

EDITORIAL

Un año más, Buran resurge de sus cenizas para ofrecer a sus lectores una nueva oportunidad de descubrir el apasionante mundo de las nuevas tecnologías y de la multitud de posibles aplicaciones de éstas a la vida cotidiana. A través de éste conjunto de artículos que os presentamos, tanto de profesores como de alumnos de las distintas escuelas y universidades destacadas, se intenta mantener el principal objetivo de nuestra revista: la difusión y el intercambio de ideas y conocimientos entre la comunidad universitaria y científica en general. Sacar una nueva Buran a la luz es pues una tarea conjunta tanto de vosotros, fieles y nuevos lectores, como de nosotros, los miembros de la Rama de Estudiantes de Barcelona que, pese a las diversas dificultades que se nos presentan, intentamos, semestre a semestre, haceros llegar una nueva publicación.

Es por ello que, al igual que os agradecemos el masivo envío de artículos para su publicación en nuestra revista, hecho que deseamos no decaiga nunca, os agradeceríamos también vuestra colaboración activa en la edición de la revista. Este llamamiento puede ser orientado especial pero no exclusivamente hacia los alumnos de primeros cursos de nuestro Campus, para los cuales la colaboración en esta Revista les permite integrarse en la cultura de asociaciones de estudiantes (en horas bajas actualmente), aportar un valor añadido a su experiencia académica y personal, y, por encima de todo, establecer un grupo de amigos muy diferente al que se crea durante la convivencia semestral en clase, en definitiva, un conjunto de amigos que te acompañan durante toda la carrera.

Por último informaros que se introducen algunos cambios en la revista a partir de éste número. Como podeis observar las fechas de publicación han cambiado pues a partir de ahora se intentará hacerlas coincidir con el principio de los dos cuatrimestres académicos de nuestra Escuela; y por otro lado, al final de los artículos encontrareis un breve resumen biográfico sobre los autores para que podais conocerlos un poco más. Esperamos que estos cambios sean de vuestro agrado y, si no, estamos abiertos, como siempre, a cualquier tipo de sugerencia.

Nada más, esperamos disfrutar de nuevo de Buran y, una vez más, haceros llegar nuestro deseo de involucrar a más gente en este proyecto.

Rama de Estudiantes del IEEE Barcelona

COORDINACIÓN BARCELONA

Marc Caballero Gómez

EDICIÓN BARCELONA

José A. López Salcedo

Marc Caballero Gómez

Felipe Calderero

Eduard Calvo

Jara Clara Pascual Soldevilla

Marc Fàbregas Bachs

Enric Muntané Calvo

José Cástor Vallés Martínez

Josep Pegueroles Vallés

REVISIÓN

Marc Caballero Gómez

José A. López Salcedo

DISEÑO PORTADA

Alfredo C. López Salcedo

AGRADECIMIENTOS

II. Dir. Juan A. Fernández Rubio,
Ángel Cardama, Jorge Luis Sánchez Ponz, Javier
Macías Guarasa,

y a los puntos de distribución en la UPC:
Abacus, CPET, CPDA y Kiosk Campus Nord.

We would also like to thank Ms. Laura Durrett
(IEEE Student Services Manager), and IEEE
International for their helpful support, encouragement
and financial funding for distributing Buran across
South American Region 9 IEEE Student Branches.

IMPRESIÓN

RET, s.a.l.

FOTOMECAÑICA

Sistemes d'Edició

La organización se reserva el derecho de publicar los artículos. La opinión expresada en los artículos no tiene por qué coincidir con la de la organización.

Agradecemos las colaboraciones hechas desinteresadamente, y a causa de la falta de espacio, pedimos disculpas a todas aquellas personas a las cuales no se les ha publicado su colaboración. Esperamos que en un próximo número tengan cabida.



ABSORCIÓN DE RADIACIÓN PROCEDENTE DE TERMINALES MÓVILES GSM

Vicent Ferrer i Pérez¹, Luis Nuño Fernández²

Escola Tècnica Superior d'Enginyers de Telecommunicació – Universitat Politècnica de València
Camí de Vera, s/n – 46022 – València

¹Vicente.Ferrer-Perez@ece.ericsson.se, ²lnuno@dcom.upv.es

Resumen.- ¿Son peligrosos los Sistemas de Comunicaciones Móviles? Ésta es una pregunta que se han hecho muchos medios de comunicación dado el revuelo social de los usuarios respecto a esta duda. De hecho, pese a que es bien conocida la influencia que determinadas ondas de radio tienen sobre el cuerpo humano (Rayos X, Radiación Gamma...), la posibilidad de aparición de tumores debidos al tipo de radiación emitida por los terminales y las estaciones de Telefonía Móvil se ha destacado como el más importante motivo de preocupación.

En nuestro trabajo se ha intentado resumir en lo posible el estado actual de las múltiples investigaciones y estudios publicados sobre el tema, así como desarrollar un modelo numérico específico y de precisión que permitiese evaluar el cumplimiento de la normativa vigente en materia de terminales móviles.

1.- INTRODUCCIÓN

La zona de las microondas dentro del Espectro de las Radiofrecuencias es la utilizada para el transporte de una parte substancial de las actuales Redes de Comunicaciones Móviles, así como para el acceso a Servicios Multimedia Interactivos. El futuro desarrollo tecnológico y de servicios exigirá mayores prestaciones debido al aumento de este tipo de tráfico. Así, en muy poco tiempo se considerará como normal no tan sólo la comunicación mediante la voz, sinó también el envío de mensajes de texto, imágenes, vídeo, la navegación por Internet y la posibilidad de realizar transacciones económicas seguras. Todo ello gracias a un pequeño terminal multifunción, móvil y personal.

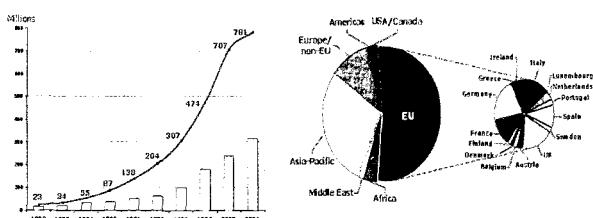


Figura 1.- Crecimiento real y estimado de los usuarios GSM hasta Diciembre del 2000 (izquierda). Las barras azules muestran la ganancia neta por año. Distribución a nivel mundial de los usuarios del sistema GSM (derecha).

La desorientación y falta de información relativa a la seguridad frente a la exposición de los usuarios a la Radiación de Microondas procedente de este tipo de terminales y de sistemas de telecomunicación se ha traducido de manera concreta en temores al uso de los terminales móviles y el emplazamiento de las antenas de las estaciones base de las redes móviles de los operadores.

Estos miedos son un enemigo muy difícil de combatir tanto por los operadores como por los fabricantes. Así, Ericsson, Nokia y Motorola han confirmado que trabajan de manera conjunta par advertir los niveles de radiación emitidos por sus terminales, y plantean la posibilidad de informar a los usuarios mediante etiquetas adhesivas, pese a reafirmarse en la no-existencia de datos concluyentes que permitan afirmar que existe una relación directa entre los teléfonos móviles y determinados riesgos para la salud de sus usuarios.

Las instituciones locales de diferentes ciudades han comenzado a aplicar medidas drásticas a la espera de informes técnicos definitivos, ordenando la desactivación de antenas ya instaladas y prohibiendo la instalación de nuevas. La respuesta oficial por parte del Gobierno Central ha sido el anuncio de la publicación de una normativa encargada de regular las Emisiones Radioeléctricas, la cual fijará una serie de límites y obligaciones para las instalaciones base de Telefonía Móvil, entre otras estaciones del sector de las telecomunicaciones¹. Este esperado proyecto establecerá unos límites de exposición para garantizar la protección sanitaria, basado en la evidencia científica disponible hasta la fecha, y tomando en consideración la Recomendación del Consejo de la Unión Europea de 12 de Julio de 1999 relativa a la exposición del público en general a los Campos Electromagnéticos. Esta recomendación europea está en la línea de las recomendaciones internacionales emitidas por la Comisión Internacional sobre la Protección frente a Radiaciones No-Ionizantes (ICNIRP) y los trabajos efectuados por el organismo de normalización europeo reconocido (Comité Europeo de Normas Electrotécnicas, CENELEC).

1.1.- Estudios y publicaciones

Ya hemos comentado anteriormente que uno de los principales factores negativos a la hora de defender la inocuidad de las radiaciones emitidas por los terminales y las antenas de Telefonía Móvil tanto la falta de información hacia los usuarios, como la disparidad de las conclusiones a las que llegan los estudios científicos sobre el tema.

En este momento, el problema del **electrosmog** (contaminación electromagnética) reside precisamente en que no hay ninguna prueba irrefutable que demuestre que las Emisiones Electromagnéticas emitidas por los terminales móviles y las estaciones base sean realmente perjudiciales para el ser humano. Ningún estudio, ni siquiera los más recientes, ha podido ofrecer nada tan concreto como para poder demostrar algo más que la simple presencia de algunos efectos, muy imprecisos o simplemente hipótesis. Pese a todo ello, la falta de pruebas no puede ser aceptada como una confirmación de que no existen efectos colaterales potencialmente dañinos.

Possiblemente hoy en día el estudio más relevante sobre este tema sea el realizado por la Organización Mundial de la Salud (OMS). Pero lamentablemente no estará finalizado hasta el año 2005, lo que, obviamente, incrementa el miedo de aquellos que defienden que durante los próximos años el problema puede ir a más. De hecho los más escépticos pronostican que la Telefonía Móvil tendrá un futuro muy similar al que ha seguido la industria tabaquera.

Así mismo, par poder resolver las dudas planteadas en el campo de la Telefonía Móvil, especialistas de toda la Unión Europea se han embarcado en un proyecto conjunto para investigar la posibilidad de que las Ondas Electromagnéticas de los terminales móviles puedan afectar la salud humana, no tan sólo con la aparición de dolores de cabeza, sino con tumores cerebrales.

El COST (comité de oficiales senior para la investigación técnica i científica), el cal fomenta la colaboración entre científicos europeos, se ha planteado dos objetivos relacionados con las telecomunicaciones. Por una parte establecer la relación entre los Campos Electromagnéticos y la salud para comprobar los indicios que apuntan a sus posibles efectos nocivos, y por otra la optimización en el diseño de Sistemas de Telecomunicaciones de Banda Ancha por Radio.

El estudio llevado a cabo por el IEGMP (Independent Expert Group on Mobile Phones), organización no gubernamental inglesa, referente a los efectos de los terminales móviles sobre la población, ha acarreado una enorme polémica debido a que todavía no se han logrado calmar las inquietudes surgidas en torno a los efectos nocivos de los terminales celulares. El informe subrayaba la preocupación respecto del nivel de investigación

alcanzado hasta la fecha, el cual no era capaz de poder seguir el acelerado ritmo de crecimiento en el uso de los terminales móviles, al mismo tiempo que no podía concretar el daño sobre la salud que era originado por los terminales.

1.2.-Parámetros evaluados

El hecho de que la exposición de los usuarios a sus terminales móviles se realice frente a Campos Radiados Próximos hace que el uso de términos como la Densidad de Potencia haya perdido su utilidad. La exposición a fuentes de bajo nivel de potencia sólo es relevante a pocos centímetros de distancia del elemento radiante, donde la Densidad de Energía Electromagnética es considerable. Pero esta condición no nos permite aplicar la típica suposición de rayos paralelos, y con ella la definición de un Flujo de potencia.

Por otra parte, se debe tener en cuenta que sólo se considerará que la Energía Electromagnética absorbida por un ser humano puede ser la causante de algún tipo de daño biológico en el mismo. El cuerpo humano está fundamentalmente compuesto por agua, electrolitos y moléculas complejas de un elevado momento dipolar, con lo que se puede afirmar extraerá Energía únicamente del Campo Eléctrico presente en su interior, siendo éste el objeto de las mediadas a tomar.

Así mismo, es preciso diferenciar entre la Radiación Ionizante y la Radiación No-Ionizante. Toda Radiación Electromagnética está constituida por lo que se denominan **quantos** de Energía, proporcionales a la frecuencia. Estos **quantos** de Radiación Ionizante (por ejemplo los Rayos X o la Luz Ultravioleta) tienen en sí mismo la Energía necesaria para poder ionizar átomos. Así, esta radiación al ser absorbida por los tejidos del cuerpo humano genera unos radicales libres que pueden resultar nocivos para el organismo. La Energía de las Microondas, afortunadamente, es del tipo No-Ionizante. Esto quiere decir que la Energía de la que disponen sus **quantos** no es suficiente como para poder romper ni siquiera los enlaces químicos más débiles. Afortunadamente, la localización espectral de los Sistemas de Comunicaciones Móviles está dentro de la zona de Radiación No-Ionizante.

De entre los diferentes métodos mediante los cuales los Campos de Microondas pueden interactuar con otros sistemas para poder transferirles Energía, son los Efectos Térmicos aquellos que pueden ser medidos y que son considerados a la hora de analizar la influencia de los Sistemas de Comunicaciones Móviles.

Se define la **Tasa de Absorción Específica** (*Specific Absorption Rate, SAR*) como la variación respecto del tiempo de la **Absorción Específica**, es decir, el incremento de Energía absorbida por un elemento diferencial de masa contenido en un volumen elemental con una densidad determinada:



$$SAR = \frac{d}{dt} \left(\frac{dU}{dm} \right) = \frac{d}{dt} \left(\frac{dU}{\rho \cdot dV} \right) \quad [W/Kg]$$

La **SAR** está relacionada con el Campo Eléctrico en un punto mediante la siguiente expresión analítica:

$$SAR = \frac{1}{2} E^2 \quad W/Kg$$

$$\begin{cases} \sigma = \text{Conductividad del tejido, medida en } [S/m] \\ \rho = \text{Densidad volumétrica de masa del tejido, medida en } [Kg/m^3] \\ E = \text{Valor de Pico del Campo Eléctrico, medida en } [V/m] \end{cases}$$

Asimismo, la **SAR** está relacionada con un aumento localizado de la temperatura en un punto del volumen de cálculo mediante la siguiente expresión:

$$SAR_c = \frac{T}{t} \quad W/Kg$$

$$\begin{cases} c = \text{Calor Específico del tejido, medido en } [J/(Kg \cdot ^\circ C)] \\ \Delta T = \text{Variación de la temperatura, medida en } [^\circ C] \\ \Delta t = \text{Duración de la exposición, medida en } [seg] \end{cases}$$

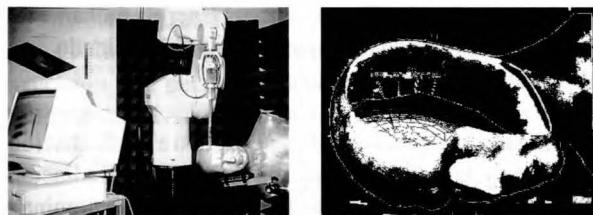


Figura 2.- Equipo de medición experimental (izq.) y distribución de la SAR (mW/g) medida con un equipo DASY2 (der.).

