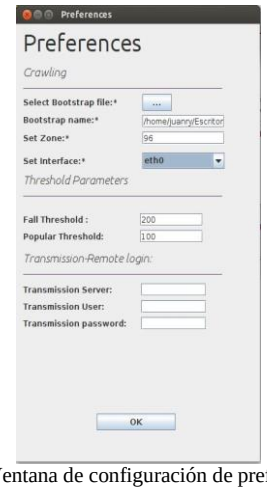


Fig. 3. Ventana de configuración de preferencias.

  - Pestaña de recursos monitorizados: Muestra información relativa a cada recurso procesado durante un periodo de monitorización. En concreto y como se puede ver en la Figura 4, se muestra información relativa a los nodos que comparten el recurso, así como el número de nodos que lo comparten y la caída sufrida con respecto al periodo de monitorización anterior. Por otro lado, se puede visualizar en una gráfica la evolución temporal del número de nodos que han compartido ese recurso. En esta pestaña también existe una serie de filtros que el usuario investigador puede aplicar para resumir la información a lo que a él le convenga.
  - Pestaña de recursos descargados: en esta pestaña se muestra una lista con aquellos recursos que ya han sido descargados a través del servidor de Transmission-Remote. Así como se visualiza una lista de aquellos recursos que se encuentran actualmente en descarga y su progreso.

V. Evaluación Experimental De La Herramienta

La fase de evaluación y test de la herramienta se ha realizado en una maquina servidora ubicada en el edificio CITIC de la universidad de Granada. Ha sido utilizada durante un periodo de tiempo de 3 semanas obteniendo resultados satisfactorios.

A continuación, se muestra el funcionamiento paso a paso de la herramienta y así se comprueba su correcto funcionamiento.

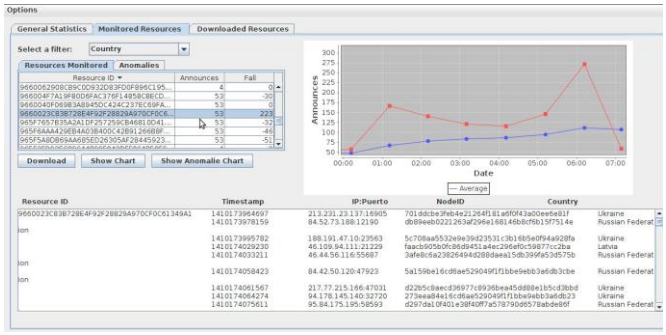


Fig. 4. Ventana del programa.

En primer lugar, una vez que la herramienta es iniciada, se despliega la ventana de configuración de preferencias. Aquí, se estableció los siguientes parámetros:

- La zona de monitorización de la red de Mainline elegida ha sido la 96. Así, todos los recursos cuyo identificador empiecen por el prefijo 96, van a ser monitorizados.
- La interfaz de red elegida es la eth0, correspondiente con la línea de acceso a internet del servidor.
- El umbral de caída es de 200 y el umbral de popularidad 100, de forma que aquellos recursos que superen estos umbrales, serán marcados como recursos anómalos y posibles recursos *botnets*.
- Por otro lado, la herramienta está diseñada para que el servidor de descarga de recursos pueda estar instalado de una máquina independiente de donde se encuentra en funcionamiento la herramienta. Por eso, cuenta con esta serie de campos donde el usuario puede determinar los parámetros necesarios para realizar el *login*.

En la pestaña de Estadísticas generales, como se puede observar en la Figura 5, se muestra el número de recursos diferentes que han sido procesados y el número de recursos que son populares durante ese periodo de monitorización, en función del umbral de popularidad ya establecido. También se muestra el número recursos que han aparecido nuevos, así como el número de recursos que tienen en común con respecto al periodo de monitorización anterior. En concreto, para este periodo de monitorización se han monitorizado 7949 recursos, de los cuales 157 son populares. Con respecto al periodo de monitorización anterior, 5354 recursos son comunes y 2595 recursos han aparecido nuevos. De este periodo de monitorización que se ha propuesto como ejemplo, se puede decir que el número de recursos que se han procesado se encuentra en la media de los recursos que se procesan para cada periodo de monitorización. Por otro lado, es destacable la cantidad de recursos nuevos que han aparecido con respecto al periodo anterior.

La interfaz gráfica también muestra información concreta de cada uno de los recursos que han sido monitorizados

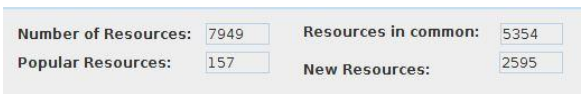


Fig. 5. Resumen de estadísticas generales después del preprocesado de la información de monitorización.

durante ese periodo δ. En la pestaña de Recursos monitorizados, el usuario puede contemplar para cada recurso, el número de nodos que comparten y la caída sufrida en el número de nodos que lo comparten con respecto al periodo de monitorización anterior. Una utilidad clave que ofrece la interfaz es la utilización de distintos filtros que permiten resumir toda la información recopilada en información útil para el usuario de la herramienta.

Si el usuario selecciona un recurso determinado de la lista, se presenta información referente a los mensajes *announce_peer* que el sistema recibió de este recurso. En concreto, se detalla: el instante de tiempo en el que llegó el mensaje, la lista de identificadores de nodo que comparten al recurso con sus respectivas direcciones IP y puertos, así como la nacionalidad de cada uno de estos nodos.

Una vez seleccionado un recurso, también es posible visualizar en una gráfica la evolución del número de nodos que lo han compartido a lo largo del tiempo, simplemente pulsando el botón *Show Chart* de la interfaz.

En la figura 6 se muestra un ejemplo de lo anteriormente descrito. Se puede ver como para el recurso seleccionado se despliega información en cuanto a los nodos que lo comparten, así como la evolución temporal del mismo. Casualmente, también se aprecia que dicho recurso ha experimentado una caída mayor que el umbral especificado (200). Este recurso, siguiendo el procedimiento que lleva a cabo el módulo de detección, va a ser marcado como recurso anómalo y posteriormente va a ser puesto en descarga a través del servidor de Transmission-Remote.

La herramienta, como ya se ha comentado, también ofrece la posibilidad de ver el historial de aquellos recursos que han sido anómalos a lo largo del tiempo. Se puede comprobar cómo el recurso de la Figura 6, aparece en la lista de recursos anómalos en la Figura 7. Por tanto, se puede deducir que el procedimiento de detección de recursos anómalos que realiza la herramienta se realiza de forma satisfactoria.

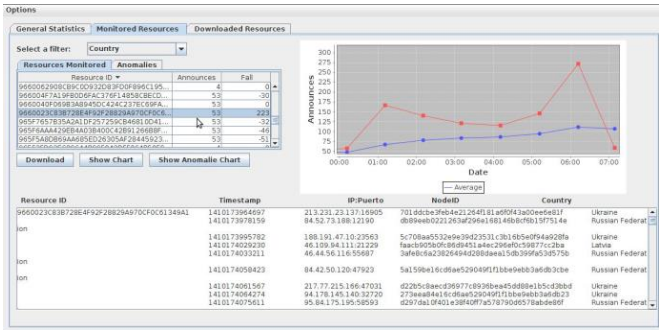


Fig. 6. Resumen de estadísticas generales después del preprocesado de la información de monitorización.

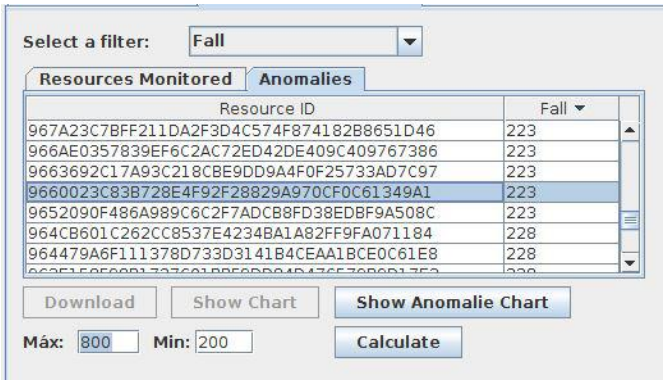


Fig. 7. Resumen de estadísticas generales después del preprocesado de la información de monitorización.

Una vez un recurso es marcado como anómalo, se procede a la descarga automática del mismo a través del servidor Transmission-Remote. El usuario, a través de la pestaña de recursos descargados, puede ver qué recursos que están actualmente en descarga, pudiendo observar su progreso de descarga, así como información sobre el recurso. Además se ofrece una lista con aquellos recursos que ya han sido descargados y que se encuentran en el directorio de descargas del servidor Transmission-Remote.

Durante el procedimiento de detección, se ha detectado que hay un recurso anómalo correspondiente al de la Figura 6. Este recurso ha sido puesto en descarga de forma automática en el servidor de Transmission-Remote, y a través de la interfaz gráfica se puede comprobar su progreso así como información adicional del mismo. (Figura 8).

VI. CONCLUSIONES

En este Trabajo Fin de Grado se ha diseñado e implementado una herramienta de detección de *botnets* parásitas P2P que permite, desde una misma aplicación, la monitorización de recursos de la red, la detección y la descarga automática de recursos anómalos, así como la presentación de resultados a través de una interfaz gráfica.

Las contribuciones más destacables de la herramienta son las siguientes:

- La herramienta implementada permite llevar a cabo una monitorización continua de una zona de la red de Mainline elegida por el usuario.

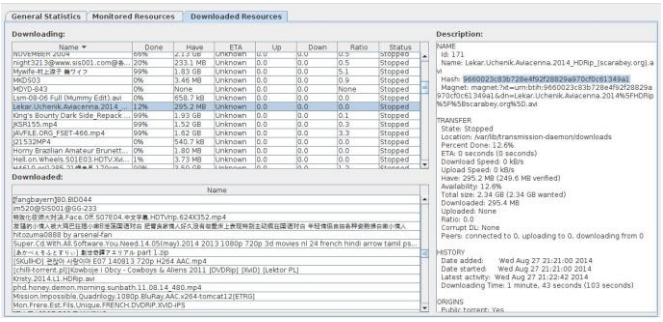


Fig. 8. Resumen de estadísticas generales después del preprocesado de la información de monitorización.

- Como consecuencia del punto anterior, el sistema extrae un modelo de normalidad de los recursos que se están compartiendo en la red de Mainline, y en función de éste, detecta posibles anomalías que pueden pertenecer a una *botnet* parásita P2P.
- Abordando uno de los objetivos fundamentales del proyecto, la herramienta permite la descarga automática de aquellos recursos que han sido detectados como anómalos. Con esto se consigue que el usuario de la herramienta no tenga que preocuparse de analizar qué recursos son anómalos, y para éstos, llevar a cabo su descarga. Así, se permite comprobar la naturaleza anómala del mismo, verificando si realmente es un recurso perteneciente a una *botnet* parásita P2P.
- Además, la herramienta permite la presentación de los resultados obtenidos en una interfaz gráfica. Así, el usuario es capaz de extraer conclusiones del procedimiento de detección de *botnets* parásitas P2P de una forma sencilla y gráfica. Por otro lado, esta interfaz permite la configuración de parámetros del sistema con los que llevar a cabo la monitorización, la detección y la descarga de recursos anómalos. Esto hace posible que el usuario no tenga que preocuparse de modificar código de programación y que toda la configuración se haga de forma gráfica e intuitiva.
- A través de esta interfaz, la herramienta también permite la descarga de aquellos recursos que, aunque no son detectados como anómalos por la herramienta, pueden tener un carácter ilógico para el usuario y quizás interese su descarga.
- La interfaz gráfica de la herramienta ofrece la posibilidad de filtrar la información recolectada durante el procedimiento. Esto permite que la herramienta sea mucho más dinámica y hace que el usuario solamente contemple aquellos datos que realmente son de especial interés para él. En concreto, la herramienta permite el filtrado de recursos cuya caída, en el número de nodos que los comparten, esté dentro de un intervalo determinado por el usuario, el filtrado de recursos en función de la nacionalidad de los nodos que los comparten y el filtrado de recursos en función del número de nodos que los comparten.
- Así, todos los puntos anteriormente citados están unificados en una sola herramienta y esta es la mayor aportación del proyecto. De esta forma, el usuario no tiene porqué preocuparse de iniciar distintos módulos ni programas independientes. Además, la herramienta se encuentra desarrollada en un único lenguaje de programación (Java) dotando de mayor integridad a la misma.
- Por último, los resultados obtenidos durante la de experimentación y validación de la herramienta fueron coherentes con lo esperado. Aunque no ha sido posible la detección de ninguna *botnet* parásita P2P.

REFERENCIAS

[1] Ihsan Ullah, Naveed Khan, and Hatim A. Aboalsamh. Survey on botnet: Its architecture, detection, prevention and mitigation. in networking, sensing and control (ICNSC). 2009.

[2] Liping Feng, Xiaofeng Liao, Qi Han, and Lipeng Song. Modeling and analysis of peer-to-peer botnets. discrete dynamics in nature and society. 2012.
[3] Rodriguez Gomez Rafael A., Macia-Fernandez Gabriel., Garcia Teodoro Pedro., Steiner Moritz., and Balzarotti Davide. Resource monitoring for the detection of parasite p2p botnets. 2014.

Monitorización y detección de anomalías en dispositivos Android

Tutor: Pedro García Teodoro; e-mail: pgteodor@ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

Autor: Alejandro Ruiz Heras; e-mail: alexrh@correo.ugr.es

***Resumen*— El número de dispositivos móviles ha sufrido un crecimiento muy rápido n los últimos años, siendo cada vez más adoptados para tareas personales y profesionales. Actualmente, el mercado está liderado por Google, con Android como sistema operativo y *Play Store* como plataforma de venta. Este hecho provoca que los desarrolladores de *malware* estén cada vez más interesados en centrar sus ataques sobre dispositivos Android. Por tanto, los riesgos de seguridad asociados a este tipo de equipos aumentan constantemente y, aunque existe una serie de propuestas enfocadas a la seguridad Android, esto sigue siendo un gran reto en estos entornos. En este contexto, este trabajo presenta una nueva herramienta capaz de monitorizar y analizar el perfil de actividad típico de un usuario para estimar el modelo asociado de comportamiento "normal". Basado en él, se procederá al diseño y desarrollo de un módulo que permita la clasificación de actividades normales o anómalas a fin de determinar la posible ocurrencia de eventos maliciosos.**

***Palabras clave*— Anomalía, comportamiento, detección, dispositivo Android, *malware*, seguridad.**

I. INTRODUCCIÓN

Los dispositivos móviles son cada vez más aceptados por los usuarios de todo el mundo. Solo considerando la venta de *smartphones*, estos ya han superado en cantidad a la venta conjunta de computadores persoanles y portátiles. Algunos estudios, como [1], afirman que el número de *tablets* y teléfonos inteligentes en los próximos años estará alrededor de un centenar de veces la de PC y portátiles.

Concretamente, desde el año 2011, Android ha demostrado un gran posicionamiento en el mercado, haciendo crecer su volumen de dispositivos como ningún otro sistema operativo lo ha hecho [2]. La Fig. 1 muestra el dominio de Android durante los años 2011-2014.

A pesar de este gran éxito, los dispositivos inteligentes presentan una menor seguridad y un mayor número de problemas de privacidad frente otro tipo de computadores en muchos aspectos. Esto se debe a varios factores, como la incorporación de numerosos sensores y elementos de comunicación (Wi-Fi, Bluetooth, GPS, etc.) capaces de acceder a información altamente sensible sobre el usuario (localización, grabación de audio, imágenes y vídeo desde su entorno, etc.) [3]. Otra fuente muy importante que provoca la mayoría de problemas de seguridad es la capacidad de incorporar aplicaciones de terceros en los dispositivos, principalmente de mercados no oficiales [4]. En el modelo de mercado abierto, los usuarios son libres de instalar aplicaciones de cualquier mercado, pudiendo estas contener, con mayor probabilidad, código malicioso.

La proliferación, unida al aumento de información personal y confidencial almacenada en dispositivos Android, las delicadas operaciones realizadas a través de ellos y el significativo incremento de vulnerabilidades a las que están expuestos, han provocado un crecimiento exponencial en la presencia de *malware* desarrollado específicamente para estos dispositivos [5].

De acuerdo con el informe de amenazas móviles publicado por *Juniper Networks* en 2012, el número de variantes de *malware* para Android aumentó un 3.325,5% durante 2011 y un 614% entre 2012 y 2013 [6]. Un informe similar de *F-Secure* revela que el número de aplicaciones maliciosas en Android recibidas durante el primer trimestre de 2012 aumentó de 139 a 3.063, en comparación con el primer trimestre de 2011 [7]. A finales de 2012 ya representaban el 97% del total de *malware* en móviles, según *McAfee* [8].

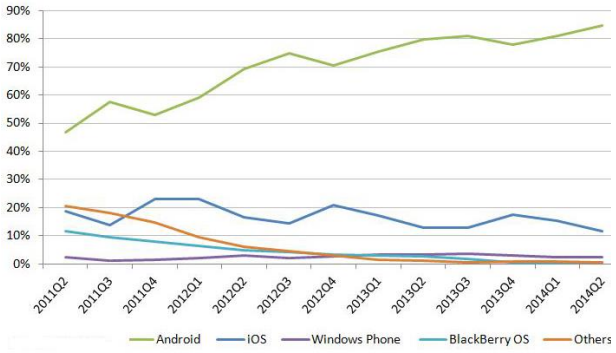


Fig. 1. Volumen a nivel mundial de los distintos OS en *smartphones* a partir de 2011.

II. Estado del arte

Debido a los grandes problemas expuestos en la Sección I, en estos últimos años han sido propuestas varias soluciones para reforzar la seguridad en entornos Android. Varias de ellas se refieren a sistemas para monitorizar las actividades del dispositivo. De esta manera, el usuario puede hacerse una idea muy intuitiva de la seguridad de este, pudiendo detener aplicaciones que utilizan permisos no deseados, desactivar la conexión a la red peligrosas, etc.

Una de las primeras herramientas presentadas es *Network Log*, la cual monitorizada las conexiones de red realizadas por las distintas aplicaciones instaladas en el dispositivo. Se proporcionan algunos datos de interés sobre dichas conexiones como las direcciones de origen y de destino, los puertos y los bytes transmitidos. Otra herramienta, *OS Monitor*, no solo muestra las conexiones, sino también información sobre los procesos ejecutados, mostrando su porcentaje de uso en el sistema y la cantidad de memoria usada. Adicionalmente, es capaz de obtener información general sobre el sistema (estado de la batería, uso de la CPU y memoria en el sistema). Otra herramienta digna de mención es *CONAN Mobile*, la cual incluye el seguimiento de conexiones IP, de permisos, la clasificación de estos por nivel de seguridad, cambios de la conexión inalámbrica, etc.

Más allá de la simple monitorización, las herramientas de detección persiguen determinar y, en su caso, notificar al usuario sobre actividades no deseadas. Para su implementación existen dos técnicas principales: estáticas y dinámicas, en función del tipo de análisis realizado. La detección dinámica suele ser eficaz en la identificación de actividades maliciosas desconocidas, pero implica una sobrecarga significativa. Por el contrario, los métodos estáticos inducen una pequeña sobrecarga en tiempo de ejecución pero son menos eficientes en la búsqueda de eventos maliciosos previamente no observados, pudiendo detectar solo los conocidos.

En los análisis estáticos se decompila el código de la aplicación y se analiza. Es muy común hacer un estudio de los permisos, como por ejemplo la herramienta Stowaway [9]. Por su parte, en [10] se propone un método de detección basado en el análisis de los ficheros *manifest* que incluyen las aplicaciones Android. Primero se extrae la información descrita en el *manifest* (categoría, nombre de cada permiso, nombre de procesos, prioridad, número de permisos, etc.). Tras ello, la información se compara con algunas palabras clave de una lista predefinida para calcular el nivel de malignidad de cada aplicación. Finalmente, este nivel o puntuación se compara con un valor umbral. Si se supera este, la aplicación es considerada como maliciosa.

Otros sistemas como *Woodpecker* [11] o *ComDroid* [12] analizan los permisos que una aplicación expone a otras aplicaciones.

También existen herramientas más concretas, como *DroidMOSS* [13], que analizan el código decompilado para detectar aplicaciones re-envasadas distribuidas a través de mercados no oficiales.

Por lo que respecta a las técnicas de detección dinámica, suelen usarse algoritmos de aprendizaje automático como los contemplados en *Andromaly* [14] o *MADAM* [15]. *Andromaly* utiliza el análisis dinámico para realizar supervisiones a partir de información tal como el uso de CPU, los procesos en ejecución y el nivel de la batería. Sobre ello, utiliza el aprendizaje automático basado en anomalías para clasificar las aplicaciones. También MADAM utiliza 13 características para detectar *malware* a nivel *kernel* y de usuario.

III. Análisis de requisitos

La solución der seguridad móvil aquí planteada consiste en una aplicación para monitorizar y detectar comportamientos anómalos en dispositivos Android, describiéndose seguidamente sus principales requisitos, tanto funcionales como no funcionales.

A. *Funcionales*

Los requisitos funcionales son declaraciones de los servicios que debe proporcionar el programa y de cómo se debe comportar en situaciones determinadas. Brevemente, estos son:

- La aplicación debe ser capaz de monitorizar en tiempo real los aspectos más relevantes del dispositivo.
- Se debe mostrar un historial con todas las notificaciones indicando la fecha en la que se produjeron. Se podrán eliminar las que se deseen.
- La herramienta tiene que indicar las conexiones IP y el puerto que cada aplicación está realizando en tiempo real. Además, debe mostrar el tráfico promedio transmitido y recibido, en bps.
- Debe realizar detección de anomalías en *background*, sin precisar la acción directa del usuario.
- El usuario puede incluir específicamente algunos estados del dispositivo no permitidos.

B. *No funcionales*

Los requisitos no funcionales especifican criterios que pueden usarse para juzgar la operación de un sistema en lugar de sus comportamientos específicos. Así, estos requisitos se refieren a características del sistema tales como fiabilidad, accesibilidad, usabilidad, estabilidad, rendimiento, etc.

Estos son:

- La aplicación será fiable, es decir, la información proporcionada debe ser representativa y coherente.
- Controlará internamente los errores y excepciones que se puedan producir.
- El sistema será capaz de almacenar datos de manera que estos queden almacenados después de finalizar la aplicación.
- Las notificaciones se mostrarán en la barra de estado de Android de forma visible y clara para el usuario.
- Permitirá la inclusión de nuevos módulos fácilmente.
- En términos de rendimiento, la interfaz de usuario no debe ser bloqueada aunque se realicen tareas de largo tiempo de procesamiento.
- Ha de ser de bajo consumo energético.

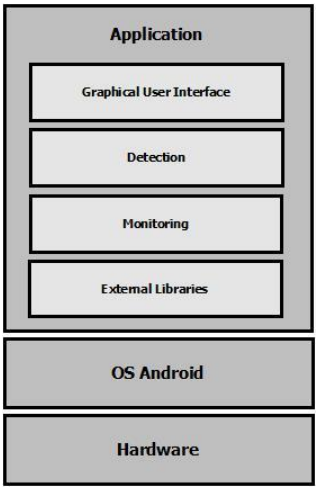


Fig. 2. Arquitectura del sistema organizada en capas.

IV. DISEÑO E IMPLEMENTACIÓN

La herramienta pretendida ha sido concebida en base a la monitorización del dispositivo desde tres perspectivas:

- Estado (encendido/apagado) de los componentes hardware multimedia (pantalla, cámara, altavoz) y las interfaces de comunicación (Wi-F, Bluetooth, GPS, interfaz 3G/4G).
- Aplicaciones instaladas y en ejecución en tiempo real, junto a los permisos de cada una.
- Comunicaciones, tanto IP como de voz.

A partir de esta información monitorizada, se procederá a la detección de anomalías para determinar y notificar las actividades inesperadas en base a dos modelos: de normalidad y heurístico.

A. *Arquitectura del sistema*

La implementación de la herramienta sigue un diseño modular, por capas, de forma que cada capa proporciona un conjunto de servicios a la inmediatamente superior.

La arquitectura del sistema final estará compuesta por diferentes capas, módulos y sub-módulos, obteniendo así un mayor rendimiento. Debido a este hecho, una característica importante es su escalabilidad, resultando muy fácil la inclusión de nuevos módulos y funcionalidades.

En concreto, tres son las capas principales (Fig. 2). La capa *hardware* es el conjunto de componentes electrónicos utilizados por la aplicación. La capa *OS* se refiere al sistema operativo responsable de gestionar todos los recursos hardware pertenecientes a la primera capa. En este caso, Android. La última capa es la de *aplicación*.

Para un rendimiento óptimo, el software se divide en cuatro módulos:

- Librerías externas: módulo formado por Android SDK (*Software Development Kit*), el cual proporciona las API necesarias para la creación de aplicaciones Android.
- Módulo de monitorización: se basa en cuatro sub-módulos encargados de monitorizar los recursos hardware, aplicaciones, comunicaciones IP y llamadas de voz, respectivamente. Para ello, estos sub-módulos se han implementado mediante la llamada a las librerías de SDK.
- Módulo de detección: determina las actividades inesperadas a partir de los datos obtenidos por el módulo de monitorización.
- Interfaz gráfica de usuario: permite visualizar la información monitorizada y configurar la detección de anomalías de una manera sencilla. Se compone de un gran número de "pantallas", a las que es posible acceder por medio de la interfaz principal (Fig. 3). Esta presenta varios botones para gestionar las tres perspectivas enfocadas, ofreciendo la opción de llevar a cabo el proceso de detección de anomalías por separado. De esta manera, el usuario puede elegir cuándo comenzar y terminar la fase de entrenamiento y la búsqueda de actividades inesperadas para cada uno de los elementos monitorizados (se usarán para ello los botones "*On/Off States Register*" y "*On/Off Notifications*").

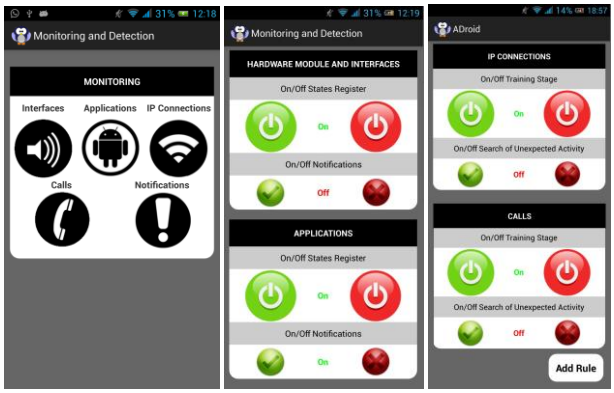


Fig. 3. Interfaz principal compuesta por dos partes: monitorización y gestión de la detección de anomalías.

De estos módulos, se han implementado los tres últimos. Se ha usado para ello Eclipse, un software compuesto por un conjunto de herramientas de código abierto para desarrollar varios tipos de proyectos.

B. *Modulo de monitorización*

De acuerdo a lo anteriormente establecido, tres serán los tipos de actividades/procesos monitorizados: interfaces, aplicaciones y comunicaciones.

Sub-módulo de monitorización en elementos hardware. La funcionalidad de este sub-módulo es comprobar el estado de las interfaces de comunicación y los dispositivos multimedia. Para ello, el proceso que se sigue es:

1. Comprobar si el dispositivo móvil en cuestión está provisto por la interfaz indicada.
2. Si este es el caso, se accede a la correspondiente biblioteca externa para conocer el estado. El vector i_t es un vector definido como $i_t = [i1_t, i2_t, i3_t, i4_t, i5_t, i6_t, i7_t]$. Los tres primeros valores corresponden a las interfaces de las comunicación: Wi-Fi, Bluetooth, 3G/4G y GPS, respectivamente. Por su parte, los tres últimos valores se refieren al hardware multimedia: pantalla, cámara y altavoz, respectivamente. Este vector es calculado periódicamente cuando el usuario presiona el botón de monitorización de los componentes hardware.
3. El estado de cada interfaz se almacena en la posición correspondiente del vector i_t. Cada interfaz puede tomar

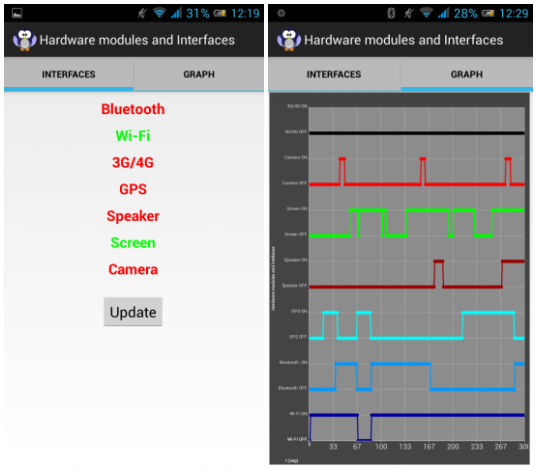


Fig. 4. Implementación de las interfaces gráficas "Interfaces" y "Graph".

tres valores diferentes. El valor lógico 0 se escribe cuando la interfaz está apagada, mientras que el 1 si está encendida. Sin embargo, si el dispositivo Android no dispone de dicha interfaz, se almacena el valor X.

4. Finalmente, se consulta i_t para mostrar la información sobre la interfaz gráfica. Si una interfaz ha tomado el valor 1, se muestra en verde. Si es 0, en rojo. Y si es X, en gris.

En la Fig. 4 se muestra el estado de cada interfaz durante los últimos 5 minutos, siendo el periodo de muestreo T=2 segundos. De esta manera, el usuario puede apreciar si una interfaz o elemento multimedia se ha activado sin su consentimiento. Es decir, si el usuario sabe a priori que un recurso no se ha activado y de repente la gráfica muestra lo contrario, una aplicación puede estar haciendo mal uso del recurso.

Sub-módulo de monitorización en aplicaciones. Por un lado, para realizar el seguimiento más completo posible sobre las aplicaciones del sistema, la herramienta muestra el nombre, el icono y la versión de todas las aplicaciones instaladas (Fig. 5). Esta lista se obtiene desde el inicio del dispositivo, lo que permite encontrar aplicaciones maliciosas que han sido instaladas de forma oculta sin dejar rastro de ello.

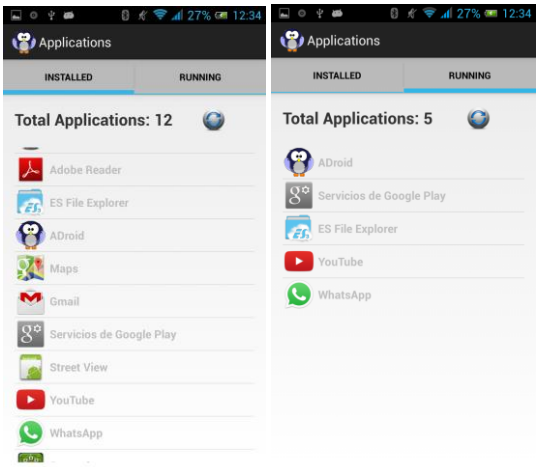


Fig. 5. Implementación de las interfaces gráficas "Applications Installed" y "Applications Running".

Por otra parte, se monitorizan las aplicaciones en ejecución en tiempo real. Esta supervisión puede proporcionar al usuario una idea sobre el nivel de seguridad que cada aplicación presenta. Así, pueden detectarse comportamientos maliciosos cuando aparecen aplicaciones en ejecución no iniciadas por el usuario. Algunos casos pueden ser *malware* distribuido en varias aplicaciones o los conocidos ataques re-delegación (una aplicación con un permiso específico realiza una tarea privilegiada en nombre de otra aplicación maliciosa que no tiene permiso).

Por último, como funcionalidades adicionales, sobre cada aplicación se incluye una descripción de cada uno de los permisos concedidos, explicando las acciones más sospechosas que pueden realizar. Así, los usuarios expertos pueden analizar e intuir la seguridad del dispositivo. También puede ser iniciada o detenida cualquier aplicación.

Sub-módulo de monitorización en conexiones IP. Las conexiones IP y las llamadas son dos formas bastante distintas de establecer una comunicación. Será importante monitorizar ambas ya que esto podrá permitir en ocasiones evitar desde robo de información, típico en conexiones IP, hasta fraudes económicos, propios en el establecimiento de llamadas.

Tradicionalmente, la monitorización del tráfico IP ha sido muy usada para determinar comportamientos sospechosos mediante la apreciación de desviaciones significativas en el perfil "normal" del tráfico. Por ello, la herramienta pretendida mostrará el número total de conexiones en tiempo real. Para cada conexión se indicará la dirección IP de destino, el puerto de destino, el nombre del paquete, la aplicación responsable de la conexión IP y el icono de esta (Fig. 6). Las conexiones podrán ser vistas mediante el botón "IP Connections".

Por último, también se mostrarán datos sobre la velocidad de tráfico:

- Tráfico trasmitido/recibido actual: se medirá el tráfico trasmitido/recibido entre muestra y muestra, y este se dividirá entre T (periodo con el que se toman las muestras).
- Tráfico promedio trasmitido/recibido durante el último día: a partir de los valores de tráfico medidos durante el último día, se realizará el promedio de todos ellos.

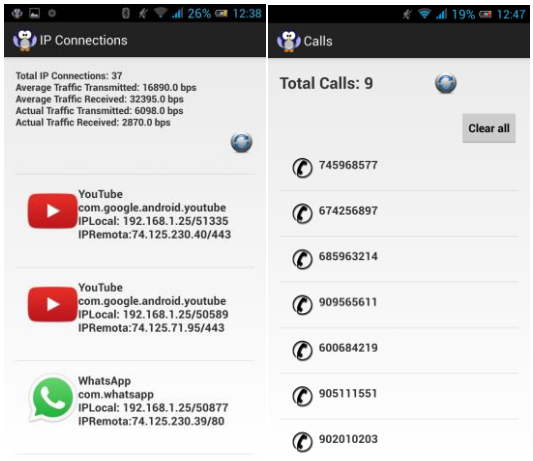


Fig. 6. Implementación de la interfaces gráficas "IP Connections" y "Calls".

A partir de toda esta información, los usuarios un poco más expertos pueden obtener una gran cantidad de datos sobre los equipos a los que se conecta el dispositivo móvil, como la ubicación, el nombre de dominio, el propietario, etc. Además, gracias al número de puerto se puede conocer el protocolo a nivel de aplicación utilizado en cada comunicación. Los servicios más típicos suelen tener un puerto conocido: HTTP utiliza el puerto 80, HTTPS el 443, SMTP el 25, etc.

Sub-módulo de monitorización de llamadas. En la monitorización de llamadas se pensó mostrar inicialmente un listado con todas las entrantes y salientes. Sin embargo, todos los *smartphone* ya incorporan un registro o *log* con dichas llamadas. Es por ello que para que el usuario se percate de posibles fraudes económicos, se listarán las llamadas salientes que:

- Nunca antes se hayan realizado.
- Sean de tarificación especial (números *premium).*

C. Modulo de detección de anomalías

La herramienta desarrollada utiliza dos "modelos" de comportamiento, uno de normalidad y uno heurístico.

El primer modelo se basa en un conjunto de cuatro tablas creadas y almacenadas sobre la base de datos. La tabla para elementos hardware almacena vectores i_t donde se indican los estados (*on/off*) de los dispositivos hardware. La segunda tabla almacena vectores con el nombre de las aplicaciones en ejecución de forma alfabética ejecutándose en un instante dado. Finalmente, para conexiones IP se guardarán las direcciones IP destino, y para llamadas la tabla contendrá los números marcados.

El segundo modelo consiste en un conjunto de reglas indicadas por el usuario explícitamente para definir qué comportamientos son o no permitidos.

En resumen, el proceso de detección de anomalías consiste en dos grandes etapas:

- Fase de entrenamiento: a lo largo de ella, se elabora el comportamiento normal del sistema completando las tablas de normalidad descritas anteriormente con cada nuevo valor encontrado. La duración de esta fase puede ser de varios días o incluso semanas, dependiendo del uso del dispositivo Android. Comienza y termina cuando son pulsados los botones "*On/Off States Register*" de cada aspecto monitorizado.
- Detección de anomalías: cuando la etapa de entrenamiento se ha completado y, en base al modelo obtenido, se determina la ocurrencia de un comportamiento anómalo, se notificará al usuario. Los botones "*On/off Notifications*" permiten iniciar/parar la detección de anomalías. Además, el usuario puede definir reglas de forma manual utilizando el botón "*Add Rule*" (estas reglas serán almacenadas en la base de datos sobre otras cuatro tablas respectivamente). Así, el sistema se hará cada vez más inteligente y fiable.

Suponiendo que la fase de entrenamiento ha sido realizada y la búsqueda de anomalías para los elementos hardware (Wi-Fi, GPS, Bluetooth…) activada, el algoritmo implementado en *background* se ejecutará de forma periódica con T=2seg. Este algoritmo ha sido implementado usando un elemento de Android llamado *Service* (componentes sin interfaz gráfica que se ejecutan en segundo plano) y el proceso seguido es:

1. Actualizar i_t con los valores de cada interfaz, utilizando para ello el módulo de monitorización.
2. Comprobar si el vector de estados obtenidos se encuentra en la base de datos de reglas.
3. Si se encuentra, se muestra una alarma en la barra de estado y se salta al paso 6, notificando este hecho.
4. Si no se encuentra como regla definida, se compara con la base de datos de "normalidad".
5. Si no aparece en esta última, se muestra una alarma en la barra de estado. En caso de que el usuario decidiese ante esta alarma que el evento reportado es normal, se almacenaría el vector en la base de datos de normalidad, considerando este estado a partir de ahora como válido. En caso contrario, se procedería a su inclusión como regla en la base de datos de heurística.

Para la detección en aplicaciones, los pasos 1-5 son similares pero comparando el vector de aplicaciones con las dos tablas correspondientes a estas. Además, se lanzará una notificación cuando se instale o actualice una aplicación, dado que muchas aplicaciones maliciosas se instalan ocultamente o se conectan a la red para actualizarse e inyectar código malicioso (re-envasado).

También para las comunicaciones los pasos anteriores son similares (se comparan direcciones IP destino y números telefónicos con las base de dato de normalidad y heurística). Además dee ello, en conexiones IP se genera una alarma cuando el tráfico real supere el promedio estimado en entrenamiento en un factor 3. Para llamadas, la notificación se produce si se establece una comunicación con un número *premiun.*

V. PRUEBAS Y RESULTADOS

Una vez desarrollado e implementado el sistema en un dispositivo real, se han realizado distintas pruebas al software con el fin de localizar fallos dentro de este. Son definidas como "pruebas que tienen como objetivo verificar la funcionalidad y estructura de cada componente". De este modo, podrá hacerse una valoración conjunta de todos los servicios ofrecidos por la aplicación. Algunas de dichas pruebas son:

Prueba 1. Verificar la correcta creación de los ficheros de almacenamiento.

Prueba 2. Comprobar si los botones de monitorización ejecutan las correspondientes *Activities (*representan el componente principal de la interfaz gráfica de una aplicación Android y, por tanto, son usadas durante la implementación para cada ventana gráfica*)* sin error y si los botones de detección funcionan correctamente.

Prueba 3. Comprobar si las interfaces gráficas de dispositivos, gráficas, aplicaciones instaladas, aplicaciones en ejecución, comunicaciones establecidas y llamadas muestran información fiable, real y de forma rápida.

Prueba 4: Verificar si la adición, eliminación y visualización de reglas es correcta.

Prueba 5. Verificar si la detección correspondiente a cada sub-módulo se realiza correctamente.

Prueba 6. Verificar la creación del perfil típico de usuario mediante una fase de entrenamiento de siete días. Tras este tiempo, comprobar la notificación de comportamientos anómalos.

Prueba 7. Verificar un consumo de batería adecuado:

1. Cargar el dispositivo móvil al nivel más alto de batería y calcular el tiempo trascurrido hasta agotarla (en ejecución habrá una lista de aplicaciones cuyo consumo es regular y constante).
2. Volver a cargar el dispositivo móvil al nivel más alto de batería y ejecutar ahora la aplicación desarrollada, lanzando los servicios en *background*.

Tras su ejecución, hay que decir que todas las pruebas presentadas anteriormente han arrojado un resultado positivo. La detección de realiza de forma rápida y eficiente, al tratarse de algoritmos no demasiado complejos. Tras haber realizado una fase de entrenamiento de siete días, los resultados obtenidos en cuanto a notificación de alarmas ha sido correcta y bastante variada. Se han registrado 423 entradas correspondientes a conexiones IP, 19 a llamadas, 21 a dispositivos y 56 a aplicaciones. El consumo de la aplicación no es demasiado elevado, por lo que el tiempo configurado para la búsqueda de comportamientos sospechosos es el adecuado. La diferencia entre ambas duraciones de batería fue mínima: 1 día, 7 horas y 35 minutos frente a 1 día, 6 horas y 3 minutos.

VI. Conclusiones y líneas futuras

A pesar de haber cumplido los objetivos inicialmente propuestos, la herramienta implementada es mejorable y ampliable en diversos aspectos. Las mejoras más importantes se refieren al módulo de detección de anomalías:

- Desarrollo de un sub-módulo capaz de realizar detección de anomalías teniendo en cuenta la combinación de dispositivos, aplicaciones y comunicaciones.
- Llevar a cabo la detección de anomalías teniendo en cuenta los permisos de cada una de las aplicaciones instaladas.
- Es de considerar la instalación de un servidor al que enviar los datos monitorizados del dispositivo móvil. Aquel se encargaría de procesar y analizar la información mediante algoritmos más complejos al no existir limitaciones de batería, cómputo o almacenamiento. Una vez analizado el comportamiento del dispositivo, el servidor reportará un informe con las posibles situaciones anómalas.

Agradecimientos

Agradecer la inestimable ayuda y orientación de mi tutor, Pedro, sin las cuales no habría podido implementar esta herramienta. Gracias por haberme dado esta oportunidad y por todos los ánimos, consejos y apoyo dados en todo momento.

Referencias

[1] IDC (International Data Corporation), "Worldwide Quarterly Mobile Phone/Smart/Tablet Tracker", (2014). Disponible: http://www.idc.com/tracker/showtrackers.jsp?prod_group_id=3

[2] IDC (International Data Corporation), "Smartphone OS Market Share", (2014). Disponible: http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

[3] E. Chin, A. P. Felt, V. Sekar, and D. Wagner (2012). Measuring user confidence in smartphone security and privacy. In Symp. on Usable Privacy and Security. In Proceedings of the Eighth Symposium on Usable Privacy and Security, vol. 1, pp. 1-16.

[4] N. Husted, H. Saidi, and A. Gehani (2011). Smartphone security limitations: conflicting traditions, In Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies. pp. 5–12.

[5] K. Dunham (2008). Mobile malware attacks and defense. Syngress.

[6] Juniper, "2013 mobile threats report,", Juniper Networks, 2013.

[7] F-Secure, "Mobile threat report q1 2012," F–Secure, 2012. Disponible: http://www.fsecure.com/weblog/archives/MobileThreatReportQ12012.pdf.

[8] McAfee, "Threats report: fourth quarter 2012", McAfee, 2013, Disponible: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf.

[9] A. P. Felt, E. Chin, S. Hanna, D. Song, D. Wagner (2011). Android Permissions Demystified. In Proceedings of the 18th. ACM Conference on Computer and Communications Security, pp. 627-638

[10] R. Sato, D. Chiba, S. Goto (2013). Detecting Android Malware by Analyzing Manifest Files. In Proceedings of the Asia-Pacific Advanced Network, vol. 36, pp. 23-31.

[11] M. Grace, Y. Zhou, Z. Wang, X. Jiang (2012). Systematic Detection of Capability Leaks in Stock Android Smartphones. In Proceedings of the 19th. Annual Symposium on Network and Distributed System Security (NDSS), pp. 1-15.

[12] E. Chin, A.P. Felt, K. Greenwood, D. Wagner (2011). Analyzing Inter-Application Communication in Android. In Proceedings of the 9th. Annual International Conference on Mobile Systems, Applications, and Services (MobiSys), pp. 239-252.

[13] W. Zhou, Y. Zhou, X. Jiang, P. Ning (2012). Detecting Repackaged Smartphone Applications in Third-Party Android Marketplaces. In Proceedings of the 2nd. ACM Conference on Data and Application Security and Privacy (CODASPY), pp. 317-326.

[14] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, Y. Weiss (2012). Andromaly: A Behavioral Malware Detection Framework for Android Devices. In Journal of Intelligent Information Systems, vol. 38, pp. 161-190.

[15] G. Dini, F. Martinelli, A. Saracino, D. Sgandurra (2012). MADAM: a Multi-Level Anomaly Detector for Android Malware. In Proceedings of the 6th. International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, pp. 240-253.

Alejandro Ruiz Heras es graduado en Ingeniería de Tecnologías de Telecomunicación (2013/2014) por la Universidad de Granada, y actualmente alumno del máster oficial de Ingeniería de Telecomunicación (2014/2015) de la UGR.

Provisión de servicios de seguridad en entornos distribuidos

Autor: Noé Fernández Llamas, e-mail: nfll@correo.ugr.es
Tutor: Pedro García Teodoro, e-mail: pgteodor@ugr.es
Titulación: Grado en Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—En la última década se ha vivido un crecimiento sin precedentes del número de dispositivos interconectados, estos sistemas son cada vez más distribuidos. Este tipo de sistemas está tomando especial relevancia en detrimento de los servicios centralizados tradicionales. Hace unos años surgió un estándar para sistemas distribuidos de tipo middleware llamada Data Distribution Service (DDS). DDS no contempla en su especificación ningún aspecto de seguridad básico, esta tarea ha recaído sobre las empresas de software que comercializan esta tecnologia. Con este proyecto se pretende el diseño, desarrollo y puesta en marcha de una solución de seguridad alternativa. El prototipo desarrollado ratifica el éxito del mismo, culminando todos los objetivos marcados y reiterando la necesidad de los servicios de seguridad en este tipo de sistemas.**

***Palabras clave*—Data Distribution Service, Internet of Things, Logical Key Hierarchy, Object Management Group, Real Time Publish-Subscribe.**

I. Introducción

LOS sistemas distribuidos involucran la interacción entre una gran cantidad de entidades independientes. DDS[**?**] facilita a los desarrolladores usar las redes comerciales actuales para la distribución de datos periódicos con estrictos parámetros de calidad de servicio. Es una solución más económica que el resto ya que evita la inversión en nuevas redes y componentes. Además, simplifica la integración y gestión de sistemas de tiempo real conjuntamente con otros sistemas de red empresariales.

La aplicación de estos sistemas va mas allá de conectar dispositivos domóticos, ya que ofrece un enorme grado de libertad a la hora de desarrollar cualquier tipo de sistema distribuido. Estos sistemas ya han sido implantados en muchos entorno de importantes empresas y organizaciones a nivel mundial. Este hecho garantiza la importancia de este tipo de sistemas y a su vez la necesidad de su desarrollo y evolución.

La seguridad de la información en sistemas distribuidos es compleja. La mayoría de las tecnologías de seguridad vigentes no son válidas. Concretamente, DDS no contempla en su especificación mecanismos de seguridad de la información. El problema del diseño de la seguridad en un sistema de estas características radica tanto en el gran número de entidades que lo forman como en las complicadas relaciones entre ellas. Además, hay que conseguir seguridad sin perder eficiencia ni afectar las comunicaciones.

Hasta ahora las empresas que han necesitado un mínimo nivel de seguridad la han tenido que implementar ellos mismos, con todo el esfuerzo que esto acarrea. Los desarrolladores pueden elegir entre comprar alguna solución comercial, desarrollar la seguridad para su sistema especifico o no implementar seguridad.

Usar un sistema DDS con ninguna seguridad es aceptable en ciertos ámbitos, pero nunca recomendable. Si se despliega en la práctica un sistema distribuido militar sin seguridad, podría ocurrir que algún intruso sin autorización accediera al sistema y realizase acciones dañinas. En la Figura **??** se observa un intruso en el sistema distribuido que actúa como publicador de órdenes.

Sobra decir que el ejército utiliza su propia implementación de DDS con seguridad de alto nivel. Esto permite observar el alcance de las consecuencias de no incluir seguridad en sistemas DDS. Nuestro sistema se ve indefenso frente a alguien que publique órdenes incorrectas o recolecte información.

II. Estado del arte

DDS se especifica con la intención de proporcionar una poderosa herramienta a los desarrolladores acorde con los sistemas actuales. Históricamente han existido sistemas similares a DDS con el mismo propósito desde el año 2004, propiedad de diversas empresas e incompatibles entre sí. Gracias a este estándar abierto del consorcio OMG se rompe con estas incompatibilidades, proponiéndose un modelo a seguir. Esto es muy beneficioso para la industria ya que propicia el desarrollo de los sistemas distribuidos, mejorando su desempeño y evolución.

Se contempla la calidad de servicio (QoS) de sistemas de tiempo real. Es de tipo publicación/suscripción. Este

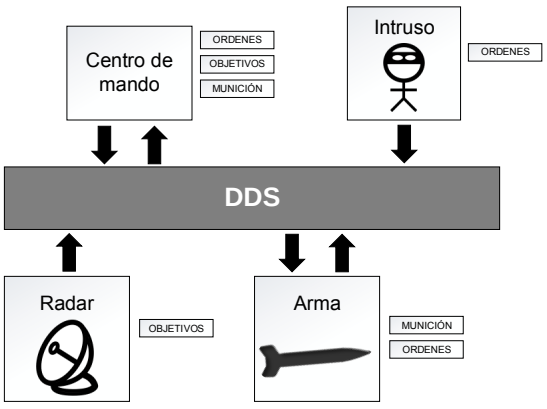


Fig. 1. Esquema DDS militar con intruso.

paradigma es novedoso en la industria y se identifica a la perfección con *sistemas de información distribuida*. Divide las entidades en dos grupos: *publicadores* y *suscriptores*. Los publicadores son los que "producen" la información y los suscriptores los que la "consumen". En la Figura **??** se observa un ejemplo sencillo del funcionamiento ideal de este paradigma. Los publicadores escriben la información en una zona de datos compartidos, llamada *Global Data Space* (GDS), y los suscriptores interesados la leen.

Para utilizar el *middleware* DDS una empresa podría llevar a cabo la implementación completa a partir de las especificaciones de OMG. Este proceso es muy costoso y no merece la pena porque existen multitud de implementaciones disponibles desarrolladas por vendedores. Algunos vendedores lo hacen con ánimo de lucro para obtener beneficios comercializando la solución. Otros liberan gratuitamente la implementación y la empresa se encarga de vender soporte y asistencia ténica. Estos vendedores en general implementan la solución DDS propuesta por el OMG, pero cuentan cada uno con diferentes características y son difícilmente interoperables. Sólo dos vendedores proporcionan mecanismos de seguridad básicos. En particular, RTI proporciona poca información respecto a cómo ha implementado la seguridad en sus sistemas.

III. Análisis de Requisitos

Mediante la especificación de los requisitos se pretende mostrar las necesidades que debe satisfacer el proyecto para su desarrollo satisfactorio. Los requisitos están escindidos en dos categorías: funcionales y no funcionales.

A. Requisitos Funcionales

- El sistema debe garantizar al menos los tres servicios de seguridad básicos: confidencialidad, integridad y autenticación[**?**].
- El sistema debe proporcionar las herramientas suficientes para la gestión correcta de la seguridad del sistema.
- Al menos la gestión de funciones criptográficas debe ser modular y extensible para que su modificación no afecte al funcionamiento del sistema. Además, es deseable que se pueda cumplir el tratado de armas internacional vigente en diferentes áreas geográficas, así como facilitar la inclusión de nuevos algoritmos criptográficos.
- El sistema debe cumplir los estrictos requisitos de tiempo real de este tipo de sistemas, no perjudicando su rendimiento en ningún caso.
- El sistema debe funcionar exitosamente en al menos una implementación de un vendedor de DDS.

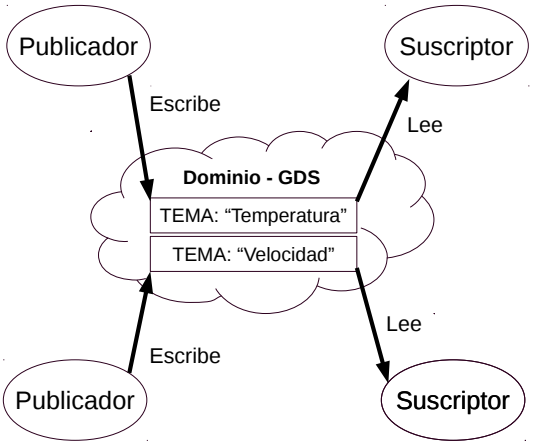


Fig. 2. Esquema de funcionamiento lógico de sistema DDS.

B. Requisitos No Funcionales

- El código debe ser extensible con el objetivo de facilitar futuras mejoras.
- El código debe ser reutilizable para que sea adaptable a múltiples sistemas. Se determina que es deseable seguir el patrón de programación estructurada.
- Las bibliotecas que se utilicen deben ser opcionales e independientes al sistema general.
- El sistema debe estar programado en un lenguaje que funcione eficientemente en multitud de arquitecturas.
- Se debe garantizar como mínimo que la implementación sea compilable con el compilador GNU GCC y que se ejecute exitosamente en sistemas Linux.

IV. Planificación

Para afrontar un proyecto de tal magnitud es necesario dividir el trabajo en diferentes tareas y asociar a cada una un tiempo para su realización. Las tareas principales son las siguientes:

- Revisión del estado del arte. Con esta tarea se pretende familiarizarse con el contexto del proyecto, estudiar los antecedentes del problema planteado y conocer las soluciones existentes en la actualidad.
- Diseño de la solución óptima. Esta tarea comprende todo el estudio y desarrollo teórico necesario para la resolución del problema.
- Implementación de la solución óptima. Esta tarea comprende todas las labores de desarrollo necesarias para conseguir una implementación válida de la solución.
- Prueba y evaluación. Esta tarea contempla todas las pruebas y evaluaciones de la solución implementada en entornos reales.
- Documentación del proyecto. Esta tarea comprende todo lo relacionado con la elaboración de la memoria del proyecto.

Se toma como fecha de inicio principios de noviembre y fecha de finalización mediados de junio. Partiendo de la división de tareas se construye el diagrama de Gantt del proyecto, donde de forma mucho más visual se presenta la planificación de todas las tareas a lo largo del tiempo.

A. Recursos

Los recursos se dividen en dos grupos: recursos de personal y recursos materiales. El personal implicado con este proyecto ha sido el alumno D. Noé Fernández Llamas y el profesor Dr. D. Pedro García Teodoro en calidad de tutor. Respecto a los recursos materiales, se distinguen dos tipos principalmente: Hardware y software. El dispositivo hardware mas destacable ha sido el ordenador personal del alumno y en lo referente al software la totalidad es gratuito de tipo software libre.

Tabla I
COSTE DE LOS RECURSOS HUMANOS.

Concepto	Coste/Tiempo	Cantidad	Total
Desarrollo	20 €/h	640h	12800€
Supervisión	100 €/h	17h	1700€
		Total:	**14500€**

Tabla II
PRESUPUESTO TOTAL DEL PROYECTO.

Concepto	Cantidad
Recursos de Personal	14500€
Recursos Materiales	60€
Gastos Indirectos	200€
Total	**14760€**

B. Estimación de Costes

Para hacer la estimación de costes se vuelve a diferenciar según el tipo de recursos. La duración total para la ejecución del proyecto es de 8 meses. Se considera que el autor ha empleado de media una jornada laboral de 4 horas, de lunes a viernes. Por lo cual se computan 640 horas de trabajo. Las reuniones del autor con el tutor han tenido lugar con una frecuencia de una cada dos semanas, es decir, dos reuniones al mes. De media una reunión suele durar 1 hora. Descontando festivos, el tutor ha computado aproximadamente 17 horas de trabajo. En la Tabla **??** se ve detallado el coste aproximado que representan los gastos de personal.

Respecto al coste de los recursos materiales, el principal objeto a tener en cuenta es el equipo informático donde se desarrollará el proyecto: un ordenador convencional. Para calcular el coste se hace una estimación del tiempo de vida de un ordenador de estas características y se calcula un precio aproximado según el uso del mismo durante el proyecto.

C. Presupuesto Total

El precio total del proyecto asciende a 14760€, CATORCE MIL SETECIENTOS SESENTA EUROS. En la Tabla **??** se puede observar el desglose global del presupuesto.

V. DISEÑO DE LA SOLUCIÓN

¿Cómo debe ser cada uno de los componentes del sistema para que este funcione en su conjunto satisfactoriamente? El diseño del sistema que proveerá los servicios de seguridad sigue un desarrollo independiente del software que soporta los sistemas distribuidos.

En primer lugar es necesario realizar un estudio del entorno objetivo del diseño, dándose especial interés al vendedor OpenDDS[**?**]. Se consigue así esclarecer y situar el módulo de seguridad dentro del esquema de un sistema distribuido. Seguidamente se analizan los agentes que intervienen en este vendedor, ya que el módulo se tendrá que adaptar según sus características. Se prosigue planteándose el módulo de manera teórica. Para abordar esta tarea satisfactoriamente se subdivide el módulo en diferentes componentes que trabajarán conjuntamente para la provisión de servicios de seguridad.

El módulo de seguridad pretendido provee con éxito las características de seguridad deseadas para un sistema distribuido. A continuación se analiza cómo se proporciona cada aspecto independientemente:

- Autenticación. Mediante el uso de claves asimétricas, el cliente tiene un par y el repositorio otro. El repositorio tiene almacenada claves públicas de los clientes e información acerca de estos.
- Autorización. Asociada a la clave pública de un cliente hay información acerca de los permisos sobre los recursos que posee.
- Integridad de los datos. Para garantizar la integridad de los datos se hace uso de funciones resumen o *hash*. Estas operan sobre los datos previos a su envío; a su llegada se calcula de nuevo el resumen y se comprueba. El código *hash* se protege con las credenciales de los clientes para que permanezca inalterado. Este proceso se conoce comúnmente como firma digital.
- Confidencialidad. Esta característica se garantiza haciendo uso de una clave de sesión simétrica dinámica en el tiempo por tema. Solo los clientes autorizados tienen acceso a esta clave; para el resto la información será ilegible. Se provee confidencialidad hacia adelante y hacia atrás, restringiendo la lectura de la información al rango de tiempo autorizado por el repositorio.
- Disponibilidad. Esta característica es inherente a DDS. Un sistema de este tipo posee los más altos estándares de disponibilidad *de facto*, garantizándose en todo momento los requisitos de tiempo real que necesite el usuario. Los repositorios de seguridad garantizan su disponibilidad gracias a que su arquitectura es federada.
- No repudio. Se garantiza no repudio de origen mediante la firma de los datos con las credenciales del publicador. El no repudio de destino no está garantizado a priori, ya que estos sistemas no son orientados a conexión y pueden contar con un número elevado de entidades destino.
- Gestión de la identidad. Se provee gracias a dos herramientas dedicadas. La primera, la entrada de terminal y la segunda, un potente entorno gráfico de interfaz de usuario que permite la gestión de un gran número de entidades de forma eficiente.

A. Planteamiento

El módulo deseado se encargará de localizar el recurso en la red jerarquizada de servidores de seguridad, autorizar el acceso al cliente, proporcionarle las credenciales del tema en concreto y el resto de funciones de seguridad necesarias. Debe funcionar conjuntamente con el sistema OpenDDS pero sin afectarlo de ninguna forma. En la Figura **??** se observa cómo quedaría el esquema de comunicaciones OpenDDS tras añadirle el módulo de seguridad.

El módulo se integra junto a las demás capas subyacentes a la capa de aplicación en el modelo de referencia por capas TCP/IP. La carga de operaciones y comprobaciones debe balancearse para el lado del servidor de seguridad, siendo lo más liviano y sencillo para el lado del cliente.

VI. IMPLEMENTACIÓN DE LA SOLUCIÓN

El desarrollo de sistemas para la provisión de servicios de seguridad en sistemas distribuidos de tiempo real es una tarea compleja. Las entidades entran y salen del sistema de forma muy dinámica y los retardos en la provisión y distribución de las claves son especialmente notables y pueden

llegar a repercutir en el sistema. Por ello, el desarrollo tiene como máxima ser lo más eficiente posible y evitar alterar el rendimiento del sistema en su conjunto. Se determina así el lenguaje de programación C++ porque cuenta con una serie de ventajas que lo hacen idóneo para este proyecto.

Para garantizar portabilidad máxima se hace uso de la biblioteca estándar de C++ y diversas librerías abiertas multiplataforma. Para el uso de características de mas bajo nivel se procederá según la familia de estándares POSIX (*Portable Operating System Interface X*)[**?**], de llamadas al sistema operativo definido por IEEE (*Institute of Electrical and Electronics Engineers*).

La implementación del proyecto es de gran magnitud y de nuevo se hace necesario escindir teóricamente el módulo de seguridad en dos agentes: el repositorio y el cliente. Para la implementación de estos dos agentes se propone tres líneas desarrollo independientes. La primera llamada *SecuRepoDDS*, hace referencia a la parte del módulo situado en el servidor de seguridad. La segunda llamada *SecuClientDDS*, hace referencia a la parte del módulo situado en la entidad publicadora/suscriptora. La tercera, llamada SecuRepoManager, hacer referencia al gestor de identidades del módulo de seguridad. En la Figura **??** se ve donde se sitúan estos tres elementos dentro del esquema del sistema distribuido OpenDDS.

Para poder afrontar la implementación del módulo es necesario seguir desacoplando los diferentes elementos de estas líneas de desarrollo. Se definen módulos comunes entre las tres aplicaciones, haciéndose mas eficiente el desarrollo. En la Figura **??** se muestran los diferentes bloques que integran cada línea de desarrollo.

SecuClientDDS es el elemento del módulo de seguridad que finalmente proporciona los servicios de seguridad a la entidad publicadora/suscriptora. Los servicios de seguridad se ofrecen según se ha visto anteriormente; en la implementación simplemente se cumplen las tareas definidas el capítulo de diseño. No se analiza a nivel de desarrollo si una clase o método de programación proporciona seguridad, ya que estos elementos son de muy bajo nivel y ofuscan la verdadera intención del módulo. Si el *framework* y los protocolos definidos son correctos, la implementación proveerá los servicios de seguridad deseados.

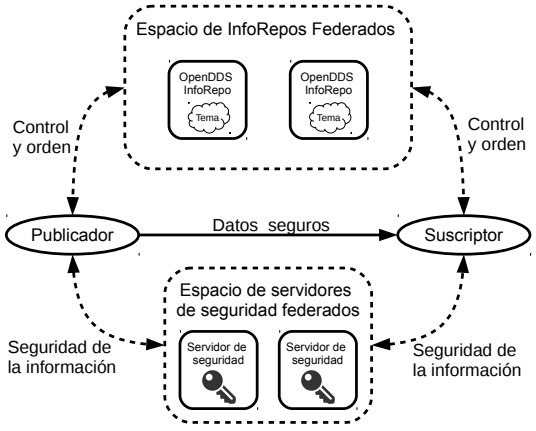


Fig. 3. Sistema con el módulo de seguridad.

VII. Prueba y Evaluación

Se prosigue con la realización de una batería de pruebas con el propósito de comprobar que el desarrollo se ha llevado a cabo correctamente y que alcanza los objetivos inicialmente marcados por el proyecto. Como es lógico, durante el desarrollo el proyecto se ha ido sometiendo a diferentes pruebas para ir verificando su avance, pero hasta ahora no se ha sometido a una batería de pruebas completa de esta magnitud. Gracias a este conjunto de diferentes pruebas que se realizan se podrá hacer un diagnóstico completo del resultado, evaluando si se ha logrado la meta inicial propuesta para cada una de las características.

En primer lugar se prueba de forma completa el funcionamiento de la interfaz de administración, procurando

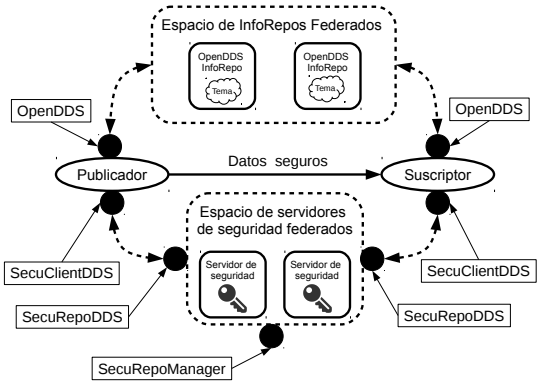


Fig. 4. Esquema de OpenDDS con los tres elementos que componen el módulo de seguridad.

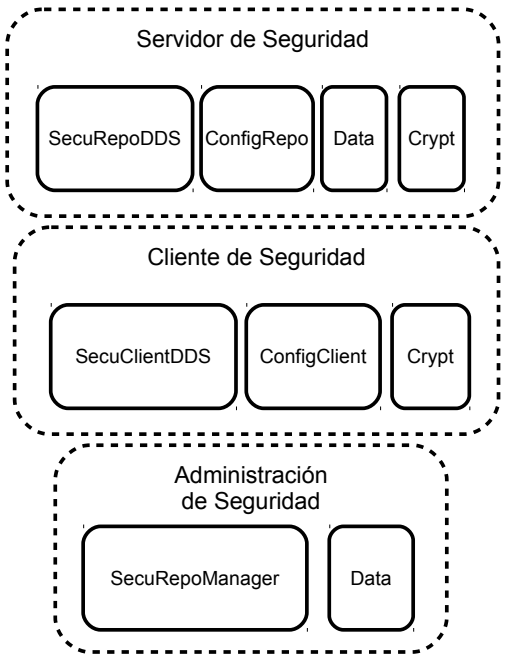


Fig. 5. Esquema de bloques agrupados de la implementación del módulo de seguridad.

demostrar que funcionan todas y cada una de las opciones disponibles. Seguidamente, se prueba el correcto funcionamiento del algoritmo de gestión de claves implementado basado en el árbol LKH. Para ello, se analiza lo que sucede en el repositorio del módulo de seguridad cuando diez clientes se adhieren a un mismo grupo ordenadamente. Para finalizar, se realiza un estudio del funcionamiento del módulo al completo, analizándose lo que ocurre tras cada evento.

VIII. Conclusiones y Líneas Futuras

Se detallan las principales conclusiones derivadas de la elaboración de este proyecto. Además, se señalan algunas posibles líneas de trabajo futuras.

A. Conclusiones

- Se ha ideado un planteamiento exitoso sobre la provisión de los servicios de seguridad en sistemas distribuidos.
- Se ha diseñado con éxito una serie de protocolos y servicios específicos para la provisión de seguridad en sistemas distribuidos.
- Se ha llevado a cabo con éxito la implementación del diseño ideado siguiendo la línea de desarrollo de un módulo software. Se ha definido un módulo para las entidades publicadoras/suscriptoras llamado *SecuClientDDS* y otro módulo servidor para la gestión de la seguridad en el sistema llamado *SecuRepoDDS*. El prototipo conseguido es totalmente funcional.
- Se ha planteado, diseñado e implementado un algoritmo de gestión de claves en grupos *multicast* eficiente e idóneo para este tipo de sistemas.
- Se ha diseñado una base de datos relacional de tipo SQL específica para este tipo de sistemas.
- Se ha integrado el módulo de seguridad dentro de una red jerárquica federada, formando en su conjunto una red bastante robusta.
- Se ha implementado un módulo gráfico con una interfaz muy útil para la gestión de la seguridad en el sistema.
- Se ha puesto de manifiesto la importancia de los servicios de seguridad en los sistemas distribuidos.
- Se ha logrado integrar el módulo de seguridad con los sistemas distribuidos actuales.
- Se ha validado y evaluado el diseño propuesto sometiéndose al prototipo del módulo de seguridad desarrollado a una diversa batería de pruebas.

B. Líneas de Desarrollo Futuras

No obstante el grado de satisfacción alcanzado con el desarrollo del presente proyecto, este es susceptible de mejorar en algunos aspectos. En concreto, una de las principales líneas de desarrollo es la mejora del prototipo para que sea apto para explotación comercial. Para alcanzar esta madurez es necesario pulir diferentes aspectos de la solución.

Los relacionados con la seguridad tratan sobre todo del uso de zonas de memoria seguras dentro de la máquina anfitrión, utilizándose vectores seguros que protegen la información de lecturas no permitidas dentro de la máquina. Respecto a mejoras de desempeño sería interesante mejorar el código del módulo para que acepte todo tipo de datos binarios de cualquier índole, consiguiéndose una ejecución aceptable en sistemas distribuidos de tipo multimedia. Respecto a los algoritmos planteados se prevé la mejora del sistema de gestión de claves, en el cual la distribución de las claves se hace en dos pasos. Primero se proporciona la nueva clave a los suscriptores y en una segunda fase se proporciona a los publicadores. Esta simple medida paliaría en gran medida las incoherencias que aparecen entre las entidades producidos por la variabilidad del retardo en la distribución de las claves en el grupo *multicast*.

No se desea que este proyecto se quede en un mero estudio académico, deseándose que lo use quien lo desee. Para ello se ha liberado el código del prototipo bajo licencia *GPLv3*. Se hospedará toda la información referente al proyecto junto al código del mismo en un repositorio público de software libre llamado *GitHub*. De esta forma se promueve que cualquier persona o profesional interesado pueda aportar lo que desee al proyecto y así lograr que alcance la madurez necesaria para uso en entornos reales. Esta decisión se toma fundamentándose en el hecho de que la seguridad de la información es un problema que afecta a toda la sociedad y la única manera de alcanzar este objetivo es si toda la comunidad de desarrolladores trabaja conjuntamente para alcanzar esta meta común.

Agradecimientos

Agradecer a mi director, Pedro, por haberme guiado durante este gran desafío, dándome ánimos y apoyándome en todo momento. Agradecer el apoyo de mis amigos, especialmente a mis queridos compañeros de grado, con los que he vivido experiencias inolvidables en los casi cuatro años de mi periodo académico en Granada. Finalmente, me gustaría agradecer a mis padres y a mi hermana el apoyo constante que me han dado durante mis estudios y muy especialmente durante la realización del proyecto.

Referencias

[1] "Data Distribution Service for Real-time Systems", Object Management Group Inc., EEUU, 2001. Disponible: http://www.omg.org/cgi-bin/doc?formal/07-01-01

[2] William Stallings, *Network security essentials: applications and standards*, 4ª ed. Prentice Hall, 2011.

[3] "OpenDDS Documentation", Object Computing Inc., EEUU, 2001. Disponible: http://www.opendds.org/documentation.html

[4] "The Open Group Base Specifications Issue 7", IEEE Std 1003.1, EEUU, 2013. Disponible: http://pubs.opengroup.org/onlinepubs/9699919799/toc.htm

Noé Fernández Llamas . Nacido el 15 de septiembre de 1992, natural de la pequeña pedanía de Campohermoso, Almería. Graduado en ingeniería de tecnologías de telecomunicación con la especialidad de telemática en la Universidad de Granada. Apasionado de las nuevas tecnologías y de los avances tecnológicos. Los campos de trabajo preferidos son el de la seguridad de la información, la robótica y el desarrollo de software. Actualmente trabajando en Madrid una compañía pionera del campo aeroespacial y de la robótica.

Teoría de la Señal y Comunicaciones

Desarrollo de técnicas de *clustering* en datos de espectrometría de masas orientadas a la detección automática de compuestos

Autor: Miguel Ángel Bellido Manganell; e-mail: mabm2810@gmail.com
Tutor: Ángel De La Torre Vega; e-mail: atv@ugr.es
Titulación: Grado en Ingeniería de Tecnologías de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—En este trabajo se ha estudiado la respuesta instrumental de un sistema de cromatografía líquida acoplada a espectrometría de masas, con el objetivo de desarrollar una técnica novedosa para la detección y la caracterización automática de compuestos en muestras químicas complejas con un alto grado de coelución. Para lograr este objetivo, se han implementado y evaluado técnicas para la supresión de ruido que reduzcan el volumen de datos. A su vez, se ha ideado, implementado y probado una técnica para la supresión de artefactos químicos de alta intensidad. Finalmente, se ha ideado, implementado y evaluado una técnica automática que permite detectar y caracterizar compuestos en muestras donde la cromatografía no sea suficiente para detectar compuestos (alto grado de coelución), obteniendo resultados muy satisfactorios que demuestran el potencial del uso de la correlación cruzada para la detección y caracterización de compuestos en muestras analizadas mediante HPLC-ESI-MS/TOF.**

***Palabras clave*— Cromatografía líquida, detección automática de compuestos, espectrometría de masas, ESI, HPLC, huella espectrométrica, MS, TOF.**

I. Introducción

A. Contexto del trabajo

Este trabajo se ha desarrollado en el contexto de una colaboración entre el departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada, el departamento de Química Analítica de la misma universidad y el Centro de Investigación y Desarrollo del Alimento Funcional.

B. Análisis de muestras químicas

Para comprender el objetivo de este trabajo, en primer lugar hay que entender que una muestra química, por ejemplo unas gotas de aceite de oliva, está formada por una variada mezcla de compuestos (distintos tipos de moléculas) en distintas concentraciones.

El objetivo del análisis de una muestra química es averiguar qué compuestos hay presentes en la muestra y con qué concentraciones. Para alcanzar este objetivo se llevan a cabo cuatro pasos; en primer lugar se detectan las señales correspondientes a los distintos compuestos. Acto seguido, se caracteriza cada uno de ellos y, según las características obtenidas, se identifica cada compuesto en las bases de datos de compuestos conocidos. Finalmente, se puede realizar una cuantificación para saber qué concentración tiene cada compuesto en la muestra.

Para poder realizar este proceso, en primer lugar hay que obtener señales a partir de la muestra. Las muestras utilizadas en este trabajo han sido analizadas mediante cromatografía líquida de alta resolución (HPLC) acoplada a espectrometría de masas por tiempo de vuelo (MS/TOF) con una interfaz de ionización por electrospray (ESI). Básicamente, la cromatografía permite distinguir los compuestos en el tiempo y la espectrometría de masas permite distinguirlos en masa.

C. Cromatografía líquida (LC)

El proceso cromatográfico se realiza inyectando la muestra, junto con una fase móvil (disolventes), en una columna separativa (tubo metálico con partículas de sílice, conocidas como fase estacionaria). A su paso por la columna, los compuestos de la muestra se verán más atraídos por la fase móvil (recorren la columna rápidamente) o por la fase fija (tardan más en salir de la columna). El tiempo en el que salen los compuestos se conoce como tiempo de retención.

Es muy importante notar que cada compuesto sale de la columna de forma continua en el tiempo, con una forma aproximadamente gaussiana. Este hecho es de vital importancia en las técnicas desarrolladas en este trabajo. En la figura 1 (gráfica superior) se observa un ejemplo de un proceso cromatográfico donde se distingue la salida de varios compuestos de la columna separativa en función del tiempo.

D. Espectrometría de masas por tiempo de vuelo (MS/TOF)

Los compuestos llegan al espectrómetro de forma continua conforme salen de la columna separativa y sus moléculas son ionizadas utilizando una interfaz de ionización por electrospray (ESI). Los iones formados son conducidos por varias cámaras hasta la zona de aceleración ortogonal, donde un campo eléctrico intermitente los impulsa al tubo de vuelo para medir el tiempo que tardan desde que son impulsados, hasta que llegan al detector, lo que se conoce como tiempo de vuelo (TOF). Conociendo el tiempo de vuelo de cada ion, dado que tanto la energía con la que han sido propulsados como la distancia que han recorrido se mantienen constantes, se puede calcular la relación masa/carga del ion.

Hay que tener en cuenta que un compuesto está formado por un tipo concreto de moléculas, las que a su vez están constituidas por átomos de distintos elementos químicos (por ejemplo oxígeno). Los átomos del mismo elemento no tienen por qué tener la misma masa, ya que pueden pertenecer a un isótopo u otro del mismo elemento. Este suceso conlleva que las moléculas de un determinado compuesto no han de tener siempre la misma masa, ya que cada variante isotópica tendrá una masa distinta.

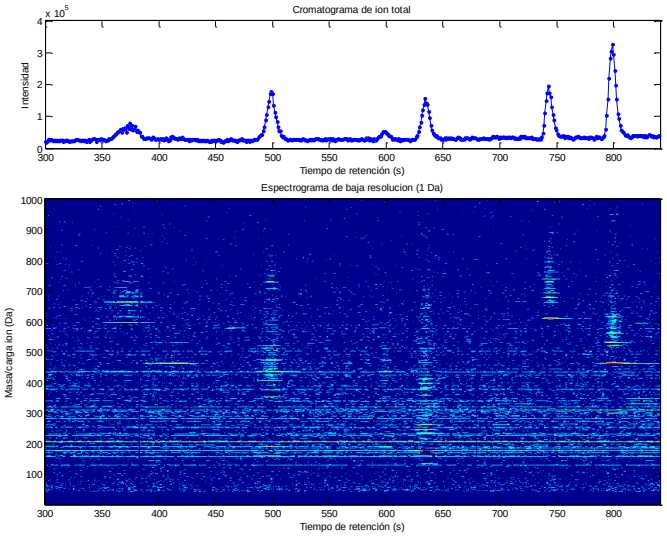


Figura 1. Ejemplo del cromatograma de ion total y del espectrograma de una muestra simple.

Además, la ionización de las moléculas puede provocar una serie de efectos adversos como la fragmentación, ionización múltiple y *clustering*, que suponen la aparición de iones con una masa distinta a la del ion principal.

Por lo tanto, cada compuesto tendrá presencia en un rango temporal concreto pero en múltiples relaciones masa/carga. Cada agrupación de entradas con igual relación masa/carga se conoce como especie iónica del compuesto. El conjunto de todas las especies iónicas que aparezcan por la presencia de un compuesto es conocido como la huella espectrométrica del mismo y es una característica propia de dicho compuesto. En la figura 1 se pueden distinguir varios compuestos (gráfica superior) y sus huellas espectrométricas (gráfica inferior).

Gracias al acoplamiento entre las técnicas anteriores (cromatografía líquida con espectrometría de masas), obtenemos un volumen muy elevado de entradas con tres valores cada una; tiempo de retención (cuándo sale cada molécula de la columna separativa), relación masa/carga (medida en daltons, Da) e intensidad (proporcional al número de iones de prácticamente igual masa que llegan en un tiempo determinado).

E. Muestras simples y complejas

Consideramos muestras simples a aquellas que tienen pocos compuestos suficientemente separados por el proceso cromatográfico. Es decir, si observamos la representación de la intensidad de todas las masas en función del tiempo de retención (lo que se conoce como cromatograma de ion total), veremos un pulso con forma gaussiana por cada compuesto abundante, resultando así trivial su detección. En la figura 1 se puede observar un ejemplo concreto de una muestra simple. En dicha figura aparece un cromatograma de ion total (imagen superior) y un espectrograma (imagen inferior), que representa la intensidad (en escala cromática) en función del tiempo de retención y de la relación masa/carga.

Consideramos muestras complejas a aquellas en las que, por tener muchos compuestos, el proceso cromatográfico no consigue separar los compuestos en el tiempo, por lo que hay muchos compuestos que salen en los mismos tiempos de retención (situación conocida como coelución entre compuestos). En la figura 2 se puede ver un ejemplo de una muestra compleja. En dicha figura se pueden observar tanto el cromatograma de ion total como el espectrograma. En el cromatograma únicamente se distinguen una serie de picos correspondientes a algunos compuestos muy abundantes, mientras que la mayoría de los compuestos permanecen ocultos por la coelución entre ellos.

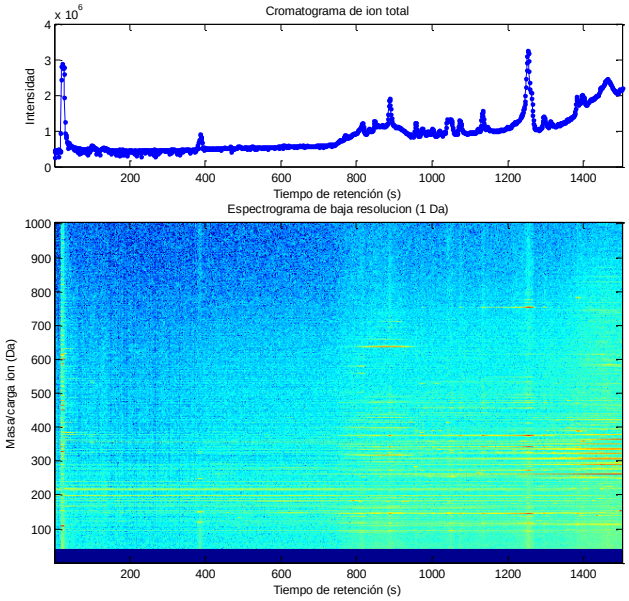


Figura 2. Ejemplo del cromatograma de ion total y del espectrograma de una muestra simple.

F. Métodos actuales para la detección y caracterización de compuestos

Generalmente, los métodos automáticos para detección y caracterización de compuestos son efectivos cuando la muestra es simple, ya que su funcionamiento consiste en distinguir los pulsos gaussianos en el cromatograma de ion total (inviable para muestras complejas). Una vez detectado cada compuesto, se caracteriza agrupando todas las especies iónicas que aparecen en su rango temporal, lo cual es lógico únicamente si ese compuesto no coeluye con ningún otro. Sin embargo, estos métodos no son capaces de obtener buenos resultados cuando la muestra es compleja, ya que la coelución entre los compuestos impide que se puedan distinguir en un cromatograma. Además, las huellas espectrométricas de los compuestos aparecerían mezcladas en el tiempo, por lo que la forma de caracterizarlos tampoco es válida (véase figura 2).

Para analizar muestras complejas, la forma más efectiva hasta el momento es la manual, que consiste en localizar de forma muy exhaustiva los pulsos gaussianos correspondientes a cada compuesto e intentar caracterizarlos observando las especies iónicas que son candidatas a formar parte de su huella espectrométrica. Este proceso requiere mucho tiempo para contrastar una gran cantidad de gráficas y de conocimientos avanzados en química analítica.

Por lo tanto, resulta evidente la necesidad de desarrollar técnicas automáticas para la detección y caracterización de compuestos en una muestra química compleja.

II. MÉTODOS

En este apartado se mostrarán tanto las técnicas únicamente implementadas (no ideadas en este trabajo) como las ideadas, implementadas y probadas en este trabajo.

A. *Preprocesado del ruido por distribución de intensidades*

La presencia de ruido iónico, estadístico y electrónico en el análisis LC-MS provoca la presencia de una gran cantidad de entradas correspondientes únicamente a ruido. Normalmente, estas entradas son de baja intensidad y no afectan seriamente la detección de compuestos, pero sí afectan significativamente al tiempo de cómputo total. Este hecho hace necesaria la implementación de técnicas que reduzcan significativamente la cantidad de ruido y, con ello, el volumen total de datos.

La técnica implementada en este apartado se basa en eliminar las entradas que estén por debajo de un umbral de intensidad, ya que se considerarán ruido. Como es lógico, cuanto mayor sea el umbral de intensidad, más ruido se eliminará. Sin embargo, un umbral de intensidad alto incrementa el riesgo de eliminar información importante (por ejemplo, una especie iónica poco abundante de un compuesto). Por lo tanto, hay que buscar un valor de intensidad que permita eliminar el máximo de ruido, manteniendo al mínimo la probabilidad de eliminar información valiosa.

La solución a este dilema se basa en la distribución de las intensidades. Si observamos el histograma de éstas, podemos distinguir claramente la presencia de dos modos distinguibles, como se ha intentado ejemplificar en la figura 3, correspondiente a un caso concreto analizado en este trabajo. El primer modo muestra la presencia de muchas entradas de baja intensidad, correspondientes a ruido. El segundo modo representa las entradas de alta intensidad correspondientes a los compuestos. Suprimiendo las entradas pertenecientes al primer modo, eliminamos gran parte del ruido de baja intensidad pero mantenemos al mínimo la probabilidad de perder información valiosa.

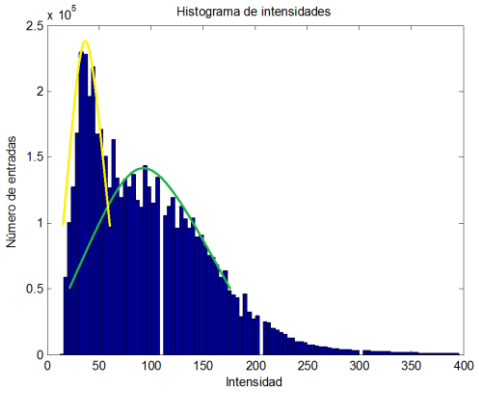


Figura 3. Ejemplo de histograma de intensidades

B. *Preprocesado del ruido por continuidad temporal*

Como se mencionó anteriormente, los compuestos salen de la columna cromatográfica con una forma aproximadamente gaussiana. Por lo tanto, las entradas correspondientes a compuestos aparecerán en tiempos contiguos y en masas prácticamente iguales, mientras que las entradas debidas a ruido aparecerán de forma aleatoria en todo el rango de tiempos y de masas. Teniendo esto en cuenta, se puede hacer un criterio, para distinguir entre ruido y compuestos, en el que, si una entrada en un tiempo T_0 tiene entradas en el tiempo anterior (T_0-1) y en el posterior (T_0+1) con prácticamente la misma masa, entonces esas entradas serán debidas a un compuesto. En caso contrario será debida a ruido. En la figura 4 se observa de forma muy evidente la continuidad de las entradas debidas a un compuesto (entradas centrales de la imagen) y la discontinuidad de las entradas debidas a ruido (bordes de la imagen).

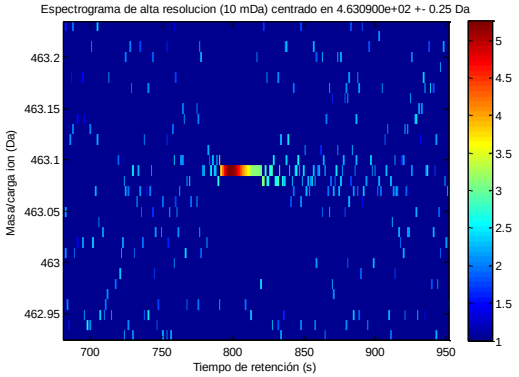


Figura 4. Ejemplo de espectrograma para un rango pequeño de masas.

C. *Detección y supresión de artefactos químicos*

Entre los datos obtenidos del análisis, encontramos una serie de señales que no son propiamente ruido, pero que por su alta intensidad afectan a la detección mucho más que éste. Estas señales las conocemos como "artefactos químicos" y se pueden observar en el espectrograma como líneas continuas horizontales (constantes en masa) con una alta intensidad. Los artefactos químicos son provocados por la ionización de la fase móvil y fija que salen de forma continua de la columna separativa, llegando a la cámara de ionización.

Los artefactos químicos afectan muy negativamente a la detección de compuestos ya que presentan una intensidad muy elevada que provoca una gran cantidad de falsos positivos en la detección, por lo que han de ser eliminados como parte de un preprocesado.

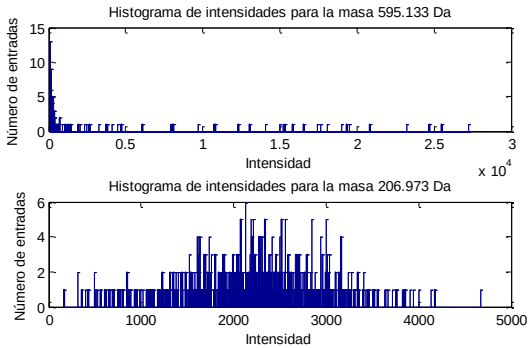


Figura 5. Ejemplo de los histogramas de intensidades de un compuesto (gráfica superior) y de un artefacto químico (gráfica inferior).

En este trabajo se ha ideado una técnica para distinguir entre compuestos y artefactos químicos. Esta técnica se basa en que, aunque ambas señales presentan una intensidad muy elevada, los compuestos salen únicamente de forma abundante en un rango de tiempos determinado y, por tanto, tienen muchas entradas de poca intensidad y pocas entradas de muy alta intensidad. Por contra, los artefactos químicos presentan entradas de alta intensidad distribuidas de forma uniforme durante todo el análisis. El factor más importante a tener en cuenta es que los compuestos tienen un rango de intensidades muy elevado (por la forma gaussiana de sus pulsos), mientras que los artefactos químicos tienen, en comparación, un rango de intensidades mucho menor. Estos hechos se reflejan en el ejemplo de la figura 5, donde se observa el histograma de intensidades de un compuesto (gráfica superior) y el histograma de intensidades de un artefacto químico (gráfica inferior). La gran diferencia entre ambas formas nos permite

identificar los artefactos químicos recorriendo el rango de masas y buscando histogramas de intensidad que tengan características similares a las observadas en la figura 5 (gráfica inferior).

D. Herramienta automática para la detección y la caracterización de compuestos en muestras químicas complejas obtenidas mediante HPLC-ESI-MS/TOF.

El objetivo principal de este trabajo ha sido probar la viabilidad de una técnica innovadora para la detección y la caracterización automática de compuestos en muestras químicas complejas.

La herramienta desarrollada se basa en el concepto de que los compuestos salen de la columna separativa con una forma aproximadamente gaussiana. Además, dado que el proceso de ionización se realiza al salir el compuesto de la columna separativa, todas las especies iónicas correspondientes al mismo compuesto tendrán exactamente la misma forma cromatográfica (intensidad en función del tiempo de retención), con una mayor o menor intensidad en función de la abundancia de cada especie iónica. En la figura 6 se observa un ejemplo de la forma cromatográfica de dos especies iónicas pertenecientes al mismo compuesto.

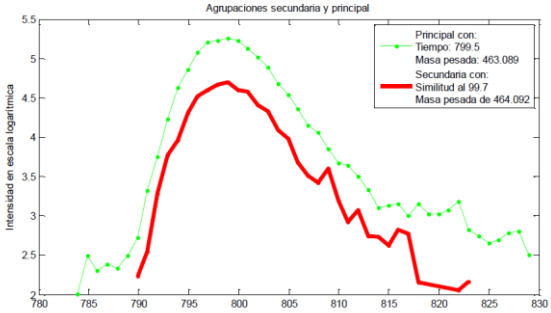


Figura 6. Ejemplo de la forma cromatográfica de dos especies iónicas del mismo compuesto.

Teniendo en cuenta los conceptos anteriores, la técnica ideada detectará los compuestos buscando especies iónicas muy abundantes (de forma que encuentre al menos una de cada compuesto) en una búsqueda muy rápida y las comparará entre sí de forma que, si la correlación cruzada entre la forma cromatográfica de dos especies iónicas es un valor cercano al 100%, entonces ambas especies iónicas pertenecen al mismo compuesto (ya que tienen igual forma cromatográfica). Por el contrario, si la correlación cruzada entre las formas cromatográficas de dos especies iónicas es un valor bajo, las especies iónicas pertenecerán a compuestos distintos. Una vez realizado este proceso, habremos encontrado la especie iónica más abundante de cada compuesto (o ion principal) y, por tanto, habremos completado el proceso de detección de compuestos.

Cabe destacar que la detección se ha realizado comparando (por correlación cruzada) las especies iónicas entre sí, por lo que aunque dos (o más) compuestos coeluyan, su correlación cruzada será baja por no tener la misma forma cromatográfica y, por tanto, se podrán detectar dos (o más) compuestos que estén coeluyendo, superando así el problema de la coelución.

La caracterización de cada compuesto se realiza agrupando las especies iónicas asociadas a dicho compuesto en su huella espectrométrica. Para ello, se compara (por correlación cruzada) la especie iónica principal de cada compuesto encontrado, con todas las posibles especies iónicas que se encuentren en su rango temporal. Al igual que se hacía en la detección, si la correlación cruzada da un valor muy elevado, entonces la especie iónica formará parte de la huella espectrométrica del compuesto. De esta forma se caracteriza cada compuesto por separado aunque sus huellas espectrométricas estuviesen mezcladas por la coelución, ya que se distinguen entre sí por correlación cruzada.

El proceso realizado, de forma general, es el siguiente:

- Aplicación de un umbral de intensidad elevado. Este paso es fundamental, ya que permite detectar los compuestos muy rápidamente. El valor del umbral ha de ser cogido con cuidado ya que, un valor demasiado bajo hace que el proceso sea muy lento, mientras que un valor demasiado alto puede hacer que suprimamos la especie iónica más abundante de algún compuesto y, por tanto, no lo detectemos.
- Las entradas con masa muy cercana y tiempos de retención contiguos, se agrupan en una especie iónica, agrupando así todas las entradas en las distintas especies iónicas.
- Una vez se tienen las distintas especies iónicas, se comparan entre sí por correlación cruzada y se distingue la especie iónica más abundante (o principal) de cada compuesto.
- Partiendo de la especie iónica principal de cada compuesto, en los datos en los que no se ha aplicado un umbral de intensidad (el mínimo para quitar ruido), se recorre todo el rango de masas buscando (por correlación cruzada) las demás especies iónicas del compuesto, agrupándolas en su huella espectrométrica.

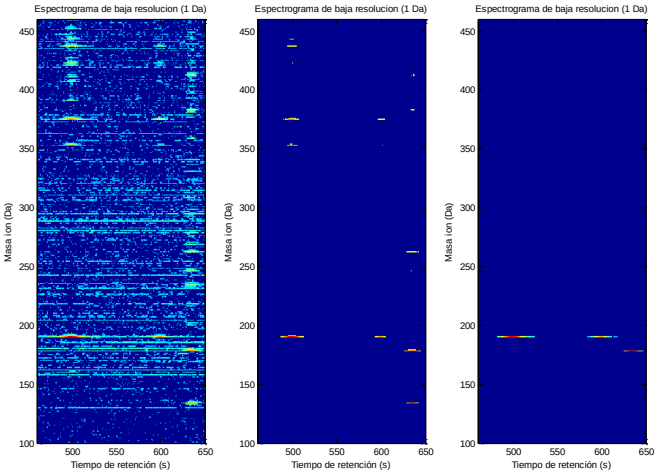


Figura 7. Ejemplo de secuencia de espectrogramas en la detección.

Para entender mejor este proceso, en la figura 7 se muestra, a modo de ejemplo, una secuencia donde se observa, de izquierda a derecha, las distintas situaciones en varios pasos del proceso. El espectrograma de la izquierda muestra una zona de los datos antes de aplicar el umbral de intensidad. En el espectrograma central se muestran las entradas tras la aplicación de un umbral alto de intensidad. Estas entradas se agrupan en las especies iónicas y se comparan entre sí, quedando finalmente las especies iónicas principales de cada compuesto, como se muestra en el espectrograma de la derecha. Como se puede observar, en este rango de tiempo y masa se han detectado tres compuestos.

Continuando con el ejemplo anterior, la caracterización de la huella espectrométrica para los tres compuestos detectados se puede observar en la figura 8. Correlacionando las especies iónicas principales encontradas (espectrograma central) con

todas las especies iónicas de todo el rango de masas (espectrograma de la izquierda), se agrupan las especies iónicas en las tres huellas espectrométricas (espectrograma de la derecha).

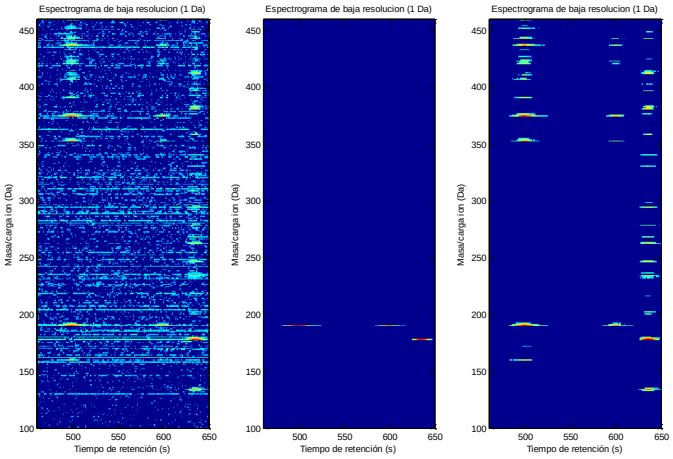


Figura 8. Ejemplo de secuencia de espectrogramas en la caracterización.

E. Experimentos para la evaluación

La evaluación de las técnicas de preprocesado de ruido y de la técnica de supresión de artefactos químicos, se realiza de forma cuantitativa según sus resultados en muestras complejas.

Para evaluar la técnica de detección y caracterización de compuestos, el proceso es mucho más complejo ya que no se puede comparar con ningún método automático actual (no consiguen enfrentarse a una situación con coelución). Por lo tanto, se va a realizar la evaluación comparando sus resultados con los obtenidos por un equipo de expertos en química analítica cuando realizaron la detección y la caracterización de forma exhaustiva y manual, utilizando en ambos casos los mismos datos.

III. RESULTADOS

A. Datos utilizados para la evaluación

Se han utilizado dos colecciones distintas de muestras; una colección de muestras simples preparadas en el laboratorio y una colección de muestras complejas obtenidas de aceite de oliva.

La colección de muestras simples consiste en la mezcla preparada en laboratorio de varios estándares polifenólicos, en distintas proporciones según la muestra. Por lo tanto, en cada una de estas muestras se sabe qué compuestos han de aparecer y en qué proporción, por lo que la evaluación consistirá en comprobar que los compuestos detectados coinciden con los mezclados en esa muestra en el laboratorio. En la figura 1 se observa la representación de una de estas muestras.

La colección de muestras complejas está formada por extractos fenólicos de distintos aceites de oliva. Estas muestras tienen una gran cantidad de compuestos que coeluyen entre sí, por lo que es muy difícil realizar en ellas la detección y caracterización de compuestos.

B. Preprocesado de ruido

Para comprobar la eficacia de los métodos de preprocesado de ruido, se han aplicado de forma conjunta en una de las muestras complejas. En primer lugar se ha aplicado el preprocesado de ruido con un umbral de intensidad bajo, correspondiente al cruce entre los dos modos mostrados en el histograma de la figura 3. Tras la aplicación del umbral, se ha utilizado la condición de continuidad temporal, eliminando las entradas que no presenten entradas de igual masa en el instante anterior y posterior. Aplicando este filtrado, se ha logrado reducir el volumen de entradas de 6.717.788 a 661.560 (reducción de más del 90%).

C. Identificación y supresión de artefactos químicos

Para evaluar este método se puede observar la reducción del número de entradas de alta intensidad antes y después de eliminar los artefactos químicos. En la figura 9 se muestra el resultado de aplicar la supresión de artefactos químicos a una muestra simple, donde se observan claramente las líneas de masa continua (artefactos químicos) que se han eliminado. De forma cuantitativa, se ha pasado de 1.200 entradas de alta intensidad a 429 entradas de alta intensidad, consiguiendo así una reducción del 64,25%.

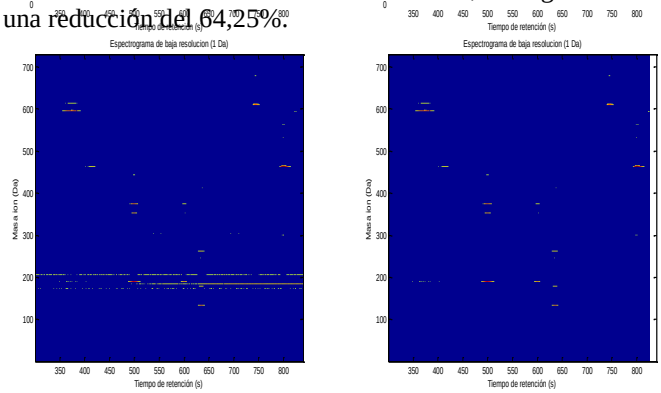


Figura 9. Supresión de artefactos químicos en una muestra simple.