Lamentablemente, esta última expresión está restringida a asumir el hecho de que las medidas se realizan bajo unas condiciones ideales, no termodinámicas, situación en la que son despreciables los efectos por pérdidas de calor debidas a la difusión térmica, radiación de calor o termorregulación (factor este último de elevada importancia dado que la sangre actúa como elemento termorregulador natural del cuerpo humano).

Las ecuaciones anteriores son válidas para Campos Electromagnéticos con una variación temporal armónica y régimen permanente, como es el caso de la señal de excitación empleada en nuestro análisis. Las maneras de evaluar los parámetros establecidos para verificar la normativa de seguridad son varias. Así, nos encontramos con diferentes métodos numéricos (métodos analíticos y semianalíticos, método de los momentos, técnica generalizada de los multipolos, método de los elementos finitos, técnicas híbridas...) y experimentales (métodos térmicos, scánders automatizados y maniquíes de material dieléctrico).

1.3.- Normativa vigente

Por lo que respecta a la normativa vigente, al tratar de aspectos relativos a la seguridad de las personas es necesaria la definición de organismos reconocidos a nivel nacional e internacional, encargados de definir los límites o estándares a los que deben adaptarse los fabricantes de equipos de comunicaciones móviles.

En los EE.UU. la **Comisión Federal de Comunicaciones (FCC, Federal Communications Commission)** es el organismo responsable de regular el sector de las telecomunicaciones, salvedad hecha del Gobierno Federal, y tiene la potestad de dictaminar sus propias normas. Asimismo, la **Administración Nacional para la Información y las Telecomunicaciones (NTIA, National Telecommunications and Information Administration)** del **Departamento de Comercio** de los EE.UU. se encarga de la regulación y asignación del Espectro de Radio-Frecuencias.

Por lo que respecta a Europa, los organismos de estandarización oficialmente reconocidos son tres: el **Comité Europeo de Normalización, CEN**, el **Instituto de Normalización Europeo de Telecomunicaciones, ETSI**, y el **Comité Europeo de Normalización Electrónica, CENELEC**, el cual tiene competencia reguladora en el área de los equipos electrónicos.

Grupo II	ANSIC95.1-1992	BrEN50166-22	TTC/IMPT
	Extramo controlado	Trabajadores	Condición P
SAR promediada en todo el cuero	0.08 W/Kg	0.08 W/Kg	0.4 W/Kg
SAR valor máximo	1.6 W/Kg	2 W/Kg	8 W/Kg
Promedio Temporal	30 minutos	6 minutos	6 minutos
Promedio Espacial (volumen cúbico)	1 gr	10 gr	1 gr

Tabla 1.- Límites de exposición en los EE.UU., Europa i Japón.

ESTUDIO REALIZADO

Ante el interés que suscitaba un tema como éste, surgió la posibilidad de desarrollar un Proyecto Fin de Carrera que buscara obtener resultados clarificadores acerca de la medida de la **SAR** en diferentes condiciones de uso de un terminal móvil genérico.

Objetivos

Se partió de un estudio previo desarrollado en el mismo Departamento de Comunicaciones, y se intentó cumplir una serie de objetivos específicos:

- Definir un modelo numérico perfeccionado de cabeza del usuario y terminal móvil genérico que permitiera llevar a cabo diversas simulaciones para poder evaluar el cumplimiento de la normativa vigente en materia de **SAR**.

- Llevar a cabo una serie de simulaciones que permitieran diferenciar los principales factores de influencia a la hora de medir la **SAR**.
- Evaluar la posible conveniencia de utilizar diversas configuraciones específicas con materiales absorbentes que permitieran reducir los niveles de **SAR** obtenidos para la configuración más desfavorable, según los resultados de la primera serie de simulaciones.
- Analizar la posible degeneración que la utilización de materiales absorbentes podía introducir en las prestaciones del terminal móvil, para poder así garantizar que las estructuras absorbentes no imposibilitan la utilización del terminal en la red.
- Corroborar en la medida de lo posible los resultados numéricos con simulaciones en la Cámara Anecoica de la E.T.S.Enginyers de Telecomunicació de la Universitat Politècnica de València.
- Con todo, evaluar las prestaciones y adaptabilidad del paquete informático utilizado para realizar las diferentes simulaciones.

Paquete informático utilizado

Una de las opciones de las que dispone cualquier grupo investigador es la de hacer uso de utilidades de simulación capaces de resolver de manera numérica tanto la emisión como la inmunidad de gran variedad de dispositivos electrónicos, así como su efecto sobre el cuerpo humano. En nuestro caso, el paquete informático utilizado ha sido **MAFIA (Maxwell Finite Integration Algorithm)**. El porqué de la utilización de este tipo de aplicaciones radica en el hecho de que el análisis de dispositivos electrónicos complejos, o en general de problemas electromagnéticos complejos, requiere de fuertes inversiones tanto de dinero como de tiempo, necesarias para la construcción, medida y validación de los prototipos diseñados, y **MAFIA** era un paquete informático de prestaciones avaladas por más de 20 años de utilización.

Funcionalmente, **MAFIA** puede dividirse en tres bloques claramente diferenciables, denominados módulos, los cuales son: **PREPROCESADO o Módulo M, CÁLCULO o Módulo T3, y POSTPROCESADO o Módulo P**, si bien el bloque de cálculo está formado por diferentes módulos independientes entre sí, cada uno de los cuales está diseñado para abordar problemas específicos.

El denominado **Módulo M** se encarga de definir el modelo de simulación del problema en concreto, mediante la definición de una malla tridimensional donde se pueden definir formas y elementos caracterizados posteriormente por sus propiedades electromagnéticas. De entre todas sus características

podemos citar: la posibilidad de utilizar geometría cartesianas y cilíndricas en dos y tres dimensiones; amplia variedad de formas predefinidas; capacidad de simular planos, cables y filamentos; capacidad de generar estructuras complejas mediante operaciones lógicas entre formas predefinidas; capacidad de diferenciar entre 64 materiales diferentes; posibilidad de mallado automático y de posterior refinamiento de la malla...

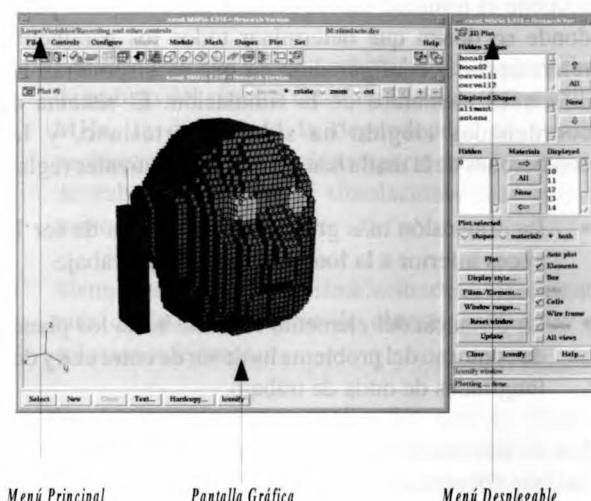


Figura 3.- Aplicación gráfica de usuario del simulador EM MAFIA 4.014

El denominado **Módulo T3** permite la resolución de las ecuaciones de Maxwell en el dominio temporal en tres dimensiones para un sistema coordenado cartesiano, permitiendo así el cálculo de los Parámetros de Dispersión de dispositivos de radiofrecuencia, y de Diagramas de Radiación de antenas. Las características propias de este módulo se pueden resumir en: posibilidad de trabajar con condiciones de contorno abiertas; definición de materiales con pérdidas; análisis de efectos superficiales; inclusión de diversas fuentes y señales de excitación...

El denominado **Módulo P** es el encargado del tratamiento de los datos obtenidos después de la ejecución del módulo de simulación. Permite al usuario el combinar los datos de los Campos Electromagnéticos para poder definir los parámetros específicos que le interesen, en nuestro caso se deberá definir tanto el Algoritmo de Ponderación, como el parámetro de **SAR**, el Coeficiente de Reflexión de la antena, su Impedancia de Entrada... Podemos resumir sus características como: posibilidad de trabajar con geometrías 2D y 3D, cartesianas y cilíndricas; utilización de operaciones matemáticas sobre los datos de los Campos Electromagnéticos; posibilidad de representación en 2D y 3D...



Modelo desarrollado y condiciones de simulación

Para poder utilizar **MAFIA**, se debe adecuar el problema electromagnético a las características del simulador, es decir, definir una estructura con un mallado adecuado, obtener los Campos Electromagnéticos y combinar los datos para obtener los parámetros deseados.

Para el **Módulo M** se han definido las tres estructuras más importantes de nuestro análisis: la cabeza del usuario, el terminal móvil bajo estudio, y la mano del usuario que sostiene el terminal móvil. Asimismo, es en este punto donde se tienen que determinar todos los parámetros referentes a la configuración en que se dispondrán los diferentes elementos de la simulación. El sistema de coordenadas elegido ha sido el cartesiano, y las condiciones de la malla han seguido las siguientes reglas:

- La dimensión más grande de la malla ha de ser 10 veces inferior a la longitud de onda de trabajo.
- La distancia del elemento radiante hasta los planos de contorno del problema ha de ser de entre una y dos longitudes de onda de trabajo.

Así, en función de la precisión requerida se ha hecho un mallado diferente de las estructuras (1.2 cm en las regiones exteriores, uniforme de 5 mm para el modelo de cabeza del usuario, y de 1.25 mm para la zona del terminal móvil).

El modelo de cabeza del usuario se ha definido con un total de 22 capas de 5 mm de grosor, situadas simétricamente en el plano YZ. La cabeza se sitúa en posición vertical sobre el plano XY, mirando hacia el semieje positivo Y. Sus dimensiones máximas son 15.5x21.5x21 cm. Las orejas se han modelado como una capa adicional a ambos lados del modelo de la cabeza.

Dentro del modelo de la cabeza del usuario se han definido las estructuras del cerebro, los ojos, el cráneo, los dientes, la médula espinal, la columna vertebral y las cavidades nasal, bucal y de la garganta.

El modelo de mano del usuario diferenciaba entre la estructura muscular de la misma y su estructura ósea interna.



Figura 4b.- Modelo numérico realizado para el terminal móvil con la mano.

En cuanto al modelo del terminal móvil, estaba formado por una caja metálica de dimensiones 1.04x4.68x12.45 cm en el caso de la antena monopolo y 2.25x4.25x12 cm para la antena impresa. En ambos casos, el terminal se ha colocado con sus dos caras mayores perpendiculares al eje X. De hecho, para poder simular la posición de uso habitual en la que el terminal quedaba inclinado, se procedió a girar la estructura de la cabeza del usuario puesto que los elementos de las antenas del terminal requerían de una definición muy precisa.

La antena monopolo se modeló mediante un filamento de longitud $\lambda/4$, y los primeros 5 mm actuaban como alimentación de la misma, definida la alimentación como un generador de corriente sinusoidal en paralelo de 100 mA de amplitud.

Finalmente, cada una de las estructuras absorbentes se han definido en torno al elemento radiante (antena monopolo) en la parte más próxima al modelo de cabeza del usuario. Las estructuras diseñadas han sido un semicilindro, un semicono y un sector angular de cilindro que cubriese completamente la zona del modelo de la cabeza del usuario expuesta a la antena.

El **Módulo T3** no incluía grandes variaciones, diferenciando entre la excitación sinusoidal de las simulaciones de cálculo de los niveles de **SAR**, y la excitación del pulso de señal para simular el comportamiento frecuencial del Coeficiente de Reflexión y la Impedancia de Entrada (tan sólo obtenida para simulaciones con la antena monopolo).

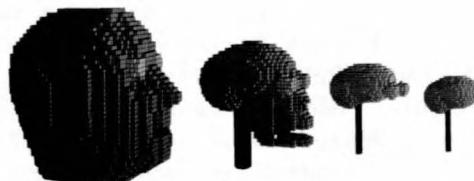


Figura 4a.- Modelo numérico realizado para la cabeza del usuario .



Figura 5a.- Modelo numérico realizado para la antena impresa.

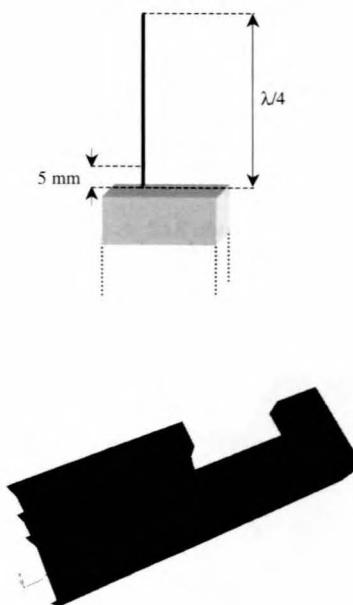


Figura 5b.- Modelo numérico realizado para el terminal móvil con la antena monopolo .

El **Módulo P** extraía las componentes real e imaginaria del Campo Eléctrico en el interior de cada uno de los tejidos, y con él la potencia absorbida por el tejido en concreto. En la antena y gracias a monitorizar la tensión y la corriente en la misma, obtenemos el valor de la potencia radiada, así como el Coeficiente de Reflexión y la Impedancia de Entrada en el caso de las antenas monopolo. Finalmente, se ha desarrollado diversos algoritmos específicos de promediado de forma cúbica, tal y como exige la normativa, para 1gr. y 10 gr. de masa, a fin de poder comparar los resultados obtenidos con los límites exigidos. Este último paso no ha sido muy fácil dada la diferente densidad de cada tejido analizado y la definición de malla uniforme del modelo de cabeza del usuario.

RESULTADOS OBTENIDOS

Se presentan a continuación los resultados obtenidos en las diferentes simulaciones realizadas, teniendo siempre presente que las conclusiones a las que se ha llegado no se pueden tomar como definitivas, sino más bien como complementarias al conjunto de estudios realizados sobre el tema.