D. Detección y caracterización de compuestos en muestras simples

Aplicando la herramienta en la muestra simple mostrada en la figura 3, se detectan y caracterizan 7 compuestos. De los 7 compuestos detectados, 5 de ellos habían sido mezclados en la muestra y los otros 2 eran contaminantes presentes en la muestra, por lo que la detección ha sido correcta.

E. Detección y caracterización de compuestos en muestras complejas

En la aplicación de la herramienta a una muestra de la colección de extractos de aceites de oliva (muestras complejas por su alto número de compuestos con mucha coelución), se han detectado 83 compuestos. De forma manual, los expertos en química analítica encontraron 31 compuestos en esta muestra. De los 83 compuestos detectados, 27 coinciden con los encontrados manualmente y 37 son compuestos detectados por la herramienta pero no encontrados manualmente. Los 19 restantes son falsos positivos provocados por un lavado precoz de la columna separativa. En la figura 10 se observa un ejemplo de los 37 compuestos encontrados por la herramienta desarrollada pero no de forma manual. En dicha figura se observar que el compuesto coeluye con otros y, por tanto, no se puede distinguir de forma manual pero sí con el proceso desarrollado.

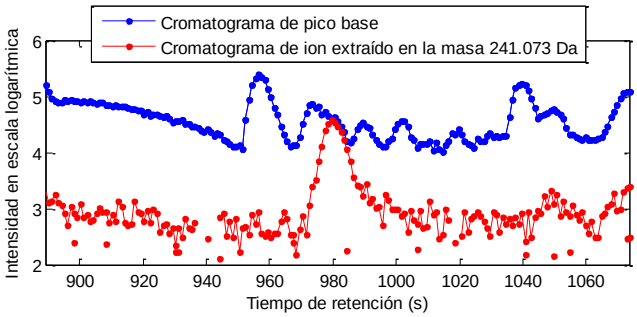
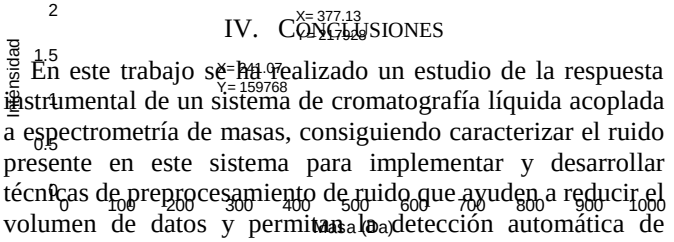


Figura 10. Cromatograma de uno de los compuestos encontrados en la muestra con la herramienta desarrollada pero no encontrados manualmente.



IV. Conclusiones

En este trabajo se ha realizado un estudio de la respuesta instrumental de un sistema de cromatografía líquida acoplada a espectrometría de masas, consiguiendo caracterizar el ruido presente en este sistema para implementar y desarrollar técnicas de preprocesamiento de ruido que ayuden a reducir el volumen de datos y permitan la detección automática de compuestos en un análisis posterior.

La efectividad de las técnicas de preprocesado de ruido, tanto la basada en la aplicación de un umbral de baja intensidad, como la basada en la continuidad temporal de los compuestos, ha sido probada y evaluada en situaciones ideales (muestras simples) y reales (muestras complejas), obteniendo resultados muy satisfactorios.

La técnica de identificación de artefactos químicos ha sido completamente ideada y desarrollada en este trabajo, donde se ha comprobado también su eficacia en muestras simples y complejas. Los resultados obtenidos han sido muy buenos en todas las situaciones donde se han evaluado.

La técnica de detección y caracterización de compuestos se desarrolló bajo la idea de probar la eficacia de que se basase en una técnica de procesamiento de señal, la correlación cruzada. Como se ha podido comprobar en este trabajo, la comparación de especies iónicas por correlación cruzada de sus perfiles cromatográficos, permite la detección y la caracterización de compuestos tanto en muestras simples como complejas, siendo capaz de superar el problema de la coelución entre compuestos. Por lo tanto, la demostración realizada en este trabajo abre un nuevo camino para el desarrollo de técnicas automáticas de detección y caracterización de compuestos en muestras químicas incluso en situaciones con un elevado grado de coelución.

Agradecimientos

Me gustaría agradecer a mi familia y amigos su constante apoyo y motivación a lo largo de todo el transcurso del trabajo. A mi tutor, Ángel De La Torre, me gustaría agradecerle todo el tiempo y esfuerzo dedicado a ayudarme a mejorar académica y laboralmente. También me gustaría agradecer al departamento de Química Analítica que me prestasen la posibilidad de acceder a los datos de las muestras químicas obtenidas por su departamento. Por último, pero no por ello menos importante, mi agradecimiento a la Universidad de Granada por todos los acuerdos que ha forjado con revistas y organizaciones científicas.

Referencias

[1] J. Throck Watson, O. David Sparkamn, "Introduction to Mass Spectrometry: Instrumentation, Applications, and Strategies for Data Interpretation", 4 th, J. Wiley & Sons, ed., New York, 2007.

[2] Gary Siuzdak, "Mass Spectrometry for Biotechnology", California, USA: Academic Press, 1996.

[3] Andrea Weston, Phyllis R. Brown, "High Performance Liquid Chromatography & Capillary Electrophoresis: Principles and Practices", California, USA: Academic Press, 1997.

[4] Kenneth A. Rubinson, Judith F. Rubinson, "Análisis Instrumental", Madrid: Pearson Educación, S.A, 2001.

[5] Shaoping Fu *et al.* (2003). Tentative Characterization of Novel Phenolic Compounds in Extra Virgin Olive Oils by Rapid-Resolution Liquid Chromatography Coupled with Mass Spectrometry. *Journal of Agricultural and Food Chemistry*, 57, pp. 11140-11147.

[6] Shaoping Fu *et al*. (2009). Characterization of isomers of oleuropein aglycon in olive oils by rapid-resolution liquid chromatography couple to electrospray time-of-flight and ion trap tandem mass spectrometry. *Rapid Communications in Mass Spectrometry*, 23, pp. 51-59.

[7] C. Roldán *et al.* (2013). Identification of active compounds in vegetal extracts based on correlation between activity and HPLC–MS data. *Food Chemistry*, 136, pp. 392-399.

[8] R. García-Villalba *et al*. (2010). Characterization and quantification of phenolic compounds of extra-virgin olive oils with anticancer properties by a rapid and resolutive LC-ESI-TOF MS method. *Journal of Pharmaceutical and Biomedical Analysis*, 51, pp. 416-429.

[9] Anestis Antoniadis *et al*. (2010). Peaks detection and alignment for mass spectrometry data. *Journal de la Société Française de Statistique,* vol. 151 No. 1.

[10] Curtis A. Hastings *et al*. (2002). New algorithms for processing and peak detection in liquid chromatography/mass spectrometry data. *Rapid Communications in Mass Spectrometry*, 16, pp. 462-467.

[11] A. de la Torre *et al*. Algoritmo de reducción del ruido en datos de espectrometría de masas. *VII Colloquim Chemiometricum Mediterraneum.* Departamento de Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada.

[12] A. de la Torre *et al.* Alineamiento automático de datos en espectrometría de masas basado en descenso de gradiente. *VII Colloquim Chemiometricum Mediterraneum.* DTSTC, Universidad de Granada.

[13] S. Mota *et al*. Procesamiento comparativo de datos HPLC-MS orientado a la identificación de compuestos bioactivos en muestras complejas. *VII Colloquim Chemiometricum Mediterraneum.* DTSTC, Universidad de Granada.

[14] A. de la Torre *et al*. Desreplicación basada en la correlación entre datos espectrométricos y bioactividad para la identificación de compuestos bioactivos en extractos vegetales. *VII Colloquim Chemiometricum Mediterraneum.* DTSTC, Universidad de Granada.

[15] J. Lozano-Sánchez *et al.* (2010). Prediction of extra virgin olive oil varieties through their phenolic profile. Potential cytotoxic activity against human breast cancer cells. *Journal of Agricultural and Food Chemistry*, 58, pp. 9942-9955.

[16] Fernández-Panchón *et al.* (2008). Antioxidant activity of phenolic compounds: from in vitro results to in vivo evidence. *Critical Reviews in Food Science and Nutrition*, 48(7), pp. 649-671.

[17] García-Lafuente *et al.* (2009). Flavonoids as anti-inflammatory agents: implications in cancer and cardiovascular disease. *Inflammation Research*, 58(9), pp. 537-552.

[18] Rosa Mª Quirantes Piné. (2012). "Caracterización y estudios metabolómicos de compuestos fenólicos bioactivos mediante técnicas separativas acopladas a espectrometría de masas". Tesis doctoral. Universidad de Granada.

[19] Ihsam Iswaldi. (2012). "Caracterización de compuestos fenólicos mediante técnicas separativas acopladas a espectrometría de masas de extractos vegetales con bioactividad demostrada". Tesis doctoral. Departamento de Química Analítica. Universidad de Granada.

[20] Mª Isabel Borrás Linares. (2013). "Uso de técnicas separativas acopladas a espectrometría de masas de alta resolución para estudios metabolómicos de nutracéuticos y matrices vegetales". Tesis doctoral. Departamento de Química Analítica. Universidad de Granada.

[21] Chao Yang *et al*. (2009). Comparison of public peak detection algorithms for MALDI mass spectrometry data analysis. *BMC Bioinformatics*, 10:4.

Modelado y parametrización en un sistema de detección no destrutiva ultrasónica

Autor: Juan Manuel Soto Rueda, e-mail: juanchu@correo.ugr.es
Tutor: Antonio Miguel Peinado Herreros, e-mail: amp@ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*— En el contexto de la evaluación no destructiva ultrasónica, en este trabajo se ha diseñado un sistema de detección y cuantificación de daño en placas de fibras de carbono. Para ello se ha hecho uso de un modelado mecánico *sparse* de la señal, que representa de forma sencilla las interacciones del ultrasonido y el material testado, con el fin de extraer una serie de vectores de características representativos. Concretamente, aquí se trabaja tanto con parámetros cepstrales como con otros derivados de la transformada discreta del coseno. Posteriormente, a las características originales extraídas se les aplican diferentes técnicas de reducción dimensional con el fin de eliminar la información redundante que contienen. Finalmente, se introducen en un sistema de clasificación basado en análisis discriminante con el objetivo de discriminar la severidad del impacto al que se sometió el material de prueba. Este enfoque incrementa notablemente la tasa de acierto del clasificador, reduciendo además el coste computacional.**

***Palabras clave*— Análisis discriminante, evaluación ultrasónica no destructiva, extracción de características, modelado sparse de señal, reducción dimensional.**

I. Introducción

El objetivo de este trabajo es el análisis de daños a un espécimen de fibra de carbono reforzado con polímero (CFRP). Este tipo de material se emplea ampliamente en la actualidad en sectores como la construcción, la industria o la aeronáutica debido a sus excelentes propiedades mecánicas: gran rigidez, baja densidad, resistencia a la corrosión y un bajo coeficiente de expansión térmica. Sin embargo, sus propiedades se pueden ver afectadas por algún tipo de impacto durante el proceso de fabricación, así como por la fatiga que pueda sufrir el material con el tiempo. Incluso si estos daños no son visibles, la integridad mecánica puede verse afectada, de manera que se requieren mecanismos de exploración de este material para la localización de defectos.

Con este fin, una de las alternativas que se suelen emplear es la evaluación no destructiva (END) ultrasónica, ondas acústicas por encima de los 20 KHz que nos proporcionan un método no invasivo, eficiente y a bajo coste para analizar la estructura interna de los materiales. Este tipo de mediciones suelen ser muy precisas y nos ofrecen una información muy detallada (localización, tamaño y orientación) de las discontinuidades presentes en un material [1]. El parámetro más importante que se debe tener en cuenta en END es la frecuencia de trabajo, la cual se ajustará principalmente en función del material a explorar y los siguientes requisitos de nuestro sistema:

- Sensibilidad, que es la capacidad de detectar pequeñas discontinuidades. Ésta se incrementa conforme aumentamos la frecuencia del ultrasonido, puesto que se trabaja con longitudes de onda menores, lo que permite una exploración más fina de los defectos del material.
- Resolución o capacidad de discriminar dos defectos muy cercanos entre sí, para lo que conviene emplear una frecuencia lo más elevada posible.
- Capacidad de penetración. A mayor frecuencia la penetración del ultrasonido es más superficial.

La complejidad interna de la estructura de CFRP hace que la interpretación del ultrasonido no sea inmediata puesto que típicamente aparecen numerosos ecos solapados. Por ello se hace necesario un conjunto robusto de parámetros adecuado que permita extraer información relevante del espécimen, los cuales serán extraídos de un modelado mecánico del CFRP. Típicamente este modelo suele ser todo-polos, pero en este artículo se empleará un modelo *sparse* de la señal que ha funcionado muy bien en trabajos similares [2] - [3]. En cuanto a parametrizaciones, por lo general se han utilizado ampliamente el cepstrum, la transformada discreta del coseno (DCT) o *wavelets* ya que proporcionan representaciones compactas del ultrasonido [4].

Una vez que se dispone de parámetros representativos se requiere una cuantificación de la severidad del daño que sufre el material, para lo cual se necesita un diseño de un sistema de clasificación automática que discrimine entre distintas categorías de daños. Para ello se utilizará el análisis discriminante, que ha alcanzado buenos resultados en distintos trabajos del ámbito de la END [5]. Además, se va a incluir un paso previo a la clasificación que consiste en una reducción dimensional de los vectores de parámetros, de manera que sean más representativos de los distintos niveles de daño. De esta manera, se consigue un sistema de clasificación con una gran tasa de acierto, al eliminar gran parte de la información superflua antes de utilizarla para discriminar defectos en el espécimen de CFRP bajo test.

II. Marco experimental

En este trabajo el material es una placa CFRP simétrica con 4 capas, de manera que las capas 1 y 4 son iguales entre sí, al igual que las capas 2 y 3. Dicho material se somete

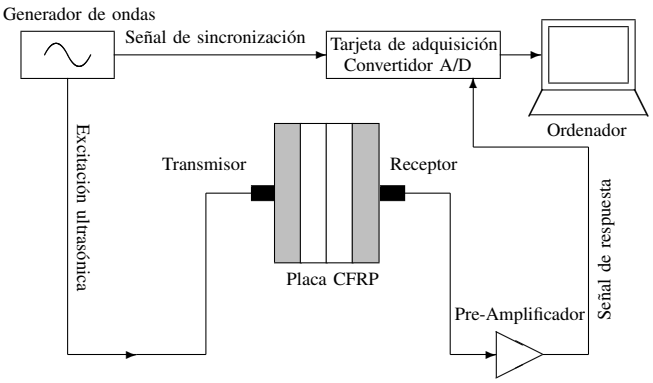


Fig. 1: Configuración experimental del sistema de medida.

a un test de impacto, lanzando contra él varios proyectiles con diferentes energías cinéticas y generando así 5 niveles de daño, etiquetados desde 1 a 5 según su severidad creciente. El montaje experimental para monitorizar las señales ultrasónicas se muestra en la figura 1, en la que se observa cómo se fijan dos transductores a los extremos del espécimen con gel acoplante (para evitar la atenuación del ultrasonido en el aire). La excitación es una señal senoidal de 5 MHz y 5 Vpp de amplitud, mientras que las señales de respuesta se registran durante 15 μs (momento en el que dejan de observarse reflexiones entre el espécimen y los transductores). Después se procede a una preamplificación de 40 dB y a un muestreo con un conversor analógico/digital de alta resolución, empleando una frecuencia de F_s=100 MHz, consiguiendo de esta manera N_s=1500 muestras. Finalmente, se aplica una cuantización uniforme de 12 bits.

Este procedimiento de medida se repite 40 veces para cada energía de impacto, de manera que generamos una base de datos con 40×6 señales (incluyendo también medidas para la placa sin dañar, a las que etiquetamos como nivel 0 de daño, a fin de tomarlas como referencia). Cada medida es el promedio de 300 capturas consecutivas de la señal, logrando así incrementar la razón de señal/ruido (SNR) alrededor de 24.7 dB. El preprocesado de las señales concluye con un enventanado Hamming para realzar los ecos secundarios de la señal ultrasónica, los cuales proporcionan información valiosa de cara a la clasificación de los daños de acuerdo a [6].

III. Diseño de la solución propuesta

En esta sección se describe cada uno de los módulos del clasificador diseñado basado en la combinación de técnicas de reducción dimensional y análisis discriminante, representado en la Fig.2.

A. Modelado mecánico

Al propagarse una onda ultrasónica a través de un material multicapa puede atravesar capas con diferentes propiedades. En tal caso, una parte de la onda se refleja, mientras que otra parte se propaga según las impedancias acústicas de los materiales que las forman [7]. Para modelar la propagación de la onda ultrasónica en el espécimen CFRP analizado se emplearán dos modelos desarrollados por Fuentes et al. [2], que sirven para describir los fenómenos de transmisión y reflexión que se muestran en la Fig.3. Aquí se describirán únicamente las variantes todo-polos de dichos modelos, puesto que son las que mejores resultados han proporcionado.

En primer lugar consideramos la 1ª aproximación mecánica ($AM1$) del modelo, que se basa en asumir que los coeficientes de transmisión T son mucho mayores que los de reflexión R, de manera que se pueden omitir éstos últimos. De esta manera se obvian las reflexiones del ultrasonido en el interior del espécimen al atravesar capas diferentes y se obtiene el modelo representado mediante la función de transferencia de la Ecuación 1,

$$H_{AM1}(z) = \frac{bz^{-M}}{\sum_{k=1}^{p} a_k z^{-k} + \sum_{k=2M}^{2M+s} a_k z^{-k} + 1} \quad (1)$$

donde M representa el espesor de la placa, b es un factor de ganancia y los parámetros s y p son los órdenes de las sumatorias del denominador, conocidas como predictores de orden bajo y de orden alto respectivamente. Cabe destacar que el modelo empleado difiere del clásico todo-polos, puesto que los coeficientes a_k no son consecutivos: es lo que se denomina modelo *sparse*. La precisión del modelado puede mejorarse si incluimos las reflexiones internas que se aprecian en la figura 3, lo cual se hace a través de un predictor adicional en el denominador de la función de transferencia del modelo. Este modelo constituye la 2ª aproximación mecánica ($AM2$) y se expresa formalmente como se muestra en la Ecuación 2,

$$H_{AM2}(z) = \frac{bz^{-M}}{\sum_{k=1}^{p} a_k z^{-k} + \sum_{k=2m}^{2m+r} a_k z^{-k} + \sum_{k=2M}^{2M+s} a_k z^{-k} + 1} \quad (2)$$

donde los parámetros m y r denotan el orden del nuevo predictor que modela la ubicación de una interfaz virtual J_v (ver Fig.3). Ésta no deja de ser un punto intermedio del material en el cual se concentran los efectos de todas las reflexiones internas.

B. Parametrizaciones

En el presente trabajo trabajamos con dos tipos de parametrizaciones, ambas derivadas a partir de los modelos

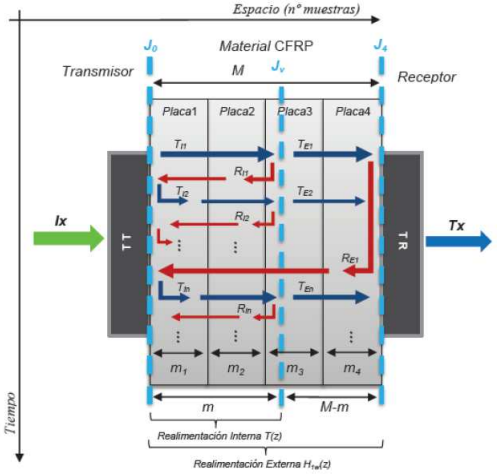


Fig. 3: Propagación de la onda en el espécimen CFRP.

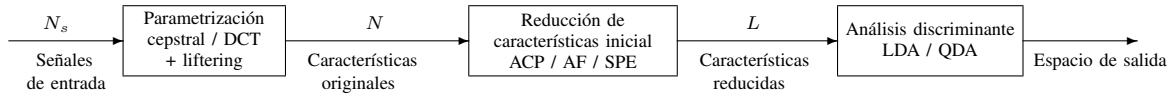


Fig. 2: Diagrama del sistema completo, con una etapa de reducción de características y otra de clasificación.

mecánicos expuestos en la Sección III-A. La primera de ellas es la DCT, entre cuyas ventajas se debe destacar el hecho de que sea una transformada real y que presenta una buena capacidad para compactar la información de la señal original en unos pocos coeficientes transformados. Por otro lado también se analiza una parametrización basada en el cepstrum c_h asociado al modelo mecánico, definido como se muestra en la Ecuación 3 en la que $\mathscr{F}$ representa la transformada de Fourier, $H(\omega)$ es el espectro en frecuencia del modelo y k denota el índice de cuefrencia. La principal ventaja de emplear el cepstrum reside en su propiedad de deconvolución [8].

$$c_h(k) = \mathscr{F}^{-1}[log|\mathscr{F}[h(n)]|] = \mathscr{F}^{-1}[log|H(\omega)|] \quad (3)$$

Ambas parametrizaciones requieren una reducción preliminar de parámetros debido a que normalmente muchas de sus componentes poseen valores cercanos a 0, lo cual supone mucha información irrelevante y que no contribuye a caracterizar las señales. Por ello se les aplica un *liftering*, esto es, un enventanado para eliminar las cuefrencias superiores (con lo que se logra suavizar el espectro, eliminando su rizado pero conservando la envolvente) o las componentes de la DCT cuando acaban tendiendo a cero.

C. Técnicas de reducción dimensional

El objetivo primordial de este paso es reducir el tamaño de los vectores de características, desde N hasta L ($L < N$), condensando la información original en un número menor de parámetros más representativos de los niveles de daño que los originales. Además, de esta manera se logra evitar el fenómeno de Hughes, también conocido como efecto de pico [9]. Éste es un problema muy común en los problemas de clasificación automática, generando un decaimiento del rendimiento del clasificador cuando la dimensionalidad de los datos de entrada es extremadamente grande o éstos se encuentran muy dispersos y con ruido. Las principales técnicas de reducción dimensional utilizadas han sido:

- Análisis de componentes principales (ACP).
  Consiste en una transformación lineal que selecciona aquellas componentes que proporcionan mayor poder resolutivo, es decir, las que presentan mayor varianza. Así, los datos originales N-dimensionales son proyectados en un espacio de menor tamaño L ($L \ll N$) donde se encuentran más decorrelados [10]. Para aplicar el ACP a nuestros datos, éstos deben tener una gran SNR. Además, se asume una gaussiana para cada una de las clases, por lo que la media y la varianza deben ser suficientes para describir la distribución de probabilidad de las mediciones en cada una de las clases. En la Ecuación 4 se muestra cómo se realiza el mapeo de los datos, siendo $\boldsymbol{W}$ la función de transformación, $\boldsymbol{X}$ ($\boldsymbol{X} \in \Re^N$) los datos originales y $\boldsymbol{Y}$ ($\boldsymbol{Y} \in \Re^L$) los vectores de características tras ser reducidos.

$$\boldsymbol{Y} = \boldsymbol{W}^T\boldsymbol{X} \quad (4)$$

  La matriz $\boldsymbol{W}$ está formada por los L autovectores asociados a los mayores autovalores de la matriz de covarianza de $\boldsymbol{X}$ ordenados decrecientemente [11]. Cuanto mayor sea L, mejor será la aproximación, aunque por lo general con unas 4-5 componentes se retiene más del 90% de la variabilidad original del conjunto de datos (si éste se ajusta bien a las hipótesis del ACP).
- Análisis de factores (AF).
  Esta técnica de reducción dimensional asume que los vectores de características de N componentes se pueden explicar mediante combinaciones lineales de un número menor L de variables. Éstas últimas se conocen como factores comunes $\boldsymbol{F}$. Además, se agrega un término de error conocido como factores únicos $\boldsymbol{U}$ para cada una de las variables N originales, llegando a la definición de la Ecuación 5.

$$\boldsymbol{X} = \boldsymbol{AF} + \boldsymbol{DU} \quad (5)$$

  En la ecuación anterior $\boldsymbol{X}$ es un vector columna que denota las variables originales, $\boldsymbol{D}$ es una matriz diagonal y $\boldsymbol{A}$ se conoce como matriz factorial, siguiendo la notación de [11]. El objetivo del análisis factorial es encontrar los coeficientes de dicha matriz que maximizan la variabilidad explicada a través de los factores comunes.
  Para reducir las dimensiones del vector de parámetros original es posible aproximar $\boldsymbol{X}$ empleando únicamente los factores comunes una vez hemos calculado la matriz $\boldsymbol{A}$, como sigue:

$$\boldsymbol{X} \approx \boldsymbol{AF} \quad (6)$$

  Tanto el ACP como el AF son técnicas lineales. Sin embargo, existe una importante diferencia conceptual entre ambas. Por un lado, el ACP se queda con aquellas características más significativas, pero escogidas entre las originales. Sin embargo, el AF genera una serie de nuevas características (los factores comunes) que tratan explicar las características originales asumiendo que éstas se pueden describir a través de un modelo subyacente en las mismas.
- *Stochastic proximity embedding* (SPE).
  Este algoritmo autoasociativo trata de insertar los datos N-dimensionales originales en un espacio euclídeo de menor dimensión (de tamaño L), preservando la métrica original de los datos [12]. De esta manera, SPE parte de una configuración inicial aleatoria de los puntos originales en el espacio reducido e iterativamente va refinando la distribución de los mismos y ajustando sus coordenadas para que las distancias en el espacio mapeado d_{ij} sean proporcionales se aproximen a las que existían en el espacio original, a las que denotaremos

por r_{ij}. SPE está especializado en modelar estructuras no lineales en las que por lo general, las distancias euclídeas y las proyecciones ortogonales no funcionan adecuadamente. Matemáticamente, equivale a minimizar la función de estrés que se muestra en la Ecuación 7,

$$S = \frac{1}{r_{ij}} \frac{\sum_{i<j} f(d_{ij}, r_{ij})}{\sum_{i<j} r_{ij}} \tag{7}$$

donde $f(d_{ij}, r_{ij})$ es una función de error por pares de puntos que se define a continuación:

$$f(d_{ij}, r_{ij}) = \begin{cases} (d_{ij} - r_{ij})^2 & \text{si } r_{ij} \leq r_c \text{ o } d_{ij} < r_{ij} \\ 0 & \text{si } r_{ij} > r_c \text{ o } d_{ij} \geq r_{ij} \end{cases} \tag{8}$$

Siendo r_c un valor predefinido que indica el radio en el que asumimos vecindad entre dos puntos.

Estas tres técnicas de reducción han sido las que mejores resultados han proporcionado, si bien se han analizado también otras alternativas interesantes como el mapeo no lineal de Sammon [13] y la clasificación de gran margen [14].

D. Clasificación basada en análisis discriminante

Llegados a este punto, mediante alguna de las técnicas de reducción dimensional del apartado anterior, se ha limitado el tamaño de los vectores de características de N a L componentes. El objetivo ahora es asignar una de las K clases o categorías de daño a cada una de las mediciones, lo cual puede hacerse maximizando la función discriminante g_k de la Ecuación (9),

$$g_k = -\frac{(\boldsymbol{x} - \boldsymbol{\mu_k})^T \boldsymbol{\Sigma_k}^{-1} (\boldsymbol{x} - \boldsymbol{\mu_k})}{2} + log(P(k)) - \frac{log(|\boldsymbol{\Sigma_k}|)}{2} \tag{9}$$

donde $\boldsymbol{\mu_k}$, $\boldsymbol{\Sigma_k}$ y $P(k)$ son respectivamente el centroide, la matriz de covarianza y la probabilidad *a priori* de la clase k ($0 \leq k \leq K-1$). De esta manera, cada medición $\boldsymbol{x}$ se clasifica como perteneciente a la clase k cuando el valor de g_k es mayor que el obtenido con cualquier otra de las clases.

La ecuación anterior genera fronteras cuadráticas para separar las diferentes categorías de daño, por lo que se conoce como discriminante cuadrático (QDA) [15]. También se puede optar por simplificar esta regla de clasificación, suprimiendo el último sumando de la Ecuación 9. Esto equivale a suponer que todas las K clases están caracterizadas por una misma matriz de covarianza ($\boldsymbol{\Sigma_k} = \boldsymbol{\Sigma}$). Dicha hipótesis nos conduce a la Ecuación (10), donde las separaciones entre clases se establecen mediante fronteras lineales. Por ello, se conoce como función discriminante lineal (LDA) [5] - [16].

$$g_{k,LDA} = -\frac{(\boldsymbol{x} - \boldsymbol{\mu_k})^T \boldsymbol{\Sigma}^{-1} (\boldsymbol{x} - \boldsymbol{\mu_k})}{2} + log(P(k)) \tag{10}$$

Es destacable el hecho de que tanto LDA como QDA permiten proyectar los datos en un espacio de menor dimensión en el que se maximiza la separabilidad entre clases (entendida ésta como una mayor distancia entre centroides de clases diferentes). Además, hay que tener en cuenta que el rendimiento de ambos clasificadores depende del tamaño de los vectores de características, así como hasta qué punto los datos de cada clase de daño se ajustan a una distribución normal multivariable [11].

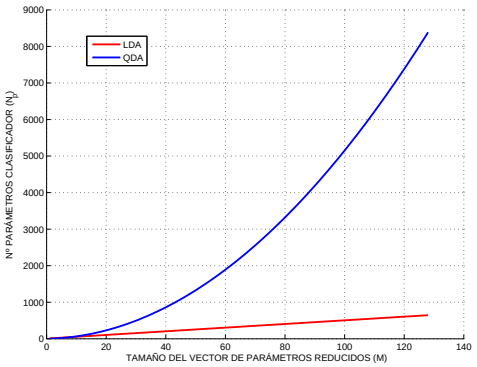


Fig. 4: Comparativa de los parámetros que requieren los clasificadores.

A continuación, en las ecuaciones (11) y (12) se compara el número de parámetros N_p que se deben estimar en cada clasificador para delimitar las fronteras entre las distintas categorías de daño.

$$N_{P,LDA} = (K-1)(L+1) \tag{11}$$

$$N_{P,QDA} = (K-1)\left(\frac{L(L+3)}{2} + 1\right) \tag{12}$$

Viendo las ecuaciones anteriores queda patente que la complejidad de LDA es $\mathcal{O}(L)$, mientras que la de QDA $\mathcal{O}(L^2)$. Un ejemplo de ello se observa en la figura 4, donde se compara el número de parámetros que requieren ambos clasificadores para un caso con $K = 6$ clases y vectores de características de hasta 128 componentes. Se comprueba que en QDA el número de parámetros a estimar se dispara rápidamente, lo que generaría clasificadores muy poco robustos. Este hecho nos permite justificar nuevamente la necesidad de introducir técnicas de reducción dimensional, ya que si se trabaja con los vectores de características sin reducir, la complejidad haría prácticamente inviable QDA.

Por tanto, LDA tiene ventaja en cuanto a mayor sencillez, lo que facilita el entrenamiento del sistema cuando no se dispone de una gran base de datos. Además, QDA presenta serios problemas con conjuntos de datos mal condicionados, por ejemplo, cuando contienen mucha información redundante. Sin embargo, como contrapartida, QDA proporciona fronteras de decisión más flexibles.

E. Interfaz gráfica

Para facilitar la utilización del sistema de clasificación, se ha diseñado una interfaz gráfica en MATLAB empleando

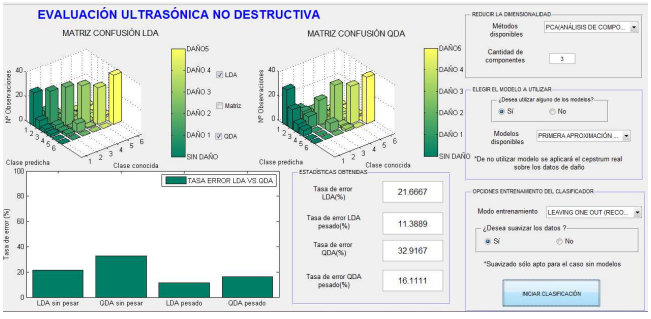


Fig. 5: Interfaz diseñada mediante GUIDE de MATLAB.

Tabla I: Error ponderado ($w_{err}[\%]$) comparando los modelos mecánicos empleando parametrización cepstral

Parametrización y modelo	Análisis Discriminante	Técnicas de reducción	L-componentes conservadas en el espacio de salida 3	4	5	6	7	8	9	10
Cepstrum AM1	LDA	ACP	11.38	6.66	5.97	7.63	7.91	12.22	19.16	17.22
		AF	6.38	5.83	4.44	8.47	8.47	15.27	23.75	28.88
		SPE	7.91	8.88	7.36	14.58	24.02	25.13	44.82	52.68
	QDA	ACP	16.11	7.22	6.11	5.69	3.75	3.33	3.33	2.91
		AF	7.63	6.52	5.97	4.44	5.00	4.58	4.16	2.63
		SPE	8.75	6.94	5.27	7.08	5.13	5.00	3.88	5.41
Cepstrum AM2	LDA	ACP	6.11	4.30	3.47	0.55	2.36	6.80	8.47	13.61
		AF	5.41	5.00	2.36	2.36	4.86	11.11	14.02	16.66
		SPE	4.3	4.16	3.88	7.77	12.91	43.05	44.30	53.88
	QDA	ACP	5.41	4.48	1.94	0.27	0.55	0.00	0.00	0.00
		AF	5.55	4.02	1.38	1.11	0.83	0.69	0.13	0.13
		SPE	5.00	3.33	2.91	1.80	1.11	0.41	0.13	0.00

GUIDE de cara al usuario final, tal y como se muestra en la Fig. 5. Ésta permite la selección de distintos parámetros de interés, entre ellos: modelo mecánico utilizado, parametrización elegida, técnica de reducción dimensional, número de componentes tras la reducción dimensional, tipo de análisis discriminante aplicado o el tipo de visualización de los resultados. Permitiendo este tipo de modificaciones se facilita su utilización para la clasificación de otros conjuntos de datos diferentes.

IV. Evaluación del sistema

Como se detalló en la Sección II, nuestro conjunto de datos consiste en 240 señales, 40 para cada una de las 6 categorías de daño consideradas. En primer lugar se les aplica una parametrización basada en alguno de los modelos mecánicos. A continuación se aplica un proceso de *liftering* para retener 128 coeficientes (en el dominio cepstral) o 50 (en el caso de la DCT), el cual se puede considerar como una primera etapa de reducción de características. Después se emplea alguna de las técnicas de la Sección III-C para reducir aún más el tamaño de los vectores de parámetros, de manera que se conservan entre 3 y 10 características en el espacio de salida (ver figura 2). Éstos últimos son los que sirven de entrada al sistema de clasificación en sí.

Para aprovechar de manera óptima el conjunto de datos disponible, el entrenamiento/test del mismo se hace mediante *leaving-one-out*. Así, se promedian 39 mediciones para entrenar un vector de parámetros de referencia (ya sea cepstral o DCT) para que sea representante de cada categoría, mientras que la medición restante se emplea para test. Rotando las mediciones de test empleadas se logra tener un sistema entrenado siempre con 39 mediciones por categoría de daño, pero evaluado sobre todas las medidas. Para etiquetar una muestra de test como perteneciente a una clase de daño, se medirá la distancia de su vector de parámetros con el de referencia de todas las clases y se asignará la que esté más cerca.

Para evaluar la tasa de acierto del sistema se emplea un error ponderado w_{err}, según el cual se penaliza más al sistema cuando confunde categorías de daño muy alejadas entre sí. Si $R(i,j)$ representa la matriz de confusión, con $i = 1, ..., 6$ y siendo $R(i,j)$ el número de mediciones que sabemos que pertenecen a la clase i pero se han clasificado erróneamente como parte de la clase j, entonces el error se expresa a través de la Ecuación 13.

$$w_{err}[\%] \quad = \quad 100 \times \frac{\sum_{i=1}^{6}\sum_{j=1}^{6} R(i,j) \cdot \frac{|i-j|}{3}}{240} \qquad (13)$$

Los principales resultados obtenidos se recogen en las Tablas I y II. En la primera de ellas se compara el error ponderado alcanzado con los parámetros cepstrales extraídos de cada uno de los dos modelos, $AM1$ y $AM2$, en función del número L de componentes preservadas para la etapa de clasificación. En primer lugar resulta evidente que $AM2$ logra menor error de clasificación, por lo que aunque requiere más parámetros (dispone de más predictores que ajustar) resulta más apropiado para modelar la señal ultrasónica. Por otro lado, cabe destacar el severo efecto Hughes que sufren los clasificadores LDA, de manera que su precisión depende fuertemente de L: existe un valor óptimo de este parámetro, y si nos alejamos del mismo (ya sea con valores de L muy grandes o muy pequeños) las prestaciones de la clasificación se degradan rápidamente. Típicamente, los mejores valores de L oscilan entre 5 y 6. Por el contrario, las clasificaciones con QDA no parecen verse tan afectadas por el efecto Hughes, hasta el punto que la dependencia de la tasa de aciertos con L es más suave, pudiéndose definir un rango más amplio de valores de L en los que el sistema funciona bien. Sin embargo, esto no significa que QDA evite por completo el fenómeno de pico ya que a partir de valores muy grandes de L ($L > 13$) las prestaciones del clasificador QDA también se degradan, de manera similar a lo sucedido con LDA.

En la Tabla II se muestran los resultados obtenidos con parametrización DCT extraída del modelo $AM2$. Comparando con los resultados que se mostraban en la Tabla I de la parametrización cepstral asociada a dicho modelo, se observa como el rendimiento es similar en ambos casos si bien el efecto de pico es algo más suave. En general, la DCT empieza a proporcionar buenos resultados con menor número de coeficientes L que el cepstrum. Sin embargo, los mejores resultados se han obtenido con el cepstrum aunque se necesitaba un mayor tamaño del vector de características.

Finalmente, cabe destacar que la elección de cualquiera de las tres técnicas de reducción dimensional recomendadas (ACP, AF y SPE) proporciona una tasa de acierto muy similar, de manera que los factores más determinantes que acotan la precisión del sistema son el tipo de análisis discriminante aplicado y el tamaño de los vectores de características L.

Tabla II: Error ponderado ($w_{err}[\%]$) con parametrización DCT basada en el modelo $AM2$

Análisis Discriminante	Técnicas de reducción	L-componentes conservadas en el espacio de salida 3	4	5	6	7	8	9	10
LDA	ACP	3.75	1.25	0.55	2.64	7.91	11.38	12.77	12.22
	FA	3.19	0.55	0.55	3.19	10.13	10.83	10.00	8.19
	SPE	3.33	1.66	0.97	2.50	11.94	12.64	11.25	14.44
QDA	ACP	3.61	1.11	1.11	0.41	0.97	0.27	0.41	0.41
	FA	5.00	1.80	0.41	0.27	0.41	0.27	0.13	0.13
	SPE	5.27	1.94	0.55	0.55	0.27	0.13	0.13	0.00

V. Conclusiones

En este artículo se ha analizado un procedimiento de clasificación que discrimina adecuadamente la severidad de los daños que sufre una placa de CFRP sometida a impactos de diversa energía cinética, tras lo que se concluye:

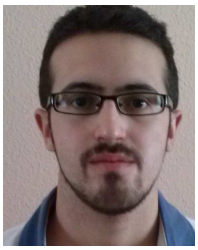
1) Ambos modelos mecánicos todo-polos, *AM1* y *AM2*, sirven para extraer vectores de características representativos de las distintas categorías de daño, si bien *AM2* es superior al tener en cuenta las reflexiones internas que se producen entre las capas de la placa de test.
2) Tanto la parametrización cepstral como la basada en DCT consiguen buenos resultados puesto que ambas concentran la información de la señal ultrasónica en unos pocos coeficientes altamente significativos.
3) El esquema propuesto, basado en técnicas de reducción dimensional y clasificación mediante análisis discriminante, ofrece una tasa de acierto muy elevada en comparación a trabajos anteriores [2] - [6]. Este hecho es debido a que se elimina gran parte de la información irrelevante contenida en el conjunto de características extraídas de los modelos antes de pasar a la etapa de clasificación en sí.
4) Las técnicas de reducción de características utilizadas (ACP, AF o SPE) contribuyen a mitigar el fenómeno Hughes en la clasificación, así como al ahorro computacional.

Agradecimientos

Deseo expresar mi más profundo agradecimiento al profesor Antonio Peinado por la supervisión del presente trabajo, así como al Laboratorio de Evaluación no Destructiva por las mediciones del espécimen CFRP.

Referencias

[1] S.C. Wooh y I.M. Daniel, "Enhancement techniques for ultrasonic nondestructive evaluation of composite materials", *Journal of Engineering Materials and Technology*, 1990, págs. 175-182.
[2] B. Fuentes, J.L. Carmona, N. Bochud, A.M. Gómez y A.M. Peinado, "Model-based cepstral analysis for ultrasonic non-destructive evaluation of composites", *IEEE ICASSP*, Kyoto, 2012, págs. 1717-1720.
[3] N. Bochud, A.M. Gómez, G. Rus, J.L. Carmona y A.M. Peinado, "Robust parametrization for non-destructive evaluation of composites using ultrasonic signals", *IEEE ICASSP*, Praga, 2011, págs. 1789-1792.
[4] G. Cardoso y J. Saniie, "Performance evaluation of DWT, DCT and WHT for compression of ultrasonic signals", *IEEE Ultrasonics Symposium*, 2004, vol.3, págs. 2314-2317.
[5] M. Deriche, "Defect classification in NDT applications using frequency features, LDA and a KNN classifier", *Australian Journal of Basic and Applied Sciences*, 2014, vol.8(7), págs. 485-498.
[6] A.M. Peinado, J.L. Carmona, N. Bochud, A.M. Gómez y G. Rus, "Representación cepstral de ultrasonidos para evaluación no destructiva en placas de fibra de carbono", *TecniAcústica: 41º Congreso Nacional de Acústica*, León, 2010.
[7] K. F. Graff, "Wave motion in elastic solids", Dover Publication, Inc., 1975.
[8] S.C. Wooh y C. Wei, "Cepstrum-based deconvolution of ultrasonic pulse-echo signals from laminated composite materials", *12th Engineering Mechanics Conference*, 1998, págs. 1-4.
[9] G. Hughes, "On the mean accuracy of statistical pattern recognizers", *IEEE Transactions on Information Theory*, 1968, vol.14(1), págs. 55-63.
[10] C. Miao, Y. Wang, Y. Zhang, J. Qu, M.J. Zuo y X. Wang, "A SVM classifier combined with PCA for ultrasonic crack size classification",*Canadian Conference on Electrical and Computer Engineering*, 2008, págs. 1627-1630.
[11] C.M. Cuadras, *Nuevos Métodos de Análisis Multivariante*, Barcelona, 2014, capítulos 5-11, págs. 77-222.
[12] D.K. Agrafiotis, D. Bandyopadhyay y E. Yang, "Stochastic Proximity Embedding: A Simple, Fast and Scalable Algorithm for Solving the Distance Geometry Problem", en *Distance Geometry : Theory, Methods, and Applications*, Ed. Springer, 2013, capítulo 14, págs. 291-311.
[13] J.W.Sammon, "A Nonlinear Mapping for Data Structure Analysis", *IEEE Transactions on Computers*, 1969, vol.18(5), págs.401-409.
[14] K.Q. Weinberger, J. Blitzer y L.K. Saul. "Distance metric learning for large margin nearest neighbor classification.", *Advances in neural information processing systems*, 2005, págs. 1473-1480.
[15] M.A. Roula, A. Bouridane, F. Kurugollu y A. Amira, "A quadratic classifier based on multispectral texture features for prostate cancer diagnosis", *Seventh International Symposium on Signal Processing and Its Applications*, IEEE, 2003, vol.2, págs. 37-40.
[16] J. Li, B. Zhao y H. Zhang, "Face Recognition Based on PCA and LDA Combination Feature Extraction", *1st International Conference on Information Science and Engineering*, 2009, págs. 1240-1243.



Autor Juan Manuel Soto Rueda (Granada, 1990). Tras finalizar los estudios de Ingeniería de Telecomunicación (2007-2014) e Ingeniería en Electrónica (2012-2014) en la Universidad de Granada, se encuentra actualmente cursando el Máster Oficial en Ciencia de Datos e Ingeniería de Computadores.
Interesado en el modelado y procesado de señal digital, desarrolló una beca de iniciación a la investigación en el Departamento de Teoría de la Señal, Telemática y Comunicaciones durante el curso 2012-13. Actualmente se encuentra colaborando en un proyecto de monitorización ultrasónica de tejidos en el Laboratorio de Evaluación No Destructiva de la Universidad de Granada.

Tutor Antonio Miguel Peinado Herreros.
Recibió los títulos de máster en Física y de doctorado en la Universidad de Granada, en 1987 y 1994 respectivamente. Ha sido profesor asociado al Departamento de Teoría de la Señal, Telemática y Comunicaciones desde 1996, y a partir de 2010 es catedrático asociado al mismo así como coordinador del grupo de investigación SIGMAT.
Es autor de numerosas publicaciones, incluyendo el libro *Speech Recognition Over Digital Channels* (Ed.Wiley), y ha servido como revisor para varias revistas y conferencias internacionales. Sus principales líneas de investigación actuales abarcan el reconocimiento robusto de voz, la codificación de audio, la transmisión robusta de señales multimedia de audio/vídeo y el procesamiento del ultrasonido.

Algoritmos de selección de regiones de interés en imágenes cerebrales estructurales y funcionales para la evaluación de la progresión de la atrofia cerebral y el hipometabolismo en la enfermedad de Alzheimer

Autor: Alberto Martínez Sánchez, e-mail: albmartsan@gmail.com
Tutores: Javier Ramírez Pérez de Inestrosa, e-mail: javierrp@ugr.es
Juan Manuel Górriz Sáez, e-mail: gorriz@ugr.es
Titulación: Ingeniería de Telecomunicaciones
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—En el presente capítulo se propone un nuevo modelo estadístico para la clasificación multimodal de imágenes de resonancia magnética y de imágenes de tomografía por emisión de positrones para su uso en el diagnóstico precoz de la enfermedad de Alzheimer. Se han diseñado y evaluado varios algoritmos para clasificar imágenes de resonancia magnética que han sido segmentadas en tejidos de materia blanca y materia gris e imágenes de tomografía por emisión de positrones, con objeto de maximizar la tasa de acierto de los clasificadores mientras el coste computacional se minimiza. Así, se ha optado por emplear conjuntos de máquinas de soporte vectoriales, se han empleado criterios de ordenación de vóxeles y se han determinado los parámetros de clasificación óptimos. De especial interés resulta el último algoritmo diseñado, en el que se propone un método que combina la información de las tres modalidades de imágenes disponibles de cada sujeto.**

***Palabras clave*—Enfermedad de Alzheimer, Conjunto de SVM, PET, IRM, Diagnóstico Asistido por Ordenador, Clasificador, VAF, Materia Blanca, Materia Gris.**

I. Introducción

La enfermedad de Alzheimer es la forma más común de demencia, un término general para la pérdida de memoria y otras habilidades intelectuales lo suficientemente serias para interferir en la vida cotidiana. La Organización Mundial de la Salud (OMS) define la enfermedad de Alzheimer como una dolencia degenerativa cerebral primaria, de etiología desconocida, que presenta síntomas neuropatológicos y neuroquímicos característicos. Afecta al 5-7 % de las personas de más de sesenta y cinco años y al 80 % de los mayores de 85 años [1] [2].

Esta enfermedad afecta a más de 30 millones de personas en todo el mundo, de los cuales 8 millones son europeos y más de 800.000 residen en España. Además, debido al progresivo envejecimiento de la población en los países desarrollados, se espera que estos números se tripliquen en 2050. A todo esto hay que añadir que la única manera para diagnosticar la enfermedad de Alzheimer de una manera completamente segura es el análisis post-mortem del cerebro del sujeto [3] [4]. Hasta entonces, mientras el paciente vive, los médicos sólo pueden emitir un diagnóstico posible o probable de la enfermedad de Alzheimer. Este diagnóstico se realiza tradicionalmente de dos formas. La primera es mediante unos test, consistentes en una batería de preguntas para la evaluación de la función cognitiva, que hacen posible discriminar entre la existencia o no existencia de demencia y evaluar la gravedad de la demencia en caso de que exista [5] [6]. Entre los test empleados cabe destacar el Examen del Estado Mental Mínimo [7] , la Escala de Deterioro Global [8] o la Escala de Evaluación para la Enfermedad de Alzheimer [9]. Sin embargo, el empleo de estos test no aporta un diagnóstico muy fiable puesto que factores exógenos como el estado de humor del paciente pueden suponer una puntuación errónea y, por tanto, un diagnóstico erróneo. El segundo método consiste en un análisis visual de las imágenes cerebrales. Así, se pueden obtener imágenes del cerebro, que pueden ser clasificadas en función de si ofrecen información sobre la anatomía del cerebro (imágenes estructurales) o si aportan información sobre su metabolismo o su actividad cerebral (imágenes funcionales).

Sin embargo, un análisis visual de estas imágenes tampoco resulta una opción infalible para el diagnóstico, puesto que en este caso también intervienen factores exógenos que pueden influir en el diagnóstico, como son la experiencia del profesional que realiza el diagnóstico o las limitaciones del ojo humano, que puede impedir que el profesional detecte ciertas irregularidades en las imágenes.

Se estima que, mediante las baterías de test neuropsicológicos y el examen visual de las imágenes neurológicas, un profesional de la salud puede emitir un diagnóstico con una fiabilidad del 70% [10]. Para intentar aumentar la precisión del diagnóstico, en los últimos años se está intentando encontrar algún método que resulte completamente objetivo. Así, se han desarrollado los sistemas de ayuda al diagnóstico por ordenador o sistemas CAD. Si bien estos sistemas suponen únicamente una ayuda al diagnóstico y no una herramienta en sí, su uso por parte de un profesional de la salud permite

aumentar la fiabilidad del diagnóstico.

II. Imágenes cerebrales

En el presente trabajo se ha desarrollado un sistema de ayuda al diagnóstico que emplea imágenes de resonancia magnética (imágenes estructurales) e imágenes de tomografía por emisión de positrones, también llamadas PET (imágenes funcionales).

Las imágenes de resonancia magnética son imágenes obtenidas de manera no invasiva, que emplean los campos magnéticos para obtener información de tejidos blandos del cuerpo humano. La aplicación de un campo magnético sobre el cuerpo humano hace reaccionar a los núcleos atómicos presentes en el cuerpo, y estas reacciones pueden ser recogidas mediante una bobina. Concretamente, para la obtención de estas imágenes se ajusta el escáner a la frecuencia de resonancia de las moléculas de hidrógeno, de manera que se obtiene una representación de los tejidos del cuerpo de acuerdo con el nivel de densidad de los fluidos que lo forman [11].

Las imágenes PET se obtienen gracias a la radiación que emite un radiotrazador o radiofármaco previamente introducido en el cuerpo del paciente. El radiofármaco se distribuirá por el cuerpo siguiendo la tasa metabólica de la molécula que compone este radiofármaco, obteniendo pues como resultado información acerca del metabolismo del paciente. Las imágenes empleadas en el presente trabajo se han obtenido mediante el uso del radiotrazador 18F, también conocido como fluorodeoxyglucosa, un análogo de la glucosa que será distribuido principalmente al cerebro y a células tumorales, debido a la gran tasa de consumo de glucosa que presentan este tipo de células [12] .

III. Sistemas CAD

Los sistemas CAD emplean técnicas de aprendizaje automático, una rama de la Inteligencia Artificial que permite dotar a los computadores de la capacidad de aprender, de manera que se vuelven capaces de generalizar ciertos comportamientos a partir de una información no estructurada suministrada en forma de ejemplos. Concretamente, en este trabajo se hará uso del aprendizaje automático supervisado, consistente en el empleo de ejemplos previamente etiquetados para el entrenamiento del clasificador. La técnica empleada para la construcción del clasificador será las máquinas de vectores de soporte o SVM [13], que consiste en un modelo que representa el conjunto de entrenamiento en el espacio, separando las clases a clasificar mediante el hiperplano óptimo, entendiendo este como aquel que maximiza la separación entre ambas clases. A través de un conjunto de muestras previamente etiquetado, se entrena a la máquina de vectores de soporte y se prueba su rendimiento (a través de los conjuntos de entrenamiento y test), de manera que la máquina de soporte es capaz de generalizar la regla de etiquetado y etiquetar muestras nuevas.

Grupo	Sujetos	Sexo M/F	Edad Media/Std	Puntos MMSE/Std
NC	68	43/25	75.81/4.93	29.06/1.08
MCI	111	76/35	76.39/6.96	26.68/2.16
AD	70	46/24	75.33/7.17	22.84/2.91

Tabla I
Datos demográficos de la base de datos

IV. Preprocesado

Las imágenes con las que se va a trabajar en este proyecto han sido obtenidas del proyecto ADNI. Nacido en 2004 con el objetivo de encontrar métodos más sensibles y precisos para la detección de la enfermedad de Alzheimer en etapas tempranas y señalar su avance a través de biomarcadores, el proyecto ha recopilado y analizado miles de escáneres cerebrales, perfiles genéticos y biomarcadores en la sangre y en el fluido cerebroespinal, que son usados para medir el progreso de la enfermedad o los efectos de un tratamiento. El estudio cuenta actualmente con más de 1000 participantes, incluyendo sujetos sin demencia, sujetos con deterioro cognitivo leve y sujetos diagnosticados como enfermos de Alzheimer.
Debido a la gran cantidad de participantes en el proyecto y a la amplia variedad de escáneres y protocolos seguidos para la toma de las imágenes, el proyecto ADNI ha desarrollado ciertos pasos de preprocesado con objeto de obtener un conjunto de imágenes estandarizado. Estos pasos de preprocesado difieren en el caso de las imágenes de resonancia magnética y en el caso de las imágenes PET.
Adicionalmente al preprocesado que ofrece la iniciativa ADNI, en el presente trabajo se ha hecho uso del software SPM (Statistical Parametric Mapping), un programa que permite realizar test estadísticos a nivel de vóxel. El preprocesado que ofrece este programa permite, entre otros, situar las imágenes cerebrales en un mismo espacio anatómico estándar, paso conocido como normalización espacial, de manera que es posible la comparación de las imágenes.

V. Base de datos

Como podemos ver en la tabla I nuestra base de datos consta de 68 sujetos diagnosticados como sanos, 70 sujetos diagnosticados como enfermos de Alzheimer y 111 sujetos catalogados como sujetos con deterioro cognitivo leve. Este último grupo se compone de sujetos que si bien por sus puntuaciones en los test neuropsicológicos no pueden diagnosticarse como enfermos de Alzheimer tampoco pueden ser considerados como sujetos sanos. En cuanto a la edad de los sujetos, podemos ver que son todos de una edad parecida y que la distribución por sexos, si bien presenta un mayor número de hombres que de mujeres, el sexo no supone una diferencia para el ámbito de este estudio, por lo que podemos afirmar que las conclusiones resultantes de este trabajo se deberán únicamente a cambios cerebrales provocados por el deterioro cognitivo.

VI. Sistema Propuesto

Mediante el uso de esta base de datos presentada anteriormente, se han desarrollado diversos algoritmos para la ayuda al diagnóstico de la enfermedad de Alzheimer.

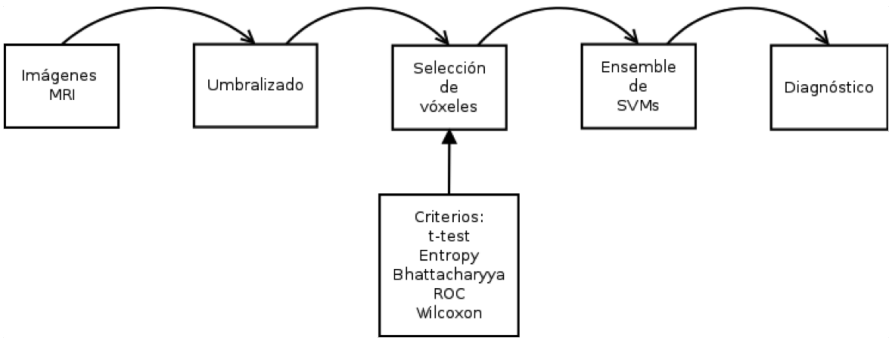


Fig. 1. Algoritmo para imágenes de Resonancia Magnética

A. Algoritmo para imágenes MRI

En 1 podemos ver los pasos seguidos por el algoritmo que se encargará de la clasificación de las imágenes de resonancia magnética. El primer paso a realizar es el del umbralizado. Este bloque va a permitir seleccionar los vóxeles de interés, acelerando de esta manera la velocidad de la clasificación. Así, aquellas regiones del cerebro cuyos vóxeles que, en los pacientes diagnosticados como sanos, presenten muy poca actividad, así como los vóxeles que se encuentran fuera de los bordes del cerebro, no se considerarán en los siguientes pasos. Con este fin, se construye una máscara mediante el promediado de todos los sujetos sanos y se seleccionan aquellos vóxeles cuyo nivel de intensidad sea mayor que un cierto umbral t, encontrándose como umbral óptimo para las imágenes de resonancia magnética un valor del 10% de la intensidad máxima
Seguidamente, se seleccionan los subconjuntos que constituirán el conjunto de entrenamiento y el conjunto de test. El esquema empleado para seleccionar estos subconjuntos es la validación cruzada de K iteraciones. Consiste en dividir el conjunto de muestras en K espacios de igual tamaño y mutuamente excluyentes, de manera que para cada iteración se selecciona un espacio para evaluar el rendimiento del clasificador, empleando el conjunto formado por la unión de todos los otros K-1 espacios para entrenar el clasificador. Una vez hemos definido los conjuntos, se seleccionan los vóxeles que se emplearán en el estudio empleando varios criterios para medir la separabilidad de las clases. Concretamente, estos criterios son el test t de Student o t-test, la curva ROC, el criterio de Bhattacharyya, la divergencia de Kullback-Leibler o criterio Entropy y el test U de Mann-Whitney-Wilcoxon o simplemente Wilcoxon. Podemos encontrar más información acerca de estos criterios para medir las diferencias entre clases en [14].

Así, se escoge uno de los 5 criterios y se obtiene como resultado los vóxeles ordenados de acuerdo con su poder discriminativo. Posteriormente, se selecciona el número de vóxeles con los que se va a trabajar, que vendrá definido por un parámetro al que llamaremos umbral. Esta selección de vóxeles resulta de vital importancia, y resulta un paso que debe realizarse con cuidado, puesto que los vóxeles que no estén contenidos en umbral serán descartados, eliminando la información que aportan. Así, se realiza un ranking de vóxeles de acuerdo con su poder discriminativo, y se seleccionarán los vóxeles de mayor a menor poder discriminativo, buscando encontrar un compromiso entre el coste computacional requerido al evaluar un número considerable de vóxeles y la tasa de aciertos que arrojará el clasificador [14].

Finalmente, se construye un conjunto de SVMs [15], que será el encargado de la construcción propiamente dicha de los clasificadores. Con objeto de obtener un diagnóstico lo más preciso posible, se ha recurrido a los ensemble o conjunto de SVMs, es decir, a combinar la salida de varias máquinas de soporte vectoriales independientes entre sí. Así, se construyen varias máquinas de vectores de soporte, cuyo número vendrá determinado por el valor de un parámetro denominado tamaño del subconjunto. Este parámetro indica el número de vóxeles con los que trabajará la primera SVM implementada. La segunda SVM trabajará con un número de vóxeles igual al doble de este valor, hasta que, finalmente, la última SVM implementada emplee todos los vóxeles disponibles. Resulta necesario indicar que los vóxeles estarán ordenados de mayor a menor poder discriminativo. Para la construcción de estos M subconjuntos f_m con los que trabajarán las SVMs implementadas, se sigue la regla:

$$f_m = \bigcup_{j=1}^{\lfloor n(\frac{m}{M})^{\alpha} \rfloor} x_{r_j} \tag{1}$$

donde α es un parámetro que representa la tasa de incremento del número de vóxeles añadidos en cada iteración. El número de máquinas de soporte vectoriales que se emplearán en cada caso dependerá tanto del número de características que se deben evaluar como del tamaño del subconjunto seleccionado. Una vez se han entrenado estas SVMs, se pasa a la fase de test. Ante una nueva imagen I, se extraen M conjuntos de características $x_{f_m}^{test}, m \in 1,...M$. Se aplica cada modelo de SVM al respectivo subconjunto de características para obtener una clasificación:

$$y_m^{pred} = \mathbf{w}_m^T \mathbf{x}_{f_m}^{test} + b_m \tag{2}$$

Posteriormente, este resultado de la clasificación se combina empleando un esquema de votación simple para determinar a qué clase corresponde la imagen que se está testando.

$$y_{test} = sgn(\frac{1}{M} \sum_{m=1}^{M} y_m^{pred}) \tag{3}$$

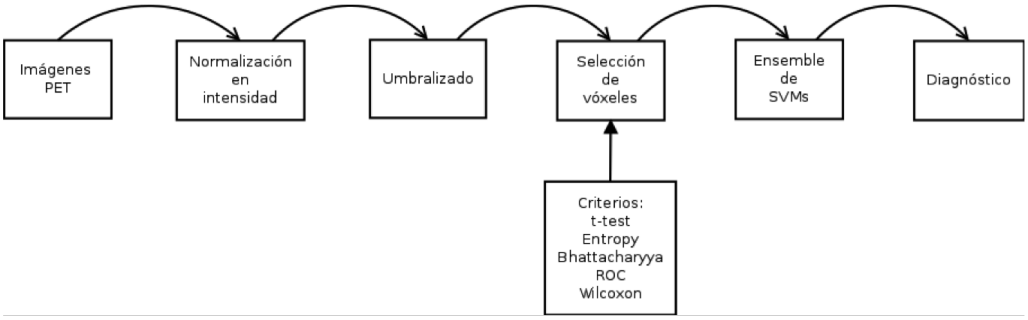


Fig. 2. Algoritmo para Imágenes de tomografía por emisión de positrones

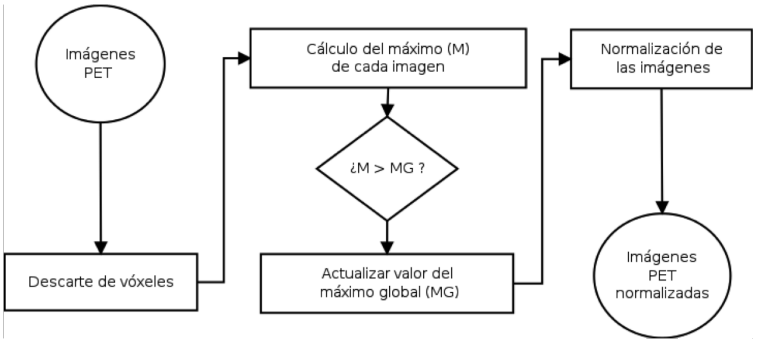


Fig. 3. Algoritmo para la normalización de imágenes de tomografía por emisión de positrones

B. Algoritmo para imágenes PET

El segundo algoritmo que se ha diseñado en este trabajo es el que permite la construcción de un clasificador de imágenes de tomografía por emisión de positrones. Tal y como podemos ver en 2, los pasos que sigue este algoritmo son idénticos a los que sigue el algoritmo de 1 a excepción del primer paso, el paso de normalización en intensidad. Este paso resulta imprescindible para obtener un buen rendimiento del clasificador, ya que lo que estamos comparando son las intensidades de los vóxeles que se encuentran en unas posiciones concretas. Las imágenes facilitadas por la iniciativa ADNI son sometidas a una normalización en intensidad en los pasos de pre-procesado [16]. Para ello se genera una imagen promedio a partir de las imágenes normalizadas espacialmente y se normalizan las imágenes empleando una máscara específica para cada sujeto, de manera que el promedio de los vóxeles dentro de la máscara es igual a 1. Este procedimiento esta definido en la guía de Protocolos para la obtención de las imágenes PET para ADNI.

Sin embargo, un análisis de los histogramas de un sujeto diagnosticado como sano y otro sujeto diagnosticado como enfermo de Alzheimer nos permite comprobar que las intensidades de los vóxeles se encuentran en un rango en el que la comparación directa de estas intensidades no resulta una tarea fácil. Por ello, se introduce una nueva normalización, que dará como resultado unas intensidades comprendidas en el rango $[0,1]$. El procedimiento empleado para conseguir esta normalización consiste en evaluar todas las imágenes de la base de datos, con objeto de encontrar el valor del máximo global al que normalizar las imágenes. El primer paso consiste en encontrar el máximo de cada imagen. Para ello, se realiza un procedimiento similar al realizado en [17], donde el máximo de cada imagen se obtiene promediando el 3% de los vóxeles de mayor intensidad, pero con ciertas peculiaridades. Si tomamos el 3%, las imágenes pueden estar expuestas a saturación, ya que se está tomando un valor relativamente pequeño. Las imágenes PET presentan un pico en los primeros niveles de intensidad, el cual se corresponde con regiones no pertenecientes al espacio cerebral y que aportan, por tanto, información irrelevante. Para solventar este hecho se establecen 50 bins para las imágenes y los valores de intensidad con los que se trabaja se toman a partir del décimo bin, descartando de esta manera gran parte de la información que aporta este pico. Posteriormente, se calcula la media del 0.1% de los vóxeles de mayor intensidad, tomando este valor ya que en una amplia selección de artículos se ha encontrado este valor como el óptimo ([4], [18], [19]). Seguidamente se toma el valor más alto encontrado y se normalizan todas las imágenes a este valor. Podemos ver un esquema del algoritmo planteado para la normalización en 3.

Además de este paso adicional, en el paso de umbralizado se ha seleccionado como umbral un valor igual al 25% de la intensidad máxima.

C. Algoritmo de clasificación conjunta

Con el objetivo de obtener un diagnóstico lo más fiable posible, se ha decidido construir un clasificador que emplee tanto la información proveniente de las imágenes PET como la información ofrecida por las imágenes de resonancia magnética de la materia gris y la materia blanca. El diagnóstico final se obtendrá como una combinación lineal de los diagnósticos de cada clasificador por separado. Antes de tomar esta decisión conjunta, se hará un estudio

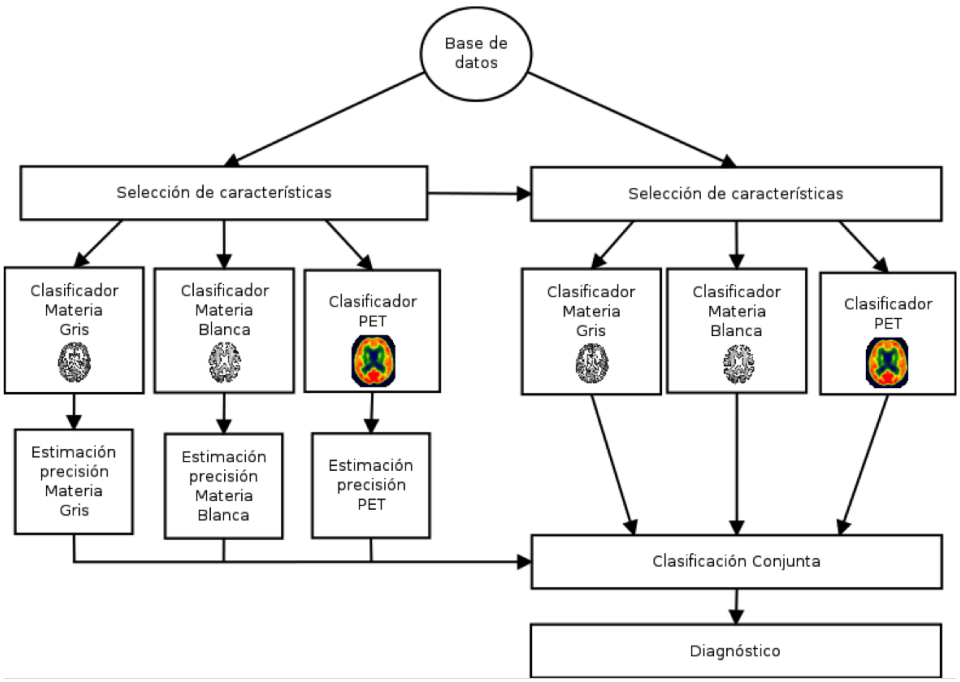


Fig. 4. Algoritmo para Imágenes de Resonancia Magnética

individual con cada clasificador, de manera que se obtenga su probabilidad de acierto y ésta pueda emplearse para ponderar el diagnóstico de cada clasificador. Así, una vez se obtienen estos pesos, se asigna a una etiqueta a cada diagnóstico (por comodidad y al tener únicamente dos clases, estas etiquetas serán $-1, +1$) y se multiplica la etiqueta por el peso correspondiente, entendiendo este peso como la tasa de acierto de cada clasificador individual. En este esquema, la decisión final se obtiene mediante la suma de estos resultados, diagnosticando como perteneciente a una clase o a otra de acuerdo con el signo del resultado obtenido, siguiendo un esquema similar al que se ha presentado en (3). Esto es lo que vemos representado en (4), representando y_{C_i} a la etiqueta correspondiente a cada uno de los 3 clasificadores, λ_i a su peso asociado y y_{C^*} a la etiqueta final.

$$y_{C^*} = sgn(y_{C_1} \cdot \lambda_1 + y_{C_2} \cdot \lambda_2 + y_{C_3} \cdot \lambda_3) \qquad (4)$$

Resulta necesario indicar que, para garantizar que no se está sobreentrenando a los clasificadores, el estudio previo para determinar los pesos de cada clasificador se realiza con un subconjunto de entrenamiento y un subconjunto de test diferentes a los que se emplean para el diagnóstico obtenido en la decisión final. En la figura 4 podemos ver el esquema que sigue el algoritmo de clasificación multimodal.

VII. Resultados y conclusiones

En el presente trabajo se ha presentado un sistema de diagnóstico por ordenador que emplea imágenes de tomografía por emisión de positrones (PET) e imágenes de resonancia magnética (MRI) de las segmentaciones de materia gris y materia blanca con el objetivo de discriminar entre enfermos de Alzheimer, sujetos sanos y sujetos con deterioro cognitivo leve. Empleando los vóxeles de las imágenes para diseñar los vectores de características (metodología Voxels as Features o VAF), se han implementado varios clasificadores que recurren a la salida de un conjunto de máquinas de vectores de soporte para la toma de decisión. Se ha conseguido probar que, a través de la combinación en un esquema de voto por mayoría simple de las salidas del conjunto de máquinas de vectores de soporte es posible alcanzar tasas de acierto superiores a las que arrojan los clasificadores que únicamente emplean una máquina de vectores de soporte para la toma de decisión. De especial mención resulta el último algoritmo implementado, donde se ha diseñado un clasificador multimodal capaz de combinar la información de las imágenes de resonancia magnética y de las imágenes de tomografía por emisión de positrones a través de un esquema de voto por mayoría ponderado donde se combina la información de los clasificadores unimodales anteriormente presentados. Se ha probado también que este algoritmo arroja tasas de clasificación superiores a los clasificadores anteriormente estudiados, por lo que se recomienda su uso en un sistema de ayuda al diagnóstico por ordenador.

En el sistema implementado se ha conseguido identificar el mínimo número de vóxeles a evaluar sin que el rendimiento del clasificador se vea afectado, reduciendo así el tiempo y el coste computacional requerido. Además, se ha evaluado la influencia de elegir un determinado tamaño para los conjuntos de entrenamiento y test, así como la influencia del número que conformará el conjunto de SVMs para la construcción del clasificador, buscando encontrar los parámetros óptimos que conducirán a la mayor tasa de acierto posible. Así, tras las diferentes pruebas realizadas, se han determinado los parámetros óptimos, entendiendo óptimos como aquellos que maximizan el rendimiento del clasificador mientras que se reduce el tiempo computacional. De esta manera, se ha determinado que el número óptimo de SVMs que deben formar

el conjunto de SVMs es de 2, el número mínimo de vóxeles que deben emplearse es de 1000 vóxeles para las imágenes de resonancia magnética, tanto para las segmentaciones de materia blanca y materia gris, y 2500 vóxeles para imágenes de tomografía por emisión de positrones. En cuanto a la técnica de evaluación k-fold, se ha concluido que la técnica 10-fold es la que arroja mejores resultados. Finalmente, se ha concluido que el criterio ROC es el que arroja las tasas de acierto más altas en la clasificación NOR vs AD, con una tasa de acierto de más del 96%, el criterio Wilcoxon para la clasificación NOR vs MCI, con unas tasas de acierto superiores al 92%, y para la clasificación MCI vs AD el criterio que arroja mayores tasas de acierto resulta nuevamente el criterio ROC, con valores mayores del 87%.

Así, la reducción de vóxeles supone pasar de 2122945 vóxeles en el caso de las imágenes PET y de 510340 vóxeles en el caso de las imágenes de resonancia magnética a 2500 vóxeles para imágenes PET y a 1000 vóxeles en el caso de imágenes de resonancia magnética, lo que supone unas reducciones del 99.9896% y del 99.8% respectivamente. Esta reducción de vóxeles es aún mayor si se tiene en cuenta que las imágenes con las que se ha trabajado en este proyecto se habían sometido a varios métodos de preprocesado, destacando el realizado por la iniciativa Alzheimer's Disease Neuroimaging Initiative (ADNI) o el realizado por el programa Statistical Parametric Mapping (SPM).

Cabe destacar que el etiquetado de las imágenes de la base de datos ADNI no está libre de errores, por lo que el entrenamiento con imágenes correctamente etiquetadas conducirá a tasas de clasificación más altas. Las fluctuaciones que sufren los resultados de la clasificación pueden indicar que la clasificación de las clases NOR vs MCI y MCI vs AD en el caso conjunto no es tan buena como la que puede realizar alguno de los clasificadores individuales. Sin embargo, sabemos que debido a la suma de errores la tasa del clasificador conjunto puede verse mermadas. Un análisis detallado de las gráficas permite ver que aparecen casos donde los resultados de la clasificación conjunta son más altos o, al menos, iguales a los resultados de los clasificadores individuales.

Finalmente, en líneas de trabajo futuras podría estudiarse el rendimiento global del sistema cuando se emplea un clasificador conjunto que, además de emplear los tres tipos de imágenes empleados en este trabajo, añadiese más tipos de imágenes que hayan probado su utilidad en el estudio de la enfermedad de Alzheimer, como pueden ser las imágenes de tomografía computarizada de emisión de fotón único (SPECT) o las imágenes de resonancia magnética funcionales (fMRI). Asimismo, podría estudiarse el rendimiento del sistema cuando se emplean técnicas como la conocida como Análisis en Componentes Independientes (Independent Component Analysis) [20], puesto que el uso de este tipo de técnicas ha probado ofrecer mejores resultados que las técnicas que emplean los vóxeles como características ([16], [19]).

AGRADECIMIENTOS

En primer lugar me gustaría agradecer a Javier, no sólo la oportunidad de realizar este proyecto, sino también por su disponibilidad, su cercanía y su gran ayuda a lo largo de su realización, poniendo en mi mano todas las herramientas y la motivación para poder finalizar este trabajo.
También me gustaría agradecer a todas las personas que han estado a mi lado durante esta etapa, especialmente a mi familia, sus palabras de ánimo, que han resultado ser de inestimable ayuda.

REFERENCIAS

[1] Grupo de trabajo de la Guía de Práctica Clínica sobre la atención integral a las personas con enfermedad de Alzheimer y otras demencias. *Guía de Práctica Clínica sobre la atención integral a las personas con enfermedad de Alzheimer y otras demencias*. Plan de Calidad para el Sistema Nacional de Salud del Ministerio de Sanidad, Política Social e Igualdad. Agència d'Informació, Avaluació i Qualitat en Salut de Cataluña; 2010. Guías de Práctica Clínica en el SNS: AIAQS Núm. 2009/07

[2] Alzheimer, A. (1907). *Über eine eigenartige erkrankung der hinrinde*. Allgemeine Zeitschrift für Psychiatrie und Psychischgerichtliche Medizin LXIV, 146-148.

[3] McKhann, G., Drachman, D., Folstein, M., Katzman, R., Price, D., & Stadlan, E. M. (1984). *Clinical diagnosis of Alzheimer's disease Report of the NINCDS/ADRDA Work Group* under the auspices of Department of Health and Human Services Task Force on Alzheimer's Disease*. Neurology, 34(7), 939-939.

[4] López Pérez, M. (2010). *Nuevos modelos estadísticos para detección de patrones de hipo/perfusión-metabolismo en imágenes de tomografía funcional cerebral*. Tesis Doctoral. Ph. D. thesis, Universidad de Granada.

[5] http://www.biopsicologia.net/Nivel-5-Discapacidad/2.2.05.12.4.-Pruebas-neuropsicologicas.html. [Última consulta: 27 de diciembre de 2013]

[6] Allegri, R., Harris, P., & Drake, M. (2000). *La evaluación neuropsicológica en la enfermedad de Alzheimer*. Rev Neurol Arg, 25(supl 1), 11-5.

[7] Folstein, M. F., Folstein S. & McHugh, P. R. (1975). *'Mini-Mental State'. A practical method for grading the cognitive state of patients for the clinician*. J Psychiatr Res.12:189-198.

[8] Sheikh, J.I, & Yesavage, J.A. (1986). *Geriatric Depression Scale (GDS): Recent evidence and development of a shorter version*. NY: The Haworth Press.

[9] Rosen, W. G., Mohs, R. C., Davis, K. L. (1984). *A new rating scale for Alzheimer's disease*. The American Journal of Psychiatry, Vol 141(11), 1356-1364.

[10] Modrego, P. J. (2006). *Predictors of conversion to dementia of probable Alzheimer type in patients with mild cognitive impairment*. Current Alzheimer Research, 3(2), 161-170.

[11] Brown, R. W., Thompson, M. R., & Venkatesan, R. (1999). *Magnetic resonance imaging*. E. M. Haacke (Ed.). New York:: Wiley-Liss.

[12] Illán, I. A., Górriz, J. M., Ramírez, J., Salas-Gonzalez, D., López, M. M., Segovia, F., Chaves, R., Gómez-Rio, M., & Puntonet, C. G. (2011). *^{18}F-FDG PET imaging analysis for computer aided Alzheimer's diagnosis*. Information Sciences, 181(4), 903-916.

[13] Vapnik, V. N., (1995). *The Nature of Statistical Learning Theory*. Springer- Verlag, Berlin.

[14] Theodoridis, S., & Koutroumbas, K. (2008). *Pattern recognition*. IEEE Transactions on Neural Networks, 19(2), 376.

[15] Varol, E., Gaonkar, B., Erus, G., Schultz, R., & Davatzikos, C. (2012). *Feature ranking based nested support vector machine ensemble for medical image classification*. In Biomedical Imaging (ISBI), 2012 9th IEEE International Symposium on (pp. 146-149). IEEE.

[16] Martínez, F. J. (2013). *Mapas de activación funcional basados en medidas de significancia estadística y en el análisis de factores y componentes*. Master thesis, Universidad de Granada.

[17] Saxena, P., Pavel, D. G., Quintana, J. C., Horwitz, B. (1998). *An Automatic Threshold-Based Scaling Method for Enhancing the Usefulness of Tc-HMPAO SPECT in the Diagnosis of Alzheimer's disease*. In: Medical Image Computing and Computer-Assisted Intervention - MICCAI, Lecture Notes in Computer Science. Vol. 1496. pp. 623-630.

[18] Illán, I. A. (2009). *Análisis en Componentes de Imágenes Funcionales para la Ayuda al Diagnóstico de la Enfermedad de Alzheimer* (Doctoral dissertation, Ph. D. Thesis, Universidad de Granada (Junio 2009)).

[19] Chaves Rodríguez, R. M. (2013). *Un nuevo modelo de interconectividad funcional cerebral mediante reglas de asociación aplicado a la detección de alteraciones neurológicas*. Ph. D. thesis, Universidad de Granada.

[20] Hyvärinen, A., & Oja, E. (2000). *Independent component analysis: algorithms and applications*. Neural networks, 13(4), 411-430.

Diseño e implementación de un equipo portátil para la adquisición de potenciales evocados auditivos del tronco cerebral

Autor: Miguel Franco, e-mail: migue88@correo.ugr.es
Tutores: Joaquín T. Valderrama, Isaac Álvarez; e-mails: jvalderrama@ugr.es, isamaru@ugr.es.
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*— El registro de potenciales evocados auditivos se utiliza en hospitales y clínicas de todo el mundo como método de detección de patologías auditivas y para estimar de forma objetiva el umbral de audición. Este documento proporciona una descripción completa y de bajo coste de un sistema de alto rendimiento de registro de potenciales evocados auditivos del tronco cerebral. Se describe el sistema de registro de potenciales detalladamente, mostrando la configuración de cada una de las etapas y justificando su funcionalidad. Asimismo se demuestra la necesidad de aumentar la razón de rechazo al modo común para las aplicaciones de electrocardiografía y encefalografía, para lo cual se ha propuesto la técnica del dispositivo de pierna derecha. La mejora de la eficiencia en este tipo de dispositivos permitirá una menor cantidad de ruido derivado de interferencias eléctricas y de origen electromagnético.**

***Palabras clave*—dispositivo de pierna derecha, potencial evocado auditivo, respuesta evocada auditiva, tronco cerebral.**

I. INTRODUCCIÓN

La respuesta evocada auditiva representa la actividad eléctrica que el sistema nervioso genera en respuesta a un estímulo de origen sonoro o eléctrico. Esta actividad eléctrica se compone de una serie de picos de voltaje de amplitudes muy pequeñas, representados con números romanos, que son generados en diversos puntos del camino auditivo [4] y que se puede registrar mediante unos electrodos de superficie (y el correspondiente sistema de medida). La principal utilidad clínica del registro de estos potenciales es la evaluación de los umbrales auditivos del paciente y la detección de ciertas patologías, aunque también es de utilidad en el ámbito de la investigación. Los potenciales de interés para este documento son los generados en el tronco cerebral (ABR, *auditory brainstem response*), que ocurren en los primeros 10 ms desde que se genera el estímulo [7]. El método más común utilizado para determinar el umbral auditivo del paciente consiste en la progresiva disminución de la intensidad del estímulo para detectar el nivel más bajo que aparece en la onda V.

En este artículo se describe el diseño e implementación de un equipo portátil capaz de adquirir potenciales evocados auditivos del tronco cerebral. Uno de los mayores desafíos que supone la realización de este sistema es la minimización del ruido; debido a la reducida amplitud de la señal biológica a registrar (varias centenas de nanovoltios) se deben realizar grandes amplificaciones sobre las muestras tomadas, lo cual implica una gran contaminación por artefactos de distinta índole. Entre estos artefactos cabe destacar el ruido eléctrico del preamplificador, los potenciales de acción asociados a actividad neuro-muscular del propio paciente o interferencias electromagnéticas de origen diverso, como por ejemplo las causadas por la red eléctrica. En un intento de reducir este grupo de artefactos se realiza un promediado de un gran número de registros para mejorar la relación señal-ruido. Esta promediación requiere que cada respuesta auditiva esté sincronizada con el estímulo que la originó de modo que, con un número suficientemente grande de respuestas promediadas, los artefactos no sincronizados tienden a anularse mientras que la respuesta no se ve afectada por la promediación, al presentar retardos fijos con respecto al estímulo y estar sincronizada con el mismo. Además de esta respuesta promediada (que es el único método que ofrecen los equipos convencionales) podemos aplicar técnicas de tratamiento digital sobre la señal completa para reducir aún más el ruido registrado.

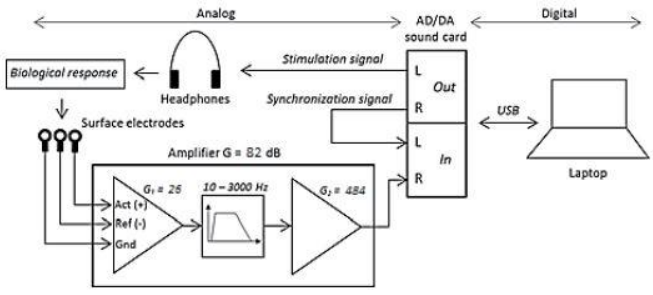


Fig. 1. Esquema general del sistema de registro de potenciales [16].

II. Sistema de registro de potenciales

En la Figura 1 se puede apreciar el procedimiento de registro de potenciales evocados auditivos. En primer lugar se estimula el sistema auditivo mediante clics de duración de 0.1 ms, cuya intensidad es configurable desde el ordenador. Éste genera una señal compuesta por un tren de impulsos que se manda de manera síncrona a través de las dos salidas de un conversor analógico-digital / digital-analógico (AD/DA). Una de las salidas del conversor AD/DA se conecta a una de sus entradas con el propósito de sincronizar el estímulo para así poder realizar la promediación, mientras que la otra salida se conecta a unos auriculares a través de los cuales se excita el sistema auditivo del sujeto para posteriormente registrar la señal deseada (en este caso un electroencefalograma) junto con el ruido mediante tres electrodos situados en la cabeza. Este electroencefalograma que se acaba de obtener pasa por un amplificador, el cual está compuesto por una etapa de pre-amplificación (reducción de ruido en modo común junto con una pequeña amplificación), una etapa de filtrado para eliminar las frecuencias que no son de interés y una etapa amplificadora. Además, con el objetivo de reducir aún más el ruido común a los electrodos, el amplificador consta de un dispositivo de pierna derecha (RLD, right leg drive) [22] que se encarga de realimentar una cantidad de corriente segura [21] al cuerpo del paciente para situar la tierra del sistema y la tierra del sujeto al mismo nivel. Por último, tras pasar por el amplificador la señal se graba de manera síncrona junto con la señal de sincronización por ambas entradas de la tarjeta de sonido y se procesa en el ordenador [1].

El diseño del amplificador se ha realizado por etapas. Para la etapa pre-amplificadora se ha determinado que el modelo implementado por Texas Instruments INA128 es el más adecuado para el sistema, debido principalmente a su producto ganancia-ancho de banda reducido, a su alta tasa de rechazo al modo común (CMRR, common mode rejection ratio), a su ganancia modificable, lineal y estable, a su alta impedancia de entrada y a su baja impedancia de salida. Se ha establecido una ganancia de 26 dB para evitar que el potencial de offset introducido por los electrodos (0.3 V) sature etapas posteriores del amplificador. En la etapa de filtrado, al ser la frecuencia de interés de entre 10 Hz y 3000 Hz se implementaron dos filtros analógicos de segundo orden en cascada, uno paso alta y uno paso baja para acotar ese rango de frecuencias. Tras esta etapa hay una segunda etapa de gran amplificación de la que se encargan dos amplificadores en configuración no inversora situados en cascada, conformando una ganancia final del sistema de 82 dB. Los La Figura 2 muestra el diagrama del circuito amplificador completo. Además del amplificador se implementaron dos dispositivos RLD con el propósito de poder comparar el rendimiento de cada uno de ellos haciendo uso del mismo sistema y condiciones ambientales. Para ello la elección del dispositivo RLD activo es controlable a través de un conmutador. Para la etapa de filtrado, amplificación y para el dispositivo RLD se ha hecho uso de operacionales OP-227 [23] debido a su alto producto ganancia-ancho de banda, y por su reducido nivel de ruido.

III. Dispositivo de pierna derecha

La razón de rechazo al modo común es un parámetro crítico en un amplificador diferencial, y en especial en aplicaciones de electrocardiografía y electroencefalografía. En este tipo de aplicaciones la principal interferencia es la causada por la red eléctrica. Además, el CMRR del sistema puede degradarse como consecuencia de una serie de desajustes en componentes internos o de factores externos en el camino de la señal, lo cual puede traducirse en hasta un 20% más de contaminación de la señal. Por tanto la mejora de este parámetro ha sido objeto de muchos estudios, habiéndose desarrollado muchas y muy diversas técnicas para mejorarlo. Para este proyecto se implementó un dispositivo RLD, el cual se encarga de realimentar una cantidad de corriente segura al sujeto con el objetivo de que el nivel de la tierra del sistema y la del sujeto sea el mismo. Una gran parte del desarrollo del proyecto ha consistido en diseñar y simular diferentes configuraciones del dispositivo RLD con el objetivo de obtener el mejor CMRR posible. Mediante el uso de herramientas como Pspice y Matlab se determinó que dos de los modelos simulados eran los que mejor rendimiento proporcionaban, con lo que fueron los modelos elegidos para ser implementados en el proyecto. Sus esquemáticos se pueden observar en la Figura 3. Para evaluar el rendimiento

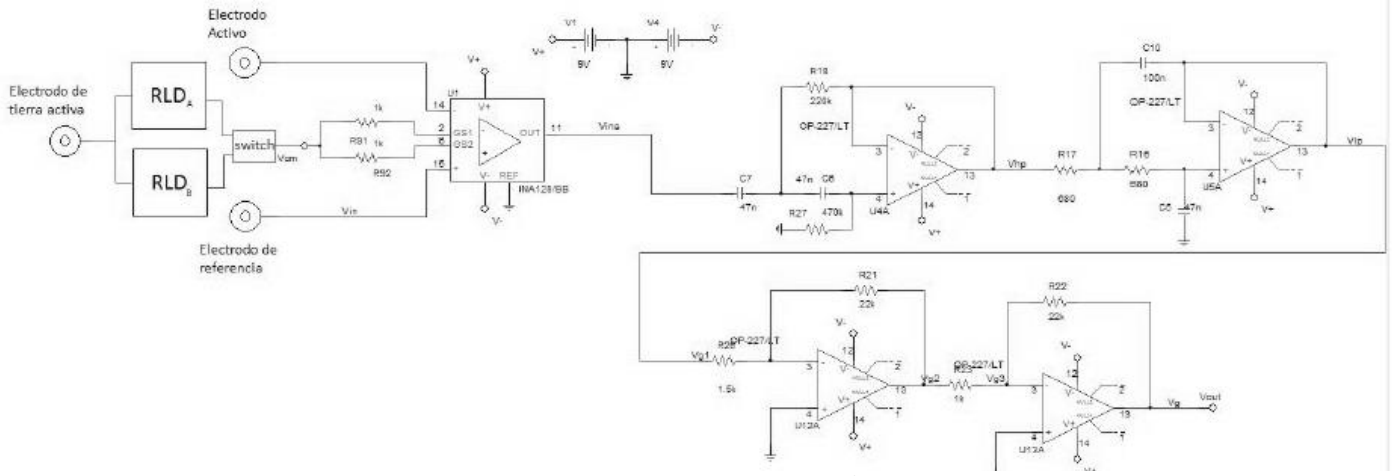


Fig. 2. Diagrama del circuito amplificador.

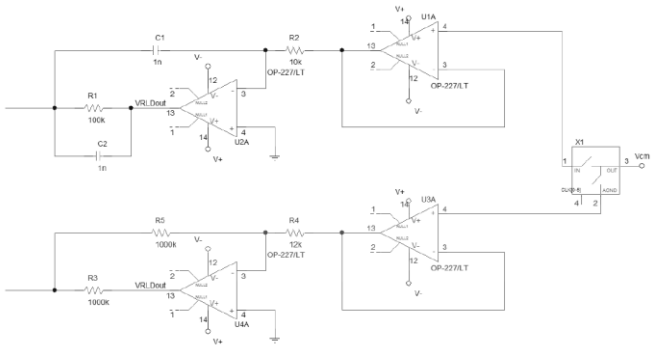


Fig. 3. Par de dispositivos RLD implementados.

de estos dos dispositivos se realizaron dos experimentos en varios sujetos bajo las mismas condiciones ambientales. Otras técnicas que se considerarán para futuras implementaciones son las que se nombran a continuación: un escudo de Faraday, el cual reduce el nivel de interferencia de la fuente de energía que entra en el sistema, además de proteger el dispositivo y los componentes de interferencias ambientales; una capacidad de aislamiento, la cual se encarga de reducir el CMRR del sistema aislando la tierra del dispositivo y la del paciente, y por último un filtro notch para eliminar la componente de 50 Hz (Europa y Asia) o 60 Hz (EEUU) de la red eléctrica. Sin embargo hay que tener mucho cuidado con este último para que las señales del mundo real no se comprometan con este tipo de filtrado, dado que hay que asegurarse de que la información de fase no está sesgada debido a la operación de filtrado.

El circuito completo (amplificador y dispositivos RLD) fue implementado tanto en una placa de inserción como en una placa de baquelita para poder comprobar el funcionamiento físico y poder obtener registros reales en diferentes sujetos.

IV. Resultados

El rendimiento del sistema descrito fue evaluado mediante la realización de dos experimentos en cuatro sujetos normoyentes. El primer experimento fue diseñado para obtener una medida de la eficiencia de ambos dispositivos RLD implementados y determinar aquel con un rendimiento mayor. Para ello no se introdujo ningún estímulo en ninguno de los cuatro sujetos, y se realizaron cuatro tomas de registro en cada uno de ellos, dos para cada RLD, una en condiciones de baja contaminación ruidosa y otras en un ambiente con muchas interferencias, mayoritariamente causadas por la red eléctrica. Este experimento mostró que en las frecuencias de interés uno de los circuitos se comportó de forma más robusta frente al ruido que el otro, además de registrar menos interferencias incluso en condiciones favorables. El segundo experimento fue diseñado para registrar potenciales evocados auditivos del tronco cerebral. Se emplearon para ello estímulos de 10.000 clics a una tasa frecuencial de 33 Hz [18] y unos niveles de intensidad de entre 40 y 100 dB nHL. Los registros tomados por los electrodos se amplificaron y guardaron mediante el conversor AD/DA. La Figura 4 muestra una serie de registros reales tomados de uno de los sujetos, lo que prueba que el sistema de registro de potenciales implementado es capaz de obtener señales

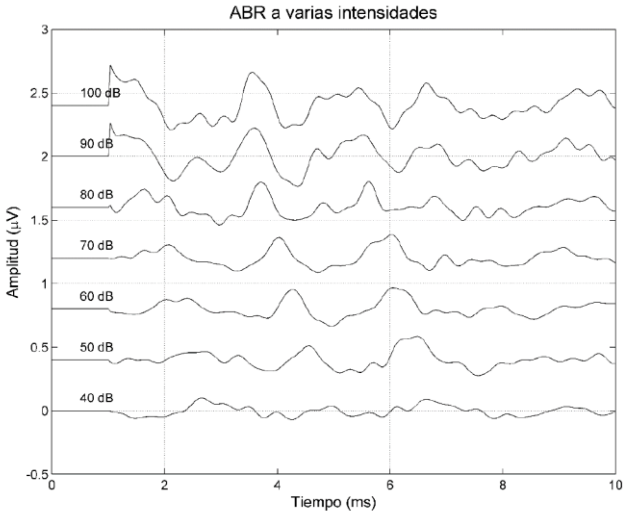


Fig. 4. Registro de potenciales del tronco cerebral a varias intensidades.

similares tanto en amplitud como en morfología a los potenciales originales dado que se pueden identificar claramente las componentes más importantes de los potenciales, presentando la misma latencia y amplitud.

V. Conclusiones

Este documento proporciona una descripción completa y de bajo coste de un sistema de alto rendimiento de registro de potenciales auditivos del tronco cerebral. El sistema descrito incluye un amplificador, una tarjeta externa de sonido que actúa como conversor AD/DA de dos canales de entrada/salida, electrodos, cables y conectores y un ordenador portátil con módulos software. El sistema de registro de potenciales aquí presentado posee un mayor grado de flexibilidad y portabilidad que los sistemas de registro comerciales, lo cual puede resultar útil para determinadas aplicaciones de investigación. Se ha descrito el sistema de registro de potenciales detalladamente, mostrando la configuración de cada una de las etapas y justificando su funcionalidad. Asimismo se demuestra la necesidad de aumentar el CMRR para las aplicaciones de electroencefalografía y electrocardiografía, proporcionándose aquí varias técnicas para su mejora y haciendo especial hincapié en la técnica del dispositivo RLD. Se han simulado varias configuraciones de dispositivos RLD con un programa de simulación y se han implementado físicamente dos de estas configuraciones. Además, se ha evaluado cuál de ellas es más eficiente mediante la realización de dos experimentos. La búsqueda de dispositivos RLD eficientes permitirá registrar electroencefalogramas con menor cantidad de ruido derivado de interferencias eléctricas y de origen electromagnético.

Agradecimientos

Esta investigación ha sido financiada por el proyecto “Diseño, implementación y evaluación de un sistema avanzado de registro de potenciales evocados auditivos del tronco (PEAT) basado en señalización codificada” (TEC2009-14245), Plan Nacional de I+D 2008-2011,

Ministerio de Economía y Competitividad (Gobierno de España); por la "Granada Excellence Network of Innovation Laboratories – Startup Projects for Young Researchers Programme (GENIL-PYR 2014), Campus de Excelencia Internacional, Ministerio de Economía y Competitividad (Gobierno de España); y por la beca de "Formación de Profesorado Universitario" (FPU, AP2009-3150), Ministerio de Educación, Cultura y Deporte (Gobierno de España).

REFERENCIAS

[1] Bahmer, A., Peter, O., Baumann, U., (2008) "Recording of electrically evoked auditory brainstem responses (E-ABR) with an integrated stimulus generator in Matlab", Journal of Neuroscience Methods, vol. 173, pp. 306-314.

[2] Burkard, R., Shi, Y., Hecox, K.E., (1990) "A comparison of maximum length and legendre sequences for the derivation of brain-stem auditory-evoked responses at rapid rates of stimulation", Journal of Acoustical Society of America, vol. 87, pp. 1656-1664.

[3] Delgado, R.E., Özdamar, O., (2004) "Deconvolution of evoked responses obtained at high stimulus rates", Journal of the Acoustical Society of America, vol. 115, pp. 1242-1251.

[4] Eggermont, J.J., (2007) Electric and magnetic fields of synchronous neural activity. En: Auditory Evoked Potentials. Basic principles and clinical application. Lippincott Williams & Wilkins, pp. 2-21.

[5] Elberling, C., Don, M., (2007) Detecting and assessing synchronous neural activity in the temporal domain (SNR, Response detection). En: Auditory Evoked Potentials. Basic principles and clinical application. Lippincott Williams & Wilkins, pp. 102-123.

[6] Eysholdt, U., Schreiner, C., (1982) "Maximum length sequences: A fast method for measuring brain-stem-evoked responses", Audiology, vol. 21, pp. 242-250.

[7] Hall, J.W., (2007) New handbook of Auditory Evoked Responses, Allyn and Bacon, Boston MA.

[8] ISO 389-x. Acoustics – Reference zero for the calibration of audiometric equipment – Part 1-9. International Organization for Standard.

[9] Jewett, D.L., Williston, J.S., (1971) "Auditory-evoked far fields averaged from the scalp of humans", Brain, vol. 94, pp. 681-696.