Los criterios seguidos en las simulaciones se pueden resumir como sigue:

- Las simulaciones se han hecho a las dos frecuencias de trabajo del sistema GSM en Europa: 900 y 1800 MHz, la que, dada la dependencia de varios parámetros de la simulación respecto de la frecuencia de trabajo, hace que las simulaciones sean más o menos largas en el tiempo.
- Siempre se han hecho las simulaciones en el supuesto más desfavorable, a fin de obtener respuestas y soluciones idóneas.
- En las simulaciones realizadas con la antena monopolo, se procedió a identificar parámetros de operatividad de la misma (Coeficiente de Reflexión e Impedancia de Entrada).

Variables de influencia en la estima de la SAR

Las simulaciones se han centrado en evaluar la influencia de diversos parámetros modificables en las mismas. Estos parámetros han sido: la frecuencia de trabajo, el grado de complejidad del modelo (en cuanto a la cantidad de tejidos diferenciados en el mismo), la presencia o no de la mano del usuario en el modelo, la posición de uso del terminal móvil, la distancia de separación entre el terminal y el modelo de cabeza del usuario, y la presencia de paredes (modeladas como paredes metálicas) próximas al modelo de simulación.

Tejido	Frecuencia 900 MHz		Frecuencia 1800 MHz		ρ (Kg/m ³)
	ϵ	σ (S/m)	ϵ	σ (S/m)	
Cartílago	42.6531	0.7823	40.2155	1.2868	1100
Cerebro	45.8055	0.7665	43.5449	1.1531	1080
Columna Vertebral	16.6208	0.2416	15.5620	0.4317	1850
Cráneo	16.6208	0.2416	15.5620	0.4317	1850
Dientes	16.6208	0.2416	15.5620	0.4317	1850
Hueso (Mano)	20.7878	0.3400	19.3422	0.5882	1800
Médula Espinal	32.5310	0.3736	30.8669	0.8428	1000
Músculo	55.9555	0.9691	54.4423	1.3894	1040
Ojos (Humor Vítreo)	69.9018	1.6362	68.5734	2.0325	1010

Tabla 2.- Propiedades de los materiales dieléctricos empleados en el modelo numérico de simulación.



Tejido	$SAR_{Max} (W/Kg)$			$SAR_{Avg} (W/Kg)$			$SAR_{Total} (W/Kg)$		
	Modelo cabeza	Modelo de mano	Posición de uso	Modelo cabeza	Modelo de mano	Posición de uso	Modelo cabeza	Modelo de mano	Posición de uso
Cartil.	9.20233	8.95176	9.16584	7.47741	9.43866	6.46968	6.26696	6.53748	5.93108
Cereb.	0.20575	0.19786	0.11449	0.14398	0.14117	0.07463	0.14663	0.13981	0.07937
Músc.	8.01920	8.56886	5.78956	6.01093	6.55297	5.49797	4.01663	4.31715	3.69895
Ojos	0.00469	0.01011	0.00280	0.00242	0.00526	0.00153	0.00270	0.00588	0.00172

Tabla 3.- Valores de SAR obtenidos en el modelo simple (sólo cuatro tejidos diferenciados). Frecuencia de trabajo 1800 MHz.

Las principales conclusiones a las que nos permitieron llegar las simulaciones se pueden resumir en:

- La antena monopolo se caracteriza por una elevada penetración de los Campos Electromagnéticos en el interior de los tejidos humanos próximos.
- Los niveles de **SAR** obtenidos a frecuencias más elevadas, son más elevados.
- La influencia del grado de complejidad del modelo utilizado en las diferentes simulaciones, así como la presencia o no de la mano del usuario, no introducen grandes variaciones en los resultados.
- La posición de uso del terminal móvil reduce en varias unidades los niveles de **SAR** obtenidos en los promediados, y aparece como un parámetro muy importante a la hora de realizar las simulaciones. Esta reducción es comprensible si se tiene en cuenta que el hecho de girar el terminal aleja la antena de los tejidos de la cabeza del usuario. El efecto es más notable a menor frecuencia de trabajo (antena más larga).
- La separación del terminal móvil influye proporcionalmente en la reducción de los niveles de **SAR**.
- La proximidad de paredes en torno al usuario es más negativa (aumentan los niveles de **SAR**) cuanto más grande es.

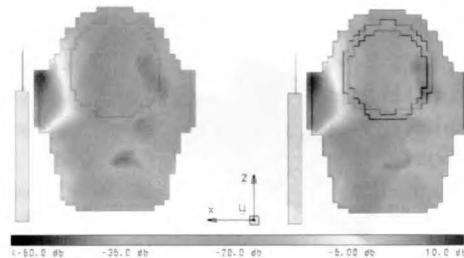


Figura 6b.- Distribución gráfica de la SAR con el modelo simple (cuatro tejidos diferenciados) i complejo (nueve tejidos diferenciados) obtenida para 1800 MHz.

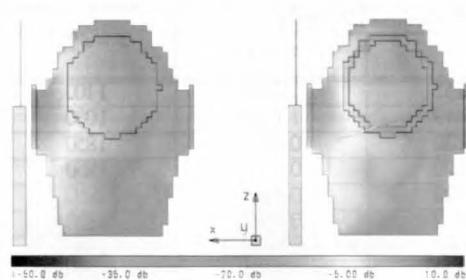


Figura 6a.- Distribución gráfica de la SAR con el modelo simple (cuatro tejidos diferenciados) i complejo (nueve tejidos diferenciados) obtenida para 900 MHz.

Utilización de elementos absorbentes I

El primer intento para minimizar los niveles de **SAR** fue intentar acoplar estructuras absorbentes en torno a la antena monopolo. En las dos frecuencias de análisis se utilizó un material de constante dieléctrica $\epsilon_r = 1-0.1j$, y las estructuras dieléctricas empleadas fueron las citadas anteriormente (semicilindro, semicono y sector angular de cilindro). Un segundo parámetro que podía variarse en las simulaciones para buscar la reducción de la **SAR** fue el separar parcialmente las estructuras absorbentes del elemento radiante (una distancia de 2 mm). Los resultados obtenidos se muestran en la Tabla 4.

Las principales conclusiones a las que se llegó se pueden resumir en:

- La degradación de las propiedades de la antena es mayor cuando las frecuencias de trabajo son inferiores.
- A una frecuencia de 900 MHz los efectos de la reducción de los niveles de **SAR** son mínimos, y se pierde potencia radiada por la antena.
- A una frecuencia de 1800 MHz se consigue una reducción de los niveles de **SAR**, pero insuficiente.
- De las tres configuraciones diseñadas, fue la de semicilindro la que ofreció unos mejores resultados.

Tejido	Frecuencia 900 MHz						Frecuencia 1800 MHz					
	SAR_{900} (W/Kg)		SAR_{1800} (W/Kg)		SAR_{1800} (W/Kg)		SAR_{900} (W/Kg)		SAR_{1800} (W/Kg)		SAR_{1800} (W/Kg)	
	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.
Cart.	5.3413	5.7654	4.5200	4.7718	4.0248	4.3573	6.9452	7.6343	5.5934	6.3230	4.8228	5.3001
Cereb.	0.7034	0.7614	0.4914	0.5320	0.6000	0.7144	0.1668	0.1832	0.1174	0.1289	0.1191	0.1307
Músc.	5.9751	6.4923	4.2801	4.7049	3.6282	3.9254	6.3858	7.0222	4.6296	5.0818	3.1177	3.4257
Ojos	0.0375	0.0407	0.0158	0.0172	0.0182	0.0197	0.0038	0.0042	0.0019	0.0021	0.0021	0.0024

Tabla 4.- Valores de SAR obtenidos para el modelo simple (sólo cuatro tejidos diferenciados) con la configuración de elementos absorbentes I, estructura de semicilindro.

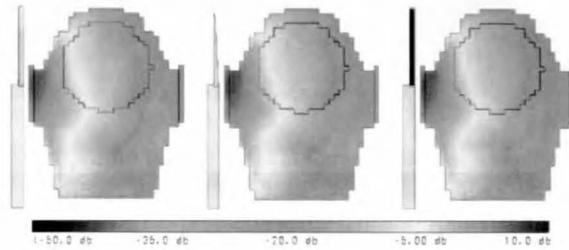


Figura 7a.- Distribución gráfica de la SAR en el modelo simple (cuatro tejidos diferenciados) obtenida a 900 MHz con la configuración de materiales absorbentes I (semicilindro, semicono y sector angular de cilindro).

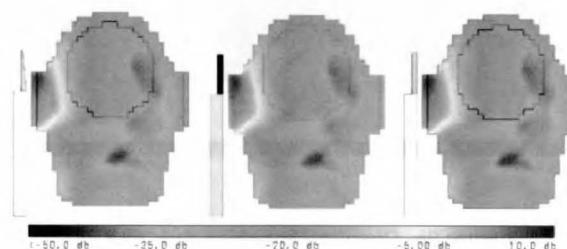


Figura 7b.- Distribución gráfica de la SAR en el modelo simple (cuatro tejidos diferenciados) obtenida a 1800 MHz, con la configuración de materiales absorbentes I (semicilindro, semicono y sector angular de cilindro).

Utilización de elementos absorbentes II

En el segundo intento de utilización de estructuras absorbentes, se mantuvieron tanto las estructuras como la variación de la distancia de separación, pero se emplearon materiales dieléctricos diferentes según la frecuencia de trabajo. Así, a 900 MHz se utilizó un material caracterizado por $\epsilon_r = 10\text{-}5j$, y a 1800 MHz por $\epsilon_r = 10\text{-}10j$. Los resultados obtenidos para la estructura de semicilindro fueron los mostrados en la Tabla 5.

Las principales conclusiones a las que se llegó son prácticamente idénticas a las de la serie de simulaciones anterior. Pese a la reducción de los niveles de SAR a 900 MHz era significativa, la degradación de las propiedades de la antena la hacían prácticamente inservible.

Utilización de elementos parásitos

Para poder evitar la utilización de elementos absorbentes, se pensó en la posibilidad de colocar elementos parásitos que permitieran conformar el Diagrama de Radiación, minimizando la incidencia de radiación en los tejidos de la cabeza del usuario. Así, se utilizaron configuraciones de un monopolo parásito, dos monopolos parásitos equidistantes, y una plancha de metal de un grosor mínimo, todos ellos situados entre la antena y el modelo de cabeza. Los resultados obtenidos a la frecuencia de 1800 MHz fueron los que se muestran en la Tabla 6.

Tejido	Frecuencia 900 MHz						Frecuencia 1800 MHz					
	SAR_{900} (W/Kg)		SAR_{1800} (W/Kg)		SAR_{1800} (W/Kg)		SAR_{900} (W/Kg)		SAR_{1800} (W/Kg)		SAR_{1800} (W/Kg)	
	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.	Separ.
Cart.	2.2846	6.1531	1.5115	5.2634	1.5284	4.6617	4.0551	1.6490	2.1861	0.7054	1.7011	1.0257
Cereb.	0.2807	0.8149	0.1873	0.6940	0.2565	0.7665	0.0833	0.0831	0.5359	0.0532	0.0655	0.0665
Músc.	1.9548	6.9353	1.4062	4.9208	1.3261	4.1822	2.6889	1.8519	1.4857	0.8917	0.9345	0.6248
Ojos	0.0151	0.0428	0.0064	0.0181	0.0076	0.0208	0.0044	0.0053	0.0021	0.0023	0.0025	0.0028

Tabla 5.- Valores de SAR obtenidos para el modelo simple (sólo cuatro tejidos diferenciados) con la configuración de elementos absorbentes II, estructura de semicilindro.



Tejido	$SAR_{Max} (W/Kg)$			$SAR_{Avg} (W/Kg)$			$SAR_{Vary} (W/Kg)$		
	Monop. Parásito	Doble Monop.	Plancha	Monop. Parásito	Doble Monop.	Plancha	Monop. Parásito	Doble Monop.	Plancha
Cartil.	5.70142	2.82827	1.98333	4.00994	1.85386	1.23475	2.67467	1.4374	1.02481
Cereb.	0.04941	0.04638	0.02792	0.02836	0.02797	0.01637	0.03446	0.03475	0.01912
Músc.	2.53015	2.0521	1.45594	1.80749	0.00805	0.84921	1.2802	0.84559	0.56098
Ojos	0.01028	0.00997	0.00575	0.00524	0.00215	0.00294	0.00566	0.00556	0.00319

Tabla 6.- Valores de SAR obtenidos para el modelo simple (sólo cuatro tejidos diferenciados) con la configuración de elementos parásitos.

Las principales conclusiones a las que se llegó se pueden resumir en:

- Se produce una reducción interesante de los niveles de SAR.
- El comportamiento del elemento parásito degradó notablemente las prestaciones de la antena, desapareciendo incluso la sintonía en frecuencia, y reduciéndose las propiedades de radiación de la misma.

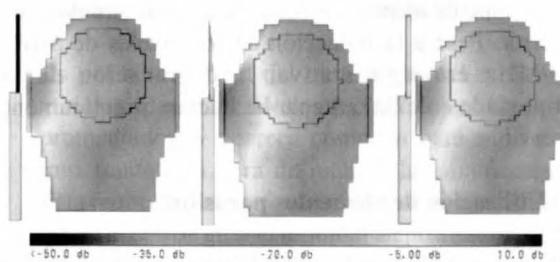


Figura 8a- Distribución gráfica de la SAR en el modelo simple (cuatro tejidos diferenciados) obtenida a 900 MHz, con la configuración de materiales absorbentes II (semicilindro, semicono y sector angular de cilindro).

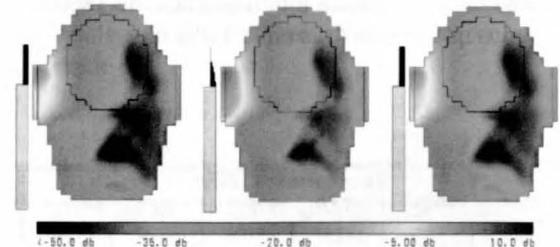


Figura 8b- Distribución gráfica de la SAR en el modelo simple (cuatro tejidos diferenciados) obtenida a 1800 MHz, con la configuración de materiales absorbentes II (semicilindro, semicono y sector angular de cilindro).