[10] Jewett, D.L., Caplovitz, G., Baird, B., Trumpis, M., Olson, M.P., Larson-Prior, L.J., (2004) "The use of QSD (q-sequence deconvolution) to recover superposed transient evoked-responses", Clinical Neurophysiology, vol. 115, pp. 2754-2775.

[11] Özdamar, O., Bohórquez, J, (2006) "Signal-to-noise ratio and frequency analysis of continuous loop averaging deconvolution (CLAD) of overlapping evoked potentials", Journal of the Acoustical Society of America, vol. 119, pp. 429-438.

[12] Özdamar, O., Bohórquez, J, Ray, S.S., (2007) "Pb(P1) resonance at 40 Hz: Effects of high stimulus rate on auditory middle latency responses (MLRs) explored using deconvolution", Clinical Neurophysiology, vol. 118, pp. 1261-1273.

[13] Reid, A., Thornton, A.R.D., (1983) "The effects of contralateral masking upon brainstem electric responses", British Journal of Audiology, vol. 17, pp. 155-162.

[14] Thornton, A.R.D., Slaven, A. (1993) "Auditory brainstem responses recorded at fast stimulation rates using maximum length sequences", British Journal of Audiology, vol. 27, pp. 205-210.

[15] Thornton, A.R.D., (2007) Instrumentation and Recording Parameters. En: Auditory Evoked Potentials. Basic principles and clinical application. Lippincott Williams & Wilkins, pp. 73-101.

[16] Valderrama, J. T., Álvarez, I., de la Torre, A., Segura, J.C., Sainz, M, Vargas, J.L., (2011) "Educational approach of a BAER recording system based on experiential learning", Technics Technologies Education Management, vol. 6, pp. 398-407.

[17] Valderrama, J. T., Álvarez, I., de la Torre, A., Segura, J.C., Sainz, M, Vargas, J.L., (2012) "Recording of auditory brainstem responses at high stimulation rates using randomized stimulation and averaging", Journal of the Acoustical Society of America, vol. 132, pp. 3856-3865.

[18] Valderrama, J. T., de la Torre, A., Álvarez, I., Segura, J.C., Thornton, A.R.D., Sainz, M, Vargas, J.L., (2014) "A study of adaptation mechanisms based on ABR recorded at high stimulation rate", Clinical Neurophysiology, vol. 125, pp. 805-813.

[19] Valderrama, J. T., de la Torre, A., Álvarez, I., Segura, J.C., Thornton, A.R.D., Sainz, M, Vargas, J.L., (2014) "Automatic quality assessment and peak identification of auditory brainstem responses with fitted parametric peaks", Computer Methods and Programs in Biomedicine, vol. 114, pp. 262-275.

[20] Wong, P.K.H., Bickford, R.G., (1980) "Brain stem auditory evoked potentials: the use of noise estimate", Electroencephalography and Clinical Neurophysiology, vol. 50, pp. 25-34. [1] Bahmer, A., Peter, O., Baumann, U., (2008) "Recording of electrically evoked auditory brainstem responses (E-ABR) with an integrated stimulus generator in Matlab", Journal of Neuroscience Methods, vol. 173, pp. 306-314.

[21] Safe current limits for electromedical apparatus. ANSI/AAMI ES1-1993.

[22] Winter, B.B. and Webster, J.G. (1983). Driven-right-leg circuit design. IEEE Transactions on Biomedical Engineering, Vol 30, No 1. Pp. 62 - 66.

[23] Texas Instruments, Precision Operational Amplifiers, 2002.

Miguel Franco obtuvo la licenciatura en Ingeniería de Telecomunicación por la Universidad de Granada, en 2014. Actualmente trabaja como consultor en una empresa del sector privado

Joaquín T. Valderrama obtuvo la licenciatura en Ingeniería de Telecomunicación y la licenciatura en Administración y Dirección de Empresas por la Universidad Europea de Madrid, en 2008. Actualmente, realiza sus estudios de doctorado en el Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada.

Isaac M. Álvarez obtuvo la licenciatura en Ingeniería de Telecomunicación por la Universidad de Málaga, en 2004, y el grado de doctor por la Universidad de Granada, en 2007. Actualmente es Profesor Contratado Doctor en el Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada.

Filtrado de señales de electrocardiograma

Autor: Roberto Maldonado Cuevas, e-mail: *rmaldonado@correo.ugr.es*
Tutor: Juan Manuel Górriz Sáez, e-mail: *gorriz@ugr.es*
Tutor: Javier Ramírez Pérez de Inestrosa, e-mail: *javierrp@ugr.es*
Titulación: Grado en Ingeniería de Tecnologías de la Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—En este documento se aborda, de manera resumida, el filtrado de señales obtenidas a partir de la actividad eléctrica del corazón. El texto está orientado a proporcionar una visión general de cómo afectan y cómo pueden reducirse los diferentes artefactos que contaminan una señal de electrocardiograma. Las técnicas de filtrado que se describen van desde un simple filtrado FIR a técnicas novedosas que implican la aplicación de la transformada de Wavelet o la descomposición empírica en modos. Para la aplicación de cada uno de los métodos, que se expondrán en secciones posteriores, se usarán tanto señales de electrocardiograma generadas mediante software así como señales reales obtenidas a partir de la página web de Physionet. Para cada método se calculará la relación señal ruido como coeficiente cualitativo del filtrado.**

***Palabras clave*—corazón, descomposición empírica en modos, electrocardiograma, filtrado, Physionet, ruido baseline wander, ruido muscular, ruido procedente de la línea eléctrica, transformada de Wavelet.**

I. Introducción

El electrocardiograma (ECG) es una de las técnicas más usadas para el diagnóstico de enfermedades cardíacas. Se basa en la colocación de unos electrodos en unos puntos estratégicos de la piel del paciente con la finalidad de registrar la actividad eléctrica del corazón. Generalmente, la obtención de estas señales bioeléctricas se realiza en presencia de ruido, por lo que se necesita recurrir a algoritmos del tratamiento digital de señales para conseguir las señales lo más libres posibles de ruido para su posterior análisis clínico. Los posibles ruidos o artefactos que se tratarán de reducir son: el ruido procedente de la línea eléctrica, el ruido de baseline wander y el ruido muscular.

Los movimientos mecánicos que ejecuta el corazón para realizar su función de bombeo tienen su origen en un impulso eléctrico que despolariza o repolariza las células del corazón, provocando una contracción o relajación en la pared muscular del mismo. Este impulso eléctrico es el causante de la morfología que posee el ECG. Así, dependiendo de que zona del corazón esta activando o relajando el ECG puede ser dividido en diferentes ondas o segmentos [1]:

- Onda P: indica el comienzo de un nuevo pulso, es de morfología suave y refleja la despolarización auricular.
- Onda QRS: habitualmente denominado complejo QRS, es la onda de mayor amplitud del pulso y en ella se ve reflejada la despolarización ventricular.
- Onda T: indica la repolarización ventricular y posee una morfología suave.

En la ilustración (1) se muestra un electrocardiograma en el que se pueden diferenciar los diferentes segmentos.

II. Artefactos y técnicas

Los artefactos que se intentarán reducir son: el ruido procedente de la línea eléctrica (PLE), el ruido de baseline wander (BW) y el ruido muscular (EMG). En este apartado se indicarán las principales causas y características de cada uno de estos artefactos y qué técnicas han sido empleadas para la reducción de los mismos.

A. Ruido procedente de la línea eléctrica

Es uno de los artefactos más habituales que se pueden añadir a la señal de ECG. Es un ruido caracterizado por ser una interferencia sinusoidal de frecuencia 50 Hz, o 60 Hz, acompañada incluso de armónicos. El acoplamiento del ruido procedente de la línea eléctrica (PLE) en el electrocardiograma (ECG) provoca que el análisis e interpretación del mismo sea más difícil.

En el registro de un electrocardiograma las posibles causas por las que la PLE puede interferir son: inducción magnética, corrientes de desplazamiento inducidas tanto en las derivaciones como en el propio cuerpo, imperfecciones en los equipos de registro e interconexión con otros equipos [2].

Para la reducción de este artefacto se proponen las técnicas de: filtrado ranura, filtrado no lineal adaptativo, filtrado de Wiener y filtrados adaptativos (NMLS y RLS).

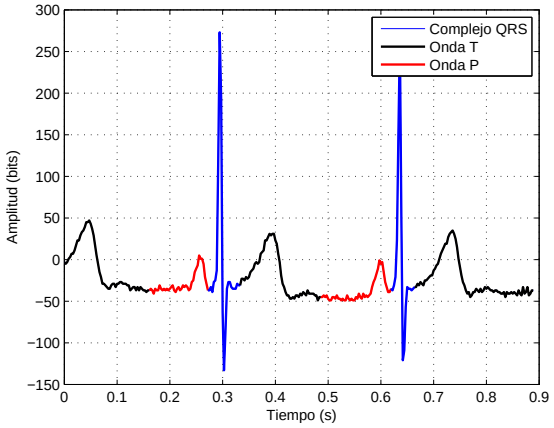


Fig. 1. Señal de electrocardiograma real, ECG 16272 de la base de datos de ritmo sinusal de Physionet, en la que se indican mediante colores los diferentes segmentos que componen el electrocardiograma: onda R (rojo), complejo QRS (azul) y onda T (negro).

B. Ruido de baseline wander

El ruido de baseline wander (BW) o, línea de base en español, es una interferencia de baja frecuencia que produce una deformación en la señal de ECG que puede provocar imprecisiones en la interpretación clínica. Generalmente está contenida en frecuencias por debajo de 0.5-1 Hz, aunque puede contener frecuencias más altas en algunos casos, y su origen es debido a diversos factores como: el movimiento y respiración del paciente o el mal contacto de los electrodos. Este ruido se ve plasmado en un ECG cuando éste no se sitúa sobre una linea de base continúa, sino que existen pequeñas fluctuaciones. La eliminación de este artefacto es uno de los primeros pasos en el proceso de análisis del ECG. En la figura (2) se muestra un electrocardiograma que posee ruido de BW.

Para la reducción o eliminación de este artefacto se han aplicado las técnicas de: filtrado FIR simple y con alteración de frecuencia de muestreo, filtrado IIR hacia delante y hacia atrás, ajuste polinómico, filtrado adaptativo, filtrado media-mediana junto a transformada de Wavelet, descomposición empírica en modos.

C. Ruido muscular

El último de los artefactos que se tratan es el ruido muscular (EMG). Es el artefacto más perjudicial de los tres que se abordan y debe su origen a la actividad eléctrica que se genera por la contracción muscular. Por lo tanto, es un artefacto presente sobre todo en técnicas de registro de ECG que impliquen la actividad del paciente como el test de estrés o el electrocardiograma ambulatorio. Con respecto a la características de este artefacto, es un ruido aleatorio; ya que depende del grado de contracción muscular, y también es un ruido intermitente en el sentido en el que se añade al ECG sólo en los intervalos de tiempo en los que se produce la contracción muscular.

El principal inconveniente que presenta este ruido es que su densidad de potencia espectral se extiende a lo largo de todo el complejo PQRST de la señal de electrocardiograma por lo que procedimientos para la reducción de este artefacto relacionados con el filtrado simple de la señal son ineficientes. Por consiguiente, para la reducción o eliminación de este ruido se recurren a dos técnicas basadas en la transformada de Wavelet y la descomposición empírica en modos.

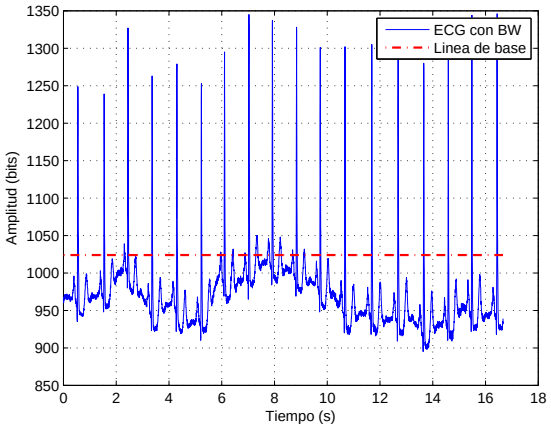


Fig. 2. Señal de electrocardiograma real, ECG 101 de la base de datos de arritmia de Physionet, con presencia de ruido de baseline wander (azul) y línea de base (rojo).

III. Transformada de Wavelet

La transformada de Wavelet (WT: *Wavelet Transform*) es una técnica en la que, al igual que ocurre con otras transformadas, la señal inicial es descompuesta en funciones básicas. En este caso, esta transformada descompone la señal en unas funciones denominadas Wavelets. La WT surge como alternativa a la transformada de Fourier, en la que la señal se descompone en sinusoides, ya que presenta el inconveniente de que no mantiene la información tiempo-frecuencia cuando se aplica. Sobre todo, la WT es una técnica idónea para el estudio de señales no estacionarias y transitorias [3].

Existen multitud de tipos de Wavelet en las que se puede descomponer la señal: Symlets, Daubechies, Haar, Biortogonal... Todas ellas tienen que común que son señales de duración limitada, media nula y cuya energía está concentrada en un intervalo pequeño de tiempo. En la ilustración (3) se muestra un tipo de Wavelet.

De esta transformada existen tanto versión continua como discreta, aunque en este texto sólo se centra en la WT discreta. La transformada de Wavelet discreta (DWT) puede ser implementada mediante un banco de filtros compuesto por un filtro paso alta y un filtro paso alta complementarios [4]. De este modo, si la señal es filtrada paso baja se obtiene lo que se denomina coeficientes de aproximación (cA) que proporcionan la mayor parte de la información de la señal; en el caso de ser filtrada paso alta se obtienen los coeficientes de detalle (cD) que dan información menos relevante sobre la señal filtrada. Este proceso de obtención de ambos coeficientes puede aplicarse iterativamente en el que ahora la señal a descomponer son los coeficientes de aproximación obtenidos en la iteración anterior. Con este proceso se consigue descomponer la señal inicial en diferentes niveles obteniendo tras el proceso un vector de coeficientes de aproximación y tantos vectores de detalle como niveles de descomposición de la señal.

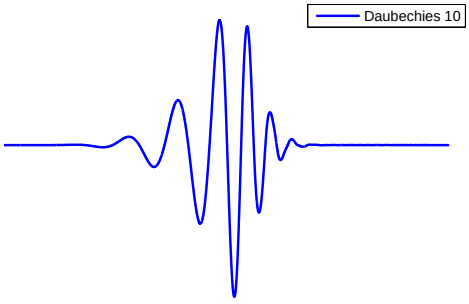


Fig. 3. Ejemplo de señal de Wavelet: Daubechies de orden 10.

IV. Descomposición empírica en modos

La descomposición empírica en modos (EMD: '*Empirical Mode Decompositión*) es una técnica novedosa usada para el análisis de datos no estacionarios [5]. El fundamento de esta técnica es descomponer la señal a tratar en un número finito de funciones denominadas funciones de modo intrínseco (IMF: *Intrinsic Mode Functions*).

Para que una señal sea considerada un IMF debe de cumplir dos condiciones:

- El número de extremos (máximos y mínimos locales) y el número de cruces por cero deben ser iguales.
- El valor medio de la envolvente definida por los máximos locales y la definida por los mínimos locales debe ser 0.

Para descomponer la señal en estos IMFs se realiza un proceso denominado *sifting*. Suponga que se tiene una señal *x(t)* la cual se quiere descomponer mediante EMD. El primero de los pasos para la obtención de un IMF es localizar los máximos y mínimos locales de la señal para, a partir de ellos, calcular la envolvente superior e inferior. Una vez determinadas ambas envolventes, se calcula la media de ambas para seguidamente substraerla a la señal inicial *x(t)*.

El resultado de realizar esta operación generalmente no se considera un IMF ya que no cumple las dos condiciones expuestas anteriormente por lo que el proceso de *sifting* debe ser aplicado en varias ocasiones hasta cumplirlas. Cuando la señal resultante las cumpla, se considera que se ha obtenido el primer IMF. Para obtener más IMFs se realiza el proceso de *sifting* a la señal definida como la substracción de la señal *x(t)* y el primer IMF. La señal resultante de la substracción es conocida como residuo.

Una de las características generales que se observan al descomponer una señal en diferentes IMFs y el residuo final, es que la frecuencia de las componentes decae conforme aumenta el orden de éstas tal y como se muestra en la ilustración (4).

V. Reducción de ruido de baseline wander

De todos los métodos expuesto para la reducción de BW en este apartado sólo se describirán, para no exceder la longitud del artículo, los relativos a la técnicas de WT y EMD :

A. Filtro media-mediana junto a transformada de Wavelet

Esta técnica se basa en la aplicación de un filtro conjunto media - mediana para obtener la contribución de BW a la señal de ECG y, posteriormente, esta estimación es suavizada mediante la WT [6].

Una señal contaminada con ruido de BW es procesada mediante un filtro conjunto media mediana donde la salida de sendos filtros es:

$$y(n) = (1-\alpha)\bar{x}(n) + \alpha\tilde{x}(n) \quad (1)$$

donde α es una variable que toma valores entre 0 y 1 e indica la contribución de cada uno de los filtros.

Una vez se obtiene la señal de salida del filtro, la contribución del BW a la señal de ECG, se realiza un suavizado de la misma con ayuda de la WT ya que esta primera estimación del BW puede introducir distorsión en la señal. Para ello, la salida del filtro es descompuesta en diferentes niveles (*M*) y se comienza un proceso iterativo en el que la señal comienza a ser reconstruida desde el nivel *M*. En cada reconstrucción de la señal, se aplica un test de t-Student en el que se compara la media de la diferencia entre la salida del filtro y la señal reconstruida comprobando si es nula, primera hipótesis, o no nula, segunda hipótesis. En la iteración en la que la se rechaza la primera de las hipótesis del test, el proceso finaliza. El último paso es substraer la estimación del BW a la señal de ECG original.

En la figura (5) se muestra cómo se suaviza la estimación del BW tras aplicar WT.

B. Descomposición empírica en modos para la reducción de baseline wander

Esta técnica se basa en el conocimiento de la distribución en frecuencia del ruido de BW y de los IMFs en los que se descompone la señal al aplicar EMD [7]. De este modo, teniendo constancia de que la frecuencia de este ruido es baja y los últimos IMFs son los de menor frecuencia, se realiza

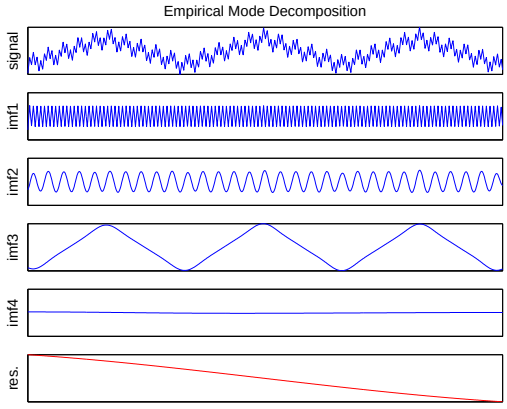


Fig. 4. Descomposición en funciones de modo intrínsecas: la señal ha sido descompuesta en 4 IMFs y un residuo. Se puede comprobar cómo la frecuencia de los IMFs es menor conforme se aumenta el orden de los mismos.

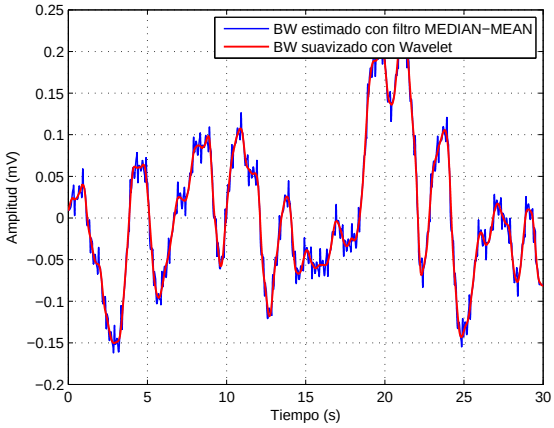


Fig. 5. Contribución del baseline wander a la señal de ECG original. En azul se muestra la estimación realizada a partir del filtro conjunto media-mediana y en rojo el resultado obtenido tras aplicar la transformada de Wavelet a la contribución obtenida con el filtro conjunto.

un filtrado paso baja a cada uno de los IMFs obteniendo de este modo, una estimación del BW. El filtrado que se lleva a cabo se denomina filtrado multi-banda en el que a cada una de las componentes de IMF, incluido el residuo, se le aplica un filtro de diferentes características. A continuación se detalla el fundamento de esta técnica:

Suponga que se tiene una señal de ECG contaminada con BW que ha sido descompuesta en *n* IMFs:

$$x(t) = \sum_{i=1}^{n+1} c_i(t) \tag{2}$$

De todos IMFs obtenidos existe uno, denominado Q, a partir del cual comienza la contribución del BW a la señal de interés. Para determinar dicho IMF, como ya se ha comentado, se realiza un filtrado paso baja a cada IMF y residuo:

$$\begin{aligned} y_1 &= h_1 * C_{n+1}(t) \\ y_2 &= h_2 * C_n(t) \\ &\vdots \end{aligned} \tag{3}$$

Las frecuencias de corte obtenidas son aplicadas de forma que la frecuencia de mayor valor *(i=0)* es aplicada al residuo, la siguiente *(i=1)* es aplicada al último IMF y así sucesivamente. El hecho de que la frecuencia de corte no sea uniforme para todos los IMFs y se reduzca conforme disminuye el orden es debido a que en IMFs de menor orden existe mayor contribución de la señal de interés que del baseline wander.

Una vez se realiza el cálculo de la salida para cada filtro, se calcula la varianza de cada y_i para obtener la componente *Q*. Para ello se recurre a un límite denominado ζ el cual determina si una componente dada es considerada IMF *Q*. Se comparan de forma descendente la varianza de los IMFs comprobando que $var(y_{Q-1}) > \zeta$ y $var(y_Q) \leq \zeta$, si se cumplen ambas desigualdades esa componente es la denominada componente *Q*.

Ya conseguida la componente *Q*, simplemente tenemos que realizar la estimación del BW:

$$\hat{BW}(t) = \sum_{i=1}^{Q} y_i(t) \tag{4}$$

Por último la estimación es substraída a la señal de ECG original:

$$\hat{x}(t) = x(t) - \hat{BW}(t) \tag{5}$$

VI. Reducción de ruido muscular

Para la reducción o eliminación de este artefacto se recurren a dos técnicas basadas en transformada de Wavelet y descomposición empírica en modos.

A. Descomposición empírica en modos para la reducción de ruido muscular

Este método se basa en la descomposición de la señal de electrocardiograma en diferentes IMFs y en modificar aquellos que contribuyen al ruido muscular para, posteriormente, realizar una reconstrucción de la señal de ECG [7]. La modificación que se lleva a cabo en cada uno de dichos IMFs consiste en un enventanado de los mismos sobre el complejo QRS consiguiendo, eliminar el ruido y mantener intacto el complejo QRS de la señal de ECG.

Una vez la señal ha sido descompuesta en los diferentes IMFs, el primer paso que se realiza es identificar qué IMFs contribuyen al ruido muscular de la señal. Para ello, se acepta la premisa de que el ruido que contamina a la señal de ECG es de media nula mientras que la señal de interés no. Además se conoce que el ruido muscular generalmente es un ruido que se extiende por los IMFs de mayor frecuencia, es decir, los primeros IMFs. En consecuencia, se aplica un test estadístico denominado test de t-Student en el que se comprueba si la media de la suma parcial de los IMFs es nula. Se expresa la suma parcial de orden *M* como:

$$C_{sp}^{M} = \sum_{i=1}^{N} c_i(t) \tag{6}$$

El orden de suma parcial comienza en 1 y aumenta hasta conseguir que se rechace la primera hipótesis del test de t-Student, es decir, que la media de la suma parcial ya no sea nula. En el caso en que, la señal de ECG sea de media nula y la aplicación del test dé como resultado un número de IMFs considerados ruidosos mayor de 5, dicho valor será restringido a 5.

El siguiente paso es delimitar los complejos QRS que conforman cada pulso de la señal de electrocardiograma. Para ello, la primera tarea es determinar los puntos fiduciales de la señal de ECG situados en el punto máximo del segmento R de cada pulso. Seguidamente se calcula la suma de los tres primeros IMFs dando como resultado la señal *d(t)*. A partir de esta señal y con ayuda de las posiciones de los puntos fiduciales, se obtiene a izquierda y derecha de cada uno de ellos el mínimo local y el cruce por cero. La pareja de cruces por cero obtenida para cada punto fiducial delimitan la longitud del complejo QRS.

Una vez se tienen definidos todos los complejos QRS se puede crear una ventana que posea una región plana durante ese intervalo de tiempo y que vaya atenuando hasta llegar al valor 0. En este caso, se utilizará una ventana de Blackman-Tukey en la que su región plana queda definida por los cruces por cero (τ_1) y su zona de transición ($|\tau_1 - \tau_2|$) es no abrupta para reducir distorsiones. Esta región de transición varía en función del orden del IMF al que se le va a aplicar, de este modo, para órdenes altos la curva decaerá de forma más suave que para el caso de los primeros IMFs tal y como se indica en la ilustración (**??**).

También se crea una ventana complementaria a la ventana de Blackman-Tukey que tiene la finalidad contraria a la ventana inicial: atenuar el complejo QRS y añadir una pequeña porción de ruido evitando así cambios abruptos en el complejo QRS.

Una vez quedan definidas las ventanas y sobre qué IMFs deben ser aplicadas, la señal de ECG reconstruida sigue la expresión:

$$\hat{x} = \sum_{i=1}^{P} w(t)c_i(t) + \sum_{i=1}^{P} \alpha_i w_{comp}(t)c_i(t) + \sum_{i=P+1}^{N} c_i(t) + r_N(t) \tag{7}$$

donde *P* es el orden de IMFs considerados ruidosos y α_i es un coeficiente de atenuación que varia entre 0 y 1.

B. Transformada de Wavelet con thresholding

Esta técnica se basa en la aplicación de un thresholding a los coeficientes de detalle de la señal obtenidos tras la aplicación de la WT [8]. El método esta basado en un algoritmo presentado por Johnstone y Donoho donde muestran como reducir el ruido de una señal eliminando algunos coeficientes de detalle de la señal original [9].

El primer paso para realizar la WT a la señal de ECG para obtener los diferentes coeficientes de aproximación y detalle. Una vez es descompuesta la señal, se aplica un umbral a los coeficientes de detalle.

El umbral que se aplica es denominado *'soft thresholding'*[10]. El *'soft thresholding'* sigue la siguiente ecuación:

$$cD_{st} = \begin{cases} sgn(cD)(|cD| - T) & si \quad cD \geq T \\ 0 & si \quad cD < T \end{cases} \tag{8}$$

donde *cD* son los coeficientes de detalle y *T* es el valor del umbral.

Para el cálculo del umbral, cuyo valor es adaptativo y supone una mejora de la ecuación inicial propuesta por Donoho [10], se calcula mediante la siguiente ecuación:

$$T_i = \frac{1}{\mu_i}\sigma_i\sqrt{2log(N_i)} \tag{9}$$

El parámetro μ_i es calculado como:

$$\mu_i = max(|cD_i|) \tag{10}$$

Y σ es la varianza del ruido y se obtiene de la siguiente forma:

$$\sigma_i = \frac{mediana(|cD_i|)}{0.6745} \tag{11}$$

Y N_i es la longitud de los coeficientes de detalle en el nivel *i*.

Una vez es aplicado el *'soft thresholding'* a los coeficientes de detalle, la señal es reconstruida a partir de los coeficientes de aproximación y los nuevos coeficientes de detalle.

VII. Resultados

En este apartado se van a presentar los resultados obtenidos para las técnicas que se han explicado en este artículo. Para la aplicación de todos los métodos se han usado tanto señales de ECG generadas mediante el software *Matlab* como señales reales de la base de datos de *Physionet* [11]. Al igual que la señales de ECG, los artefactos que presentan pueden ser obtenidos de la base de datos real o generados mediante *Matlab*.

A. Filtro media-mediana junto a transformada de Wavelet

Para la aplicación de este método se va a usar una señal de ECG sintética y un ruido de BW también sintético. El valor de α que indica la contribución de cada filtro ha tomado un valor de 0.5 y la ventana necesaria para el calculo de la media y mediana de la señal tiene una longitud de un tercio de la frecuencia de muestreo, en este caso, toma un valor de 166 muestras. Para la aplicación de la WT se ha usado como Wavelet la señal Daubechies de orden 6 y la estimación del BW ha sido reconstruida con 9 niveles. Con respecto a la SNR obtenida, se ha conseguido una mejora de 5.9 dB con respecto a la SNR inicial. En la ilustración (6) se muestra cómo ha mejorado el ECG tras la ampliación del método.

B. Descomposición empírica en modos para la reducción de baseline wander

En este caso, para ejecutar esta técnica se va a utilizar una señal de ECG real obtenida de la base de datos de arritmia, concretamente la señal 103. A ella se le ha añadido mediante simulación el artefacto de baseline wander. Se ha descompuesto la señal en 12 IMFs y se ha aplicado como frecuencia de corte inicial (ω_0) un valor de 0.8. El factor *M* toma el valor 80 y el IMF a partir del cual comienza la contribución del BW ha resultado ser el IMF número 8. Con respecto a la SNR la mejora ha sido de 6.38 dB. En la figura (7) se indica el resultado obtenido.

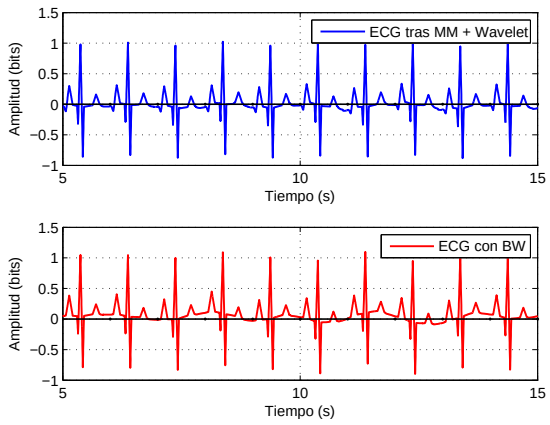


Fig. 6. Comparativa entre la señal obtenida tras la aplicación del método filtro media-mediana con WT y señal original con BW. Tanto señal de ECG como artefacto son sintéticos. Se puede comprobar cómo se ha reducido el BW de la señal inicial.

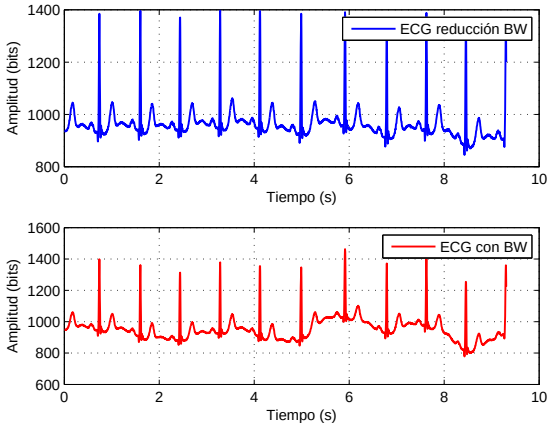


Fig. 7. Comparativa entre la señal obtenida tras la aplicación del método EMD para reducción de BW y señal original con BW. En este caso la señal es la señal 103 de la base de datos de arritmia y el artefacto es simulado. Se puede comprobar cómo se ha reducido el BW de la señal inicial.

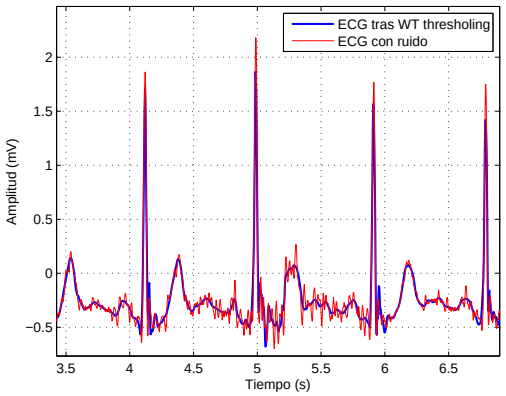


Fig. 8. Comparativa entre la señal obtenida tras la aplicación del método WT para reducción de EMG y señal original con EMG. En este caso la señal es la señal 103 de la base de datos de arritmia y el artefacto obtenido de la base de datos de test de estrés (rojo). El resultado (azul) ha sido centrado sobre una zona del ECG en la que el EMG era presente.

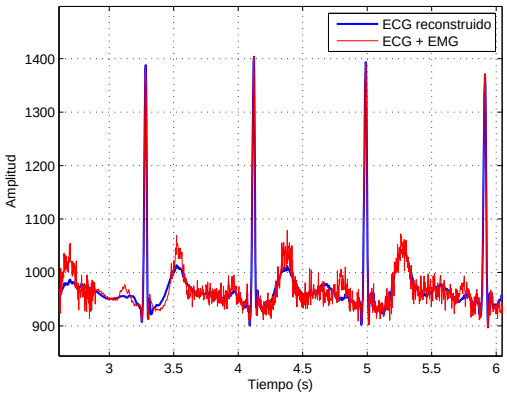


Fig. 9. Comparativa entre la señal obtenida tras la aplicación del método EMD para reducción de EMG y señal original con EMG. En este caso la señal es la señal 103 de la base de datos de arritmia (rojo) y el artefacto es generado mediante *Matlab*. El resultado (azul) ha sido centrado sobre una zona del ECG en la que el EMG era presente.

C. Transformada de Wavelet con thresholding

Esta técnica ha sido aplicada sobre una señal de ECG real y se le ha añadido ruido muscular real obtenido de la base de datos de test de estrés. Para la realización de la WT se ha usado como Wavelet la señal Daubechies de orden 4 y ha sido aplicada en 3 iteraciones. En la ilustración (8) se muestra cómo se ha reducido el ruido muscular de la señal de ECG.

D. Descomposición empírica en modos para reducción de ruido muscular

Para la aplicación del último de los métodos aquí descritos se utiliza una señal real y un ruido muscular simulado mediante *Matlab*. La señal ha sido descompuesta en 12 IMFs y las ventanas de Blackman-Tukey han sido aplicadas a los 5 primeros IMFs. El resultado de la aplicación de este método se observa en la ilustración (9).

VIII. Conclusiones y vías futuras

Con respecto a los métodos aplicados para la reducción de cada artefacto, si bien todos no han podido ser descritos en este artículo, se ha podido comprobar que cumplen con el objetivo de reducir o eliminarlos por completo. Para el caso de la eliminación del PLE, al ser un artefacto de características muy definidas, técnicas de filtrado simple son suficientes. En referencia al ruido de BW considero que la aplicación de métodos que estimen la contribución del BW a la señal y su posterior substracción, es más aconsejable que los métodos de filtrado ya que pueden eliminar componentes de frecuencia de interés de la señal de ECG. Por último para la reducción de EMG, teniendo en cuenta la dificultad que presenta este artefacto, cualquiera de las técnicas aplicadas cumple con el objetivo. Personalmente, ha sido un trabajo muy gratificante en el que se han aplicado conceptos obtenidos a lo largo del grado a aplicaciones médicas donde gran parte de la población puede verse beneficiada.

Como vías futuras se puede destacar la aplicación de nuevos métodos, el cálculo de nuevos factores que indiquen la calidad del filtrado, o incluso, la aplicación de estos métodos en tiempo real.

Agradecimientos

Agradezco a toda la gente que me ha ayudado durante estos años en la universidad en especial a mi familia y tutores de proyecto.

Referencias

[1] P. Laguna and L. Sornmo, *Bioelectrical Signal Processing in Cardiac and Neurological Applications*, 2005.
[2] J. C. H. . J. G. Wester, "60-Hz Interference in Electrocardiography."
[3] A. Primer, *Introduction to Wavelet and Wavelet Transforms*. Prentice-Hall, 1998.
[4] M. Misiti, Y. Misiti, G. Oppenheim, and J.-M. Poggi, *Wavelet Toolbox for use with Matlab*. MathWorks.
[5] N. E. Huang *et al.*, *The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis*. The Royal Society, 1996.
[6] W. Hao, Y. Chen, and Y. Xin, "Ecg baseline wander correction by mean-median filter and discrete wavelet transform," *IEEE EMBS*, 2011.
[7] M. B. Velasco, B. Weng, and K. E. Barner, "ECG signal denoising and baseline wander correction based on the empirical mode decomposition," 2008.
[8] G. Georgieva-Tsaneva and K. Tcheshmedjiev, "Denoising of electrocardiogram data with methods of wavelet transform," *Internacional Conference on Computer Systems and Technologies*, 2013.
[9] D. L. Donoho and J. M. Johnstone, *Ideal spatial adaptation by wavelet shrinkage*. Oxford Journals, 1992.
[10] D. L. Donoho, "De-noising by soft-thresholind," *IEEE Transactions on Information Theory*.
[11] PhisioNet, "Base de datos de electrocardiogramas." [Online]. Available: http://physionet.org/cgi-bin/atm/ATM

Roberto Maldonado Cuevas 5 de Abril de 1992, Granada. Graduado en Ingeniería de Tecnologías de la Telecomunicación por la Universidad de Granada.

Método automático de seguimiento de respuestas evocadas auditivas basado en la parametrización de series de registros

Autor: José M. Morales; email: yo@jmme.com
Tutores: Joaquín T. Valderrama; e-mail: jvalderrama@ugr.es Isaac Álvarez; email: isamaru@ugr.es

Titulación: Ingeniería de Telecomunicación

Departamento de Teoría de la Señal, Telemática y Comunicaciones

Universidad de Granada

***Resumen*—Los potenciales evocados auditivos del tronco cerebral son una herramienta de evaluación objetiva de la audición ampliamente utilizada en hospitales y clínicas a nivel internacional. El uso de métodos automáticos favorece la evaluación y detección de parámetros característicos que puede ayudar a un diagnóstico muy preciso. Este artículo presenta un método de seguimiento de respuestas evocadas auditivas mediante parametrización de series de registros (*SSP*). El método está basado en el proceso que sigue un experto en la evaluación subjetiva de un registro. Este método es validado con la realización de dos experimentos. En el primero, se observan los resultados para series de registros sintetizadas artificialmente. El segundo evalúa transformaciones en la morfología de series de registros reales. Estas series de registros se adquirieron en una fase previa experimental. Los resultados de este trabajo indican que el método parametriza de forma precisa los parámetros de latencia, compresión y amplitud. Por tanto, podría utilizarse para evaluar la calidad y detectar de forma automática la presencia de respuesta biológica.**

***Palabras clave*—Tronco cerebral, PEAT, método automático, evaluación, detección**

I. Introducción

Los potenciales evocados auditivos del tronco cerebral (PEAT) son la respuesta neuroeléctrica que produce el nervio auditivo frente a un estímulo sonoro [1]. La naturaleza no invasiva del proceso de registro de estas señales ha favorecido su uso. Su utilización se extiende por (a) el ámbito clínico, donde se usa como herramienta para la detección de déficits auditivos y (b) la investigación, en donde se utilizan para analizar mecanismos involucrados en el proceso auditivo. Los PEAT aparecen durante los 10 ms posteriores a una estimulación acústica [2]. Se pueden observar una serie de ondas que son denominadas por letras romanas [3]. Aunque se pueden identificar hasta 7 ondas, los picos III y V son los más robustos.

La calidad del registro depende de la probabilidad de la existencia de una respuesta de origen biológico: Un registro de mayor calidad permitirá obtener resultados más concluyentes. Esta evaluación se puede realizar de manera subjetiva (por parte de un experto) u objetiva (por procedimientos automáticos). Los métodos automáticos proporcionan la evaluación uniforme, sin estar sujetos a la variabilidad asociada a las evaluaciones subjetivas [4], las cuales se ponen de manifiesto en este estudio. Los métodos de evaluación automática de la calidad (a) permiten mejorar el proceso de registro al detener la adquisición cuando la calidad sea suficiente; y (b) se unifica el protocolo de obtención y evaluación. Existen varios métodos de evaluación automática de la calidad. Entre ellos podemos destacar el basado en el coeficiente de correlación (r) y la estimación de la SNR utilizando un único punto (F_{SP}). El método del coeficiente de correlación se basa en la reproducibilidad de dos registros PEAT consecutivos obtenidos de forma similar para determinar la presencia/ausencia de respuesta biológica [5]. El método F_{SP} estima la calidad del registro teniendo en cuenta la energía de la señal y la variabilidad de un único punto [6].

Este proyecto presenta un nuevo método de seguimiento de respuestas evocadas auditivas mediante Parametrización de Series de Registros (*Set of Signal Parametrization*, *SSP*). Este método está basado en el proceso que sigue un experto para la evaluación de un registro. Analiza las transformaciones en la morfología de los PEAT registrados en diferentes condiciones de registro. El método *SSP* podría tener aplicaciones en la evaluación de la calidad de los registros y en la detección de la existencia de respuesta de origen biológico. Resultados preliminares de este trabajo se presentaron en el congreso International *Evoked Response Audiometry Study Group* (IERASG), Nueva Orleans (Junio 2013). También se presentó en el 6º Simposio CEA de Bioingeniería 2014 – Asociación Nicolo, Granada (Junio 2014).

II. Descripción del método

A pesar de la contrastada utilidad de los métodos objetivos, a día de hoy, deben utilizarse como herramienta de unificación de la evaluación de un profesional a otro.

Ejemplos de estos métodos subjetivos pueden ser la replicación de respuesta, la evaluación por parte de un grupo de profesionales y el seguimiento de respuesta. Éste último se basa en observar los cambios que se producen en la respuesta al modificar el estímulo (intensidad o tasa de estimulación). Para una variación de la intensidad se produce un desplazamiento en latencia y amplitud común a todas las ondas características. Por otro lado, para una variación de la tasa de estimulación este cambio se produce de manera más abrupta para las componentes más centrales. El comportamiento esperado para una variación en la intensidad de estimulación esta comúnmente aceptado [1]. Sin embargo,

los cambios en la morfología frente a una variación en la tasa de estimulación presentan cierta controversia. Recientes estudios [7-8] y este mismo estudio, presentan resultados que soportan este comportamiento.

La labor del experto consiste en la determinación de la presencia o ausencia de respuesta neuronal al estímulo acústico. Para ello, una estrategia común consiste en la realización de un seguimiento de las respuestas auditivas frente a la variación de algún parámetro de estimulación.

Se presenta a continuación el método automático SSP, cuyo funcionamiento se aproxima a la forma en la que un experto realiza la evaluación subjetiva.

A. Método de parametrización de series de registros (SSP)

Se parte de la obtención de una serie de registros. Esa serie de PEAT habrá sido adquirida variando alguno de los parámetros de estimulación (intensidad y tasa). De la misma forma que lo haría un experto al realizar un seguimiento de respuesta, el primer paso es establecer cuál será el registro de referencia ($\mathbf{x_{ref}}$). $\mathbf{x_{ref}}$ será aquel en el que la identificación de las ondas características sea inmediata. En el caso de variación de la intensidad de estimulación, por ejemplo, será aquel que fue registrado al estimular con la intensidad más alta. El resto de registros de la serie son considerados registros de test ($\mathbf{x_{test}}$).

Según el tipo de estimulación, como se ha mencionado anteriormente, se espera un comportamiento. Al disminuir la intensidad de estimulación cada uno de los $\mathbf{x_{test}}$ será una versión desplazada y atenuada de $\mathbf{x_{ref}}$. En el caso de la variación de la tasa, cada $\mathbf{x_{test}}$será una versión expandida y atenuada de $\mathbf{x_{ref}}$. El método realiza una parametrización de la serie de registros de forma secuencial, ajustando de forma óptima cada $\mathbf{x_{test}}$a xref. Es decir, se busca encontrar qué factores de compresión/expansión (σ), desplazamiento temporal (δ) y factor de amplitud (A) consigue que la diferencia entre $\mathbf{x_{test}}$y $\mathbf{x_{ref}}$sea mínima. De esta forma se mide las diferencias entre los registros. Matemáticamente, la función sería de la forma:

$$x_{test}(A,\delta,\quad) = (\mathrm{A}\cdot \mathrm{x}_{ref}(\frac{t-\delta}{\sigma})) \qquad (1)$$

El método debe realizar esta búsqueda tridimensional. Para ahorrar carga de computación, esa búsqueda se reduce a una búsqueda unidimensional. En primer lugar, se realizará un barrido en compresión/expansión, para cada uno de ellos se calcularán los desplazamientos temporales y factor de amplitud y aquel que devuelva el mínimo error entre la señal de test y la de referencia será la parametrización deseada. Ese mínimo se cuantifica con ayuda del cálculo del coeficiente de determinación (R^2). El coeficiente de determinación mide la bondad del ajuste de un modelo sobre unos datos experimentales. En el caso del método SSP: el modelo son las señales de test y se quiere cuantificar cómo de bien se ajusta a los datos experimentales (señal de referencia). La Fig.1 presenta un esquema general del procedimiento.

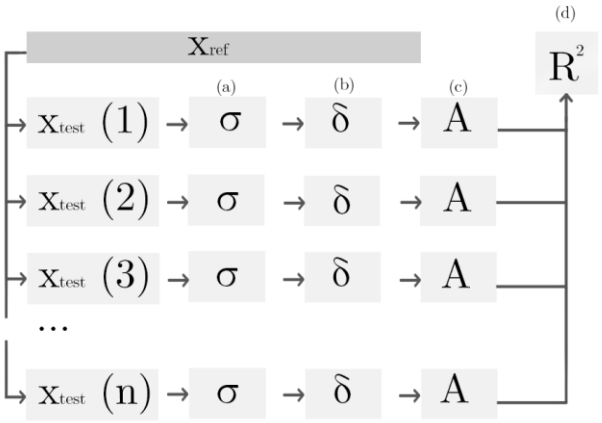


Fig.1. Esquema general del procedimiento del método SSP. (a) Cálculo del factor de compresión/expansión (b) Cálculo del desplazamiento temporal (c) Cálculo del factor de amplitud (d) Cálculo del coeficiente de determinación entre xref y la correspondiente xtest

III. EVALUACIÓN DEL MÉTODO

Para validar el rendimiento del método descrito en este proyecto se realizaron dos experimentos. En el experimento 1, se sintetizaron de forma artificial series de registros que emulasen el comportamiento de los PEAT para diferentes estimulaciones y se observó si el método era sensible a los cambios producidos. En el experimento 2, se realizó la evaluación del método con registros reales. En esta sección se presenta el proceso de adquisición de los registros y los resultados obtenidos en cada uno de los experimentos.

A. Registro EEG y procesado de señal.

El proceso de obtención de EEG consiste en estimular el sistema auditivo de un sujeto y registrar su respuesta eléctrica asociada. Los registros se tomaron en una sala minimizando las condiciones de ruido electromagnético. Se propuso que los sujetos se acomodaran para reducir el ruido miogénico. Se estableció el nivel 0 dBnHL (nivel en el que el estímulo es detectable) considerando el umbral de audición en un grupo de 24 personas (20 varones, 4 mujeres) con edades entre 14-57 años sin problemas auditivos. Se registraron los PEAT (a) variando la intensidad del estímulo y (b) variando la tasa de estimulación utilizando la técnica RSA [7]. La calibración de los niveles de intensidad se realizó usando una "*Artificial EarType 4153*" (Brüel &Kjær Sound & Vibration Measurement A/S, Nærum, Denmark). Los EEG se registraron usando tres electrodos de superficie (positivo, tierra y referencia) colocados en la piel. Se situaron en la frente (cercano al pelo), en la parte baja de la frente y en la mastoide respectivamente. El EEG fue amplificado y después filtrado. La señal se muestreó a 25 KHz y fue cuantificada con 16 bits para su almacenamiento. El procesamiento de datos se realizó utilizando algoritmos implementados en MATLAB. Se puede encontrar una descripción más detallada del sistema de registro en [9]. Todos los sujetos registrados fueron voluntarios y se les informó detenidamente del protocolo. La Fig.2 muestra las series adquiridas variando la intensidad de estimulación.