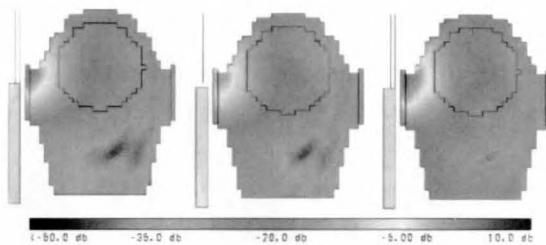


Figura 9a- Distribución gráfica de la SAR en el modelo simple (cuatro tejidos diferenciados) obtenida a 900 MHz, con la configuración de elementos parásitos.

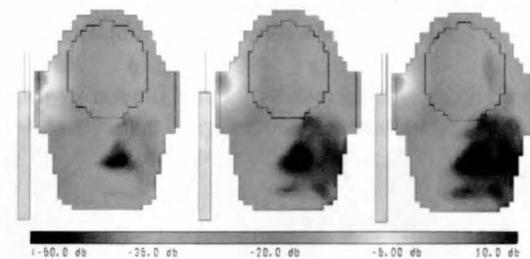


Figura 9b- Distribución gráfica de la SAR en el modelo simple (cuatro tejidos diferenciados) obtenida a 1800 MHz, con la configuración de elementos parásitos.

Utilización de antenas impresas

Cada vez más aparecen terminales con antenas del tipo *microstrip*, integradas en los terminales móviles. Es por ello que el estudio de este tipo de antenas y su comparación en términos de SAR se hace evidente. Así, se implementó un modelo de antena impresa publicado por I.E.E.E., específicamente diseñada para su funcionamiento a 1800 MHz, con dos variantes operativas: *Single Patch* y *Stacked Patch*. Las simulaciones se realizaron con el terminal móvil en posición de uso habitual (girado), y sus dimensiones se ajustaron a las indicadas en la propia publicación. Los resultados obtenidos se muestran en la Tabla 7.

Tejido	$SAR_{Max} (W/Kg)$			$SAR_{Avg} (W/Kg)$			$SAR_{Min} (W/Kg)$		
	Monop.	Single Patch	Stacked Patch	Monop.	Single Patch	Stacked Patch	Monop.	Single Patch	Stacked Patch
Cartil.	2.03254	0.32471	0.11572	1.45937	0.19809	0.07587	1.36504	0.25020	0.09719
Cereb.	0.13888	0.01789	0.00845	0.05533	0.00789	0.00338	0.07193	0.01057	0.00474
Músc.	2.46007	0.48680	0.15851	1.39936	0.16277	0.06472	1.17661	0.18111	0.07472
Ojos	0.00161	0.00278	0.00094	0.00081	0.00128	0.00041	0.00074	0.00143	0.00048

Tabla 7.- Valores de **SAR** obtenidos para el modelo simple (sólo cuatro tejidos diferenciados) con la configuración de antena impresa.

Les principales conclusiones a las que se llegó se pueden resumir en:

- La reducción de los niveles de **SAR** es muy significativa (de hasta un 80 %).
- El propio diseño de la antena disuade al usuario de sostener el terminal obstruyéndola, lo que permite conservar sus propiedades de radiación prácticamente intactas.
- Su eficiencia es muy elevada (entre un 60% y un 80%).

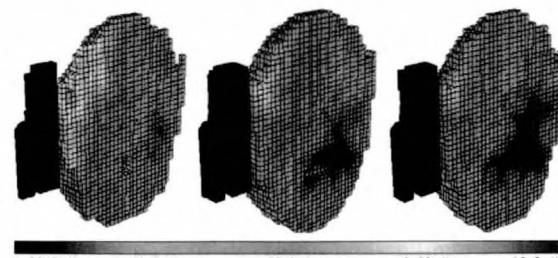
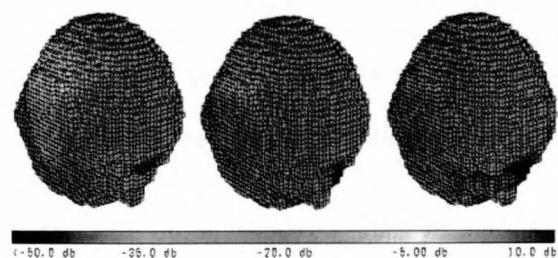


Figura 10- Distribución gráfica de la **SAR** en el modelo simple (cuatro tejidos diferenciados) obtenida a 1800 MHz con las configuraciones de antena monopolo, antena impresa “single patch”.

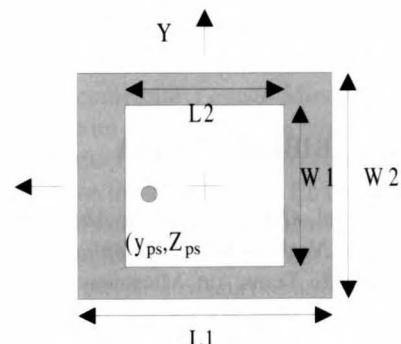
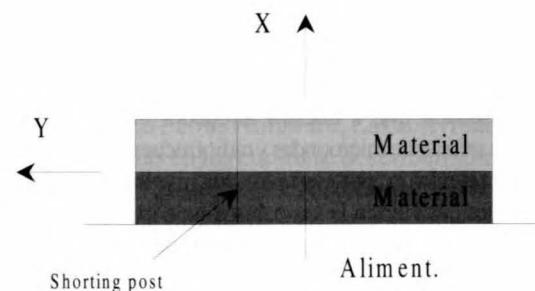


Figura 11- Esquemático genérico de las antenas impresas utilizadas.

Simulaciones en laboratorio

Se construyó un modelo simple de terminal móvil y se realizaron medidas de niveles de Campo Eléctrico en las cuatro direcciones principales del mismo tanto para la antena libre (sin absorbentes), como rodeada parcialmente (semicilindro) con diferentes materiales absorbentes disponibles. Los equipos de que se disponía sólo permitían obtener niveles de potencia recibida, y se confirmó la reducción de ésta según nuestra intención, pero fue imposible obtener niveles de **SAR** sobre un modelo, dado lo caro de este tipo de equipos.

CONCLUSIONES FINALES

La necesidad de dar respuesta a las dudas que los nuevos avances tecnológicos sugieren a sus usuarios es una condición paralela al ansia de superación tecnológica del sector. Son muchas las noticias, en la mayor parte de los casos contradictorias y confusas, relativas a los peligros que los Sistemas de Comunicaciones Móviles implican para la salud de los consumidores, y es obligación del ingeniero los máximos niveles de seguridad de estos sistemas.

Es por eso que se hace necesario disponer de estudios comparativos que puedan resumir en la manera de lo posible la situación de las diferentes investigaciones al respecto. La normativa a aplicar y los resultados y conclusiones más comunes.

Tan sólo señalar que a nuestro alrededor el mundo está plagado de señales de microondas y radiofrecuencia(emisoras de radio y televisión, por ejemplo), los niveles de potencia de las cuales convierten la contribución de los Sistemas de Comunicaciones Móviles prácticamente despreciable.

Hasta la fecha no existe ningún estudio reconocido que deje probada la existencia de efectos negativos serios para la salud humana a largo plazo. La confianza general de los usuarios y de los fabricantes respecto del uso de los terminales móviles y estaciones base debería, pues, ser cada vez mayor.

BIBLIOGRAFÍA

- [1] Gandhi, P. et al, «*Electromagnetic Absorption in the Human Head and Neck for Mobile Telephones at 835 and 1900 MHz*», IEEE Trans. on Microwave Theory and Techniques, October 1996, vol. 44, No. 10, pp. 1884-1897
- [2] Gandhi, P. et al, «*Comparison of Numerical and Experimental Methods for Determination of SAR and Radiation Patterns of Handheld Wireless Telephones*», Bioelectromagnetics, 1999, vol. 20, pp. 93-101.
- [3] Martínez González, A. M., «*Evaluación de la interacción electromagnética entre los radioteléfonos y el tejido humano para nuevos sistemas de comunicaciones móviles*», Septiembre 1998, ETSIT, U.P.V.
- [4] Watanabe, S. et al, «*Characteristics of the SAR Distributions in a Head Exposed to Electromagnetic Fields Radiated by a Hand-held Portable Radio*», IEEE Transactions on Microwave Theory and Techniques, October 1996, vol. 44, No. 10, pp.1874-1883.
- [5] C. Gabriel, «*Compilation of the dielectric properties of body tissues at microwave frequencies.*» Brook Air Force Technical Report AL/OE-TR-1996-0037.
- [6] J.T. Rowley, R.B. Waterhouse, «*Performance of shorted microstrip patch antennas for mobile communications handsets at 1800 MHz.*» IEEE Trans. Antennas and Prop., vol. MAP-47, no. 5, pp. 815-822, May 1999.

AUTOR



Nacido en Alcoy, provincia de Alicante, el 28 de Enero de 1.973. Hizo sus estudios de EGB, BUP y COU en esta ciudad, obteniendo el *Premio al mejor Expediente Académico* durante su estancia en el Instituto de Bachillerato. Titulado como Ingeniero el 18 de Julio de 2.000 por la *Escola Tècnica Superior d'Enginyers de Telecomunicació* de la *Universitat Politècnica de València* con *Proyecto Fin de Carrera* sobre "*DISEÑO Y ANÁLISIS DE ESTRUCTURAS ABSORBENTES PARA LA REDUCCIÓN DE LA RADIAZIÓN DE LOS TELÉFONOS MÓVILES HACIA EL USUARIO*", calificado con *Matrícula de Honor, 10*. Ha participado en diversos cursos de formación convocados por la *U.P.V.* y la *Rama IEEE* de Valencia, centrados en temas de Redes de Comunicaciones Móviles, Redes de Comunicaciones y otros convocados por el *Col·legi Oficial d'Enginyers de Telecomunicació*.

Gracias a la realización de su P.F.C. ha estado galardonado con: el *Premio NOKIA al Mejor Proyecto Fin de Carrera en Internet Móvil y Soluciones Móviles de Tercera Generación* otorgado por el *Col·legi Oficial d'Enginyers de Telecomunicació* en su *XXI Edición*; y *Premio al Mejor Proyecto Fin de Carrera en Redes de Comunicaciones Móviles* otorgado por el *Aula NORTEL Networks* en la *E.T.S.E.T. – U.P.V.*

Asimismo, es autor y coautor de diversos artículos aceptados en congresos y publicaciones técnicas: Reducción de la radiación de los teléfonos móviles hacia el usuario (*TELEC-2000 International Conference*); Estudio de diversas soluciones para la reducción de la radiación procedente de los teléfonos móviles hacia el usuario, (*National URSI Symposium*, Zaragoza, Spain, Sept. 2000); *Analysis of Proposals to Reduce SAR Levels from GSM Terminals* (*IEEE International Microwave Symposium 2001*); *Proposals for Reducing SAR Levels from GSM Mobile Phones* (Pendiente de su revisión y aceptación por la *IEE Electronic Letters.*); Exposición Humana a Campos Electromagnéticos procedentes de Terminales MÓVILES GSM (*XI Jornadas Telecom I+D 2001*); *Evaluation and proposals to reduce SAR levels from GSM terminals* (Pendiente de presentación para la *XXVIIth General Assembly* de la *Unió Científica Internacional de Ràdio URSI*).

Actualmente trabaja en el *Centro I+D de Ericsson España* en Madrid, dentro de la *Unidad TD/MFE* centrada en el diseño de nodos para las redes *GSM / GPRS / UMTS*, desarrollando aplicaciones propietarias en lenguaje Java.



DOCENCIA EN ROBÓTICA MÓVIL

Antonio Falcón Martel¹, Oscar Déniz Suárez²

¹Catedrático de Ciencias de la Computación e Inteligencia Artificial

²Licenciado en Informática. Estudiante de doctorado

Universidad de Las Palmas de Gran Canaria.

Resumen.- Cada vez son más las posibilidades y recursos con los que cuenta el profesorado universitario para impartir conocimientos en temas de contenido disciplinar en continua fase de cambio y adaptación como es el caso de la Robótica Móvil. Son ya muy pocos los centros que no disponen de alguna plataforma móvil más o menos elaborada. En este trabajo presentamos las experiencias derivadas de la impartición de dos cursos de robótica móvil, uno de ellos desarrollado en un ámbito no universitario. En particular, se describen y analizan las posibilidades y limitaciones de dos productos hardware, el kit Lego®

MindStorms y la plataforma Pioneer 2-DX de ActivMedia Robotics, así como uno software, el entorno Saphira, utilizados en el contexto de las actividades prácticas de los mencionados cursos.

1.- INTRODUCCIÓN

En los últimos tiempos ha aumentado significativamente el número de recursos a la disposición del profesorado universitario para el desempeño de las actividades prácticas asociadas a los contenidos teóricos. En el caso de la robótica móvil, muchos centros cuentan ya con plataformas de diseño relativamente elaborado. Estos recursos, antes dedicados casi exclusivamente a tareas de investigación, de forma natural pueden ahora utilizarse en la propia docencia, la cual mejora en calidad.

En este trabajo se exponen las experiencias e ideas extraídas a raíz de la impartición por los autores de dos cursos de Robótica Móvil. Uno de los cursos constituye la asignatura “Sistemas Robóticos Móviles” de la titulación de Ingeniería Informática, en la Universidad de Las Palmas de Gran Canaria, la cual tiene carácter optativo en cuarto curso de carrera [1]. El otro, que contó con la colaboración de la Consejería de Educación, Cultura y Deportes del Gobierno de Canarias y el Museo Elder de la Ciencia y la Tecnología, se impartió a profesores de enseñanza secundaria con el fin de iniciar la introducción de la robótica móvil en la Enseñanza Secundaria Obligatoria (la concepción de este curso seminal tiene como origen trasladar conceptos, principios e ideas a los niveles inferiores del sistema educativo de forma que se generen aptitudes y vocaciones en el ámbito de la Robótica Móvil).

En primer lugar se describirá y analizará las posibilidades del producto Lego® Mindstorms (Lego es una marca registrada del grupo LEGO.) en el contexto reseñado. Seguidamente indicaremos diversas posibilidades de ampliación del producto estándar, tanto a nivel hardware como software. Las actividades prácticas propuestas en los cursos se describen someramente en la sección de Prácticas. A continuación se analizará el entorno Saphira de desarrollo y simulación de aplicaciones de robótica móvil, así como la plataforma móvil Pioneer de ActivMedia Robotics, a la hora de estudiar experimentalmente sistemas basados en comportamientos. Por último, resumiremos las conclusiones más importantes alcanzadas.

2.- LEGO® MINDSTORMS

El producto comercial Lego® Mindstorms [2]-[5] se presenta como un juguete de coste relativamente medio-alto. El producto responde a las expectativas creadas en este mercado en los últimos años. En un contexto menos lúdico, las características del mismo permiten aplicar hasta cierto punto aspectos prácticos de la robótica móvil, lo cual lo convierte en una herramienta atractiva para la docencia. Prueba de ello son los diversos centros que ya hacen uso de él [6]-[10].

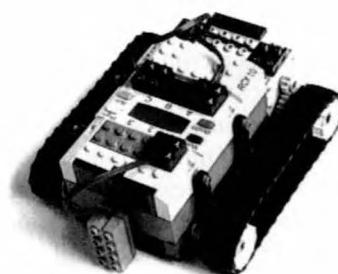


Figura 1. plataforma móvil simple con los sensores del kit.

El elemento central de Lego® Mindstorms es el llamado RCX, que contiene el microcontrolador. El RCX se alimenta con pilas, y alrededor de él se construye el robot con piezas Lego® tradicionales. El RCX dispone de tres



salidas PWM y de 3 entradas a las cuales podemos conectar diversos sensores, incluyendo el kit dos sensores de contacto y un sensor de infrarrojos. El RCX dispone también de un elemento de comunicación por infrarrojos. Lo abierto de las posibilidades de diseño hacen este kit particularmente atractivo. En la siguiente figura se puede ver un ejemplo de plataforma móvil simple con los sensores del kit.

Lego® Mindstorms es un producto versátil basado en el microcontrolador H8/3292. Aunque con ciertas limitaciones en la programación y el hardware accesible externamente, representa una evolución de conceptos similares utilizados con anterioridad, como es el caso del Brick desarrollado en el MIT [11]. La programación del RCX se realiza en un PC. El programa binario se transfiere al RCX mediante una torre emisora/receptora de infrarrojos, que se conecta a un puerto serie. El producto se entrega con un CDROM que contiene dos entornos de programación distintos.

Al utilizar pilas, el robot es autónomo, y puede comunicarse por infrarrojos con el PC o con otro robot.

Uno de ellos es enormemente sencillo, pues permite diseñar el programa en base a bloques gráficos. Sin embargo, para ciertas aplicaciones resulta más flexible programar en el lenguaje NQC [12]. NQC es un lenguaje de sintaxis sencilla, similar al C, que cuenta con un excelente editor, el RCX Command Center [13]. La mayoría de las limitaciones del lenguaje vienen impuestas por el propio hardware del RCX. Entre ellas hay que destacar la falta de números en coma flotante (las únicas variables que existen son los enteros de 16 bits con signo). Además, solo se permite usar un máximo de 32 variables. Por otro lado, la sencillez del lenguaje permite implementar fácilmente comportamientos reactivos básicos. También se puede hacer uso de multitarea, lo cual facilita enormemente la escritura de ciertas aplicaciones de naturaleza muy reactiva [14]. Al utilizar pilas, el robot es autónomo, y puede comunicarse por infrarrojos con el PC o con otro robot. Esto último permite la posibilidad de implementar estrategias básicas de comportamientos de grupo [15]-[16], o de realizar la computación en el PC. Existe un control OCX que puede utilizarse con los lenguajes de programación visual más comunes para comunicarse directamente con el RCX. El sensor de infrarrojos permite implementar aplicaciones sencillas e ilustrativas como seguimiento de líneas, búsqueda de zonas iluminadas o, utilizado conjuntamente con la ventana de comunicación por infrarrojos del RCX, construir un detector de obstáculos.

A pesar de las limitaciones indicadas, creemos que el producto es apropiado para el desarrollo de una parte de

las actividades prácticas asociadas a los contenidos teóricos de una asignatura de introducción a la robótica móvil. Una de las mayores ventajas del producto la representan sus posibilidades de ampliación.

3.- POSIBILIDADES DE AMPLIACIÓN

Las posibilidades de ampliación del Lego® Mindstorms son sustanciosas, lo cual ha sido uno de los factores determinantes a la hora de considerarlo positivamente.

Existen numerosas ampliaciones al hardware del RCX que puede construirse uno mismo, entre las que se incluyen diseños para sensores de rotación, temperatura, etc..

Hardware

Las posibilidades de ampliación hardware podemos dividirlas en dos: productos comerciales de Lego® y ampliaciones de tipo “hágalo usted mismo”. De un lado se dispone del *Ultimate Accessory Kit* de Lego®. Este producto contiene un sensor de rotación de 16 pasos por vuelta (que pueden convertirse en más según la relación de engranajes que se utilicen), un mando a distancia, un sensor de contacto y piezas adicionales. Con sensores de rotación, que también pueden adquirirse por separado, es posible realizar aplicaciones con realimentación del movimiento (“cerrar el bucle”), así como poner en práctica nociones básicas de odometría para una plataforma diferencial. En particular, una de las prácticas asignadas en el curso consiste en realizar el experimento del cuadrado bidireccional [17] y comprobar la reducción de los errores de odometría. Otro producto Lego® de expansión lo constituye el *Vision Command*. Este producto incluye una cámara USB que puede captar secuencias a 30 frames por segundo. Con *Vision Command* pueden ponerse en práctica aplicaciones básicas de visión artificial, como detección de zonas de color, etc [18]. No obstante, su uso parece no estar muy extendido aún, y la calidad del proceso es en ciertos aspectos deficiente, en comparación con otros productos de bajo coste en el mercado.

Existen numerosas ampliaciones al hardware del RCX que puede construirse uno mismo, entre las que se inclu-

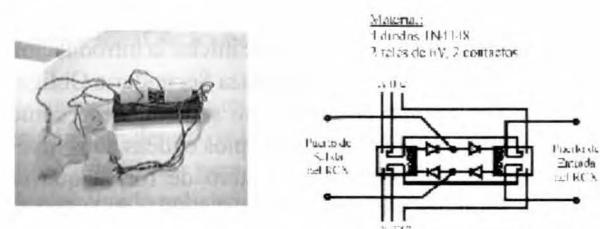


Figura 2. Esquema del multiplexor.

yen diseños para sensores de rotación, temperatura, etc.. Una de las limitaciones del RCX, el tener solo 3 puertos de entrada, puede evitarse fácilmente de varias formas. Una posibilidad es conectar más de un sensor de contacto al mismo puerto de entrada, e incluso conectar un sensor de luz y uno de contacto a un puerto. Para más sensores, existen varias alternativas, como la de construir un multiplexor en el tiempo, como el que mostramos en la figura siguiente. Su funcionamiento se basa en la utilización de uno de los puertos de salida del RCX, y en la capacidad de éstos de adoptar tres estados distintos: polaridad directa, inversa, y desconectado. Con este simple diseño se pueden conectar hasta tres sensores distintos a una entrada del RCX. Cambiando periódicamente el estado del puerto de salida se consigue conectar los distintos sensores al puerto de entrada. Se ha creado un programa para LegOS (ver más adelante) que controla el multiplexor [19]. El multiplexor expuesto destaca por su simplicidad de montaje y bajo coste.

Software

Al igual que en el caso de ampliaciones hardware, existe una gran variedad de herramientas software adicionales, la mayoría de ellas de libre distribución. Es destacable la gran variedad de lenguajes de programación que pueden utilizarse: FORTH, Smalltalk, Java, etc. También hay que destacar la gran cantidad de programas ejemplo y aplicaciones disponibles en código fuente.

Probablemente el esfuerzo más importante de ampliación software del RCX es LegOS [20]. LegOS es un sistema operativo para el RCX, diferente del original de Lego®. La programación para LegOS se realiza en C estándar. Muchas de las limitaciones anteriormente mencionadas desaparecen en LegOS. Entre sus características más atractivas cabe destacar: números en coma flotante, número no limitado de variables, semáforos POSIX y un mayor control sobre el hardware del RCX. Con LegOS se ha podido realizar aplicaciones de control con redes neuronales sencillas. La desventaja fundamental de LegOS estriba en que no es aún un producto muy elaborado, lo cual hace que puedan encontrarse "bugs".

Prácticas diseñadas

En el contexto de los cursos reseñados, el diseño de las prácticas con el kit Lego® Mindstorms se orientó a alumnos cuyos conocimientos en cinemática y dinámica son escasos. Las actividades prácticas diseñadas fueron las siguientes:

- Construcción de un vehículo tipo tanque con dos sensores de contacto y uno de luz y desarrollo de un programa NQC para seguimiento de líneas y evitación de obstáculos. Se construye un circuito con cinta adhesiva negra.
- Desarrollo de un programa NQC que ante la detección de un obstáculo asuma que se ha colisionado con otro

robot e inicie un intercambio de mensajes a través del puerto IR para establecer un protocolo de continuación de movimientos.

- Desarrollo de un programa en NQC o para LegOS para hacer que el robot se acerque a una fuente luminosa, a la vez que evite obstáculos.
- Desarrollo de un vehículo de Braitenberg [21] que cumpla los requisitos de la práctica anterior. La computación necesaria se realiza mediante un perceptrón.
- Realización del test del cuadrado bidireccional. El test permite corregir errores de odometría sistemáticos. En este caso se hace uso de los sensores de rotación ya mencionados, uno por cada rueda.

Con el fin de ilustrar la diferencia entre robots móviles con ruedas y robots con patas, en el curso impartido a profesores de enseñanza secundaria se construyó un robot móvil con 6 patas no independientes. El diseño de este robot puede consultarse en [22]. Con respecto a las prácticas en la asignatura "Sistemas Robóticos Móviles", se formaron 5 grupos, cada uno compuesto de 4 alumnos. Cada grupo se hizo cargo de un kit, responsabilizándose (a principios de curso) por escrito de cuidar todas sus piezas y las pilas entregadas. Es necesario señalar que, si bien son comparativamente más caras, las pilas recargables resultan imprescindibles. La actividad práctica de la asignatura correspondía a un total de 30 horas, a razón de dos horas semanales. Las únicas características requeridas por el laboratorio son ordenadores PC con un puerto serie libre, mesas amplias y cargadores de pilas.

Los criterios de evaluación utilizados en la asignatura fueron:

- Un cuaderno de experimentos, donde se recojan los diseños, planteamientos, problemas y estrategias adoptadas, con un recorrido cronológico de la actividad realizada.
- Vídeo explicativo que muestre el funcionamiento correcto del robot móvil según las prácticas propuestas. Con el fin de grabar las secuencias de vídeo se instaló una Web Cam en el laboratorio de prácticas.
- Memoria sintética del trabajo (Descripción del hardware final, tareas que lleva a cabo el robot, software documentado...)

5.- SAPHIRA

Saphira [23] es un entorno de desarrollo y simulación de aplicaciones de robótica móvil. Saphira ya ha sido utilizado con éxito como herramienta educativa en el ámbito universitario [24] y en el investigador. Existen versiones de libre distribución, para diversos sistemas operativos,



con la única limitación de no poder usarlas con un robot físico.

Para poder utilizar Saphira para desarrollar aplicaciones es necesario tener instalado algún compilador de C. Creemos que las posibilidades del simulación de Saphira, así como la posibilidad de utilizar su librería C para crear aplicaciones complejas lo hacen un recurso de gran valor en el contexto que nos atañe. Esta librería permite utilizar funciones de lectura de sonars, sensores de contacto y un sistema de visión opcional. Saphira permite simular y ejecutar las aplicaciones desarrolladas de forma transparente. Existe una versión multiagente de Saphira, capaz de controlar varios robots. Utiliza la arquitectura *Open Agent* (de libre distribución para propósitos no comerciales) que, entre otras posibilidades, permite el control de los agentes a través de Internet.

En el ámbito de los cursos impartidos por los autores, se utilizó Saphira para desarrollar actividades prácticas relacionadas con el control borroso de robots móviles y los sistemas basados en conductas. Entre otras posibilidades, Saphira permite crear comportamientos y combinarlos mediante reglas borrosas para dar lugar a actividades más complejas [25]-[26]. Además, Saphira incluye determinados comportamientos básicos, como detección de obstáculos o movimiento a velocidad constante. Los comportamientos se escriben en una mezcla de C y un lenguaje de especificación

alrededor a una distancia relativamente fija. Una vez diseñados los programas, se procede a su simulación en Saphira y, una vez comprobada su validez, se ejecutó con una plataforma móvil física Pioneer (ver figura siguiente). En este nivel es importante que los alumnos tengan conocimientos básicos de lógica difusa.

La plataforma diferencial Pioneer, producto comercial de ActivMedia Robotics, está preparada para funcionar con Saphira y, además de un anillo de sonars y sensores de contacto, dispone de una amplia variedad de accesorios como módem radio, cámaras, láser, etc. Es de destacar la precisión de los codificadores de las ruedas, así como su capacidad de carga.

Además de la posibilidad de escribir aplicaciones de control borroso, Saphira incluye un lenguaje llamado Colbert. Colbert es un lenguaje de control reactivo, de sintaxis parecida a la de C, que permite emplear concurrencia y el paradigma de los autómatas de estados finitos en la programación. La utilización conjunta de Saphira y una plataforma móvil permite poner en práctica conceptos más avanzados como actividades complejas, realimentación visual, construcción de mapas, etc.

CONCLUSIONES

En virtud de lo expuesto en los apartados anteriores, donde se analizan las posibilidades docentes de una solución hardware y una software, se plantea la validez de dichas soluciones para el desempeño de las actividades prácticas asociadas a los contenidos teóricos de un curso universitario de introducción a la robótica móvil.

La solución hardware expuesta no supondría una inversión económica excesiva. Por otro lado, como se ha explicado las limitaciones del producto pueden superarse de diversas formas. En general la respuesta de los alumnos resultó positiva, en tanto en cuanto la actividad práctica se hizo más amena. Es de destacar el entusiasmo que el kit consiguió imprimir a los alumnos.

Actualmente se está estudiando la posibilidad de diseñar actividades prácticas más elaboradas para cursos posteriores, especialmente relacionadas con comportamientos de grupo. La solución software descrita destaca por ser de libre distribución para fines educacionales, así como por la potencia de sus capacidades de simulación.