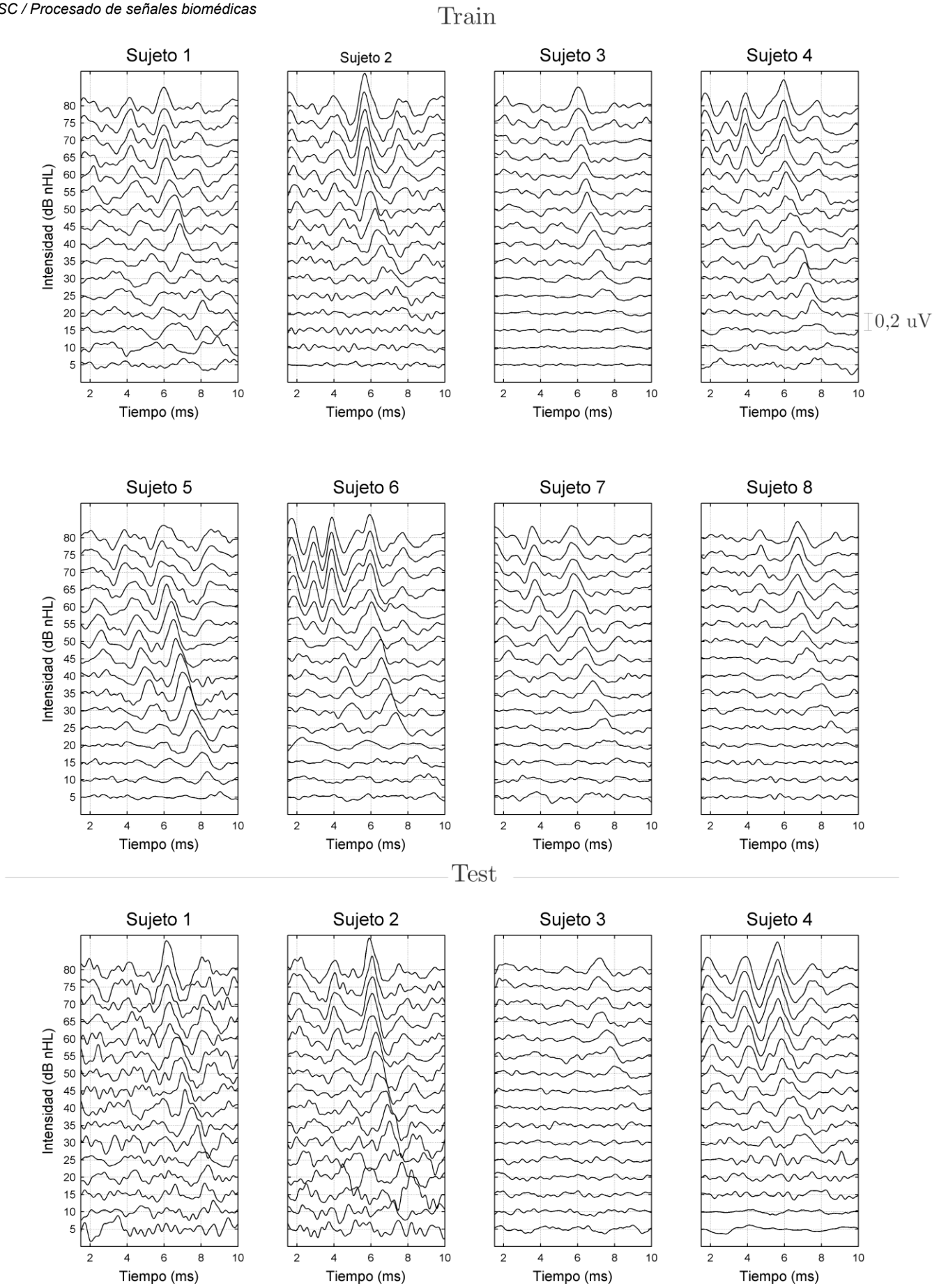


Fig. 2. Series de registros obtenidas variando la intensidad de estimulación.

B. *Experimento 1*

Sujetos y métodos

Este experimento evalúa la eficacia del seguimiento automático de los cambios en las respuestas mediante el método SSP. Se sintetizaron distintas series de registros en las que se modificó un parámetro de forma conocida (latencia, amplitud, compresión) de la señal y se comparó con el resultado parametrizado por el método. Las series de registros se sintetizaron a partir de uno de los registros reales adquiridos. Una vez seleccionado un registro de referencia, se le modificó (a) la latencia-amplitud y (b) la compresión-amplitud. Los valores de sintetizado se eligieron en base a la bibliografía existente [10].

Resultados

Para facilitar el proceso y obtener resultados más concluyentes se fijó el factor de compresión a uno para la evaluación de la serie sintetizada latencia-amplitud y el desplazamiento igual a cero para la sintetizada compresión/expansión-amplitud. Las Tablas I y II muestran que el coeficiente de determinación (R^2) es igual a la unidad, lo cual indica que el modelo se ajustó perfectamente a los datos experimentales. Es decir, que el ajuste de la señal de test con la señal de referencia fue óptimo. La diferencia entre los valores impuestos y los medidos de forma automática es igual a cero.

C. *Experimento 2*

Sujetos y métodos

Para llevar a cabo la experimentación con registros reales se realizó la adquisición para un total de 24 sujetos. Para cubrir los dos tipos de estimulación, de estos 24 sujetos, 12 fueron estimulados realizando una variación en la intensidad de estimulación y 12 realizando una variación en la tasa de estimulación. Los sujetos fueron 9 varones y 3 mujeres con edades comprendidas entre los 15 y los 60 años para el caso de barrido en intensidad; para el caso de variación en tasa de estimulación la muestra fue de 11 varones y 1 mujer con edades entre los 24-60 años. Ninguno de los sujetos sufría alguna anomalía auditiva detectada. Para intensidad, se realizó un barrido desde 0 a 80 dBnHL en pasos de cinco dB con estimulación convencional, tomando el registro de 80 dBnHL como $\mathbf{x_{ref}}$. En segundo lugar, para distintas tasas se variaron desde los 55 a los 250 Hz usando la técnica de *Randomized Stimulation Averaging (RSA)* [7].Esta técnica nos permite registrar los PEAT a altas tasas de estimulación usando estímulo con *jitter* . El *jitter* de una secuencia de estimulación mide la cantidad de dispersión del intervalo interestímulo (distancia temporal entre dos pulsos) en comparación con la presentación periódica. En este estudio se generaron secuencias con 4 ms de jitter. $\mathbf{x_{ref}}$ se determinó como el registro de 55 Hz. Además se registraron dos series de registros sin estimulación. En este caso el sistema de adquisición registraba el EEG del sujeto sin ser estimulado acústicamente. En total, el número de PEAT utilizados ascendió a un total de 304 (12 sujetos a 16 intensidades cada uno, 12 sujetos a 8 tasas diferentes cada sujeto y 2 sujetos con 8 registros sin estimulación cada uno).

TABLA I

Parámetros medidos por el método SSP para una señal sintetizada (latencia-amplitud). Se muestra el coeficiente de determinación, la latencia de la onda V, el factor de compresión σ y amplitud con respecto a la señal de referencia x_{ref} y la diferencia entre los valores impuestos y los medidos por el método.

Intensidad (dBnHL)	**R^2**	**δ (ms)**	**A**	**Δδ**	**ΔA**
75	1	0,28	1,1	0	0
70	1	0,36	1,15	0	0
65	1	0,4	1,25	0	0
60	1	0,48	1,5	0	0
55	1	0,64	2	0	0
50	1	0,76	2,2	0	0
45	1	0,96	2,5	0	0
40	1	1,12	3	0	0
35	1	1,36	3,4	0	0
30	1	1,64	3,8	0	0
25	1	1,96	4,2	0	0
20	1	2,32	4,6	0	0
15	1	2,72	5	0	0
10	1	3,16	7	0	0
5	1	3,48	10	0	0

TABLAII

Parámetros medidos por el método *SSP* para una señal sintetizada (compresión-amplitud). Se muestran el coeficiente de determinación, la latencia de la onda V, el factor de compresión σ y amplitud con respecto a la señal de referencia x_{ref} y la diferencia entre los valores impuestos y los medidos por el método.

Tasa (Hz)	**R^2**	**σ**	**A**	**Δ σ**	**ΔA**
55	0,999	0,980	1,10	0	4,0e-3
71	0,999	0,950	1,15	0	5,6e-3
83	0,999	0,919	1,25	2e-4	5,8e-3
100	0,999	0,899	1,50	2e-4	7,1e-3
125	0,998	0,879	2,01	2e-4	0,1032
167	0,996	0,850	2,21	0	0,0117
250	0,995	0,819	2,51	2e-4	0,0146

De cada grupo de 12 participantes, se utilizaron 8 para entrenamiento del método y 4 para la evaluación. El entrenamiento consistió en medir de forma manual los valores de latencia de la onda V, la amplitud interpico (distancia entre la amplitud de la onda V y su valle) de la misma y la distancia entre las ondas III y V. De esta forma, se elaboró un vector de promedio/desviación típica que permitió tener en cuenta las posibles variaciones de latencia que pudiese haber entre sujetos sin llegar a incluir ondas adyacentes o erróneas. Los resultados de estos vectores son consistentes con la bibliografía [8]. En concreto, como se puede observar en la Fig.3 los resultados obtenidos para el entrenamiento de los registros adquiridos variando la tasa de estimulación apoya el comportamiento esperado. La distancia de las ondas III-V aumenta conforme lo hace la tasa de estimulación [7-8]. Finalmente se procesaron los registros de evaluación con el método SSP.

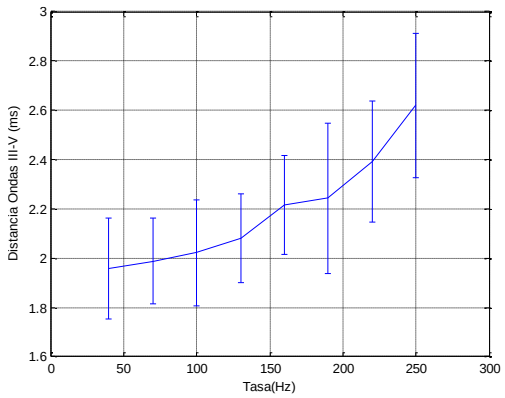


Fig. 3.Distancia de las ondas III-V para una variación de la tasa de estimulación.

Resultados

En este experimento, el método SSP es evaluado procesando series de registros reales. Las Tablas III y IV muestran los resultados.

En registros donde se ha variado la intensidad de estimulación, se espera observar un aumento de la latencia de la onda V y una reducción de la amplitud de la señal. La Tabla III muestra este comportamiento, ya que el factor de desplazamiento (δ) y el de amplitud (A) aumentan conforme disminuye la intensidad de estimulación.

En el caso de registros en los que se ha variado la tasa de estimulación, el comportamiento esperado consiste en un aumento en la distancia de las ondas III-V (expansión de la señal) y una atenuación de las ondas características. La Tabla IV muestra que se cumple este comportamiento y para mayor tasa de estimulación el factor de compresión es menor. Un factor de compresión menor se traduce en que la señal de test debe ser más comprimida para ajustarse con la de referencia.

Además se demuestra la utilidad del coeficiente de determinación. Siempre que no supere un umbral a determinar, los valores parametrizados no tendrán ningún tipo de valor. La calidad del ajuste se ve deteriorada conforme el coeficiente de determinación disminuye. De ahí la importancia de una correcta determinación del umbral. En este proyecto, se determinó un umbral de forma experimental, fijando estevaloren*0,64*.

TABLA III

Parámetros de latencia y amplitud con respecto a x_{ref} medidos por el método *SSP* de forma automática para series de registros reales (Intensidad).

Intensidad (dBnHL)	**R^2**	**δ (ms)**	**A**
75	0,857	0,04	1,04
70	0,821	0,08	1,05
65	0,864	0,04	1,03
60	0,811	0,12	1,19
55	0,759	0,28	1,55
50	0,708	0,32	1,34
45	0,601	0,52	1,89
40	0,762	0,68	1,63
35	0,727	0,96	1,57
30	0,484	1,00	2,01
25	0,264	1,32	3,69
20	0,415	1,84	2,19
15	0,362	2,36	2,05
10	0,040	3,24	8,85
5	0,191	3,36	4,52

TABLA IV

Parámetros de latencia, factor de compresión y amplitud con respecto a x_{ref} medidos por el método *SSP* de forma automática para series de registros reales (Tasa).

Tasa (Hz)	**R^2**	**σ**	**A**
55	0,807	0,980	1,42
71	0,779	0,976	1,50
83	0,558	0,973	0,64
100	0,713	0,939	1,40
125	0,720	0,943	2,05
167	0,453	0,920	1,92
250	0,422	0,872	3,43

IV. DISCUSIÓN Y CONCLUSIONES

Este proyecto presentó un método automático de seguimiento de respuestas evocadas auditivas mediante parametrización de series de registros (*Set of SignalParametrization, SSP*). El método intenta aproximar el proceso que sigue un experto en la evaluación de una serie de registro. Este proceso consiste en realizar un seguimiento de los cambios que sufre un registro al realizar una modificación en la intensidad o tasa de estimulación. Las ventajas del uso de métodos automáticos para la evaluación de la calidad de los PEAT ya fue demostrada por Arnold [4]. El uso de métodos automáticos nos permite: en primer lugar, mejorar el proceso de adquisición, deteniéndolo cuando tenga una calidad suficiente y en segundo lugar, unificar el protocolo. Este artículo describe y evalúa el rendimiento del método SSP con la realización de dos experimentos. En el primero, se observan los resultados obtenidos para series de registros sintetizadas con valores conocidos; en el segundo de los experimentos, se realiza el mismo procedimiento para series de registros reales. En este trabajo se ha realizado la adquisición de registros ABR reales a varias intensidades y tasas de estimulación.

Los resultados indican que el método parametriza automáticamente de forma precisa las transformaciones en la morfología que experimentan los PEAT frente a una variación en algún parámetro de la estimulación. Además, al entrenar el método se demostró el significado y necesidad de un factor de compresión asociado al comportamiento de los registros adquiridos variando la tasa de estimulación.

Una posible aplicación práctica de este método puede ser la evaluación de manera automática la calidad de los registros y la detección de la existencia de respuesta de origen biológico.

AGRADECIMIENTOS

Esta investigación ha sido financiada por el proyecto "Diseño, implementación y evaluación de un sistema avanzado de registro de potenciales evocados auditivos del tronco (PEAT) basado en señalización codificada" (TEC2009-14245), Plan Nacional de I+D 2008-2011, Ministerio de Economía y Competitividad (Gobierno de España); por la "Granada Excellence Network of InnovationLaboratories – StartupProjectsfor Young Researchers Programme (GENIL-PYR 2014), Campus de Excelencia Internacional, Ministerio de Economía y Competitividad (Gobierno de España); y por la beca de "Formación de Profesorado Universitario" (FPU, AP2009-3150), Ministerio de Educación, Cultura y Deporte (Gobierno de España).

PUBLICACIONES RELACIONADAS

[1] Valderrama J.T., Morales J.M., Alvarez I., de la Torre A., Segura J.C., Sainz M., Vargas J.L. "**Automatic Quality Assessment and Response Detection of Auditory Evoked Potentials based on Response Tracking**."Presentación oral en el International Evoked Response Audiometry Study Group (IERASG), Nueva Orleans (Junio 2013).

[2] Morales J.M., Valderrama J.T., Alvarez I., de la Torre A., Segura J.C., Sainz M., Vargas J.L.(2014)"**Método automático de seguimiento de respuestas evocadas auditivas basado en la parametrización de series de registros**."Cognitive Area Networks 1(1) 75-80Disponible: http://www.nicolo.es/paginas/SCB2014/documentos/cogan_no_001_vol001_v307s.pdf

REFERENCIAS

[1] Hall J.W., "New Handbook of Auditory Evoked Responses", Pearson; Allyn and Bacon, Boston, MA(2007)

[2] Burkard R.F., Don M., "The Auditory Brainstem Response"en el libro"Auditory Evoked Potentials, Basic Principles and Clinical Application", Lippincott Williams & Wilkins, Baltimore, MD(2007) Chapter 11

[3] Jewett D.L., Willinston J.S., (1971) "Auditory-evoked far fields averaged from the scalp of humans", Brain 94 (4) 681-696

[4] Arnold S.A.,(1985) "Objective versus visual detection of the auditory brain stem response", Ear and Hearing 6 83) 144-150

[5] Weber B.A., Fletcher G.L., (1980) "A computerized scoring procedure for auditory brainstem response audiometry", Ear and Hearing 1 (5) 233-236

[6] Elberling C., Don M., (1984) Quality estimation of averaged auditory brainstem responses, Scandinavian Audiology 13 (3) 187-197

[7] Valderrama, J. T., Álvarez, I., de la Torre, A., Segura, J.C., Sainz, M, Vargas, J.L., (2012) "Recording of auditory brainstem responses at high stimulation rates using randomized stimulation and averaging", *Journal of the Acoustical Society of America*, vol. 132, pp. 3856-3865.

[8] Valderrama J.T., de la Torre A., Alvarez I., Segura J.C., Thronton A.R.D., Sainz M., Vargas J.L. (2014)"A study of adaptation mechanisms based on ABR recorded at high stimulation rate" Clinical Neurophysiology 125 805-813

[9] Valderrama, J. T., Álvarez, I., de la Torre, A., Segura, J.C., Sainz, M, Vargas, J.L., (2011) Educational approach of a BAER recording system based on experiential learning, Technics Technologies Education Management 6 (4) 876-889

[10] Valderrama, J. T., de la Torre, A., Álvarez, I., Segura, J.C., Thornton, A.R.D., Sainz, M, Vargas, J.L., (2014) "Automatic quality assessment and peak identification of auditory brainstem responses with fitted parametric peaks", Computer Methods and Programs in Biomedicine, vol. 114, pp. 262-275

Jose M. Morales obtuvo la licenciatura en Ingeniería de Telecomunicaciones por la Universidad de Granada en 2014.

Joaquín T. Valderrama obtuvo la licenciatura en Ingeniería de Telecomunicación y la licenciatura en Administración y Dirección de Empresas por la Universidad Europea de Madrid, en 2008. Actualmente, realiza sus estudios de doctorado en el Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada.

Isaac M. Álvarez obtuvo la licenciatura en Ingeniería de Telecomunicación por la Universidad de Málaga, en 2004, y el grado de doctor por la Universidad de Granada, en 2007. Actualmente es Profesor Contratado Doctor en el Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada.

Multiclasificación multimodal mediante el análisis de imágenes de resonancia magnética y tomografía de emisión de positrones para el diagnóstico precoz de la enfermedad de Alzheimer

Tutores: Javier Ramírez Pérez de Inestrosa; e-mail: javierrp@ugr.es
Juan Manuel Górriz Sáez; e-mail: gorriz@ugr.es

Titulación: Ingeniería de Telecomunicación

Departamento de Teoría de la Señal, Telemática y Comunicaciones

Universidad de Granada

Autor: Manuel Martín Moya, e-mail: mmmoya@correo.ugr.es

***Resumen*— En el presente proyecto se implementa un sistema formado por varios clasificadores y dos tipos de neuroimagen: imágenes de resonancia magnética y tomografía de emisión de positrones (PET), con el objetivo de integrar este sistema en un entorno de Diagnóstico Asistido por Ordenador (CAD) para la detección precoz de la enfermedad de Alzheimer.**

Para ello se cuenta con un atlas regional de 116 regiones cerebrales y un pre-procesamiento previo de las imágenes.

La técnica de clasificación usada es MLDA (Enfoque basado en LDA de máxima incertidumbre), y como método estadístico para la selección de características el método t-test.

Se busca variar distintos parámetros del sistema para obtener los mejores valores de sensibilidad, especificidad y precisión en la clasificación de cualquier sujeto en dos grupos: sujetos sanos o de control (NC) y pacientes enfermos (AD).

Finalmente se propone la clasificación de sujetos con deterioro cognitivo leve (MCI), obteniendo resultados prometedores.

***Palabras clave*— Área Bajo la Curva, Clasificador, Diagnóstico Asistido por Ordenador, Enfermedad de Alzheimer, LDA, Materia Blanca, Materia Gris, MLDA, PET, Región De Interés, RM.**

I. INTRODUCCIÓN Y MOTIVACIÓN

La enfermedad de Alzheimer (EA) es la demencia neurodegenerativa más frecuente y un creciente problema de salud, puesto que aproximadamente el 50-60 % de los pacientes con demencia se estima que padecen la enfermedad [1]. El diagnóstico definitivo de esta enfermedad tan sólo puede hacerse post mortem y requiere la confirmación histopatológica de las placas amiloides y los ovillos neurofibrilares. El diagnóstico temprano y preciso de la enfermedad no es sólo difícil, sino además crucial en la perspectiva de futuros tratamientos. Puesto que, actualmente, no se ha encontrado soluciones terapéuticas altamente efectivas para curar la enfermedad (ni tan sólo una posible vacuna), se propusieron, años atrás, abrir una gran variedad de líneas de investigación para encontrar algún sistema que, mediante el procesamiento computarizado de neuroimágenes o sistemas de diagnóstico basado en computador, CAD (Fig. 1), pueda clasificar a un determinado paciente en varios grupos: sujetos sanos o de control, sujetos con Alzheimer, sujeto con leve deterioro cognitivo, etc., por lo que es crucial encontrar un biomarcador válido y objetivo para distinguir pacientes con EA de etapa temprana de controles sanos [2].

Las técnicas de aprendizaje automático y clasificación de patrones vienen desempeñado un papel importante en la exploración de las diferencias cerebrales entre pacientes con EA y controles sanos, mediante la comparación de niveles de intensidad de los distintos voxels de cada imagen. Numerosos estudios han demostrado que estas técnicas, en combinación con datos de varias modalidades de neuroimagen, como la estructural y funcional, son útiles para la búsqueda de dichos biomarcadores para la EA.

De este modo, a través del desarrollo de un clasificador de patrones que garantice una alta fiabilidad, mediante valores de sensibilidad, especificidad y precisión igual o cercanos al 100%, se podría llevar a cabo un diagnóstico altamente precoz a través del procesamiento de neuroimágenes, previamente tomadas al paciente, en fases de la enfermedad donde ni siquiera se padecen síntomas alarmantes y en momentos donde el médico especialista todavía no le es posible percatarse de cualquier indicio de la enfermedad.

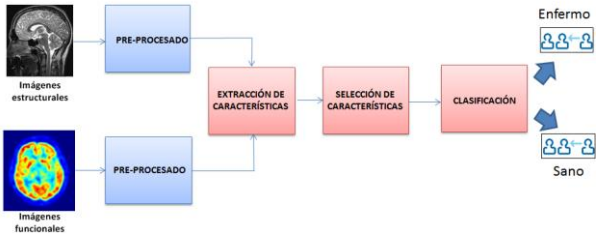


Fig. 1. Diagrama de bloques de un sistema CAD.

II. OBJETIVOS

El objetivo fundamental que se persigue es el diagnóstico precoz de la enfermedad de Alzhéimer proponiendo un sistema de multiclasificación multimodal mediante el uso de varios clasificadores y varios tipos de imágenes diagnósticas: imágenes de resonancia magnética (MRI) e imagen de tomografía de emisión de positrones (PET) en un mismo sistema. Para ello, se realizan fundamentalmente dos tareas: En primer lugar, la obtención de mapas regionales donde se destaquen las diferencias de las distintas regiones según la afectación de la enfermedad y sus diferencias en cuanto a intensidad de vóxels entre grupos sanos y grupos enfermos, y en segundo lugar encontrar los distintos parámetros óptimos que garanticen los mejores resultados de rendimiento en la clasificación de un sujeto desconocido en ambos grupos: AD y NOR.

III. DESCRIPCIÓN DEL SISTEMA

El proyecto se centra principalmente en tres etapas del sistema CAD: extracción de características, selección de características y clasificación. Previo a estas etapas, se dispone de una base de datos de tres grupos de poblaciones,

TABLA I
BASE DE DATOS PROPORCIONADA POR ADNI

Grupo	Nº sujetos	Sexo M/F	Edad media/std.	MMSE media/std.
NC	68	43/25	78.81/4.93	29.06/1.08
MCI	111	76/35	76.39/6.96	26.68/2.16
AD	70	46/24	75.33/7.17	22.84/2.91

previamente etiquetadas, para el entrenamiento de los clasificadores.

A. *Base de datos.*

La base de datos con las distintas imágenes correspondientes a sujetos de las distintas poblaciones son proporcionadas por la iniciativa ADNI. En la Tabla I se muestran las características de las tres poblaciones usadas: NC (Grupo sano o de control), MCI (pacientes con deterioro cognitivo leve) y AD (pacientes enfermos de Alzheimer).

B. *Extracción de características.*

El sistema parte de dichas imágenes pre-procesadas y

Fig. 2. Cerebro parcelado en 116 regiones mediante el atlas.

segmentadas tanto en materia gris como en materia blanca. Para cada imagen, se parcela el cerebro en distintas regiones usando para ello un atlas anatómico de 116 regiones (Fig.2). Posteriormente se calcula tanto la media como la desviación estándar del conjunto de intensidades de los vóxels que componen cada región, denominada región de interés (ROI), y se almacenan los distintos resultados numéricos en forma de matriz constituyendo el llamado espacio de medidas. Cada valor cuantitativo correspondiente a cada región se denomina característica.

C. *Selección de características.*

Una vez se extraen y se almacenan las 116 características correspondientes a las distintas regiones, se deben de seleccionar aquellas que aporten mayor información sobre la afectación de la enfermedad para mejorar las prestaciones del clasificador y aumentar su eficiencia.
Para dicha tarea, se recurre al método estadístico t-test [3] que compara el valor de cada característica, para una región dada, de dos sujetos de ambos grupos. El resultado del test se calcula mediante la expresión:

$$t = \frac{\bar{Y}_1 - \bar{Y}_2}{\sqrt{\frac{s_1}{1} + \frac{s}{}}} \qquad (1)$$

siendo N_1, el tamaño de las muestras, $\bar{Y}_1$, $\bar{Y}_2$ las medias de las muestras y s_1^2, s las varianzas de las muestras.

Mediante el nivel de significación, α, se controla el número de características que el método asume como suficientemente discriminatorias como para rechazar la hipótesis nula:

$$H_0: \ \mu_1 = \mu \qquad (2)$$

D. *Clasificación*

Con el fin de evitar problemas de singularidad e inestabilidad de la matriz de dispersión dentro de la clase, $\mathbf{S}_w$,cuando se usa el algoritmo discriminante lineal (LDA) con muestras limitadas y problemas dimensionales altos, se ha decidido usar un nuevo enfoque basado en LDA (MLDA) [4]. Dicho algoritmo consiste en calcular la matriz de dispersión dentro de la clase modificada, $\mathbf{S}_w^*$. El LDA de máxima incertidumbre se construye mediante la sustitución de $\mathbf{S}_w$ por $\mathbf{S}_\mathbf{w}^*$ en la fórmula del criterio de Fisher:

$$\mathbf{W}_{lda}^* = \arg\max_w \frac{\left|\mathbf{w}^T \mathbf{S}_b \mathbf{w}\right|}{\left|\mathbf{w}^T \mathbf{S}_w^* \mathbf{w}\right|} = \mathbf{S}_w^{*-1}(\mu_1 - \mu_2) \qquad (3)$$

dando lugar a la matriz de proyección que proyecta el espacio de muestras multidimensional $\mathbf{x}$ al espacio unidimensional $\mathbf{y}$ para facilitar la separabilidad de ambos grupos y cálculo del umbral de decisión:

$$\mathbf{y} = \mathbf{W}_{\mathbf{lda}}^* \mathbf{x} \qquad (4)$$

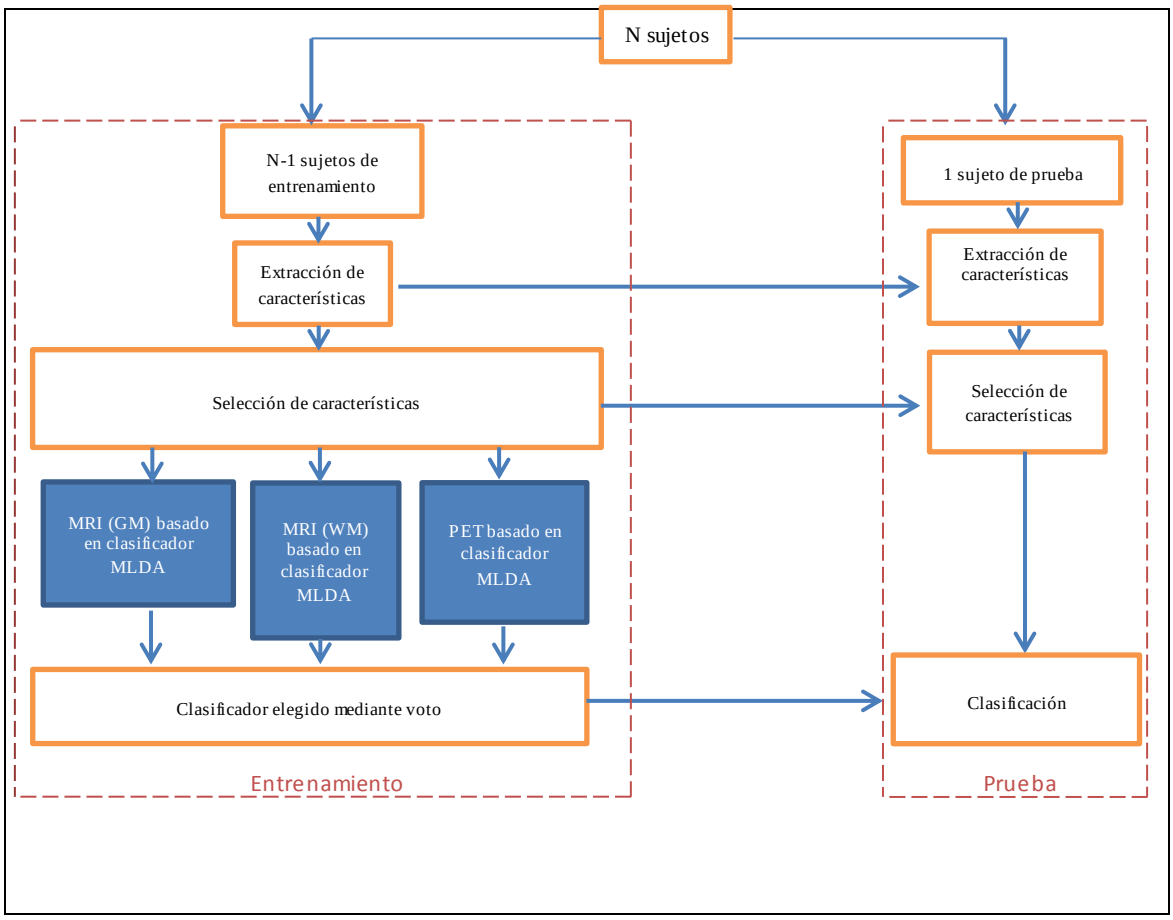


Fig. 3. Diagrama de bloques del sistema propuesto

E. *Rendimiento del Sistema.*

Para calcular el rendimiento del sistema se utiliza la técnica *Leave-one-out cross validation* (LOOCV), donde se escoge un sujeto de la base de datos para test, dejando los restantes para el entrenamiento del clasificador.

Una vez se calcula el umbral de decisión del clasificador, dicho elemento se utiliza para comparar si la predicción de la clase obtenida mediante la comparación de su correspondiente valor, en el espacio unidimensional, con el valor del umbral coincide con la etiqueta original. Dicho procedimiento se repite para los N elementos de la base de datos con el objetivo de garantizar fiabilidad al método y eliminar posibles dependencias con el sujeto escogido.

F. *Funcionamiento del Sistema.*

En la Fig.3 se muestra el funcionamiento básico del sistema multiclasificador. Como se puede apreciar, se utilizan distintos clasificadores MLDA para cada modalidad de imagen: Materia Gris (GM), Materia Blanca (WM) y PET.

En primer lugar, se seleccionan los N-1 sujetos de la base de datos para el entrenamiento dejando uno fuera, con objeto de evaluar posteriormente el sistema. Posteriormente, para cada clasificador se vuelve a realizar la técnica LOOCV, de modo que se emplean N-2 sujetos para el entrenamiento de cada clasificador. Una vez calculado el umbral de decisión de cada clasificador, se emplea el sujeto que ha quedado fuera para el cálculo de la sensibilidad, especificidad y precisión de cada uno de ellos.

En el momento en el que se haya realizado las diversas iteraciones y se hayan obtenido los diferentes valores de precisión de cada clasificador, están en disposición para realizar la predicción de la etiqueta de la clase que estima cada uno para el sujeto de test que quedó fuera en primera instancia, de manera que la decisión final de dicha etiqueta se realiza mediante elección por voto, estableciendo pesos a cada clasificador en función del valor de precisión de cada uno de ellos:

$$F(x_i) = sign\left(\sum_{k=1}^{P}(\omega_k F_k(x_i^k))\right) \qquad (5)$$

donde se escoge el signo del producto escalar entre el vector de los valores de la precisión de cada clasificador y el vector de las etiquetas que cada uno predice mediante la comparación de sus respectivos umbrales: "-1" sujeto enfermo o "+1" sujeto sano. Así, cada clasificador contribuye a la decisión final, en mayor o menor medida, en

función de la tasa de acierto obtenida en el LOOCV de sus respectivas pruebas.

Repitiendo el procedimiento para todos los sujetos de la base de datos, se obtiene finalmente las predicciones de las etiquetas de los N sujetos, pudiéndolos comparar con las etiquetas originales y calcular así los valores de rendimiento global del sistema multiclasificador.

IV. EXPERIMENTOS Y RESULTADOS

A. *Trabajando con la media como característica.*

En primer lugar se pone en marcha el sistema y se extrae sólo la media de las distintas regiones como característica. En el método t-test se suele trabajar por defecto con un nivel de significación de α=0,05 en la etapa de selección de características. Para dicho valor, se obtienen valores de rendimiento del sistema global de 80,00%, 91,12% y 85,51% de sensibilidad, especificidad y precisión respectivamente. Sin embargo, éstos no son los valores más altos que se pueden obtener, ya que para α=0,01 se obtienen valores de 81,43%, 91,12% y 86,23% respectivamente, aumentando la sensibilidad y reduciendo sustancialmente el número de características seleccionadas.

En la Tabla II se pueden apreciar cómo afecta al rendimiento del multiclasificador el trabajar con uno o varios clasificadores. Se puede destacar la poca aportación que supone trabajar sólo con la modalidad de materia blanca en la tarea de clasificación, arrojando tan sólo un 69,57% de precisión incluso para dicho valor de α óptimo, lo que implica no solo un aporte de poca información sobre las regiones afectadas , sino que apenas tiene poder de decisión en el voto. Sin embargo, se demuestra que es positivo el trabajar con todas las modalidades conjuntamente, obteniendo una precisión máxima de 86,23%.

TABLA II
VALORES DE RENDIMIENTO DEL MULTICLASIFICADOR, MODIFICANDO EL NÚMERO Y LAS DISTINTAS MODALIDADES DE CLASIFICADORES MLDA, PARA EL VALOR DE α ÓPTIMO (α =0,01)

Modalidad de imagen	Sensibilidad	Especificidad	Precisión
MRI (GM)	82,86%	83,82%	83,33%
MRI(WM)	65,71%	73,53%	69,57%
MRI (GM+WM)	82,86%	83,82%	83,33%
PET	80,00%	91,12%	85,55%
PET+MRI(GM)	80,00%	88,24%	84,06%
PET+MRI(WM)	80,00%	91,12%	85,55%
PET+MRI(GM+WM)	81,43%	91,12%	86,23%

En cuanto a las regiones más discriminatorias seleccionadas por el método estadístico, se obtienen diferentes resultados en el test para cada modalidad. Para materia gris (Fig.4), destacan las regiones como hipocampo derecho (t=-10,301), temporal inferior derecho (t=-9,368), amígdala derecha (t=-9,353) o hipocampo izquierdo (t=-8,989). Para materia blanca (Fig.5), tan solo se obtienen los resultados más altos en el hipocampo derecho (t=-5,379) e hipocampo izquierdo (t=-5,104). Sin embargo, para PET (Fig.6) se obtienen regiones diferentes con respecto a imágenes estructurales (como materia gris), destacado la región angular derecha (t=7,905), angular izquierda (t=-7,175), cingulado posterior izquierdo (t=-6,233) o precúneo derecho (t=-5,697).

Con el fin de mejorar los resultados obtenidos para α=0,01, se propone variar el valor del umbral de decisión (por defecto cero) en el entrenamiento de los clasificadores. En la Fig.7 se muestra las curvas ROC de sistema, trabajando con todas las modalidades y variando el valor de α. Analizando dichas curvas, se obtiene un punto de corte (umbral de decision= -1E-2) en la curva de α=0,1 que más se aproxima a la esquina superior izquierda de la gráfica (rendimiento óptimo), pasando a obtener valores de sensibilidad, especificidad y precisión de 85,71%, 89,71% y 87,68% respectivamente.

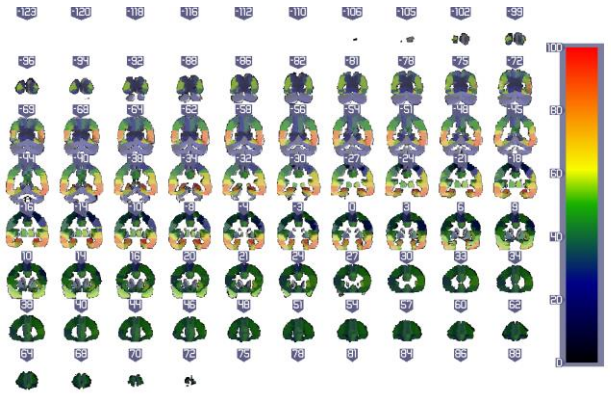


Fig. 4. : Mapa de regiones para los distintos valores de t, trabajando con materia gris (plano coronal).

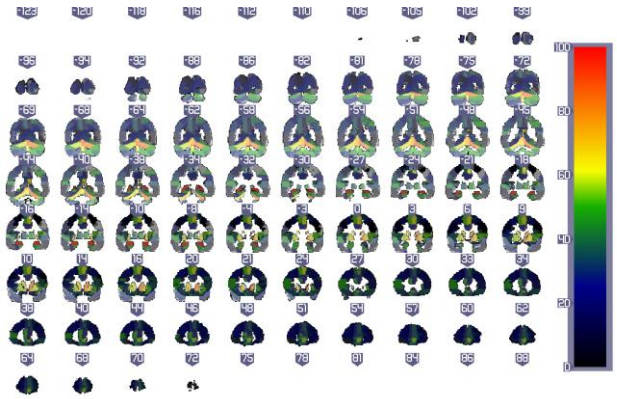


Fig. 5. : Mapa de regiones para los distintos valores de t , trabajando con materia blanca (plano coronal).

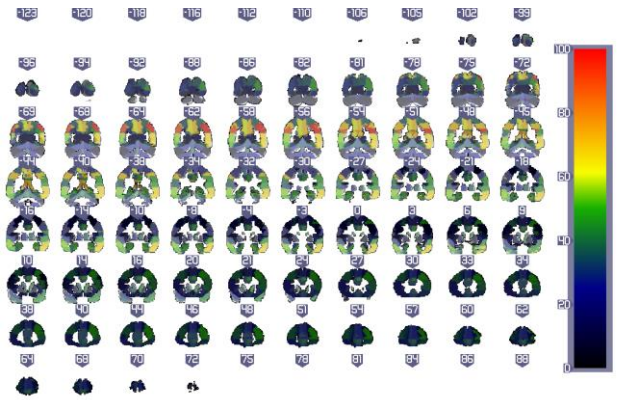


Fig. 6. : Mapa de regiones para los distintos valores de t , trabajando con PET (plano coronal).

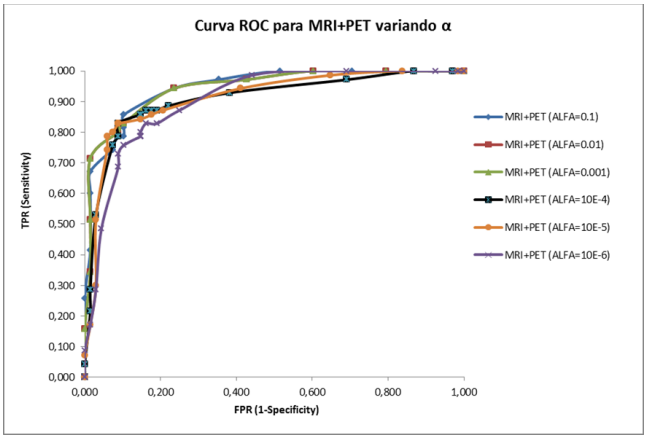


Fig. 7. : Curvas ROC de todas las modalidades, MRI+PET, para varios valores de α, usando sólo la media.

B. Trabajando con la desviación estándar como característica.

Tomando la desviación estándar de los vóxels de cada región como tipo de característica se obtienen resultados, tanto de rendimiento como en el t-test, que difieren en gran medida a los obtenidos mediante la media. En primer lugar, se refleja una mejora sustancial y significativa del rendimiento del multiclasificador, llegando incluso a valores (α=0.3) de 90,00 %, 89,71 % y 89,86 % de sensibilidad, especificidad y precisión respectivamente, donde el clasificador mejora en el diagnóstico de pacientes enfermos (sensibilidad) a costa de aumentar drásticamente el número de regiones seleccionadas.

En este caso se aprecia una gran diferencia en los resultados del test. Es el caso, por ejemplo, de la materia gris, donde ahora regiones como el hipocampo derecho (t=-6,317) no destacan como las regiones más discriminatorias, mientras que regiones como temporal inferior derecho (t=-9,504) mantienen su relevancia. En el caso de materia blanca, dicho tipo de medida no contribuye a mejorar las prestaciones: hipocampo derecho (t=-4,02), hipocampo izquierdo (t=-4,528). En PET, algunas regiones como cingulado posterior izquierdo (t=-9,844) aumentan su poder discriminatorio, mientras que otras como angular izquierda (t=-6,487) disminuyen levemente su valor.

C. Trabajando con la media y desviación estándar como característica.

Utilizando la información de ambas características, se obtienen resultados realmente positivos ya que permite reducir el número de regiones usando α=0,05 y consiguiendo mantener los resultados, hasta ahora, óptimos de sensibilidad, especificidad y precisión. Sin embargo, dichos resultados se obtienen trabajando con el umbral por defecto en el clasificador. En la Fig.8 se muestran ahora las distintas curvas ROC para diferentes umbrales y valores de α, obteniéndose incluso valores de 88,57%, 94,12% y 91,30% de sensibilidad, especificidad y precisión para α=0,05 y un umbral de decisión de 4E-3.

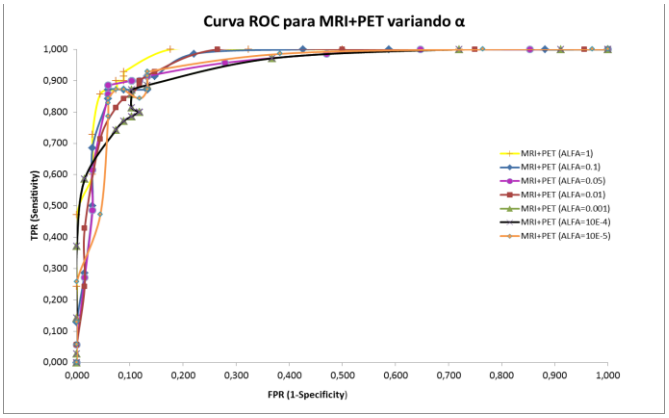


Fig. 8. : Curvas ROC de todas las modalidades, MRI+PET, para varios valores de α, usando la media y la desviación estándar.

D. Variación del método estadístico.

Los resultados obtenidos anteriormente corresponden al uso del método t-test para la selección de características. Sin embargo, es conveniente comparar los resultados con otros tipos de métodos como entropía, chernoff, ROC o wilcoxon, con el objetivo de optimizar los resultados. En la Fig.9 se

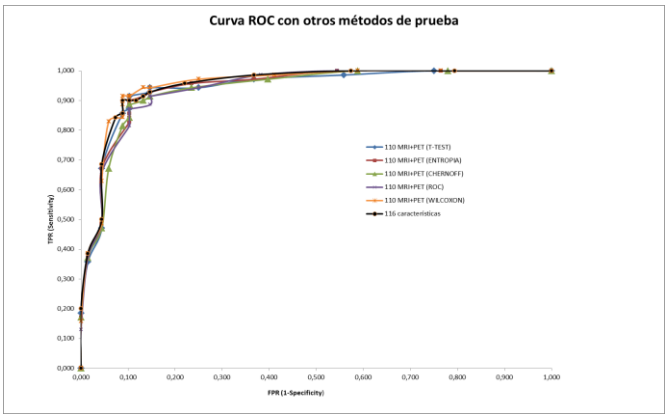


Fig. 9. : Curvas ROC de todas las modalidades, MRI+PET seleccionando 110 características, para distintos tipos de prueba.

pueden ver los distintos resultados para cada método. Tan sólo trabajando con el método wilcoxon se obtienen resultados de rendimiento cercanos a los obtenidos con t-test, siendo necesario escoger hasta 110 características. Así, para el umbral 1E-3 se obtienen valores de 91,43%, 91,18% y 91,30% de sensibilidad, especificidad y precisión, haciendo que dicho método mejore la sensibilidad, empeore la especificidad y mantenga constante la precisión a costa de utilizar un número de regiones altamente elevado.

E. Clasificación de pacientes con deterioro cognitivo leve (MCI).

Por último, se propone evaluar las prestaciones del sistema con ambas configuraciones (t-test y wilcoxon) al tratar de clasificar un sujeto en dos nuevos grupos: sujetos normales o de control (NC) y sujetos con deterioro cognitivo leve (MCI). En la Fig.10 se muestra las curvas ROC del sistema, trabajando con una y otra configuración. Es inmediato concluir que se obtienen mejores resultados trabajando con el

método t-test (α=0,05), obteniendo resultados óptimos mediante el punto de corte más cercano a la esquina superior izquierda (umbral 1E-3) y arrojando resultados de 64,86%, 89,71% y 74,30% de sensibilidad, especificidad y precisión respectivamente.

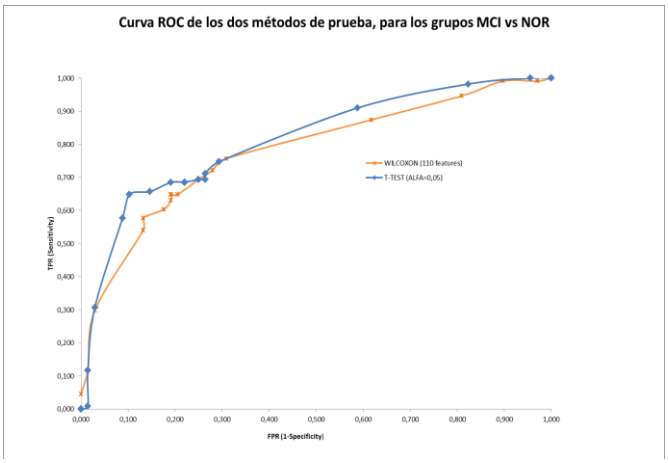


Fig. 10. : Curvas ROC de los dos métodos de prueba, para los grupos MCI y NOR.

V. CONCLUSIONES Y TRABAJOS FUTUROS.

En primer lugar, se ha experimentado la gran influencia que adquiere el tipo de característica extraídas de las distintas regiones: media y desviación estándar. El trabajar con la información que proporcionan ambas a nivel de discriminación entre regiones es de vital importancia y se han obtenido resultados realmente positivos a la hora de combinarlas. Las regiones obtenidas como altamente discriminatorias coinciden, en gran parte, con las regiones más afectadas que señalan las distintas fuentes médicas [5] y diversos estudios en la misma línea[6].

La materia blanca ha destacado como la modalidad menos recomendable a la hora de detectar regiones afectadas, debido a su naturaleza estructural, mientras que la materia gris o PET son totalmente influyentes en la decisión, obteniéndose regiones diferentes pero complementarias y se corrobora la importancia de trabajar tanto con imágenes estructurales o anatómicas como funcionales.

Se ha demostrado que el aumento del número de características o regiones seleccionadas, al menos en el método t-test, no se ha traducido necesariamente en un aumento de las prestaciones del sistema, haciendo incluso aumentar el rendimiento disminuyendo el nivel de significación α.

Aparte de seleccionar un número de características adecuado para el entrenamiento del clasificador, se ha hecho notar la relevancia de estudiar la posición del umbral de decisión, pudiendo mejorar, en todos los casos, los valores de rendimiento que el algoritmo MLDA proporciona mediante el umbral por defecto. Por tanto, se ha obtenido dos configuraciones óptimas para este sistema: método t-test, α=0,05 y umbral 4E-3 y método wilcoxon, 110 características y umbral 1E-3. Los mejores valores, por tanto, de rendimiento obtenidos para la clasificación de NC vs AD han sido: 88,57%, 94,12% y 91,30% de sensibilidad, especificidad y precisión respectivamente para el primer caso, y 91,43%, 91,18% y 91,30% de sensibilidad, especificidad y precisión respectivamente para el segundo caso.

Por último se ha estudiado el comportamiento de ambas configuraciones para la clasificación de NC vs MCI, destacando la primera configuración y obteniéndose valores de 64,86%, 89,71 % y74,30% sensibilidad, especificidad y precisión respectivamente. Se ha apreciado una disminución drástica de la sensibilidad para estos grupos, haciéndose patente la dificultad que supone encontrar regiones suficientemente diferenciables que garanticen un diagnóstico fiable de pacientes en etapas precoces de la enfermedad, por lo que todavía queda un gran margen de mejora para estos casos.

En cuanto a trabajos futuros, se propone modificar la metodología de entrenamiento y clasificación, recurriendo a otros algoritmos más sofisticados o de distinta naturaleza que MLDA, garantizando mayor rapidez y resultados mejores para los grupos NC vs MCI. Otras medidas para aumentar las prestaciones y obtener resultados más fiables y precisos podrían ser trabajar con un número más elevado de sujetos de entrenamiento y regiones en el atlas. Por último, se propone incluir más pruebas diagnósticas en el sistema como pueden ser ALFF (amplitudes de fluctuaciones de baja frecuencia), ReHo (homogeneidad regional), RFCS (fuerza de conectividad funcional regional) o fMRI (resonancia magnética funcional).

REFERENCIAS

[1] Dai, Z., Yan, C., Wang, Z., Wang, J., Xia, M., Li, K., & He, Y. (2012). Discriminative analysis of early Alzheimer's disease using multi-modal imaging and multi-level characterization with multi-classifier (M3). Neuroimage, 59(3): 2187-95.

[2] Chapman, R.M., Nowlis, G.H., McCrary, J.W., Chapman, J.A., Sandoval, T.C., Guillily, M.D., Gardner, M.N., Reilly, L.A., (2007). Brain event-related potentials: diagnosing earlystage Alzheimer's disease. Neurobiol. Aging 28:194–201.

[3] Mugera, W. (2013). Parametric & non-parametric tools of analysis. University of Nairobi. p. 2.

[4] C. E. Thomaz.(2004). Maximum Entropy Covariance Estimate for Statistical Pattern Recognition, *PhD Thesis*, Department of Computing, Imperial College London.

[5] Peña-Casanova, J. (1999). Enfermedad de Alzheimer. Del diagnóstico a la terapia: conceptos y hechos. Fundación "La Caixa", pp. 46-49.

[6] Zhang, D., Wang, Y., Zhou, L., Yuan, H., & Shen, D. (2011). Multimodal classification of Alzheimer's disease and mild cognitive impairment. Neuroimage, 55(3): 856-867.

Predicción de la progresión del deterioro cognitivo leve a la enfermedad de Alzheimer utilizando imágenes de resonancia magnética

Autor: Antonio Domínguez Navarrete; e-mail: adn10adn10@gmail.com
Tutores: Javier Ramírez Pérez de Inestrosa; e-mail: javierrp@ugr.es
Juan Manuel Górriz Sáez; e-mail: gorriz@ugr.es
Titulación: Ingeniería de Telecomunicación

Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*— La enfermedad de Alzheimer (AD) es una enfermedad neurodegenerativa de curso progresivo que constituye la causa más frecuente de demencia. El presente estudio fija como objetivo predecir si un paciente con deterioro cognitivo leve, fase prodrómica de le enfermedad, va a evolucionar a ésta en un plazo de seis meses. Se diseñan varias metodologías de operación con el fin de determinar las herramientas y técnicas más adecuadas para este tipo de estudios, utilizando imágenes de resonancia magnética. Se determina el tejido del cerebro más revelador de la enfermedad, los mejores métodos de extracción y selección de características de los pacientes que maximizan el rendimiento en la clasificación. Por último, a nivel clínico, también se obtiene la relación de regiones del cerebro más alteradas en el progreso de la enfermedad.**

***Palabras clave*— características, clasificación, conversión a AD, deterioro cognitivo leve, imágenes de resonancia magnética.**

I. INTRODUCCIÓN

Hoy en día, la enfermedad de Alzheimer (AD) afecta a más de 30 millones de personas en todo el mundo. Es una enfermedad neurodegenerativa de curso progresivo que constituye la causa más frecuente de demencia entre las personas mayores. Los síntomas principales son: déficit de funciones cognitivas, trastornos psiquiátricos y dificultades para realizar las actividades de la vida diaria. Aunque el desarrollo de la enfermedad es particular para cada persona, hay muchos síntomas comunes como los cambios estructurales en el cerebro. Sin embargo, el diagnóstico de AD se realiza en realidad cuando los síntomas cognitivos están ya presentes. Macroscópicamente, en el cerebro hay disminución del peso y volumen, es decir, se produce una atrofia de los tejidos que lo componen. Todas estas lesiones presentan una distribución selectiva con un patrón de progresión específico. [1]

El Deterioro cognitivo leve (MCI) es una fase prodrómica de la AD, y los estudios existentes han sugerido que las personas con deterioro cognitivo leve tienden a progresar a AD a una tasa de aproximadamente 10% a 15% por año. Hasta el momento no hay una cura conocida para la AD, por lo tanto, el diagnóstico preciso, especialmente del MCI, es de gran importancia para la terapia oportuna y posible retraso de la enfermedad.

Las Imágenes de Resonancia Magnética (MRI) se han establecido como una herramienta muy valiosa en el diagnóstico e investigación de muchas áreas de la medicina, gracias a su gran capacidad de proveer excelente caracterización y diferenciación de los tejidos blandos. Las MRI son muy útiles para revelar los patrones comunes en AD y en pacientes sanos con el fin de diagnosticar la AD incluso antes de la manifestación de cualquier síntoma cognitivo en la persona.

Generalmente, hay dos tipos de cambios clínicos para sujetos MCI en futuros puntos en el tiempo. En primer lugar, algunos sujetos MCI convertirán a AD después de algún tiempo (MCI converters o MCI-C), mientras que otros nunca se convertirán (MCI non-converters o MCI-NC). Es importante predecir si un determinado sujeto MCI se convertirá en AD en futuros puntos de tiempo o no. Esta es una predicción cualitativa, que puede ser resuelta a través de la clasificación entre MCI-C y MCI-NC. En segundo lugar, al ser AD una enfermedad neurodegenerativa progresiva, existen cambios continuos entre las puntuaciones clínicas medidas, por ejemplo, el Mini examen del estado mental (MMSE) y la Subescala cognitiva de evaluación de la enfermedad de Alzheimer (ADAS-Cog), en seguimiento a los puntos en el tiempo. [2]

La base primordial de este estudio va a ser el de intentar predecir si un paciente MCI va a evolucionar a AD (MCI converter) o, por el contrario, no va a convertir a AD a corto plazo (MCI non-converter). Además de intentar conseguir buenos resultados en cuanto a eficiencia de predicción, se va a pretender determinar qué parámetros y técnicas de los que se va a hacer uso para su implementación van a ser más relevantes.

II. MÉTODOS

La base de datos utilizada para realizar el estudio es facilitada por la Iniciativa de Neuroimagen de la Enfermedad de Alzheimer o ADNI (Alzheimer's Disease Neuroimaging Initiative), que desde 2005 ha estado validando el uso de biomarcadores, incluyendo análisis de sangre, pruebas de líquido cefalorraquídeo, imágenes PET y MRI, ensayos clínicos y diagnósticos. Los participantes se comprometen a varios años de estudio que está proporcionando el camino y la prevención de la AD. Actualmente ADNI está reclutando a participantes que han sido diagnosticados de Alzheimer leve a moderado. [3]

TABLA I
INFORMACIÓN DE LOS SUJETOS MCI

	MCI-C (n=67)	MCI-NC (n=61)
Varón/Mujer	40/27	47/14
Edad	74,46	74,74
MMSE (base)	26,52	27,61
MMSE (24 meses)	23,31	27,56
ADAS-Cog (base)	20,69	16,32
ADAS-Cog (24 meses)	25,92	17,19

A. *Sujetos*

Los sujetos con los que se trabaja son con los MCI (converter y non-converter) por la razón anteriormente expuesta, se desea conocer a donde conduce la evolución de su enfermedad. Este tipo de pacientes con analizados cada seis meses en un periodo de dos años, y para cada punto en el tiempo se dispone de MRI y los resultados de las pruebas MMSE y ADAS-Cog.

La Tabla I muestra las medias de los datos de este tipo de pacientes. Tienen edades comprendidas entre 55 y 86 años, y predominan los varones sobre las mujeres, 87 a 41. No se ha hecho distinción de edad ni sexo en cuanto a pruebas y resultados a lo largo del estudio. Las puntuaciones MMSE de ellos están distribuidas entre 24 y 30. Y las puntuaciones del ADAS-Cog se sitúan entre 3 y 48. Para MMSE una baja puntuación denota una mala función cognitiva, justo al contrario que para ADAS-Cog. También es apreciable la diferencia de valor de la media de estos test al principio y a los 24 meses del inicio del análisis.

Adicionalmente se dispone del punto en el tiempo de análisis en el cual los pacientes MCI convirtieron a AD. Es decir, pasaron de ser MCI non-converter a MCI converter. No es facilitado directamente por ADNI, sino que se obtiene utilizando un algoritmo complejo que se resume en comprobar, como se ha dicho, cuando un MCI-NC se transforma en MCI-C. Este dato es de vital importancia durante el desarrollo de este estudio pues supone conocer el estado cerebral y las características de un paciente en el punto aproximado en el tiempo en el que pasa a ser AD.

B. *Imágenes por resonancia magnética*

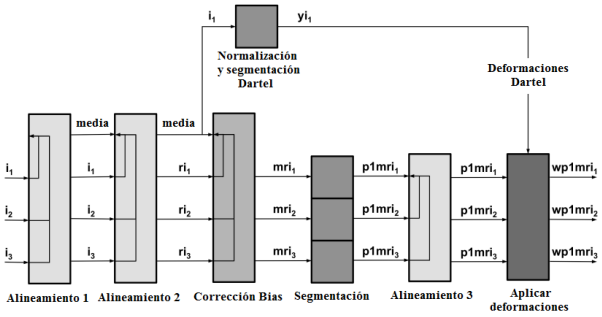
Un estudio por imágenes de resonancia magnética, MRI (Magnetic Resonance Imaging) es una técnica no invasiva que utiliza el fenómeno de la resonancia magnética nuclear para obtener información sobre la estructura y composición del cuerpo a analizar. Una resonancia magnética de la cabeza proporciona imágenes detalladas de los tejidos del cerebro y los nervios, pudiendo mostrar varias capas del tejido. Una MRI no es más que una imagen tridimensional compuesta por voxeles, siendo un voxel el equivalente al píxel en un objeto en 3D. [4]

La escala de grises permite identificar la cabeza y el cerebro, así como los distintos tejidos que componen este último. Principalmente, se distingue:

- Materia gris o GM (Grey Matter): corresponde a aquellas zonas del sistema nervioso central de color grisáceo integradas principalmente por somas neuronales y dendritas carentes de mielina junto con células gliales. En el cerebro se dispone en su superficie formando la corteza cerebral, que corresponde a la organización más compleja de todo el sistema nervioso. Se asocia con la función del procesamiento de información, es decir, a la función del razonamiento.
- Materia blanca o WM (White Matter): es una parte del sistema nervioso central compuesta de fibras nerviosas mielinizadas. Las fibras nerviosas contienen sobre todo muchos axones. La materia blanca, que por largo tiempo se pensó que era un tejido pasivo, afecta activamente cómo aprende y funciona el cerebro. Modula la distribución de los potenciales de acción, actuando como un retransmisor y coordinando la comunicación entre las diferentes regiones del cerebro. [5]

Debido a la no uniformidad del campo magnético, se precisa de una corrección antes de poder trabajar con las MRI, es decir, adecuarlas para su manipulación. Las imágenes de ADNI no están alineadas entre sí. Se antoja difícil trabajar con ellas cuando un punto del cerebro de una imagen no coincide con el mismo punto en otra imagen y, por lo tanto, imposibilita compararlas. Tampoco se puede estudiar la materia gris y blanca del cerebro de manera independiente debido a la dificultad de establecer el límite de cada una de ellas de manera exacta, únicamente de manera visual y aproximada. Por todo ello, es de vital importancia realizar un preprocesado de las MRI. Se utiliza la llamada Morfometría Basada en Vóxel o VBM (Voxel-Based Morphometry). Es una técnica de análisis en neuroimagen que permite la investigación de diferencias focales en la anatomía del cerebro, usando una aproximación estadística paramétrica. [6][7]

FIGURA 1
PREPROCESADO LONGITUDINAL DE VBM PARA LAS MRI



La Fig. 1 muestra el diagrama del preprocesado. Después de un alineamiento inicial, la media de estas imágenes alineadas es calculada y usada como plantilla para siguientes alineamientos. Entiéndase alineamiento como normalización. Además, la imagen media anterior, se usa para corregir las no homogeneidades de las imágenes en los siguientes pasos. Tras la segmentación, se utilizan las plantillas de cada tejido para normalizar las segmentaciones resultantes, usando mapas de probabilidad de cada tejido. Por último, se alinean de nuevo. El resultado final es el de disponer de las segmentaciones de GM y WM de cada paciente para cada punto en el tiempo. [8]

C. *Selección de características*

Tras elegir todo el conjunto de características de las que se hace uso de los datos de los pacientes, es necesario hacer una selección de las más relevantes con objeto de reducir su número. Esto no sólo disminuye la complejidad computacional, sino que, a priori, mejorará los resultados de clasificación. Se utilizan tres técnicas distintas:

•Prueba t de student (t-test): se refiere a la distribución de frecuencia de las desviaciones estándar de muestras extraídas de una población normal. Es una familia de distribuciones de probabilidad continua que surgen al calcular la media de una población distribuida normalmente en situaciones en las que el tamaño de la muestra es pequeño y la desviación estándar de la población es desconocida. [9] El valor de t mide el grado de relación entre dos conjuntos de valores, en este caso una característica común de todos los pacientes en relación a sus etiquetas (MCI-C y MCI-NC). Este valor t se obtiene:

$$\frac{\bar{X}_1 - \bar{X}_2}{S_{X_1X_2} \cdot \sqrt{\frac{}{n_1} + \frac{}{n_2}}} \quad (1)$$

donde $S_{X\ X_2}$ es la desviación estándar combinada, 1=grupo uno, 2=grupo 2; $\bar{X}_1$ y $\bar{X}_2$ las medias de cada grupo; y n_1 y n_2 el tamaño de cada muestra. [10]

•Análisis de componentes principales (Principal Component Analysis, PCA) es una técnica de las estadísticas para la simplificación de un conjunto de datos. Es una forma de aprendizaje no supervisado que se basa enteramente en la misma base de datos de entrada sin hacer referencia a los datos de destino correspondientes (el criterio para ser maximizada es la varianza). Es una técnica estadística de síntesis de la información, o reducción de la dimensión (número de variables). Es decir, ante un banco de datos con muchas variables, el objetivo será reducirlas a un menor número perdiendo la menor cantidad de información posible. Para estudiar las relaciones que se presentan entre p variables correlacionadas (que miden información común) se puede transformar el conjunto original de variables en otro conjunto de nuevas variables incorreladas entre sí (que no tenga repetición o redundancia en la información) llamado conjunto de componentes principales. [11][12] Sean X=[x_1,…..,x_p] un cojunto de características, los componentes principales de X son las nuevas variables

$$\mathbf{Y_j} \quad \mathbf{X}\boldsymbol{t_j}, \qquad j \quad 1, \dots, p \quad (2)$$

Estos componentes principales serán utilizados como características del sistema, ya que estos contienen gran parte de la información de las variables que representa. [13]

•Regresión de mínimos cuadrados parciales (Partial Least Squares, PLS) combina características y generalizaciones de PCA y regresión lineal múltiple. Su objetivo es analizar o predecir un conjunto de variables dependientes a partir de un conjunto de variables independientes o predictores. Esta predicción se logra extrayendo de los predictores un conjunto de factores ortogonales llamados variables latentes que tienen el mejor poder predictivo. [14] Se transforman las variables observadas, **X**, en un conjunto intermedio de variables latentes (*scores*) y esas nuevas variables son usadas para la regresión con una variable dependiente, **Y**. El objetivo de la regresión PLS es predecir **Y** a partir de **X** y describir su estructura común. El criterio para el cálculo de los vectores latentes más usado en PLS es el de máxima covarianza entre scores e **Y** (o entre scores en **X** y scores en **Y**). Se pretende encontrar una relación lineal entre las variables de **X** e **Y** usando una matriz de coeficientes **B** y una matriz de errores **E**.

$$\mathbf{Y} \quad \mathbf{XB} + \mathbf{E} \quad (3)$$

Al igual que en PCA, estos coeficientes serán utilizados como características del sistema. [15]

D. Clasificación

Un método de clasificación es un algoritmo que agrupa (o discrimina) objetos, descritos mediante un vector de características, asignándolos a clases previamente definidas. El conjunto de datos experimentales o muestras en el proceso de clasificación estará formado por un conjunto de vectores de características $x_i \in R^m$, i=1,...,n, siendo m la dimensión del espacio de características H . Este conjunto de vectores de características se dividirá en dos subconjuntos: datos de entrenamiento y datos de test. [16]

Particularmente en este estudio se hace uso de Las Máquinas de Vectores de Soporte (Support Vector Machines, SVM). Es una red estática basada en kernels que realiza clasificación lineal sobre vectores transformados a un espacio de dimensión superior, es decir, separa mediante un hiperplano en el espacio transformado. Operaciones de una SVM:

-Transforma los datos a un espacio de dimensión muy alta a través de una función kernel. Se reformula el problema de tal forma que los datos se mapean implícitamente en este espacio.

-Encuentra el hiperplano que maximiza el "margen" entre dos clases. Cálculo eficiente del hiperplano óptimo.

-Si los datos no son linealmente separables encuentra el hiperplano que maximiza el margen y minimiza una función del número de clasificaciones incorrectas (término de penalización de la función). [17]

Los clasificadores lineales definen hipersuperficies o hiperplanos de decisión en espacios multidimensionales, esto es:

$$\mathrm{g(x)} \quad \boldsymbol{w^T(x)} + w_0 \quad 0 \quad (4)$$

donde w se conoce como vector de pesos y w_0 como el umbral. De esta manera si g(x)>1 pertenece a una clase, y si g(x)<1, pertenece a la otra. [18]

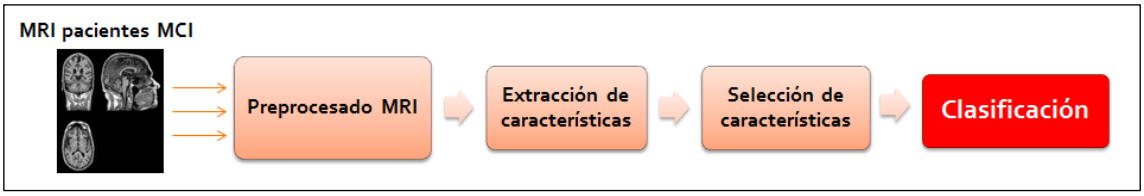
III. DESCRIPCIÓN DEL SISTEMA

Se implementan tres sistemas diferentes haciendo uso de las distintas técnicas de extracción y selección de características, aunque todos ellos persiguen el mismo objetivo. En cada sistema, además, se utilizan cuatro modelos distintos, en los que cambia las características utilizadas, el número de sesiones utilizadas como fuente de extracción de características y el tejido del cerebro utilizado para extraer éstas (véase Tabla II).

TABLA II
DISTINTOS MODELOS EN CADA SISTEMA

GM WM GM y WM	1 sesión	**(A1)** MRI
		(A2) MRI + MMSE + ADAS-Cog
	2 sesiones	**(B1)** MRI
		(B2) MRI + MMSE + ADAS-Cog

FIGURA 2
DIAGRAMA GENERAL DE LOS SISTEMAS IMPLEMENTADOS



Los modelos A1 y A2 utilizan una sesión como fuente de extracción de características, mientras que los modelos B1 y B2 utilizan dos. En los modelos A2 y B2 se añaden los resultados de las pruebas cognitivas MMSE y ADAS-Cog a las características extraídas de las MRI.

La Fig. 2 muestra el diagrama general de los tres sistemas implementados. Se realiza un proceso de extracción de características de las segmentaciones de GM y WM de las MRI de los pacientes, seguido de una selección. Finalmente, se utiliza la técnica de validación cruzada *leave-one-out* para medir el rendimiento del clasificador, obteniéndose los valores de precisión (tasa de clasificaciones correctas de todos los pacientes), sensibilidad (tasa de clasificaciones correctas de los pacientes MCI-C) y especificidad (tasa de clasificaciones correctas de los MCI-NC).

El razonamiento puesto en práctica para la predicción es común para todos los sistemas implementados y es una de las claves de este estudio. Si el fin es determinar la conversión o no de un paciente MCI en el siguiente punto de análisis en el tiempo, es lógico pensar que dicho paciente en la sesión anterior a la conversión a AD podría ser clasificado como MCI non-converter. Disponer de la sesión de conversión a AD de los pacientes MCI-C permite suponer que en las sesiones anteriores a la conversión el paciente era clasificado como MCI y que sus características cerebrales eran próximas a un paciente con Alzheimer pero sin llegar a padecerlo aún. Es por ello que se tomarán como características del sistema las pertenecientes a las sesiones anteriores a la conversión a AD para los pacientes MCI-C. Para los pacientes MCI-NC (sujetos que no convierten a AD) se tomarán las características pertenecientes a las primeras sesiones, suponiendo que el estado de estos sujetos no varía mucho a lo largo de los análisis pues son clasificados como estables. El resultado de la clasificación de un paciente se interpreta, por tanto, que el paciente en cuestión evolucionará a AD en la siguiente sesión de análisis si el resultado es 1, o no evolucionará y se mantendrá estable si el resultado es -1.

A. *Sistema basado en atlas*

El sistema es llamado así debido a que en la etapa de extracción de características se utiliza un atlas del cerebro para extraer éstas por regiones de interés (Region Of Interest, ROI). Se obtienen las medias y las desviaciones estándar de cada ROI del cerebro para las materias gris y blanca. Para ello se parte de que cada ROI en el atlas tiene una misma intensidad, de 1 a 116, habiendo 116 regiones en total.

$$\text{Media} \equiv \bar{x} \quad \frac{1}{n}\sum_{i=1}^{n} a_i \quad \frac{a_1+a_2+\cdots+a_n}{n} \qquad (5)$$

$$\text{Desviación estándar} \equiv s \quad \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(a_i-\bar{x})^2} \qquad (6)$$

donde n es el número de sumandos, en este caso voxeles de cada región, y a_i es la intensidad de cada uno de ellos.
En cuanto al método de selección de características, se utiliza un t-test, por lo tanto, se ordenan las características en orden creciente del valor t para establecer el orden de importancia de estas en la clasificación. En la clasificación se itera de 1 a 150 utilizadas para ver el comportamiento del rendimiento en base a este número.

B. *Sistema basado en voxel (PCA)*

Este sistema, a diferencia del anterior trabaja a nivel de voxel, esto es, la extracción de características se realiza mediante la obtención de las intensidades de los voxeles de las MRI. Esto supone un considerable aumento de la cantidad de datos que maneja el sistema y con ello una mayor complejidad computacional. Por este motivo, y por los buenos resultados obtenidos en el primer sistema mediante el uso exclusivo de la GM de las MRI, se opta por suprimir la WM en este sistema.

Es necesario aplicar una plantilla para suprimir los voxeles con intensidad cero que no pertenecen a la materia gris del cerebro en cada MRI, previamente a la extracción de características. Al aumentar la cantidad de datos manejados, se aplican dos técnicas de selección en este sistema. La primera de ellas es un t-test que ordene las características. Y en segundo lugar se aplica PCA para reducir un gran número de características en unos pocos componentes. El número de características que recibe PCA como parámetro tras el t-test es un nuevo parámetro del sistema y que hace variar el rendimiento. En la clasificación se itera esta vez de 1 a 50 características utilizadas.

C. *Sistema basado en voxel (PLS)*

Este sistema, es idéntico al anterior, con la única diferencia de que el segundo método utilizado para la selección es PLS en lugar de PCA. También se itera de 1 a 50 características.

IV. RESULTADOS

La Tabla III muestra los mejores resultados tras la implementación y ejecución de los tres sistemas descritos. Antes de analizarlos, cabe indicar que los dos sistemas basados en voxel son muy sensibles a modificación de parámetros en el clasificador para obtener resultados eficientes. Sin embargo, para el primer sistema los resultados obtenidos no difieren de manera significativa con los que podrían obtenerse al variar estos parámetros. Los resultados alcanzables son calculados mediante la representación de las

TABLA III
MEJORES RESULTADOS PARA LOS TRES SISTEMAS

	Sistema basado en atlas			Sistema basado en voxel (PCA)			Sistema basado en voxel (PLS)		
	GM	WM	GM+WM	10.000	20.000	50.000	10.000	20.000	50.000
A1									
Nº características	131	19	12	40	1	20	5	1	9
Precisión (%)	67,57	64,86	65,76	72,04	67,63	73,12	71,34	68,35	67,68
Sensibilidad (%)	66	64	70	67,21	62,30	62,30	75,41	59,02	77,05
Especificidad (%)	68,85	65,57	62,29	76	72	82	68	76	60
A2									
Nº características	5	16	5	50	30	19	1	1	1
Precisión (%)	72,07	68,47	72,07	76,11	74,96	70,24	72,07	68,47	72,07
Sensibilidad (%)	68	66	68	78,69	63,93	75,41	68	66	68
Especificidad (%)	75,41	70,49	75,41	74	84	66	75,41	70,49	75,41
B1									
Nº características	74	105	22	50	20	16	35	5	3
Precisión (%)	78,43	72,55	69,60	74,35	73,03	75,53	65,18	68,90	70,78
Sensibilidad (%)	73,17	65,85	68,29	68,85	65,57	75,41	78,69	77,05	67,21
Especificidad (%)	81,96	77,05	70,49	78,05	78,05	75,61	56,10	63,41	73,17
B2									
Nº características	140	21	118	16	15	15	1	3	3
Precisión (%)	81,37	79,41	79,41	76,71	75,39	78,68	68,90	68,24	71,72
Sensibilidad (%)	78,05	75,61	75,61	81,97	78,69	86,89	77,05	75,41	62,30
Especificidad (%)	83,61	81,97	81,97	73,17	73,17	73,17	63,41	63,41	78,05

curvas ROC de las clasificaciones. Con todo ello la tabla muestra los resultados obtenidos para el primer sistema, y los resultados alcanzables para los dos sistemas siguientes.

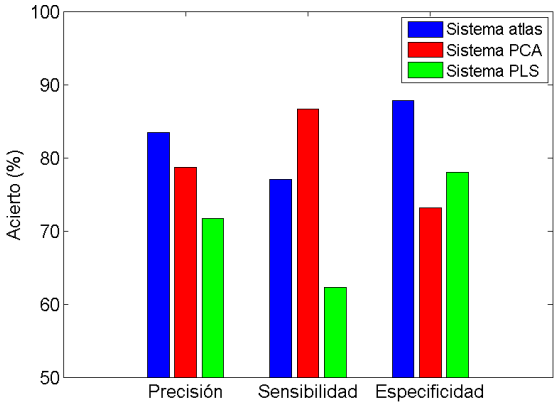
A vista general de los resultados, hay dos comportamientos comunes para todos los sistemas. El uso de dos sesiones como fuente de extracción de características mejora notablemente la precisión de la clasificación. Hecho que también sucede al incluir los resultados de las pruebas MMSE y ADAS-Cog a las características extraídas de las MRI de los pacientes en los modelos A2 y B2. Por lo tanto, para el modelo B2 es para el que se maximiza el rendimiento.

Para el primer sistema es destacable el uso de la GM del cerebro. Es con el uso de este tejido con el que mejores resultados se obtienen (81,37 de precisión). Con el uso de la WM no sólo se obtienen resultados de precisión más bajos que con la GM, sino que la adición de características de esta materia a la GM provoca una disminución de los resultados obtenidos con la GM de forma independiente. Esto se aprecia en los modelos A1 y B1 (sin la inclusión de las pruebas cognitivas). Respecto al número de características utilizado en la clasificación, los resultados tienden a estabilizarse y maximizarse para un número elevado, presentando oscilaciones cuando este número es reducido.

Para los sistemas basados en voxel se muestran los resultados en función de la variable que es el número de voxeles utilizados en PCA y PLS, respectivamente. Se comprueba que las precisiones más elevadas se obtienen para el mayor número utilizado, 50.000. Estos dos sistemas, dado el uso de los componentes de PCA y PLS como características, el número de características para el cual se obtienen los máximos del rendimiento se ve ampliamente reducido, notándose más en el uso de PLS. Con PLS, además, se obtienen resultados muy estables al variar el número de características en la clasificación. Sin embargo, se obtienen valores de precisión un escalón por debajo de los otros dos sistemas, siendo el máximo de 71,72%.

De manera más visual, la Fig. 3 muestra los mejores resultados totales obtenidos para cada sistema. El sistema basado en atlas es el que ha obtenido el valor de pico de todos los rendimientos obtenidos con un 81,37 de precisión, 78,05 de sensibilidad y 83,61 de especificidad para el uso de materia gris. Con el sistema PCA se consiguió 80,39 de precisión, 68,29 de sensibilidad y 88,52 de especificidad. Por último, con el sistema PLS, 72,07 de precisión, 64 de sensibilidad y 78,69 de especificidad.

FIGURA 3
COMPARATIVA DE LOS MEJORES RESULTADOS



Es de gran interés comprobar el nivel de este estudio. Para ello se van a mostrar resultados de otras investigaciones que han perseguido el mismo objetivo que este proyecto, con el fin de poder compararlos y sacar conclusiones positivas o negativas. Comparando los resultados de este estudio con los de la Tabla IV se comprueba que los resultados aquí obtenidos con ligeramente superiores a los de otras investigaciones, siendo el mayor valor de precisión encontrado de 79,7% (Xiaofeng Zhu y otros [19]). Sin embargo

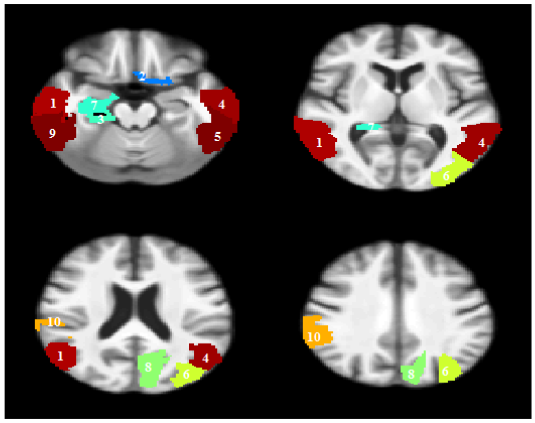
TABLA IV
MEJORES RESULTADOS OBTENIDOS EN INVESTIGACIONES SIMILARES

Precisión (%)	*Sensibilidad (%)*	*Especificidad (%)*	*Referencia*
78,4	79	78	Daoqiang Zhang, Dinggang Shen [2]
76,92	74,29	78,13	Siqi Liu, Sidong Liu [20]
79,7	95	56,1	Xiaofeng Zhu y otros [19]
71,4	69,2	73,7	Kenichi Ota, Naoya Oishi y otros [21]
-	70	61	Rémi Cuingnet y otros [22]

el que mejores resultados ofrece al ser más equilibrados sus valores de rendimiento es el de 78,4 de precisión, 79 de sensibilidad y 78 de especificidad (Daoqiang Zhang, Dinggang Shen [2]).

En cuanto a las regiones más alteradas tras el progreso de la enfermedad de Alzheimer, se van a mostrar aquellas cuyas características se han utilizado en mayor medida, y para el mejor valor de precisión obtenido. Estas son *giro temporal medio izq., corteza olfativa dcha., giro parahipocampal izq., giro temporal medio dcho., giro temporal inferior dcho., giro occipital medio dcho., hipocampo izdo., cúneo dcho., giro temporal inferior izdo. y giro supramarginal izq* (por orden de numeración en la Fig. 4).

FIGURA 4
TOP DE REGIONES MAS UTIILIZADAS EN LA CLASIFICACIÓN



V. CONCLUSIONES

En primer lugar, el uso de la materia gris del cerebro (GM) ofrece resultados más elevados respecto del uso de la materia blanca (WM), e incluso en algunos casos que ambas en conjunto. Por otra parte, el modo de extracción de características de las MRI se ha establecido como la técnica más importante de este estudio, y que ha marcado desde el principio la precisión del sistema. El sistema implementado cuya extracción se realiza mediante propiedades de regiones del cerebro en base a un atlas ha obtenido los mejores resultados de este estudio, por delante del sistema que utiliza directamente los voxeles de las imágenes como características. En cuanto a las técnicas de selección, destacar el uso del t-test y PCA, que son las técnicas con las que se ha podido comprobar realmente buenos rendimientos de clasificación.

Al margen de la calidad de resultados que ofrece el uso de la WM, debe estar relacionada de alguna forma con la enfermedad al ofrecer rendimientos de pico tan distantes del 50%, la clasificación aleatoria. Sería interesante encontrar algún modo en que la WM suponga una mejora en la clasificación y no un perjuicio como es el caso al combinarla con la GM.

Particularmente al caso de extracción por regiones, con la media y la desviación se tienen en cuenta las intensidades de cada voxel que compone cada región. Otra propiedad de la que se podría hacer uso de cara a posibles mejoras es la densidad de cada región. Es decir, sería el cociente del número de voxeles que pertenecen al cerebro (no nulos en intensidad) entre el número de voxeles total de la región.

REFERENCIAS

[1] P. Farreras y C. Rozman. Medicina Interna, Decimosexta edición - Volumen II. 2012.
[2] Daoqiang Zhang, Dinggang Shen. Predicting Future Clinical Changes of MCI Patients Using Longitudinal and Multimodal Biomarkers. 2012.
[3] Michael W. Weiner MD. Professor Principal Investigator, Alzheimer's Disease Neuroimaging Initiative. 2013.
[4] Squire, Lucy Frank; Novelline, Robert A. Squire's fundamentals of radiology. 1997.
[5] Resonancia magnética de la cabeza. Biblioteca Nacional de Medicina de E.E.U.U. http://www.nlm.nih.gov/medlineplus/spanish/ency/article/003791.htm
[6] John Ashburner and Karl J. Friston. Voxel-Based Morphometry-The Methods. 2000.
[7] Catriona D. Good, Ingrid S. Johnsrude, John Ashburner, Richard N. A. Henson, Karl J. Friston and Richard S. J. Frackowiak. A Voxel-Based Morphometric Study of Ageing in 465 Normal Adult Human Brains. 2001.
[8] Florian Kurth, Eileen Luders, Christian Gaser. 2010. VBM8–Toolbox Manual
[9] Fisher, R. A. "Applications of "Student's" distribution". 1925.
[10] George Box, William Hunter, J. Stuart Hunter. Statistics for Experimenters. 2005.
[11] Martin Sewell. Principal Component Analysis. 2007.
[12] M. López, J. Ramírez, J. M. Górriz, I. Álvarez, D. Salas-Gonzalez, F. Segovia, R. Chaves, P. Padilla, M. Gómez-Río. Principal component analysis-based techniques and supervised classification schemes for the early detection of Alzheimer's disease. 2010.
[13] Aurea Grané, Departamento de Estadística, Universidad Carlos III de Madrid. Análisis de Componentes Principales.
[14] Hervé Abdi. Partial least squares regression and projection on latent structure regression (PLS Regression). 2010.
[15] Sijmen de Jong. Simpls: An alternative approach to partial least squares regression. 1993.
[16] Fermín Segovia Román. Tesis doctoral: Análisis de Imágenes Funcionales Cerebrales mediante Modelos de Mezcla de Gaussianas y Mínimos Cuadrados Parciales para el Diagnóstico de Alteraciones Neurológicas. 2010.
[17] José Luis Alba Castro. Curso de doctorado: Decisión, estimación y clasificación.
[18] Tong Zhang. An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods - A Review. 2000.
[19] Xiaofeng Zhu, Heung-Il Suk, and Dinggang Shen. Department of Radiology and BRIC, University of North Carolina at Chapel Hill, USA. Matrix-Similarity Based Loss Function and Feature Selection for Alzheimer's Disease Diagnosis. 2014.
[20] Siqi Liu, Sidong Liu. BMIT Research Group, School of IT, University of Sydney, Australia. Early diagnosis of Alzheimer's disease with deep learning. 2014.
[21] Kenichi Ota, Naoya Oishi, Kengo Ito, Hidenao Fukuyama. A comparison of three brain atlases for MCI prediction. 2013.
[22] Rémi Cuingnet, Emilie Gerardin, Jérôme Tessieras y otros. Automatic classification of patients with Alzheimer's disease from structural MRI: A comparison of ten methods using the ADNI database. 2010.

Deep neural networks for automatic speech recognition systems

Author: Angel Bueno Rodriguez, e-mail: srsudo@gmail.com[1]
Project Guide: Dr.Umesh S, e-mail: umeshs@iitm.ac.in[2]
Degree Awarded: Dual Degree in Telecommunications Engineering
[1]**Department of Signal Theory, Telematic and Commnunications, University of Granada, Spain**
[2]**Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India**

***Abstract*—This thesis investigates how Deep Neural Networks (DNNs) can improve the performance of Automatic Speech Recognition Systems. Recent research on the field has shown that DNNs are able to provide a higher level representation and a better classification of the input. In this project, we support previous research by employing DNNs as acoustic models in order to determine a better accuracy for spoken sentences. Two different ways to implement DNNs for acoustic modeling were explored: A processor architecture (CPU) and a graphic architecture (GPU). The advantages of GPU in terms of computational cost and data-handling lead into outperforming results compared with other conventional techniques. Furthermore, the experimental results show an outperforming improvement by DNN for Resource Management (RM), TIMIT, and Hindi datasets**

***Index Terms*—Deep Learning, Speech Recognition, Deep Neural Networks**

I. Introduction

Speech recognition process in humans is so complex that many tasks are done at an unconscious level by neurons working massively in parallel inside the human brain. Current ASR systems are modeled by combination of two stadistical techniques: The Hidden Markov Models (HMMs) to deal with temporal variability of speech and the Gaussian Mixture Models (GMMs) to represent how well HMMs fits an input frame. But even most reliable ASR systems are limited as they can not exploit all the information embedded in an input frame. Neural networks stand as a rough mathematical approach of the biological brain. Although, they were not very successful as there were not good enough hardware systems to simulate massive parallelism. Recent advances in machine learning algorithms in combination with massive parallel computing lead into deep learning techniques. High-level abstractions in the input data are provided by using architectures composed of multiple non-linear transformations. The main motivation of this thesis is therefore to study the performance of DNNs as acoustic models in ASR systems. Furthermore, this thesis will focus on a GPU architecture in order to determine whether parallelism models and deep architectures improve the accuracy as they are closest to the computational brain model.

This paper is organized as follows: Section 2 gives an overview of speech recognition techniques used in the project. Section 3 explains the neural network building and training procedure, with a particular focus on DNN. In section 4, the practical implementation is shown, along with the results for Hindi, RM and TIMIT datasets. Finally, in section 5 we show the importance of the achieved results and propose future lines of research.

II. Review of Speech Recognition

A. Continuous Density Hidden Markov Model

Continuous Density Hidden Markov Model (CDHMM) [1] have been the state-of-the-art in speech recognition systems. They are composed by a probabilistic framework known as Hidden Markov Model (HMM). From a mathematical notation, HMM can be defined as $\lambda = (\Pi, A, B)$ where Π is the initial state distribution, A is the state transition matrix where a_{ij} represents the probability of going from state i to state j and B is the emission probability matrix where each element $b_j(u)$ is the probability of emitting a sound while in state i. Each state in HMM is modeled directly with K mixtures of Gaussian distributions over the state space. Thus, the $b_j(u)$ can be computed as:

$$b_j(u) = \sum_{k=1}^{K} c_{jk} G(u, \mu_{jk}, U_{jk}) \tag{1}$$

Where c_{jk} is the weight factor of the Gaussian G characterized by its covariance matrix U_{jk} and mean μ_{jk} and u the observation. Thus, we can use this probability to model the HMM states.

B. Mel-Frequency Cepstra Features

Mel-Frequency Cepstra Coefficients (MFFC) [1] are the most used features in speech recognition systems. To extract them, two major steps must be performed. The first one is done through a short time processing of the input signal where the ultimate goal is to capture the spectral envelope of the input signal. In the second stage, Mel Filterbank Analysis (MFB) is done on the low frequency range of the signal and an output coefficient is obtained. Finally, a log operation to reduce dimensionality and some additional processing as cepstra liftering is done to give the same weight for all the coefficients. Cepstra mean substraction (CMS) is also performed to reduce any unwanted effect during the recording stage. In addition, as MFCC features are very sensitive to noise, robust features extraction are computed through cepstral mean and variance

normalization (CMVN). The aim here is to set the mean of the cepstra sequence to zero and the variance equal to one. This technique is important as it provides robustness against noise.

C. Linear Discriminant Analysis

LDA is an important technique in speech recognition as it is robust to any non-linear transformation and reduces the dimensionality of the data [2]. Given a set of input features X, in an n-dimensional space, we will try to find a linear transformation $Y = w^t X$ in an m-dimensional space ($m < n$) in which the direction of w^t vector will give us the optimum discrimination. For given matrices W (within-class) and B (between-class), the best solution yields in a projection of X into the subspace of those m eigenvectors in $W^{-1}B$ which correspond to the m largest eigenvalues.

D. Feature Space MLLR

Maximum Likelihood Linear Regression (MLLR) [3] is a based likelihood technique used for adapting Gaussian mean vector in HMM systems. Starting from the adaptation data from a new speaker, MLLR updates the model mean parameters to maximize the likelihood of the adaptation data. Feature-space MLLR (fMLLR) [4] is employed in ASR systems to reduce the mismatch between the adapted models and the acoustic data for a given speaker. In a hybrid GMM-HMM model, the full covariance matrix is used and a Hessian computation in the transformed space is done in order to find the gradient. For each in-speaker transform W^s, the update rule for a $\triangle$ estimation and k step size will be given as:

$$W^s \leftarrow W^s_{n-1} + k\triangle \tag{2}$$

E. Speaker Adaptation

The motivation for using Speaker Adaptative Training (SAT)[5] is the improvement of the accuracy for another speaker taking only the utterances worth his/her speech data by maximizing the likelihood of the training data given the MLLR-adapted models. For each speaker, the estimation of optimal model and mapping function is done jointly by keeping the mean and the variance updated for each speaker, leading into some problems in terms of computational cost. The most common technique is called diagonal SAT, where only the quadratic term in the mean's objective function is stored.

III. Neural Networks

A. Multilayer perceptron model

Multilayer Perceptrons (MLPs) [6] are composed by a set of layers known as "hidden layers" in which each layer is connected to the next one as seen in figure 1. This architecture leads into a higher-order and more complex representation of the input vector. Let it be the set of inputs $x_0, x_1, ...x_P$ for which we define the desired output function $f(x, \vec{\theta})$ with $\vec{\theta} = \{w_{ij}, w_{jk},, w_{kl}\}$ the set of weights on each layer. Hence, for

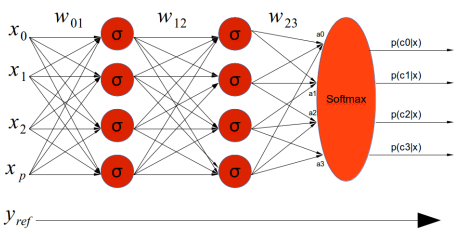


Figure 1. Multilayer perceptron with a softmax layer

a given reference model y_{ref} we define the cost function L as cross-entropy cost function given by $L = -\sum y_n log\, f_n(x, \vec{\theta})$. This function will be minimized through the training procedure.

1) Stochastic Gradient Method: The stochastic gradient descent (SGD) is an optimization method used for updating the weights during the training stage in a neural network. From a given objective function $f(x, \vec{\theta})$, we compute a forward propagation to initialize the weights. Then, we calculate the gradient with respect to the cost function and propagate it backwards to update the weights of each layer. With a given learning rate η , the new weights $w^{'}_{jk}$ between layer j and k can be updated as:

$$\triangle w_{jk} = -\eta \frac{\delta L}{\delta w_{jk}} \tag{3}$$

Where $\triangle w_{jk} = w^{'}_{jk} - w_{jk}$ and $\frac{\delta L}{\delta w_{jk}}$ the gradient operator with respect to the cost function. Notice that if the number of layers is very large, SGD is ineffective as it can be stuck in local minima. Overfitting is another issue in this model as it can lead into an undesired noise modeling. In this project, we used a different algorithm proposed by [7] and known as pre-conditioned SGD. Instead of using a fixed learning rate, a symmetric positive definite matrix-value with restricted eigenvalues is defined. Thus, the eigenvalues of this matrix decrease during the training stage. This matrix shall not depend on the current training sample or we can get a non desired direction in the feature space.

2) The softmax layer: For a classification problem we need to have a probabilistic output that lies on the interval [0,1]. This can be done by forcing the output of the last layer to represent a probability distribution with discrete values. Our objective function $f(x, \vec{\theta})$, for a given class c_i, must be written as

$$L = -\sum y_i^{ref} log\, p(c_i|x) \tag{4}$$

with $p(c_i|x)$ and y_i^{ref} belonging to the interval $[0, 1]^N$. By employing Bayes theorem, we can calculate the likelihood $p(x|c_i)$. Hence, we can perform a classification task for speech recognition as this likelihood can replace the one previously defined in GMM.

B. Restricted Boltzmann Machines

Restricted Boltzmann Machines (RBMs), as explained in [8], are graphical models that define a probabilistic function over a set of stochastic units. The upper layer is composed by

smaller set of "*hidden*" units and the lower layer is formed by a set of "*visible*" units. RBMs are considered as "*restricted*" because there are no connections between hidden and visible units in themselves respectively. This restriction is necessary in order to provide hidden units with learning capacity from visible units. RBM model is shown in figure 2.

This joint configuration of visible and hidden units has an energy distribution $E(v,h)$ defined by :

$$E(v,h) = -h^T W v - c^T v - b^T h \tag{5}$$

where W is a matrix in which each element w_{ij} is the connection between the visible unit i and the hidden unit j. The parameter h is the binary array of hidden units, v is the binary array for visible units and c_k, b_j are the bias variables. The joint probability $p(v,h)$ within units can be written as [8]:

$$p(v,h) = \exp(-E(v,h))/Z \tag{6}$$

with "$1/Z$" the partition function for all the pairs of hidden and visible vectors. Thus, the probability in a given configuration of visible units $p(v)$ is calculated as:

$$p(v) = \frac{1}{Z}\sum_h \exp(-E(v,h)) \tag{7}$$

The above expression gives an output probability according to the current energy distribution. Furthermore, we must maximize the average negative log-likelihood or $-log\,p(v)$ in order to get an effective training procedure for the RBM. The cost function L for a step size N in the optimization hyperplane is given by:

$$L = \frac{1}{N}\sum_h - log\,p(v) \tag{8}$$

Using above, it is shown in [8] that the maximization of $-log\,p(v)$ leads to :

$$\frac{\delta \log\, p(v)}{\delta w_{ij}} =< v_i h_j >_{data} - < v_i h_j >_{model} \tag{9}$$

where the operator $<>$ is the expected value. The data samples $< v_i h_j >_{data}$ can be obtained from the conditional probability within units. As the connections within units are restricted, visible units are conditionally independent given the hidden units, and hidden units are conditionally independent given the visible units. Hence, it is shown in [8] that the conditional probability in each hidden unit h_j can be computed as:

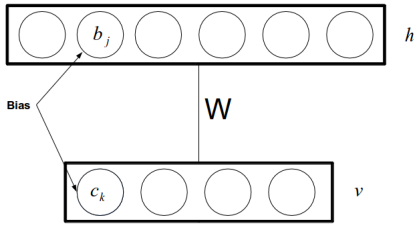


Figure 2. RBM architecture with hidden and visible units

$$p(h_j = 1|v) = \frac{1}{1+\exp[-(\sum_i v_i w_{ij} + b_j)]} \tag{10}$$

$$p(v_i = 1|h) = \frac{1}{1+\exp[-(\sum_j h_j w_{ij} + b_i)]} \tag{11}$$

But the samples concerning the model are computationally intractable as $< v_i h_j >_{model}$ is an exponential summatory over v and h vectors. Thus, a new approach is needed if we want to maximize the equation (9). A very efficient method called Contrastive Divergence (CD) was proposed by [9].

The CD algorithm is based on Gibbs sampling and conditional probabilities. For a given set of visible units $\{v\}$, the hidden units are updated jointly in parallel with equation (10). Then, the visible units must be updated from the hidden units with respect to equation (11). This algorithm can perform Gibbs sampling in k steps. Although, even if we want to learn better generative models and large number of Gibbs sampling steps are run, but we are not going to perform an efficient pre-training as the required parameters can be learned only with one Gibbs step. This one step Gibbs sampling is known as Contrastive Divergence One (CD1). It can be summarized in two main unit updates: Starting with a set of visible units, the hidden units are updated jointly in parallel. Afterwards, from the given set of hidden units, we update all the visible units in parallel to get a "reconstruction". Then, we update the hidden units again. It is faster than normal Gibbs sampling and approximates $-log\,p(v)$ reasonably well. When the samples are obtained, the weights matrix can be updated according to the following learning rule:

$$W^n = W^{n-1} + \epsilon(< v_i h_j >_{data} - < v_i h_j >_{sampled}) \tag{12}$$

The main advantage of this procedure is that overfitting can be avoided at the first update of the hidden layer just by taking the sampled binary values from the visible units. The second update can be computed using real-valued probabilities instead of binary values.

Real data follow different probability distributions. In ASR systems, MFCC features are used as input and since they are parameterized with a Gaussian distribution, it is not optimal to use a binary distribution for the visible units. The energy and the conditional probabilites are modeled with a Gaussian distribution by:

$$E(v,h) = -\sum_i\sum_j h_j w_{ij}\frac{v_i}{\sigma_i} - \sum_i \frac{(v_i - c_i)^2}{2\sigma_i^2} - \sum_j b_j h_j \tag{13}$$

$$p(h_j = 1|v) = \frac{1}{1+\exp[-(\sum_i \frac{v_i}{\sigma_i} w_{ij} + b_j)]} \tag{14}$$

$$p(v_i = 1|h) = G(c_i + \sigma_i \sum_j h_j w_{ij}, \sigma_i^2) \tag{15}$$

With $G(\mu, \sigma^2)$ as the Gaussian distribution. The main issue with Gaussian RBMs is related to the learning of the standard deviation as it becomes very complicated if CD1 is used.

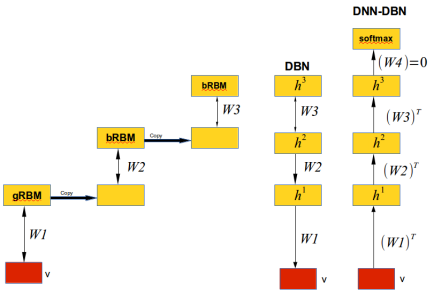


Figure 3. Deep Belief Network building procedure and final DNN-DBN.

In practice, it is normal to perform a data normalization to achieve a zero mean and variance one. Thus, we can calculate the reconstructed sample from the posterior probability without any noise.

C. Deep Belief Networks and Deep Neural Networks

Deep Belief Networks (DBNs) are defined as a "*single, multilayer generative model*" [8]. Each layer of the DBN is an RBM whose posterior probability over its hidden layer is the input for the next RBM. The main idea of stack RBMs is to improve the prior probability on the last layer just by adding another hidden layer. At the top of the structure, the connections of the last two layers are undirected, meanwhile the rest of the layers will have top-down directed generative connections, as seen in figure 3. Once the DBN has been built, the weights must be adjusted through fine-tuning procedure in order to perform the desired task.