Debido a la falta de tiempo en la asignatura, no se trató con la profundidad deseada. No obstante, actualmente se utiliza como herramienta fundamental en dos Pro-

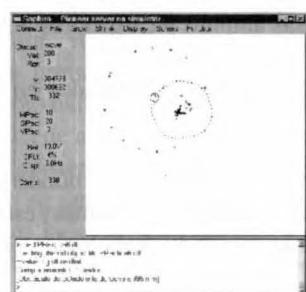


Figura 3. Entorno de desarrollo Shaphira.

de comportamientos borrosos. Saphira guarda las lecturas de los sensores en un modelo de los datos llamado LPS (*Local Perceptual Space*), a partir del cual se computan determinadas variables difusas a utilizar en los comportamientos. Las reglas difusas hacen uso de estas variables para dar como resultado un conjunto difuso de control de los motores del robot. Por último, este conjunto se *defuzzifica* para obtener un valor concreto a enviar a los motores [27]. Al tratarse de un curso introductorio se propuso una actividad práctica muy sencilla que consistía en hacer que el robot mordiese y cuando encontrase un obstáculo (utilizando los sonars) empezara a orbitarlo, esto es, a girar a su

yectos de Fin de Carrera relacionados con navegación, lo cual es a su vez un indicador de sus posibilidades.

REFERENCIAS Y BIBLIOGRAFÍA

- [1] Sistemas Robóticos Móviles, Ingeniería Informática, Universidad de Las Palmas de Gran Canaria, <http://serdis.dis.ulpgc.es/~ii-srm>
- [2] The LEGO MindStorms official site, <http://www.legomindstorms.com>
- [3] Dave Baum. «Dave Baum's Definitive Guide to LEGO MINDSTORMS». Apress, 1999
- [4] Dave Baum, Michael Gasperi, Ralph Hempel, Luis Villa. «Extreme Mindstorms: an Advanced Guide to Lego Mindstorms». Apress, 2000
- [5] Jonathan B. Knudsen. «The Unofficial Guide to LEGO MINDSTORMS Robots». O'Reilly, 1999
- [6] Página de la asignatura de robótica, Ingeniería Técnica en Informática de Sistemas, Universidad Rey Juan Carlos, <http://gsyc.escet.urjc.es/docencia/asignaturas/robotica/>
- [7] Lego Lab en la Universidad de Aarhus (Dinamarca), <http://legolab.daimi.au.dk/>
- [8] Curso del departamento de informática de la Universidad de Utrecht (Holanda), <http://www.cs.uu.nl/people/markov/lego/index.html>
- [9] Curso de robots LEGO en SUNY/Utica, <http://gozer.sunyit.edu/classes/CSC490/csc490.html>
- [10] Curso de robótica basado en LEGO en la Rice University, <http://www-brazos.rice.edu/elec201/>
- [11] The MIT Programmable Brick, <http://ics.www.media.mit.edu/groups/el/projects/programmable-brick/>
- [12] Not Quite C, <http://www.enteract.com/~dbaum/nqc/index.html>
- [13] Lego Robots: RCX Command Center, <http://www.cs.uu.nl/people/markov/lego/rcxxc/>
- [14] R. Brooks, «Cambrian Intelligence: The Early History of the New AI». MIT Press, 1999
- [15] R. Arkin, «Behavior-Based Robotics». MIT Press, 1998
- [16] R. Murphy, «Introduction to AI Robotics». MIT Press, 2000
- [17] J. Borenstein, H.R Everett, L. Feng, «Navigating Mobile Robots: Sensors and Techniques». A.K. Peters, Ltd., 1996
- [18] MindStorms RCX Sensor Input Page, <http://www.plazaearth.com/usr/gasperi/lego.htm>
- [19] Programa de control de multiplexor para LegOS, http://serdis.dis.ulpgc.es/~ii-srm/MatDocen/notas_practicas/legOS_Ejemplos/sensor_mux.c
- [20] LegOS Official Web Page, <http://www.noga.de/legOS/>
- [21] V. Braitenberg, «Vehicles. Experiments in Synthetic Psychology». MIT Press, 1984
- [22] Mindstorms Info Center, <http://www.mi-ra-i.com/JinSato/MindStorms/index-e.html>
- [23] Saphira Robot Control System, <http://www.ai.sri.com/~konolige/saphira/index.html>
- [24] CS224 - Real World Autonomous Systems at Stanford University, <http://www.ai.sri.com/~konolige/CS224/index.html>
- [25] A. Saffioti, E.H. Rusconi, K. Konolige, «Blending reactivity and goal-directedness in a fuzzy controller». Proc. IEEE Intl. Conference on Fuzzy Systems, pp. 134-139, San Francisco, CA, 1998
- [26] D. Kortenkamp, P. Bonasso, R. Murphy (Eds.), «Artificial Intelligence and Mobile Robots. Case Studies of Successful Robot Systems». MIT Press, 1998
- [27] ActivMedia Robotics, «Saphira Software Manual - Saphira version 6.1». ActivMedia Robotics, 1997

AUTORES



Antonio Falcón Martel: Catedrático de Ciencias de la Computación e Inteligencia Artificial. Profesor de las asignaturas de Visión por Computador, Sistemas Robóticos Móviles y Teoría de Sistemas, en el Departamento de Informática y Sistemas de la Universidad de Las Palmas de Gran Canaria. Director del programa de doctorado "Sistemas Inteligentes y Aplicaciones Numéricas en la Ingeniería", en la misma Universidad.



Oscar Déniz Suárez: Licenciado en Informática. Estudiante de doctorado y becario de investigación adscrito al Departamento de Informática y Sistemas de la Universidad de Las Palmas de Gran Canaria. Sus intereses investigadores se centran en robótica, interfaces percepto-efectores, y reconocimiento de caras.





ALGORITMO DE SCHEDULING M-LWDF

SIMULACIÓN PARA LA PROVISIÓN DE CALIDAD DE SERVICIO EN ENTORNOS MULTIUUSUARIO CON CANALES VARIANTES.

José Antonio López Salcedo¹, Daniel Prado Rodríguez²,

Raiül Tornay, Andreu Urruela Planas

Estudiantes de la E.T.S. Enginyeria de Telecomunicació de Barcelona (UPC)

^{1,2}Miembros de la Rama de Estudiantes del IEEE de Barcelona

Email: {jose25@casal.upc.es, daniel25@casal.upc.es, rault@yahoo.es, andreu@gps.tsc.upc.es}

Resumen - En sistemas de transmisión de alta velocidad en canales wireless, donde el espectro es un recurso altamente limitado, se hace necesaria la implementación de algoritmos de reparto de los recursos si se pretende cumplir con unos determinados requerimientos en términos de tasa de transmisión o de retardo máximo de los paquetes. El presente artículo pretende mostrar cómo los algoritmos de *Scheduling* (y en particular el algoritmo M-LWDF) pueden ofrecer mejores prestaciones en términos de tasa media de transmisión respecto a los algoritmos tradicionales de reparto de recursos, los cuales no suelen prestar atención a las circunstancias individuales que presentan los diferentes usuarios del sistema.

1.- INTRODUCCIÓN

Uno de los problemas más significativos de las comunicaciones móviles 3G es la alta variabilidad de la capacidad del canal que llega incluso a sufrir grandes variaciones de forma aleatoria en un intervalo relativamente pequeño (de algunos tiempos de slot). De hecho, en este nuevo tipo de comunicaciones móviles, la velocidad de transmisión (a la que también nos referiremos como *capacidad* o *rate*) está discretizada a un conjunto finito de valores, los cuales pueden ser escogidos en función de la calidad del canal que ha estimado el sistema.

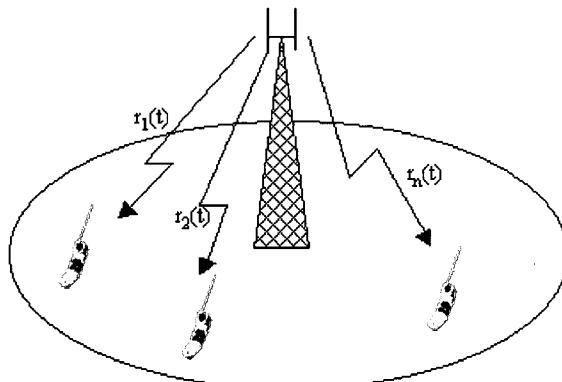


Fig. 1.1. Canal downlink compartido por n usuarios a diferentes rates instantáneos.

De este modo, por ejemplo, en un sistema monousuario los rates de transmisión elegidos se ven obligados a seguir irremediablemente las fluctuaciones del canal, ya que dichos rates o tasas de transmisión son fijadas directamen-

te por la calidad de canal observada. Por tanto, la tasa media a la cual se podrán cursar paquetes será irremediablemente la media de la distribución estadística de la capacidad del canal.

Por otro lado, en un sistema donde varios usuarios comparten el mismo recurso, éstos se ven obligados a repartirse el tiempo disponible para poder transmitir por el mismo canal. Parece entonces razonable que para cada usuario se pueda elegir o programar (en inglés, *schedule*) los instantes para transmitir en que la estimación de la calidad de su canal sea mejor. De esta forma, dado que cada usuario tendría, dentro de lo posible, sus mejores instantes para transmitir, la tasa media de transmisión de cada usuario sería superior a la media estadística de la capacidad de su canal, es decir, superior a la que habría conseguido si hubiera transmitido tanto en los instantes donde la calidad de su canal era buena como en los instantes donde esta calidad era mala.

1.1 Ejemplo

Un ejemplo que muestra la mejora en términos de tasa media de transmisión tras aplicar algún tipo de algoritmo de asignación de canal que tenga en cuenta la calidad del mismo se presenta en [1], considerando un sistema simple de dos usuarios. El rate en un slot temporal para el usuario 1 es de 76.8 kbps o bien 153.6 kbps, de manera equiprobable, mientras que el usuario 2 presenta unos rates de 156.6 kbps o bien 307.2 kbps, también equiprobables. Además, la estadística del canal para ambos usuarios es independiente, y la cantidad de datos a transmitir es ilimitada. Aplicando un criterio de asignación en que en cada slot temporal se cambia de usuario servido, el rate medio resultante para cada usuario sería de:

$$R_1 = 0.5 \cdot (0.5 \cdot 76.8 + 0.5 \cdot 153.6) = 57.6 \text{ kbps}$$

$$R_2 = 0.5 \cdot (0.5 \cdot 153.6 + 0.5 \cdot 307.2) = 115.2 \text{ kbps}$$

Sin embargo, aplicando un criterio de asignación de *justa proporcionalidad*, el canal es asignado al usuario que presente una tasa de transmisión relativamente mejor en ese instante, de modo que si ambos usuarios se encuentran en empate, la asignación se realiza de manera equiprobable.

La mejora asociada a este nuevo y sencillo criterio de asignación es un incremento de casi un 17 % en la tasa

media de transmisión de cada usuario, lo cual abre unas buenas expectativas para el estudio del Algoritmo de M-LWDF que será llevado a cabo más adelante.

En conclusión, todos y cada uno de los usuarios conseguirían aumentar su tasa media de transmisión, a costa de no transmitir cuando sus capacidades de transmisión fueran bajas (es decir, cuando la calidad se su canal fuera mala) con la esperanza de que en ese mismo instante algún otro usuario tuviera una estimación de canal comparativamente mejor que la nuestra.

2.- ALGORITMO M-LWDF

El algoritmo M-LWDF (*Modified Largest Weighted Delay First*) propuesto en [1] pretende maximizar de manera óptima la tasa de salida de todos los usuarios atendiendo a dos parámetros clásicos de calidad de servicio como son: el retardo máximo permitido y la tasa mínima garantizada. De esta forma pretende ponderar ambos parámetros para decidir a qué usuario se le asigna el recurso compartido.

El modelo que se pretende simular consiste en un canal de bajada o *down-link* compartido de un sistema multiusuario de conmutación por paquetes. Este esquema podría ser aplicado en general a una gran diversidad de sistemas de telecomunicación, sin embargo el hecho de que la característica del canal pueda variar rápidamente y de manera aleatoria, hará que identifiquemos este esquema en un escenario de comunicaciones móviles con tasa de transmisión variable.

En este entorno, cada uno de los usuarios dispone en la estación base de un cola o *buffer* donde se almacenan los paquetes que llegan con una cierta distribución de tráfico y tasa de entrada, y así poder ser posteriormente transmitidos al terminal móvil cuando se tenga la oportunidad. Estas colas se supondrán infinitas, puesto que el objetivo del estudio será propiamente el algoritmo inteligente de reparto del canal, el cual será modelado como un *servidor*, tal y como puede apreciarse en la figura 2.1.

Por otra parte, las estimaciones de los canales de los diferentes usuarios serán independientes entre ellos, haciendo que las tasas de transmisión utilizadas sean también independientes. Estas tasas de transmisión serán las que utilizará el algoritmo para determinar el criterio de asignación del canal. Tal y como especifica el nombre del algoritmo, el criterio de asignación se basa en la selección de la cola j que cumpla la relación siguiente:

$$\max_j \{ \gamma_j W_j r_j(t) \}$$

donde W_j representa el tiempo de espera en cola del primer paquete (*Head of Line delay*) o equivalentemente, el número de elementos en cola, y $r_j(t)$ la capacidad actual del canal en función de las estimaciones recibidas por los usuarios, siendo γ_j constantes positivas.

Esta ponderación para la asignación del usuario que hará uso del canal pone de manifiesto el compromiso entre el

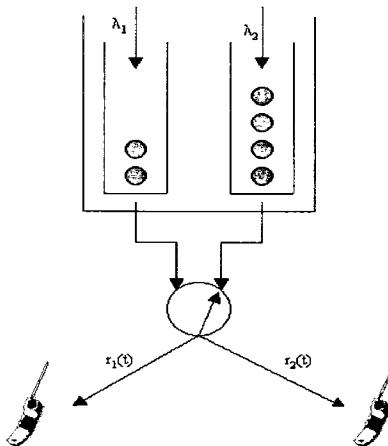


Fig. 2.1. Esquema para el algoritmo M-LWDF del modelo de colas en una celda con dos usuarios.

retardo actual en cola del paquete a servir, con la calidad del canal que se observa. De esta forma, los usuarios con mejor rate (buena calidad del canal) tendrán preferencia sobre los que observan un canal comparativamente peor; por otro lado, si el retardo actual en cola es elevado, el usuario también tendrá preferencia, a pesar que su canal no sea extremadamente bueno. Así pues, dentro de lo que es posible, el algoritmo intentará siempre maximizar el rate de salida. Aún con todo, si las necesidades de retardo máximo lo requieren, el compromiso de la expresión decide cuál de los dos factores reviste de mayor urgencia. Finalmente, el factor de ponderación γ_j sirve para ajustar de forma adecuada los diferentes requerimientos de QoS de cada uno de los usuarios.