From figure 3, the building procedure for a DBN with three hidden layers is shown. For the input MFCC features, a Gaussian RBM is trained and its weight matrix W_1 adjusted. Then, we freeze W_1 and address $(W_1)^T$ as the input data to the next hidden layer. Hence, equation (7) can be written as

$$p(v;W) = \sum_h p(h;W)\, p(v|h,W) \tag{16}$$

where the roles of visible and hidden units have changed with respect to equation (7). The training process can be done by freezing $p(v|h,W)$ and learning the remaining weights. Hence, we train the next RBM by employing the aggregated conditional probability on h_1 as the input data. This is repeated following CD1 algorithm from a bottom-up approach, forcing to learn "features of the features" in each layer. It can be proved that each time we add another hidden layer we achieve an improvement of the variational lower bound on the log probability of the training data [8]. At the end of the training, we will have a DBN with undirected connections on the two top layers and downward connections in the remaining layers.

Finally, we can convert the pre-trained DBN into a Deep Neural Network (DNN) by taking the inverse direction of the calculated weights, which are given by W_k^T (kth hidden layer). Thus, we change the connections to be directed upward between each feature detector layer in order to build a feedforward DNN. A *softmax* layer is added at the top of the DNN to compute each state of the HMM model. Then, the DNN can be discriminatively trained for HMM state prediction.

D. Deep Neural Networks and Hidden Markov Models

DNNs can be applied to predict HMMs states if a discriminative training has been performed previously. Citing from [8], the "*output probability for a given observation o_t at time t in utterance u_t for the HMM state s is given by* "

$$p(s|o_t) = \frac{\exp(a_u(s))}{\sum_{s^*} \exp(a_u(s*))} \tag{17}$$

where a_u is the activation output layer corresponding to state s. A log-likelihood for state s in observation o_t is used for recognition :

$$log\, p(o_t|s) = log\, p(s|o_t) - log\, P(s) \tag{18}$$

and $P(s)$ as the prior probability obtained from the data. Once we have defined $log\, p(o_t|s)$, we can apply the *back propagation* algorithm jointly with SGD to model the HMM states.

IV. Experimental Setup

A. Databases and Languages

The performance of DNNs as acoustic models has been tested on TIMIT, Resource Management (RM) and Mandi databases. RM consists of 3990 training sentences, recorded by 168 speaker: 109 for training and 59 for testing at a sampling rate of 16KHz. The TIMIT database is recorded on eight principal dialects of American English. It is composed by a total number of 490 speakers: 462 for training and 28 for testing.

The Mandi data was collected for building Automatic IVR systems to get the price of Agricultural commodities in Indian languages. This database comprises six major Indian languages: Tamil, Telugu, Hindi, Bengali, Assamese and Marathi at a sampling rate of 8KHz. The speakers were mostly farmers in a rural environment. Hindi was chosen for this study and we separated the whole dataset into 1 hour, 3 hours, 5 hours and 22 hours sets to show the effect of different acoustic modeling techniques in terms of the amount of training data.

B. Data preparation and feature extraction

We tested the behaviour of DNNs as acoustic models with Kaldi software toolkit. Kaldi [10] is the state-of-the-art software toolkit to build speech recognition systems. We need to perform data preparation before feature extraction in order to avoid future variations that might lead to a mismatch between the baseline and the obtained results. Input speech is windowed using 25 ms window with an overlap of 15ms. 13 dimensional MFCC are extracted from the speech signal and velocity, acceleration coefficients are appended to form 39 dimensional features. Cepstral mean normalization (CMN) is performed over these features to achieve noise robustness. The baseline continuous density HMMs (CD-HMMs) were trained using expectation maximization algorithm.

C. Deep Neural Networks in Kaldi

Before any prior training of DNNs, the input features must be improved to provide a better input representation for the DNN [10]. From CDHMM features, speaker adaptation (SAT) features are obtained by applying Linear Discrimant Analysis (LDA) in combination with Maximum likelihood linear transform (MLLT). We compute fMLLR features to normalize the speaker variation. The whole procedure yields into 40 dimensional features that are used as the input for the deep neural network. Splicing is done over these features with 9 frames before and after each center frame. Baseline performance are shown in Table I in terms of Word Error Rate (WER). DNNs are trained in Kaldi following the same receipt as in[10] and from two different approaches: CPU and parallel programming in GPU.

In the CPU approach, the first step is to make a frame-level randomization of the input by dumping all the training features to the disk. This will allow us to access the data sequentially for every epoch and avoid any possible mismatch between read data and the data expected by the DNN. Afterwards, DNN is initialized with one hidden layer and increased by two in each iteration. The training is performed by pre-conditioned SGD in a loop. The total number of iterations are defined as the number of epochs plus an extra margin, which in our simulation were set to 20. On each iteration, the cross-entropy is calculated and the learning rate decreases from the initial learning rate (0.002) to the final learning rate (0.0002) for 15 epochs and remains constant during the last 5 epochs. Finally, we average the models the final fully trained DNN is obtained.

In the GPU approach, DNN is trained as follows: First, we use 90% of the data as a proper training set and the remaining 10% is used as a validation set. Afterwards, by taking the input features, we start to stack RBMs. As the input features are Gaussian, the first RBM employs a Gaussian-Bernoulli distribution with a lower learning rate. Remaining RBMs are Bernoulli-Bernoulli with a constant learning rate. To maintain the learning rate constant, we have to use a momentum m from 0.5 to 0.9 in order to rescale the learning rate as $1 - m$. Contrastive Divergence with one Gibbs sampling step (CD1) is computed during all the RBM training. In order to avoid overfitting, L2 regularization with a penalty factor of 0.0002 is used. Samples are taken by frame-level and sentence-level shuffling. Once we have all the stacked RBM, we perform the frame-level cross-entropy training. With an initial learning rate of 0.008 and a minibatch size of 256, we train the DNN to classify frames into triphone states. The criteria used was to reduce by half the learning rate if the improvement between two iterations is less than 0.5%. This procedure is repeated until improvement is less than 0.1%. Finally, an affine transform is applied at each layer to do decorrelation. Softmax component is added at the final layer to normalize the output probabilities of each tied-state. The performance of DNN for different datasets are shown in Table II and Table III.

D. Hardware setup

All the simulations have been run on IITM Libra Cluster. DNN computations have been performed on three NVIDIA Tesla M2070 GPU, with 6GB graphic memory. Intel Xeon x5675 with 24 CPUs and with a frequency of 3.07 GHz are used for rest of the experiments.

E. Results and discussions

Table I shows the baseline parameters for the CDHMM system. Notice that LDA+MLLT features improve results when compared with basic triphone models in all the datasets. For instance, 5 hours of Hindi shows an improvement of 7.25% over basic triphone model. Also, as the database grows in time, the number of parameters also increases as the data needed to be estimated becomes larger.

Table II and Table III gives optimized baseline for DNNs. If we compare the results of Table II with LDA+MLLT features, we notice that DNN gives a relative improvement of 15.24% and 29.92% for RM and TIMIT respectively. Furthermore, if compared with CDHMM, the relative improvement is 43.69% for RM and 23.99% for TIMIT. Regarding Hindi datasets, DNN gives consistent improvement, even if the amount of data is not too large. For 1 hour of Hindi, when comparing DNNs with LDA+MLLT features, it improves 3.63% and 3 hours of Hindi improves by 8.44%. Furthermore, improvement is up to 21.21% and 31.51% for 5 and 22 hours of Hindi respectively.

The most important results are for GPU training when the dataset is too big and DNN has more labeled data to be trained properly. When compared with LDA+MLLT, a relative improvement of 1.74% and 0.35% was achieved for 1 hour and 3 hours of Hindi respectively. But for larger datasets, improvement goes up to 21.8% for 22 hours of Hindi and 34.15% for 5 hours of Hindi. Notice that the number of parameters plays an essential role in the convergence as well as the training time. There is a trade-off between the number of parameters, the convergence and the simulation time. The larger the dataset, the bigger DNNs are needed to make a proper estimation and thus, more number of parameters are needed too. It also matters how we train the DNN. For instance, a DNN model for 1 hour of Hindi in a GPU needs 3.6 million parameters, meanwhile in CPU it needs 11.6 millions parameters. This is due to the training procedure done in the scripts. In CPU training, two hidden layers are added per iteration and if the improvement is not good enough, we re-initialize the weights. This procedure yields into a slower convergence and more number of parameters, as seen in Table II. In contrast, when we are using the GPU, the training procedure takes full advantage of the parallelism and it converges faster with less number of

Table I
CDHMM BASELINE RESULTS

Dataset	#Ph	CDHMM					
		Triphone			LDA+MLLT		
		#Ts	#Ps	% WER	#Ts	#Ps	% WER
RM	47	1449	0.71	***3.41***	1479	0.71	***2.74***
TIMIT	38	402	0.22	***28.38***	395	0.22	***25.45***
Hindi (1hr)	42	383	0.14	***14.92***	382	0.14	***14.31***
Hindi (3hr)		454	0.17	***11.59***	470	0.17	***10.77***
Hindi (5hr)		571	0.33	***9.10***	577	0.33	***8.44***
Hindi (22hr)		1061	0.86	***5.75***	1090	0.86	***5.68***

#Ph - Number of Phones , # Ts - Number of tied states

Table II
DNN PERFORMANCE ON A CPU

Dataset	DNN (CPU)				
	#Hn	#Hl	#Ps	Time (min)	%WER
RM	1126	4	7.2	143	1.92
TIMIT	793		4.8	1505	21.57
Hindi (1hr)	250		11.1	70	13.79
Hindi (3 hr)	1761		11.9	126	9.86
Hindi (5 hr)	1181		7.6	252	6.65
Hindi (22 hr)	1741		12.1	970	3.89

Hn - Number of Hidden Nodes, # Hl - Number of Hidden layers, *#Ps - Parameters per million*

Table III
DNN PERFORMANCE ON A GPU

Dataset	DNN (GPU)				
	#Hn	#Hl	#Ps	Time (min)	%WER
RM	1024	6	7.2	43	1.74
TIMIT	1024	6	4.7	242	21.39
Hindi (1hr)	2000	5	3.6	32	14.26
Hindi (3 hr)	2000	7	10.6	63	10.30
Hindi (5 hr)	2048	6	19.11	123	6.60
Hindi (22 hr)	2048	6	21.3	275	3.74

Hn - Number of Hidden Nodes, # Hl - Number of Hidden layers, *#Ps - Parameters per million*

parameters. Hence, if we initialize the neural network with random parameters that are not near the convergence region, it may get stuck in a local minima and not converge into the desired region of the hyperplane. And this can be a problem in small datasets where the labeled data is limited and it can be very sensitive to overfitting. For example, as we can see in Table III, the improvement for 1 hour and 3 hours of Hindi is not so good as in Table II. Thus, if the training data is large enough and parameters are set properly, DNNs stand as an excellent acoustic models as they can reduce overfitting and preserve modeling capacity.

V. CONCLUSIONS

In this paper, we have shown experimentally that DNNs outperform CDHMMs as acoustic models due to their capacity of learning from the features, tolerating noise, and supporting parallelism. With our experimental results, we support the previous research on this field and we show that DNNs stand as an excellent solution for building ASR systems in Hindi language and works really well even for small datasets.

ACKNOWLEDGMENTS

The author would like to thank Dr. Umesh S for continuing research links with University of Granada and giving me the opportunity to do my project under his guidance at IITM Speech Lab. The author would like to acknowledge Prof. Carmen Benitez and Prof. Luz Garcia from University of Granada for helpful discussions and unending support during the exchange program. The author would like to thank all the members of Speech Lab for all the technical support. The authors are grateful to all the members of Indian DIT-ASR Consortium for collecting and transcribing agricultural Commodity data.

REFERENCES

[1] Lawrence Rabiner and Ronald Schafer, *Theory and Applications of Digital Speech Processing*, Prentice Hall Press, Upper Saddle River, NJ, USA, 1st edition, 2010.

[2] Reinhold Haeb-Umbach and Hermann Ney, "Linear discriminant analysis for improved large vocabulary continuous speech recognition", in *Acoustics, Speech, and Signal Processing, 1992. ICASSP-92., 1992 IEEE International Conference on*. IEEE, 1992, vol. 1, pp. 13–16.

[3] P.C. Woodland, J. J. Odell, V. Valtchev, and S. J. Young, "Large vocabulary continuous speech recognition using htk", in *Acoustics, Speech, and Signal Processing, 1994. ICASSP-94., 1994 IEEE International Conference on*, Apr 1994, vol. ii, pp. II/125–II/128 vol.2.

[4] Arnab Ghoshal, Daniel Povey, Mohit Agarwal, Pinar Akyazi, Lukas Burget, Kai Feng, Ondrej Glembek, Nagendra Goel, Martin Karafiát, Ariya Rastrow, et al., "A novel estimation of feature-space mllr for full-covariance models", in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*. IEEE, 2010, pp. 4310–4313.

[5] Christopher J Leggetter and PC Woodland, "Maximum likelihood linear regression for speaker adaptation of continuous density hidden markov models", *Computer Speech & Language*, vol. 9, no. 2, pp. 171–185, 1995.

[6] Marvin L Minsky and Seymour A Papert, *Perceptrons - Expanded Edition: An Introduction to Computational Geometry*, MIT press Boston, MA:, 1987.

[7] Xiaohui Zhang, Jan Trmal, Daniel Povey, and Sanjeev Khudanpur, "Improving deep neural network acoustic models using generalized maxout networks", *submitted to ICASSP*, 2014.

[8] Geoffrey Hinton, Li Deng, Dong Yu, George E Dahl, Abdel-rahman Mohamed, Navdeep Jaitly, Andrew Senior, Vincent Vanhoucke, Patrick Nguyen, Tara N Sainath, et al., "Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups", *Signal Processing Magazine, IEEE*, vol. 29, no. 6, pp. 82–97, 2012.

[9] Miguel A Carreira-Perpinan and Geoffrey E Hinton, "On contrastive divergence learning", in *Proceedings of the tenth international workshop on artificial intelligence and statistics*. Society for Artificial Intelligence and Statistics NP, 2005, pp. 33–40.

[10] Daniel Povey, Arnab Ghoshal, Gilles Boulianne, Lukas Burget, Ondrej Glembek, Nagendra Goel, Mirko Hannemann, Petr Motlicek, Yanmin Qian, Petr Schwarz, et al., "The kaldi speech recognition toolkit", in *Proc. ASRU*, 2011, pp. 1–4.

Angel Bueno received a Dual Degree in Telecommunications engineering with specialization in signal processing from University of Granada, Spain. He joined the IITM Speech Lab for one year as an international exchange student. His current main research interest is the improvement of optimization techniques in neural networks, acoustic modeling for noise robust speech recognition and stadistical methods.

Dr. S. Umesh S. Umesh completed his PhD from the University of Rhode Island in 1993, and was a Post-Doctoral Fellow at the City University of New York until 1996. From 1996 to July 2009, he was with the Department of Electrical Engineering at IIT-Kanpur, first as Assistant Professor and finally as Professor. He is currently Professor of Electrical Engineering at IIT-Madras. He has also been a visiting researcher at AT&T Research Laboratories, USA; at Machine Intelligence Laboratory Cambridge University Engineering Department, UK and the Department of Computer Science, RWTH-Aachen, Germany. He is a recipient of the AICTE Career Award for Young Teachers in 1997 and the Alexander von Humboldt Research Fellowship in 2004. His recent research interests have been mainly in the area of speaker-normalization and acoustic modeling and their application in large vocabulary continuous speech recognition systems.

Humming composer para Android

Autor: Jorge Bachs Rubio, e-mail: bachs@correo.ugr.es
Tutores: Ángel M. Gómez García, Antonio M. Peinado Herreros e Iván López Espejo, e-mails: {amgg,amp,iloes}@ugr.es
Titulación: Ingeniería de Telecomunicación
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

***Resumen*—Este proyecto trata del diseño y construcción de un sistema software, destinado a usuarios con pocos o nulos conocimientos musicales, para la creación de secuencias MIDI (Musical Instrument Digital Interface) mediante el tarareo. Para ello, el sistema implementado realiza un proceso de obtención y conversión de la señal de voz (tarareo) en una representación apropiada para su análisis posterior como MIDI. A partir de los parámetros del análisis anterior, se lleva a cabo una conversión compatible con el estándar MIDI, generando un fichero en dicho formato y permitiendo la reproducción del mismo seleccionando un instrumento en particular (piano, guitarra, etc.).**

***Palabras clave*—Android, MIDI, detección de pitch, compositor, tarareo.**

I. Introducción

La música, al igual que cualquier otra disciplina artística, evoluciona a la vez que evoluciona la raza humana. Este desarrollo se observa claramente en la forma en que nos relacionamos con ella. Han aparecido nuevas formas de tocar música, nuevas formas de escucharla, de verla y, cómo no, una gran cantidad de instrumentos y máquinas que la crean. Parece razonable por tanto, en este momento en que el desarrollo tecnológico se ve especialmente reflejado en los dispositivos móviles, realizar aplicaciones móviles musicales que de alguna forma puedan acercarnos a la música aún más. En el mercado actual de aplicaciones, la proliferación de dispositivos con software libre como puede ser Android, ha hecho posible el desarrollo de infinidad de proyectos centrados en la grabación, reproducción y composición musical.

La aplicación que se desarrolla en este proyecto se denomina *Humming Composer*, *Compositor por Tarareo*, y sirve para crear composiciones MIDI (Musical Instrument Digital Interface) a partir de melodías tarareadas por un usuario. El resultado obtenido con este proyecto permite al usuario la posibilidad de modificar algunos parámetros de la secuencia MIDI, como puede ser el instrumento con el que se reproduce, o utilizar estas secuencias MIDI en programas de creación musical profesionales, como pueden ser Ableton, Cubase u otros, para generar composiciones más ambiciosas.

La consecución final del prototipo pasa por el desarrollo de cuatro bloques principales, los cuales son descritos en detalle en la Sección II: el bloque de adquisición de voz, el detector de pitch, el bloque de afinación y el conversor a secuencia MIDI. Cada uno de los procesos por los que será sometida la señal han sido concebidos con el fin de que la melodía MIDI resultante sea reconocible incluso cuando el usuario ha cometido errores de afinación durante la entonación del tarareo. Finalmente, la Sección III recoge unas breves conclusiones acerca del trabajo realizado.

II. Descripción del Sistema

En esta sección se detallan las distintas etapas de procesado por las que pasa la señal de voz con música tarareada.

A. Adquisición de Voz

Para la captación de la señal de voz (tarareo) es necesario ajustar tres parámetros: la frecuencia de muestreo, la resolución de cuantización y el número de canales. Dado que el ancho de banda de interés de la señal es aproximadamente 4 kHz, hacemos uso de una frecuencia de muestro de $f_s = 8$ kHz de acuerdo con el teorema de Nyquist. Trabajaremos con un canal mono estableciendo la máxima resolución (16 bits) permitida usualmente en dispositivos móviles. Además, durante la captación, las muestras de señal obtenidas no deben tener ninguna compresión; por este motivo se emplea la codificación PCM (pulse-code modulation) durante la grabación.

B. Preprocesamiento del Tarareo

Para que el sistema trabaje de manera apropiada es necesario realizar un preprocesado de la señal. Este preprocesamiento consta de una normalización de la señal seguida de una segmentación de la misma en tramas de longitud determinada. La señal de voz de entrada al sistema se identifica como $S(n)$.

En primer lugar se normaliza $S(n)$ obteniéndose una secuencia de muestras $s(n)$ contenidas en el intervalo $[-1, 1]$, de la forma,

$$s(n) = \frac{S(n)}{S(\arg\max |S(i)|)}; \quad \forall n \in [1, 2, ..., N_S];\ \ 1 \leq i \leq N_S, \tag{1}$$

donde N_S corresponde al número total de muestras de $S(n)$.

Una vez normalizada, la señal se segmenta en tramas de 30 ms. Este valor fue seleccionado considerando que en aplicaciones de reconocimiento de voz se suele hacer uso de tramas de audio de duración en el rango 15-30 ms. Conocidas la frecuencia de muestreo f_s y la duración temporal de la trama, el número de muestras de la trama t-ésima, $s(n;t)$, es calculado como,

$$N = f_s \cdot t_{trama} = 8000 \frac{\text{muestras}}{\text{s}} \cdot 0.03 \frac{\text{s}}{\text{trama}} = 240 \frac{\text{muestras}}{\text{trama}}, \tag{2}$$

con $t = 1, 2, ..., T$, siendo $T = N_S - N + 1$ dado que se eligió que el desplazamiento de la ventana fuese de una

muestra. Cada una de las tramas resultantes, $s(n;t)$, se envía al bloque de detección de pitch, explicado con detalle en la Subsección II-D. Este bloque se encargará de determinar si la trama recibida contiene voz o ruido. En el caso de que la trama contenga voz, se procederá a obtener su pitch, y en el caso de que contenga ruido, se considerará la duración de la trama como si fuese un silencio.

C. Detección de la Duración de las Notas

Aunque no exista explícitamente un bloque de detección de la duración de las notas, dada su importancia, resulta interesante hacer una pequeña revisión sobre cómo el sistema gestiona la duración de estas.

Debe considerarse que se desea reproducir, mediante la secuencia MIDI, exactamente lo que se ha grabado previamente con la voz, también en términos de duración. Para ello se tiene en cuenta que la frecuencia de muestreo es de 8 kHz y que el desplazamiento de la ventana para cada trama es de tan sólo una muestra. Puesto que para cada trama se calcula un valor de pitch (nota), la tasa de generación de notas es de 1 nota/muestra. Dado que la frecuencia de muestreo nos indica que hay 8000 muestras/s, se obtiene una nota cada $C_{\text{NOTAS}} = 1.25 \cdot 10^{-4}$ s. Como se recomienda que el tarareo se realice con un fonema sordo seguido de uno sonoro (p.e. *pa*, *ta*, *da*...), se podrá contar el número de repeticiones de una misma nota que hay entre dos segmentos sin pitch (sordos) y así obtener la duración total de esta. Estos valores de duración de las notas serán necesarios para la creación de la secuencia MIDI, ya que en ésta se debe especificar cuándo comienza una nota y cuándo termina.

D. Detección de Pitch

El detector de pitch está basado en el algoritmo YIN [1], pero incorpora una serie de modificaciones destinadas a mejorar el rendimiento de la detección y a solventar las limitaciones de los dispositivos en los que se utilizará el sistema. La implementación se lleva a cabo en dos etapas. La primera de ellas realiza los pasos 2, 3 y 4 del algoritmo [1], *función diferencia*, *función diferencia de media acumulada normalizada* y *umbral absoluto*, sobre todas las tramas de la señal. La segunda etapa se encarga de descartar las tramas que hayan sido marcadas como ruido o silencio en la etapa anterior y ejecutar el paso 6 del algoritmo, *mejor estimación local*. Para ello hará uso de los resultados obtenidos en la primera etapa y de las tramas de la señal que no han sido descartadas. No se incorpora el paso 5 del algoritmo, *interpolación parabólica*, a la implementación, dado que la mejora que aportaría a los resultados es muy pequeña en relación con la carga computacional extra que tendría que soportar el dispositivo al incluirlo. En la Figura 1 se puede observar de manera gráfica un esquema del proceso de detección de pitch implementado que se explicará a continuación.

La primera etapa del detector de pitch comienza con el cálculo de la *función diferencia*, paso 2 del algoritmo YIN, sobre el segmento de voz $s(n;t)$. Como todos los procesos deben realizarse sobre todos los segmentos de voz, a partir de ahora se notará a cada segmento de voz de forma genérica como $s(n)$ por simplicidad. La forma de la *función diferencia* es:

$$d_t(\tau) = \frac{1}{W-\tau}\left(\sum_{j=1}^{W-\tau}\left(s(j)-s(j+\tau)\right)^2\right); \quad \forall j \in [1,2,...,N];\ \ \forall \tau \in [1,2,...,N_t], \tag{3}$$

donde N es la longitud, en muestras, de la trama de voz, siendo N_t el desplazamiento τ máximo considerado.

Con los valores de la *función diferencia* se calcula la *función diferencia de media acumulada normalizada* con la siguiente expresión:

$$d_t'(\tau) = \begin{cases} 1 & \tau = 0; \\ \dfrac{d_t(\tau)}{\frac{1}{\tau}\sum_{j=1}^{\tau} d_t(j)} & \tau \neq 0. \end{cases} \tag{4}$$

A continuación, en el paso 4 se establece un umbral absoluto de valor 0.1 y se elige el valor más pequeño de τ que da un mínimo en $d_t'(\tau)$ menor que ese umbral. El desplazamiento τ que ofrece una media acumulada mínima así como el valor de este mínimo se almacenan en lo que se puede definir como un proceso de *almacenamiento de mínimos*. En el caso de no encontrar valores por debajo del valor umbral, se supondrá que hay silencio o ruido y se almacenará un valor de -1.

Una vez se tienen los resultados del paso 4, comienza la segunda etapa del detector de pitch. Esta segunda etapa comienza clasificando las tramas en tramas de voz y silencio/ruido. Para ello se consideran la posición y valor del mínimo de la media acumulada de $d_t'(\tau)$. En el caso de que el valor leído sea un -1, significará que no es voz y se descartará la trama, mientras que en el caso opuesto se procederá a ejecutar el paso 6 sobre la trama seleccionada. Este paso lleva a cabo una búsqueda entre los valores vecinos de $d_t'(\tau)$ para comprobar si hay mejores estimaciones entre ellos. La búsqueda se realiza para cada índice de tiempo t, donde se busca un mínimo de $d'(T_\theta)$ para θ dentro de un intervalo pequeño $[t - T_{max}/2, t + T_{max}/2]$, siendo T_θ la estimación en el tiempo θ y $T_{\max}$ el periodo máximo esperado. Basado en esta estimación inicial, el cálculo del algoritmo es aplicado de nuevo con un rango de búsqueda restringido para obtener la estimación final usando $T_{\max} = 25$ ms y un rango final de búsqueda del $\pm 20\%$ de la estimación inicial. Como nuestra frecuencia de muestreo es de 8 kHz y $T_{\max} = 25$ ms, el intervalo de búsqueda es de $[t-100, t+100]$ muestras. Obtenido el rango de búsqueda restringido, se llega al último paso de la detección de pitch. Este paso consiste en calcular el valor mínimo de los valores de la *función diferencia de media acumulada normalizada*, $d_t'(\tau)$, que se encuentran dentro de las posiciones especificadas por el rango de búsqueda restringido. La posición del mínimo será nuestra estimación de pitch. Una vez se ha obtenido la estimación de pitch, se calcula el número de nota MIDI equivalente a esa frecuencia mediante,

$$p(f) = 69 + \left(12 \cdot \log_2\left(\frac{f}{440\ \text{Hz}}\right)\right), \tag{5}$$

donde $p(f)$ es el número de nota MIDI y f es el valor de la frecuencia de pitch en hertzios.

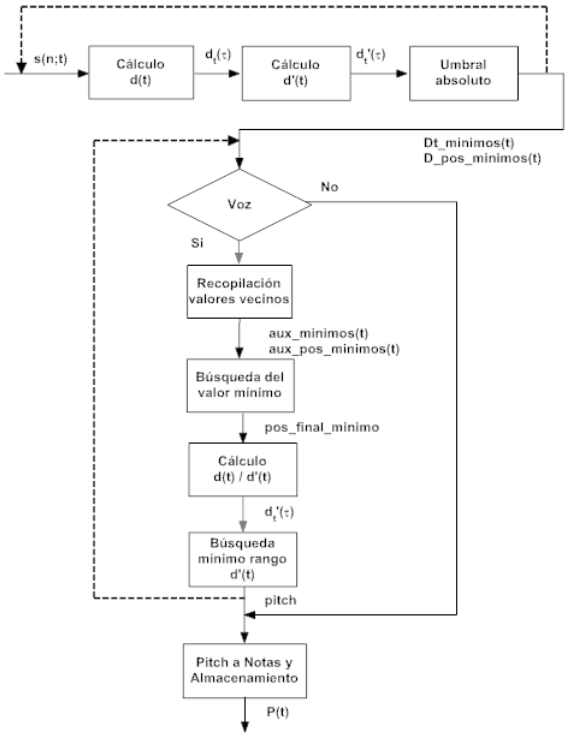


Fig. 1. Esquema del detector de pitch. Se pueden observar dos etapas diferenciadas: la primera etapa está constituida por los tres primeros bloques en horizontal. Esta etapa realiza los pasos 2, 3 y 4 del algoritmo YIN. La segunda etapa está constituida por los primeros 5 bloques verticales. Ésta descartará las tramas que no sean de voz e implementará el paso 6 del algoritmo. El último bloque vertical será el encargado de convertir las estimaciones de pitch en notas MIDI y almacenarlas. Las líneas de puntos indican que en cada etapa se vuelve al principio para cada trama y sólo se termina cuando se haya finalizado con todas las tramas.

Finalmente, todas las notas MIDI, calculadas a partir de las estimaciones de pitch, se almacenan en un vector de la forma:

$$P(t) = (p_1, p_2, ..., p_T)\,, \tag{6}$$

siendo T el número total de segmentos de voz considerados y $\{p_t;\ t = 1, 2, ..., T\}$ el conjunto de notas obtenido a partir del análisis de los segmentos.

Los resultados obtenidos realizando la detección de pitch sobre un tarareo de ejemplo se muestran en la Figura 2(a). Aunque estos resultados son aceptables, pueden observarse notas que parecen no estar en la posición que debieran. Esto se debe en gran medida a la dificultad de tararear sin desafinar por parte del usuario y a errores en la detección del pitch inherentes al estimador. Para solucionar estos problemas en la obtención de la secuencia de pitch se implementa el tercer gran bloque del sistema, el *bloque de afinación y suavizado del contorno de pitch*.

E. Afinación y Suavizado del Contorno de Pitch

Una vez que se ha estimado el pitch para todas y cada una de las T tramas, se implementa el bloque de *afinación y suavizado del contorno de pitch*. Este bloque tiene como entrada el vector $P(t)$. En condiciones normales, este vector contendrá algunas notas erróneas debido a fallos en la detección del pitch. Los factores que desencadenan errores

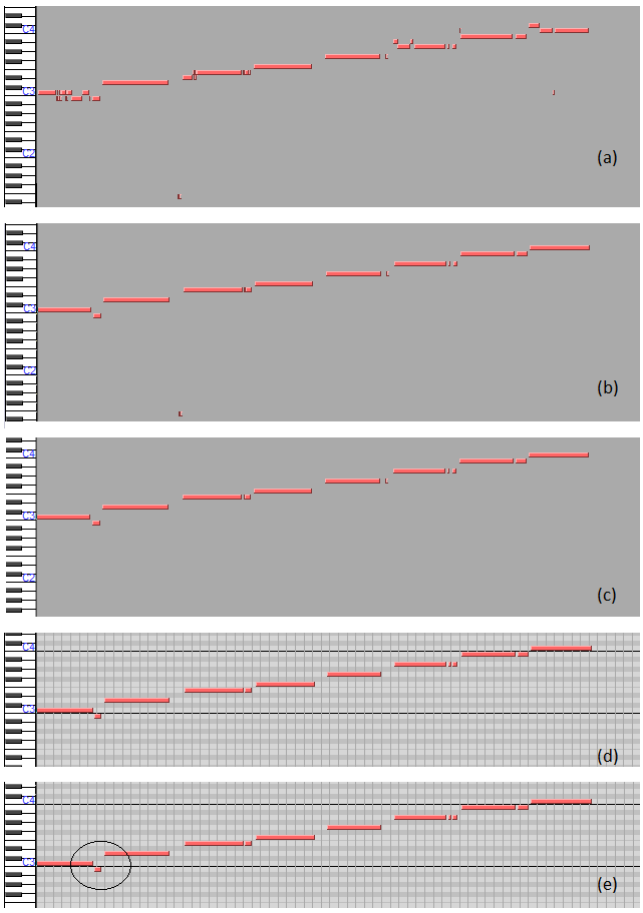


Fig. 2. Representación de las notas asociadas al valor del pitch en función del tiempo para un tarareo de una escala de *Do Mayor*: (a) original, (b) tras aplicar el suavizado entre silencios, (c) tras añadir el suavizado relativo, (d) tras añadir el suavizado en bloques, (e) tras añadir el procedimiento de afinación.

en la detección del pitch son, entre otros, desafinaciones durante la entonación de la melodía vocal, ruido acústico, limitaciones en la suposición de estacionariedad de las tramas, etc. Teniendo en cuenta que los factores expuestos están siempre presentes en el proceso de detección de pitch, se construye el elemento de *afinación y suavizado del contorno de pitch* para conseguir solventar estos factores que degradan la solución final y obtener así un mejor resultado. El bloque se construye mediante la aplicación en cascada de tres filtros de mediana y un algoritmo de afinación basado en la tonalidad musical. Los filtros de mediana fueron diseñados con el fin de suavizar el contorno de pitch y solventar, principalmente, errores causados por el estimador, mientras que el algoritmo de afinación se hizo con el fin de solucionar las desafinaciones creadas por el usuario al tararear. No obstante, se puede observar que tanto los filtros de mediana como el algoritmo de afinación se complementan. Es decir, los filtros de mediana mejoran en cierta forma las desafinaciones y el algoritmo de afinación puede resolver algunos errores inherentes al estimador.

1) Suavizado del Contorno de Pitch: El suavizado del contorno de pitch se realiza mediante la implementación en cascada de tres filtros de mediana. La particularidad de este filtro no lineal, que lo hace especialmente interesante

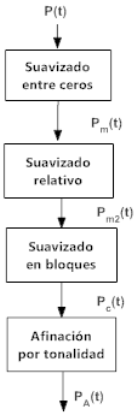


Fig. 3. Diagrama de bloques del subsistema para la mejora del contorno de pitch.

para nuestro propósito, es su capacidad para la eliminación de muestras de tipo impulsivo dejando el resto intactas. Esta característica es muy importante dado que no deseamos modificar el valor del contorno de pitch sino eliminar picos ocasionales no deseados (siendo éste el tipo de error que con más frecuencia se encuentra). La implementación de este filtrado es como sigue. Sea $P(t)$ la secuencia de notas que deseamos filtrar conteniendo T valores, la muestra t-ésima a la salida del filtro se actualiza como:

$$P_m(t) = \text{Mediana}\left(P\left(t - \frac{x-1}{2}\right), ..., P\left(t + \frac{x-1}{2}\right)\right), \quad (7)$$

donde $1 \leq t \leq T$, Mediana$(\cdot)$ es el operador de mediana y $x = 5$ es el orden del filtro (ajustado empíricamente).

En la Figura 3 se muestra la organización de los diferentes filtros de mediana en el sistema. Identificaremos a cada uno de estos filtros teniendo en cuenta la función que desempeñe. En primer lugar, se realiza el *suavizado entre silencios*, en segundo lugar el *suavizado relativo* y en tercer y último lugar el *suavizado en bloques*. La salida de los filtros se introducirá en el bloque de *afinación de secuencia* que se explica en el apartado II-E2.

a) Suavizado entre silencios: Este primer filtrado se basa en la idea de que al tararear la melodía utilizamos una sílaba para cada nota (hecho natural). Si se insta al usuario a utilizar sílabas de la forma *pa*, *ta*, *da*, etc., se puede aprovechar el fonema sordo (sin pitch) como marcador entre notas. Puesto que entre dos pitch nulos sólo hay una nota, si el entorno de pitch presenta variaciones en este periodo debe ajustarse para que sea constante. Para solucionar estas variaciones se realiza un filtrado de mediana entre cada par de pitch nulos de acuerdo con (7). Un ejemplo de los resultados obtenidos llevando a cabo este procedimiento sobre la secuencia de tarareo se muestra en la Figura 2(b).

Si comparamos estos resultados con los obtenidos anteriormente sin ningún tipo de filtrado, se observa cómo se han unificado los bloques de notas, reduciendo en gran medida las variaciones indeseadas cuando se tararea una nota determinada. No obstante, siguen apareciendo notas que parecen estar fuera de lugar y que no siguen la melodía que dibuja el resto de las mismas. Por ello se desarrolla el *suavizado relativo*.

b) Suavizado relativo: Como se muestra en la Figura 2(b), hay ocasiones en las que se producen saltos indeseados entre notas que se sitúan fuera de la melodía que las demás notas dibujan. Para solventar este problema se implementa un filtrado relativo. Dicho filtrado se realiza teniendo en cuenta las notas vecinas tal que se pueden solucionar las variaciones abruptas entre notas que no guardan relación. En nuestro caso concreto, el filtrado se lleva a cabo mediante un barrido nota a nota sobre el vector de entrada $P_m(t)$ a partir del que se crean bloques de 20 notas (ajustado experimentalmente), 10 anteriores y 10 posteriores a la nota actual. A estos bloques se les aplica el filtrado de mediana de acuerdo de nuevo con (7). La salida tras el filtrado relativo es denominada $P_{m,2}(t)$.

Este filtrado conlleva menos cambio en la secuencia de notas que el *suavizado entre silencios*. Esto se debe en gran medida a que los bloques sobre los que se implementa son pequeños (20 notas). No obstante, es una mejora sutil sobre la elección de notas. La figura 2(c) muestra un ejemplo con este filtrado.

c) Suavizado en bloques: Este tercer y último filtrado tiene dos funciones principales: la primera es concluir la fase de suavizado de la secuencia de notas y la segunda es conseguir una representación eficiente del MIDI. La conversión a secuencia MIDI viene limitada por un número máximo de BPM (beats per minute). Si se utiliza la secuencia de notas tal y como se tiene definida actualmente, se tendría una nota cada $1.25 \cdot 10^{-4}$ s, de acuerdo con lo explicado en la Subsección II-C. De esta forma, los BPM que tendría que reconocer el convertidor MIDI serían:

$$\text{BPM} = \left(\frac{60 \text{ s}}{1.25 \cdot 10^{-4} \text{ s}}\right) = 480000, \quad (8)$$

un valor excesivamente grande, ya que el máximo valor admisible es de 250000. Para solucionar este problema se propone realizar el filtrado de mediana sobre bloques de 200 notas y sustituirlos por el valor de la mediana resultante. De esta forma, el valor de los BPM se ve disminuido en un factor de 200. Esta disminución se verá también plasmada en el vector de salida del filtro, $P_C(t)$, cuya longitud será de $T/200$. Fueron elegidos bloques de 200 notas, y no otro valor, de forma experimental en función de los resultados que proporcionaban en términos perceptuales.

Por otra parte, cabe destacar que este filtrado complementa excelentemente los filtros anteriores. Mientras que estos realizan la corrección de las notas de forma detallada, este filtro lleva a cabo el proceso de forma más extensa, ya que utiliza bloques de 200 notas. Esto resulta viable, ya que los filtros de *suavizado entre silencios* y *suavizado relativo* previamente han ido agrupando las notas y solventando las variaciones erróneas de las mismas de forma detallada. Con respecto a los resultados, se puede decir que son notablemente mejores, viéndose un ejemplo de ello en la Figura 2(d), donde las notas fuera de la melodía son casi inexistentes.

2) Afinación de Secuencia: Este bloque se desarrolla con el fin de solucionar problemas de afinación causados por el usuario durante la captación de la secuencia de voz. Para ello se estudia la tonalidad musical. La tonalidad se puede definir como el conjunto discreto y ordenado de notas del que se dispone o se restringe su uso para la composición. Así pues, dependiendo de la tonalidad que tenga una melodía,

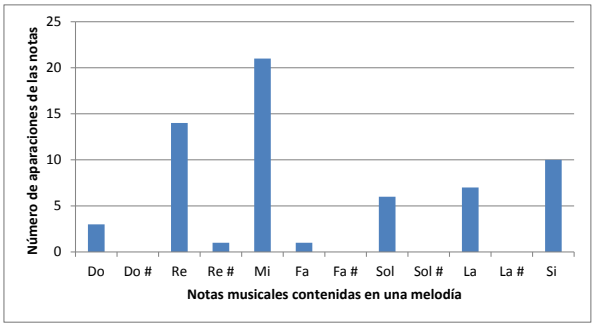


Fig. 4. Ejemplo de histograma de las notas contenidas en una melodía.

siempre y cuando se hable de música tonal, se hará uso de un conjunto particular de sonidos o notas. De esta forma, si se quisiera componer una melodía utilizando la tonalidad de *Do Mayor*, el conjunto discreto de notas que se debería utilizar estaría constituido por *Do*, *Re*, *Mi*, *Fa*, *Sol*, *La* y *Si*. Por tanto, a partir del análisis de las notas contenidas en una melodía, es posible estimar la tonalidad de ésta a partir de un recuento de los sonidos o notas musicales que acontecen. Así, las notas presentes en la melodía pero fuera de la tonalidad (supuestamente a causa de desafinaciones del usuario o, incluso, debido a fallos durante la estimación del pitch) son sustituidas por notas que están dentro de ella.

Para realizar esta *afinación de secuencia*, se comienza estimando la tonalidad de la secuencia de voz. Para lograr este cometido se genera un histograma con las notas de la señal de entrada, $P_C(t)$. El espacio muestral del histograma es el siguiente conjunto: *Do*, *Do#*, *Re*, *Re#*, *Mi*, *Fa*, *Fa#*, *Sol*, *Sol#*, *La*, *La#* y *Si*. Los valores del histograma se guardan en un vector columna que es multiplicado por la conocida como matriz de tonalidades (véase [2]), obteniéndose un vector con doce valores. Cada fila de esta matriz binaria especifica qué notas se encuentran presentes (mediante un 1) en la tonalidad representada por dicha fila. Nótese que la matriz contiene tantas filas como tonalidades consideradas. Así, cada uno de los valores del vector resultante contendrá la suma de todas las notas que entran dentro de cada una de las tonalidades y, la posición del valor máximo en este vector, indicará la tonalidad de la melodía.

A modo de ejemplo supondremos que el histograma de una melodía contiene los valores $[3, 0, 14, 1, 21, 1, 0, 6, 0, 7, 0, 10]$, donde, como puede verse en la Figura 4, el primer valor equivale al número de notas *Do* que hay en dicha melodía, el segundo al número de notas *Do*$\#$ y así sucesivamente. Si se multiplica este histograma por la matriz de tonalidades se obtiene un nuevo vector con los siguientes valores: $[62, 5, 58, 25, 39, 52, 12, 61, 11, 52, 32, 32]$. Este resultado nos indicaría que la tonalidad a la que más se acerca la melodía es a *Do Mayor*, ya que tiene un valor de 62.

Una vez que se conoce la tonalidad de una melodía y las notas asociadas a ella, el siguiente paso es solucionar los problemas de desafinación tratando las notas identificadas fuera de la misma. Partiendo de una nota que no pertenece a la tonalidad estimada, se realiza una búsqueda hacia adelante y hacia atrás en la secuencia melódica con el fin de localizar la nota más cercana (en términos temporales) que se encuentre en la tonalidad. Si la nota encontrada durante esta búsqueda difiere en medio tono de la nota que no se encontraba dentro de la tonalidad, esta última es sustituida por el valor de la nota encontrada en la búsqueda.

A continuación ilustramos el anterior procedimiento continuando con el ejemplo de la melodía cuya tonalidad estimada es de *Do Mayor*. Así, supongamos que el algoritmo de afinación comienza a recorrer la secuencia de notas y encuentra un *Re#*. Dicha nota musical no se encuentra dentro de la tonalidad de *Do Mayor*, por lo que se supone desafinada. Consideremos que comenzando la búsqueda hacia adelante y hacia atrás se halla que la nota más cercana, teniendo en cuenta los silencios, es hacia adelante un *Re*. De este modo, la nota *Re#* es sustituida por un *Re*. En el caso de que la nota más cercana hubiese sido por ejemplo un *Fa*, la nota *Re#* no se modificaría, ya que la distancia entre *Re#* y *Fa* es mayor de medio tono. La restricción de medio tono se debe a dos razones principales: la primera es que las desafinaciones más comunes suelen ser de medio tono arriba o abajo. La segunda razón es que, en algunos casos, se utilizan notas fuera de la tonalidad para dar riqueza melódica a la pieza musical. Para cerciorarnos de que esta implementación resultaba la más adecuada, se comprobó experimentalmente la afinación sin tener en cuenta notas vecinas, la afinación sin distancia mínima y la afinación con distancia mínima superior a medio tono. En todos estos casos, se solucionaban muchas desafinaciones. Sin embargo, el número de afinaciones erróneas crecía considerablemente. Por ese motivo, la implementación final observa las notas vecinas y utiliza una distancia de medio tono.

En la Figura 2(e) se muestra la salida $P_A(t)$ del proceso de afinación sobre la secuencia de voz utilizada anteriormente con fines ilustrativos (escala de *Do Mayor*). Como se puede comprobar, en la primera nota de la secuencia, *Do*, se produce una desafinación al final de la misma hacia la nota *Si*. Dado que la nota *Si* se encuentra dentro de la tonalidad de *Do Mayor*, no se modificará. Ésta es por lo tanto una de las limitaciones de este tipo de afinación por tonalidad. Si se desafina una nota produciendo otra nota dentro de la tonalidad en que se tararea, el sistema es incapaz de saber si se ha producido una desafinación. No obstante, en términos generales se comprueba que el algoritmo produce salidas perceptualmente más agradables.

F. Conversión MIDI

El último bloque implementado en el sistema *Humming Composer* es el encargado de convertir la secuencia de notas $P_A(t)$ en una secuencia MIDI. Para ello se hace uso de la librería de código libre *android-midi-lib* [3]. Esta librería desarrolla todos los eventos propios del sistema MIDI. No obstante, en nuestro caso, como solamente crearemos secuencias MIDI sencillas, los eventos que se utilizan son los siguientes:

- *Introducción del tempo de la secuencia MIDI en BPM:* En este evento sólo habrá un valor que introducir correspondiente al tempo en BPM. Éste es calculado teniendo

en cuenta que se dispone de una nota o silencio cada $1.25 \cdot 10^{-4}$ s así como la simplificación que introduce el *suavizado entre bloques*. De esta forma,

$$\text{BPM} = \frac{\left(\frac{1 \text{ nota}}{1.25 \cdot 10^{-4} \text{ s}}\right) \cdot \left(\frac{60 \text{ s}}{1 \text{ min}}\right)}{200} = 2400 \frac{\text{notas}}{\text{minuto}}. \quad (9)$$

- *Cambio de instrumento de la secuencia:* En el protocolo MIDI hay predefinido un conjunto de instrumentos de los que se hace uso a la hora de reproducir las secuencias MIDI. Dependiendo del valor de instrumento que se elija, la secuencia puede sonar como piano, tuba, guitarra, flauta, etc. Este evento se encarga únicamente de seleccionar el instrumento que se utiliza para reproducir la secuencia MIDI.
- *Inicio de una nota / Fin de una nota:* Aunque se trata de dos eventos individuales, es necesario utilizarlos conjuntamente, ya que el primero condiciona el comienzo de una nota y el segundo el fin de la misma. En el evento *Inicio de una nota* se debe introducir el valor de la nota que se quiere reproducir y la duración de esta. Para ello, se realiza sobre el vector de entrada $P_A(t)$ un proceso de *conteo de notas repetidas*. Este proceso, descrito en la Subsección II-C, contará el número de veces que se repite una nota entre dos pitch nulos, determinando así su duración. El evento *Fin de una nota* tiene como valores de entrada la nota y el momento en que debe terminar de reproducirse. Para conseguir el valor en que debe dejar de reproducirse una nota, se guardará en un vector la duración de todas y cada una de ellas y en otro la duración acumulada de las notas. Este último vector servirá de referencia de tiempo, es decir, se utilizará para seleccionar cuándo debe comenzar una nota y cuándo terminar.

III. Conclusiones

El objetivo principal de este proyecto era la creación de un compositor MIDI mediante tarareo. Con este fin se ha desarrollado un sistema capaz de detectar las características de pitch de una melodía, traducir estas características a notas musicales, determinar la duración de las mismas y convertirlas en una secuencia MIDI. Esta tarea dista de ser trivial, observándose algunos problemas en la detección del pitch, los cuales se intentan solventar mediante la implementación de ciertos bloques orientados a la afinación y suavizado del contorno de pitch basados en filtros de mediana y en la detección de la tonalidad de la melodía.

En general, se puede concluir que el objetivo planteado se resuelve en gran medida con el sistema desarrollado. Las secuencias MIDI obtenidas se asemejan bastante a las melodías tarareadas en un primer momento tanto en tono como en duración.

No obstante, cabe destacar que el margen de mejora del sistema es bastante amplio. El coste computacional en la obtención de las secuencias MIDI y las pequeñas variaciones de notas no deseadas se postulan como principales retos de mejora en futuras versiones del sistema. Algunas de estas posibles mejoras son la utilización de servidores remotos para mejorar el rendimiento, la implementación de sampler interactivos, la creación de partituras a partir de las secuencias MIDI o la inclusión de un metrónomo para el control del tempo de la grabación.

Referencias

[1] Cheveigné, A., y Kawahara, H., "YIN, A Fundamental Frequency Estimator for Speech and Music". *The Journal of the Acoustical Society of America*, 111:1917, 2002.
[2] Bachs Rubio, J., "Humming Composer para Android". Proyecto Fin de Carrera, 2014.
[3] Leffelman, A., "Android MIDI Library". *https://github.com/LeffelMania/android-midi-lib*.
[4] Titze, I. R., "Principles of Voice Production". *Prentice Hall*, 1994.
[5] Robles Schwartz, I. G., "Estimación de la Curva de Entonación para Aprendizaje de Segundo Idioma". 2009.

Jorge Bachs Rubio (Granada, 1989). Licenciado en Ingeniería de Telecomunicación por la Universidad de Granada.

Índice de autores

Índice de tutores

ISBN: 978-84-617-3239-5