3.- ESCENARIOS DE CANAL VARIANTE

3.1 Introducción

El canal de comunicaciones es el elemento clave del algoritmo, pues será el que determinará de manera directa la tasa de transmisión disponible para cada usuario, y por tanto determinará el tiempo de servicio con el que el servidor atenderá a cada uno de éstos. Además, la variabilidad de este canal será la que en gran medida defina las prestaciones del algoritmo, pues éste basa su criterio de asignación de usuario mediante el uso del rate instantáneo, el cual seguirá una u otra distribución estadística, haciendo que la evolución del algoritmo difiera en canales con una gran variabilidad de rate, respecto a otros en los que éste apenas sufre fluctuaciones.

En concreto, en un entorno de comunicaciones móviles como el que nos ocupa, la respuesta del canal suele variar de manera aleatoria a lo largo del tiempo, por lo que se hace necesario caracterizarla de forma estadística. Desde el punto de vista de la calidad de la comunicación, en general podemos decir que este tipo de canales penalizan sobre la relación señal-a-ruido en recepción (SNR) a través de diferentes efectos: desvanecimientos, multipath, ensanchamiento temporal o frecuencial de la señal transmitida.



Lejos de buscar un estudio exhaustivo sobre las causas que producen la pérdida de calidad en el canal de comunicaciones, como caso práctico sencillo nos centraremos en el estudio de los desvanecimientos de señal que se producen, pues éstos son modelables de manera simple y se adecúan perfectamente a nuestras necesidades de modelar la variabilidad de la calidad del canal.

3.2 Relación entre SNR y rate

Un aspecto importante a comentar es la relación que estableceremos para, a partir de una cierta distribución de canal que haga variar la SNR, obtener la velocidad de transmisión que puede llegar a conseguirse. Para ello haremos uso de la ecuación que planteó C. Shannon para definir la máxima capacidad de un canal de comunicaciones (bits/s), en función de su ancho de banda y de su relación señal-a-ruido:

$$C = BW \cdot \log_2(1 + SNR)$$

De esta forma, el criterio que se seguirá será el de calcular el rate instantáneo para cada usuario a partir de la capacidad de Shannon, la cual hará uso de la estimación de la SNR instantánea del canal de cada usuario en cuestión.

Sin embargo, esta SNR instantánea seguirá una cierta distribución estadística, cuya media tendremos que fijar de alguna manera. Para tener una idea del orden de magnitud en el que nos moveremos, se tomará como caso de ejemplo el sistema de comunicaciones móviles GSM, del cual tomaremos los valores de SNR para un canal equivalente de 10 kbps, el cual tomaremos como ejemplo para simulación. Los parámetros utilizados serán:

- $\text{media}\{\text{SNR}\} = 24 \text{ dB}$, $\text{std}\{\text{SNR}\} = 6 - 7 \text{ dB}$
- $BWeq = 1.25 \text{ kHz}$

3.3 Tipos de desvanecimientos utilizados

• Escenario con ecos difusos

En este caso, el escenario de propagación consta de un conjunto de ecos denominados difusos, producto de múltiples reflejos multicamino, sin que exista un camino predominante sobre el resto. Ello hace que este escenario se identifique con el caso de comunicaciones móviles en entornos urbanos complejos o interiores, pues la recepción de señal procede de múltiples caminos, todos ellos aproximadamente de igual amplitud pero sin que exista visión directa.

En estas situaciones, la envolvente de la respuesta impulsional del canal presenta una distribución estadística tipo Rayleigh. Sin embargo, nuestro parámetro de interés se basa en la estimación de SNR, la cual procede de la relación entre potencia de señal y ruido. Por ello, en un caso ideal en que se mantuviera constante la potencia de ruido, la potencia de señal se vería afectada por una distribución estadística resultado de elevar al cuadrado la distribución Rayleigh de la envolvente.

El resultado de elevar al cuadrado una distribución de tipo Rayleigh puede aproximarse por una distribución de tipo exponencial, por lo que este primer escenario de ecos difusos (entorno urbano) será simulado mediante el uso de valores de SNR instantáneos correspondientes a una variable aleatoria exponencial de media $10^{2.4} \sim 252$.

Tal y como se ha comentado en el apartado 3.1, los valores instantáneos de SNR serán introducidos en la expresión del cálculo de la capacidad teórica de Shannon, obteniendo de esta forma los rates instantáneos para cada usuario. El inverso de estos valores será el parámetro que utilizará el servidor como tiempo de servicio. Los histogramas correspondientes pueden observarse en las figuras 3.1a y 3.1b.

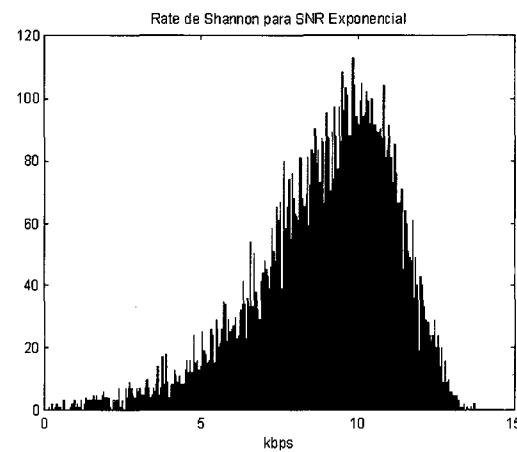


Fig. 3.1a Histograma de la capacidad de Shannon para SNR exponencial.

Éste será el peor escenario de simulación, ya que tal y como se observa en la figura 3.1a, hay gran número de realizaciones de rates instantáneos cuyos valores se encuentran bastante por debajo de la media estadística, lo cual indica que hay un gran número de instantes en los que el canal que se observa posee malas condiciones de transmisión.

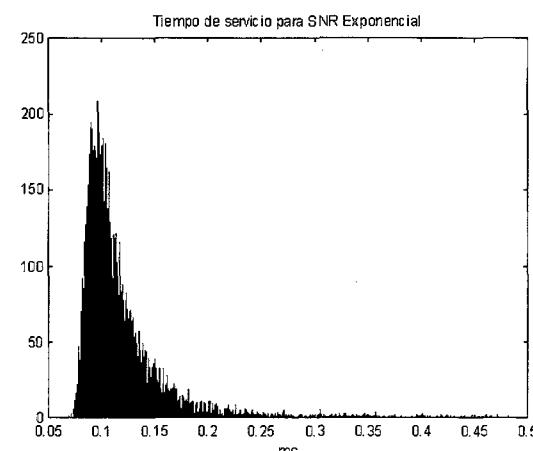


Fig. 3.1b Histograma del tiempo de servicio para una SNR exponencial.

• Escenario con ecos fijos

Este nuevo escenario corresponde a comunicaciones móviles en entornos semi-urbanos, donde existe un camino de propagación o de visión directa predominante, junto con pequeños reflejos multicamino de menor amplitud. En este caso, la envolvente del canal suele modelarse como una distribución de tipo Rice, resultando su cuadrado en una distribución que puede aproximarse de tipo Rayleigh.

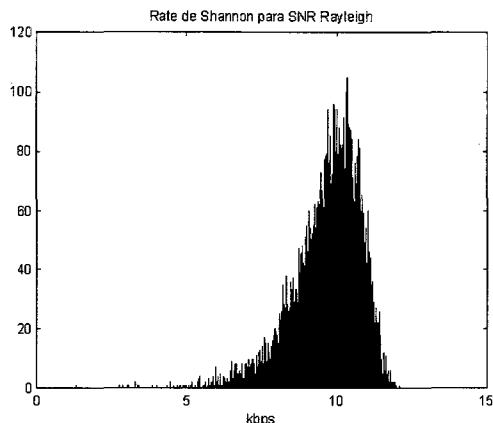


Fig. 3.2a Histograma de la capacidad de Shannon para SNR Rayleigh.

De la observación de las gráficas 3.2a y 3.2b se puede ya predecir que en este escenario los resultados del Algoritmo M-LWDF no serán tan buenos como en el caso anterior de distribución de SNR exponencial, pues los posibles rates quedan más concentrados alrededor de su valor central, de manera que los diferentes usuarios tienen más posibilidades de tener rates parecidos entre ellos. De este modo, los rates de los usuarios serían más uniformes y en algunos casos podría ser difícil poder encontrar algún usuario con un rate instantáneo claramente superior al resto, reduciendo así el margen de maniobra del algoritmo.

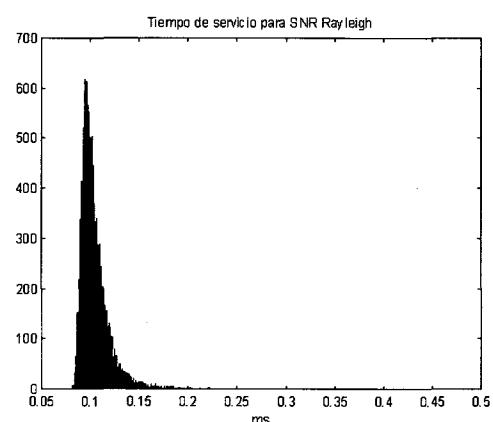


Fig. 3.2b Histograma del tiempo de servicio para SNR Rayleigh.

4.- GENERACIÓN DE TRÁFICO

Resulta de vital importancia el estudio de las prestaciones del algoritmo en presencia de varios tipos de generación

de tráfico puesto que dichos tipos se adaptan a las necesidades presentes en el sector de las comunicaciones móviles. De hecho, no es descabellado suponer que ciertas prestaciones del algoritmo pueden resultar seriamente dañadas por la presencia de cierto tipo de generación que dificulte el correcto funcionamiento del algoritmo.

En los subapartados siguientes se explica brevemente en que consisten tales tipos de generación de datos que serán utilizados en el apartado de simulaciones reales.

• Tráfico exponencial

El sistema de generación más característico en los modelos de las cadenas de Markoff es el conocido sistema de generación exponencial. Básicamente consiste en disponer las llegadas de forma que el tiempo que transcurre entre las sucesivas llegadas es una variable aleatoria exponencial de media el inverso del rate nominal. Como es conocido, la característica más importante de este tipo de generación heredadas de la naturaleza exponencial de las transiciones es su ausencia de memoria.

• Tráfico IPP

El segundo de los tráficos programados para la adaptación a sistemas reales es el conocido tráfico IPP. Este tráfico pretende adaptarse a las llamadas fuentes a ráfagas. Consiste en generar un tráfico de naturaleza exponencial durante un cierto tiempo y a continuación mantener un período de inactividad. La duración del período de inactividad tiene naturaleza exponencial, y el número de paquetes enviados en el período de actividad se resuelve mediante la utilización de una variable aleatoria discreta de naturaleza geométrica.

5.- ESTUDIO TEÓRICO SOBRE CANAL VIRTUAL

5.1 Introducción

En las secciones anteriores, se ha expuesto tanto el funcionamiento del algoritmo en estudio como las diferentes modelaciones de canales y generadores de tráfico. Si bien en el apartado siguiente, todos estos sistemas serán simulados de forma estricta dando lugar a un estudio sobre la capacidad de tráfico en sistemas reales, en esta sección del trabajo nos gustaría realizar un estudio absolutamente teórico sobre el comportamiento del algoritmo en un escenario totalmente virtual, aún cuando siendo en muchas ocasiones irreales.

Es por ello que el escenario de simulación que expondremos a continuación no tiene porqué coincidir con ningún sistema real, ni es nuestro objetivo justificar tal escenario sino los resultados que de él se obtienen pues ofrecen una visión algo teórica de las prestaciones potenciales de este algoritmo.



5.2 Planteamiento del estudio

Como se ha comentado en la introducción, el sistema se compondrá de N fuentes de generación independiente con tasa λ_i . Toda la generación de paquetes procedentes de estas N fuentes alimentará a un único servidor que buscará la mejor manera de aliviar el tráfico presente a su entrada ofreciendo ciertas prestaciones a todos y cada uno de los usuarios. De hecho la implementación impone la obtención de las mejores prestaciones en términos de retardo en el sistema. Los parámetros a los cuales vamos a estar pendientes son principalmente, el número de elementos en las colas del sistema y el retardo que este provoca sobre las muestras procedentes de los diferentes generadores. Como parámetro complementario, estaremos pendientes, no solo de la media de estos valores sino de algún percentil cuando sea necesario. Por ejemplo, no es sólo interesante estudiar cual es la media del retardo del sistema sino observar cuál fue el valor más alto de retardo descartando un 5 por ciento de las muestras más desfavorables.

Finalmente, tendríamos que definir cuales serán las variables de simulación que nosotros variaremos para poder obtener los resultados prometidos. En primer lugar, el parámetro fundamental a estudiar es la sobrecarga de tráfico que se le puede inyectar al sistema con el fin de ver hasta que punto el algoritmo es capaz de mejorar una implementación clásica. En segundo lugar, está claro que tiene que haber una relación entre tal mejora y la distribución del canal. Parece lógico que tal relación esté íntimamente ligado a la varianza del canal puesto que el canal debe ser variante para que el algoritmo encuentre momentos óptimos para efectuar sus transmisiones. Por tanto resulta muy interesante variar la varianza del canal para observar como se comporta el algoritmo. Finalmente, resulta interesante estudiar cual es el comportamiento del sistema con el aumento del número de usuarios que comparten el canal. De hecho, aumentar el número de usuarios independientes presentes en el sistema es una forma más de aumentar la varianza del canal puesto que al incorporar una nueva distribución independiente del canal, esta aumenta en el concepto general de canal compartido.

Cabe destacar que las simulaciones efectuadas se realizan con un criterio de normalización de forma que el tráfico ofrecido (con o sin sobrecarga) esté normalizado al número de usuarios.

5.3 Modelo simulado

Tal y como se ha comentado en la sección anterior, este estudio teórico ha de permitir modificar la varianza a voluntad para poder estudiar el comportamiento del algoritmo y por simular con diferentes tráficos ofrecidos respecto a la capacidad del canal. Por normalización se ha

trabajado con un servidor de tasa media de salida 10.0 paquetes/u.t. en todas las simulaciones.

Los generadores están programados, durante este estudio teórico, para generar una tasa media conjunto de 10.0 paq/u.t * OVER_TRAFIC. Donde OVER_TRAFIC es el parámetro que controla la sobrecarga de tráfico ofertado. De esta forma, un valor de OVER_TRAFIC de 1.1 ofrece un 10 por ciento más de paquetes al sistema. Como se comentaba en la sección anterior, el tráfico ofertado al sistema se dividirá en los diferentes generadores con el fin de que la oferta sea independiente al número de usuarios.

Con el fin de poder variar la varianza del canal a voluntad se ha trabajado con una programación del servidor en distribución binomial en torno al valor medio de canal. De esta forma, el rate que el servidor ofrece a cada instante puede tomar dos valores con igual probabilidad. Dichos valores se encuentran a igual distancia del valor nominal de rate: 10.0 paq / u.t. Cabe destacar que a esta distribución se le ha añadido un ruido relativamente pequeño (distribución fig 5.2) para que la política de decisión no eligiera siempre a los elementos procedentes de los primeros generados. Esto es debido a que tal y como está planteado el sistema y dado que el número de elementos en cola siempre es un entero, en caso de empate en la puntuación de asignación de canal, siempre se declaraban ganadores injustamente, los elementos procedentes de los primeros generadores. Añadiendo un pequeño ruido, tal efecto quedaba prácticamente, eliminado. La potencia de ruido añadido es suficientemente poco significativa como para no alterar la varianza de la distribución de canal. Como se puede observar en la figura, el parámetro libre de cambio es la separación de las dos deltas de la distribución para poder aumentar la varianza del sistema. De hecho si tomamos una separación d del centro de la distribución (esto es, las dos deltas están centradas en $10-d$ y $10+d$), la varianza general de la distribución podrá calcularse como indica la ecuación siguiente:

$$\sigma^2 = 0.5[(10 - \delta) - 10]^2 + 0.5[(10 + \delta) - 10]^2 = 0.5\delta^2 + 0.5\delta^2 = \delta^2$$

La distribución de canal simulada puede corresponder a un sistema donde la capacidad del canal no pueda expresarse de forma analógica o continua sino que el conjunto de valores que puede tomar sea limitado a dos.

5.4 Simulaciones efectuadas

El número de simulaciones realizadas para llevar a cabo este estudio teórico es relativamente elevado dado que para estudiar la dependencia de las prestaciones respecto a un parámetro, se ha de realizar la simulación para un conjunto de puntos de ese parámetro de forma que pueda observarse o predecirse la evolución continua de tal parámetro.

Es por ello que las simulaciones que se han llevado a cabo han consistido en medir el número medio de elementos en cola de cada uno de los generadores entrantes al sistema así como la media del tiempo de permanencia en el sistema

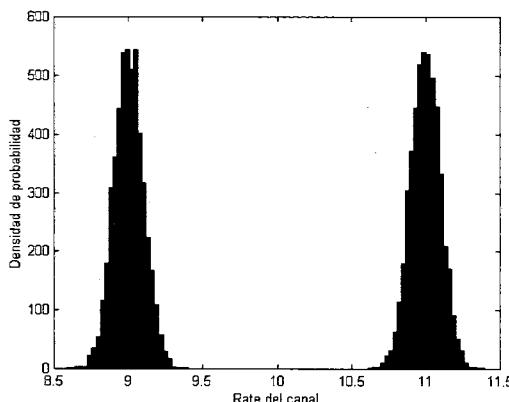


Fig. 5.1 Distribución de canal escogida para el estudio del canal virtual.

y el percentil del mismo (descartando el 5 por ciento de las muestras). Esta extracción de resultados se ha realizado para un número de 2, 6, 10 o 14 generadores. Finalmente para cada uno de estos escenarios se ha realizado una simulación para un conjunto elevado de valores de la varianza del canal.

En conclusión el número de resultados es relativamente elevado, no siendo tan interesantes los datos en sí, sino un análisis gráfico de los mismos con los comentarios pertinentes. Los resultados pueden ser analizados exhaustiva y detenidamente en el Anexo C. Por el contrario, a continuación se exponen las conclusiones extraídas.

5.5 Conclusiones

5.5.1 Simulación básica

Tomemos el escenario de N (número de generadores presentes en el sistema) igual a diez. Si ofrecemos al sistema el tráfico que es capaz de soportar en media, esto es 10 paq/u.t, observaremos que el sistema no satura como lo haría un sistema de asignación secuencial de recursos. En la figura 5.2 observamos la evolución del número de elementos en cola para diferentes valores de la varianza del canal.

Las conclusiones que se pueden extraer a la vista de los resultados son varias. En primer lugar observamos que si la varianza disminuye radicalmente de valor, el sistema empieza a saturar. Observación que resulta totalmente lógica puesto que si el rate del canal no tiene varianza, el canal se convierte en determinista y, en conclusión, no se puede mejorar la eficiencia del canal por el hecho de asignar mejor los recursos. Dicho de una forma más intuitiva no existen "mejores momentos" para transmitir y "perores momentos" porque todos son iguales. De hecho, cuando disminuimos la varianza nos enfrentamos cada vez más a un sistema M/D/1 y por tanto dicho sistema satura cuando la tasa de entrada coincide con la tasa de salida. Existe por tanto lo que podemos denominar varianza mínima para el correcto funcionamiento. Esto es, el algoritmo necesita una mínima varianza para poder soportar el tráfico que se ofrece al sistema. Dicha varianza mínima

dependerá tanto de la tasa ofrecida como del número de generadores.

En segundo lugar observamos que cuando la varianza del sistema es extremadamente elevada, la sistema también muestra una leve tendencia a la saturación. Esto es debido a que si existen valores de la distribución que provocan un tiempo en el sistema relativamente grande (varianza muy grande indica que hay valores poco probables muy desfavorables), en el momento en que estos sean tomados, el sistema perderá mucho tiempo en transmitir al rate asignando acumulando muestras en las colas de forma exagerada. De esta forma, el sistema en la siguiente asignación se ve más forzado por las exigencias temporales de los elementos acumulados que por sus preferencias de optimización. Dicho de forma más intuitiva el sistema entra en un bucle de desesperación. Ha perdido mucho tiempo en una muestra y eso le lleva a tener que expulsar como sea las muestras acumuladas. Ese "como sea" lleva al sistema a tener que volver a utilizar valores desfavorables de rate de transmisión y así sucesivamente.

5.5.2 Dependencia con el número de generadores

Como se ha comentado en las conclusiones de la simulación básica anterior, la evolución de las prestaciones del sistema (elementos en colas y tiempo medio en sistema), dependen del número de usuarios (o generadores) que intervienen en el problema. De forma intuitiva, si hay un mayor número de usuarios en el sistema, el algoritmo tendrá más diversidad a la hora de elegir el usuario candidato a transmitir. Por el contrario, también es verdad que existen más usuarios con las mismas exigencias de prestaciones con lo cual no estaba tan claro a priori hasta que punto podrían mejorar las prestaciones. Cabe resaltar, que más usuarios no implica más tráfico ofrecido dado que la carga individual es normalizada para que la carga conjunta al sistema sea idéntica a la anterior.

En la figura 5.2 podemos observar cómo evoluciona el número de elementos en cola en función del número de usuarios. A la vista de los resultados expuestos en esta gráfica podemos concluir que el aumentar el número de usuarios favorece al algoritmo dándole mayor margen de maniobra al poder escoger ante más posibilidades. De

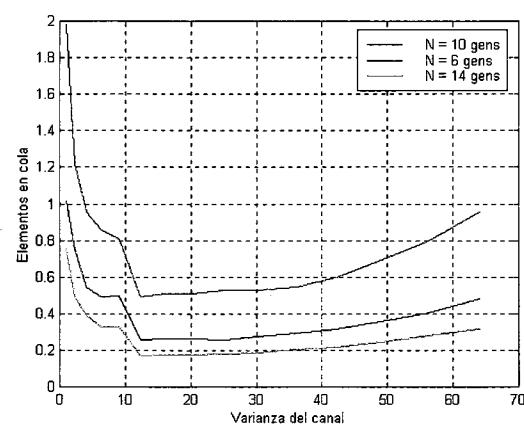


Fig. 5.2 Comparativa del número de elementos en cola.



hecho, la justificación más formal fue la facilitada en la introducción la cual apuntaba a que un mayor número de usuarios equivale a trabajar con un canal común compartido de mayor varianza.

Sin embargo, la comparativa expuesta en la figura anterior, no revela una comparación justa puesto que indica el número medio de elementos en cola de cada uno de los generadores y por tanto no el número de medio de elementos en el sistema. Por tanto, para poder afirmar las conclusiones realizadas en el párrafo anterior, de deben comparar los mismos resultados pero normalizando al número de colas presentes en el sistema. Tal comparativa puede verse en la figura 5.3 donde efectivamente continúa produciéndose una mejora pero no tan substancial. Trabajar con más usuarios implica aumentar la varianza del canal, en el sentido que un sistema que no trabaje en saturación conseguirá mejores prestaciones (número de elementos en cola menor), sin embargo, los umbrales de funcionamiento (varianza mínima), son independientes al número de usuarios, dependiendo tan sólo de la distribución del canal (varianza del canal). De este modo, dado un tráfico ofrecido podemos calcular cuál será la varianza mínima que deberá tener el canal para soportar tal tráfico independientemente del número de usuarios que se vayan a repartir dicho tráfico. Sin embargo, el número medio de elementos en el sistema sí que depende del número de usuarios. Si observamos las mejoras en términos de número de elementos en cola, mostrados en la última figura, no es esperable que se mejore mucho más por el hecho de aumentar indiscriminadamente el número de usuarios presentes en el sistema.

5.5.3 Dependencia con el tráfico ofrecido

En la primera de las secciones de este apartado se ofrecían los resultados de la simulación básica indicando que variarían substancialmente con el tráfico ofrecido. De hecho, cabe esperar que a mayor tráfico ofrecido peores prestaciones en cuanto a número de elementos en cola y tiempo en el sistema, sin embargo veremos a continuación, que el sistema consigue muy buenos resultados a costa de exigir una mayor varianza al canal. Recordemos

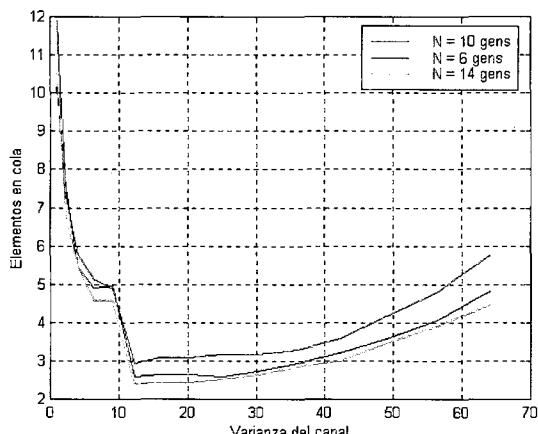


Fig. 5.3 Comparativa del número de elementos en el sistema.

que aunque modifiquemos la varianza del canal, este se encuentra siempre normalizado para que la capacidad media (la que se conseguiría en un asignación clásica secuencial) se siempre la misma.

En la figura 5.4 podemos observar la evolución del número de elementos en cola en función de la carga ofrecida al sistema. Recordemos que el parámetro de sobrecarga (OVER_TRAFFIC) indica la proporción entre el tráfico ofrecido y el tráfico medio del canal.

En la figura anterior podemos comprobar cómo se ha comportado el algoritmo en las diversas simulaciones en la cuales se le ha ido aumentando el tráfico común ofrecido por los 10 usuarios presentes en todas las simulaciones. Este es quizás el gráfico más significativo del algoritmo porque muestra claramente que el sistema satura a una varianza mínima que depende de la carga ofrecida. De modo intuitivo, a mayor tráfico ofrecido, mayor varianza exigida por el algoritmo. La figura también muestra cómo el algoritmo llega a aguantar un 70 % más del tráfico nominal a condición, eso si, que la varianza del canal sea extraordinariamente grande. Es aquí donde el realismo toma lugar indicando que las distribuciones clásicas de los canales no adquieren varianzas tan elevadas. De hecho se ha podido comprobar que un canal exponencial de media 10 paq / u.t. tiene como varianza 5.53, valor realmente pequeño en nuestro gráfico comparativo. Todavía más desfavorable resulta un canal Rayleigh de la misma capacidad porque su varianza supera levemente la unidad.

Sin embargo, la conclusión teórica del algoritmo es que si continuásemos realizando simulaciones, obtendríamos que podemos aumentar indiscriminadamente el tráfico de entrada hasta que el empeoramiento producido por la excesiva varianza (límite por la derecha) chocase con la mínima varianza exigida (límite por la izquierda). Las gráficas indican que cada vez que aumentamos el tráfico ofrecido, ambos límites tienden a acercarse más rápidamente, lo cual indica que no debe estar demasiado lejos el límite teórico de carga ofertada.

Por último, las simulaciones apuntan a unas prestaciones comunes independientes de la carga ofrecida cuando el

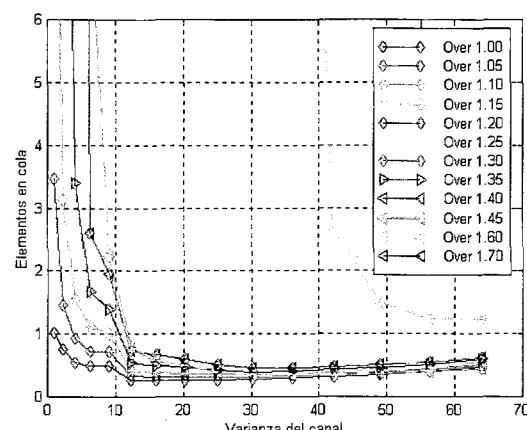


Fig. 5.4 Elementos en cola según la carga ofrecida.

escenario se encuentra lejos de los puntos de saturación. Dicha conclusión se extrae del hecho de que todas los escenarios de simulación colapsan en una misma línea cuando se alejan del codo producido por la saturación.

5.5.4 Conclusiones finales

Durante los tres últimos apartados se han introducido los aspectos más relevantes dentro de las simulaciones efectuadas en los diferentes escenarios escogidos. Se ha de comprender la limitación de las conclusiones a la realización específica de la distribución de canal, dado que el estudio tan sólo pretende analizar la dependencia de la varianza con las prestaciones del algoritmo, dejando al margen todos los momentos de mayor orden.

En segundo lugar, las conclusiones de mayor orden extraídas son la existencia de una varianza mínima en función de la carga ofertada y una mejora de las prestaciones con el aumento del número de usuarios. No podemos concluir este apartado sin formular la conclusión de la varianza mínima de forma más genérica. En la siguiente tabla se expone la varianza límite aproximada para cada uno de los valores de tráfico considerado y el tanto por ciento de veces que el rate cae por encima del tráfico ofrecido. Dicho de otro modo, partamos de una distribución gaussiana en donde considerar una varianza límite equivale a garantizar que un tanto por ciento de las realizaciones caigan al lado derecho del umbral marcado por tráfico ofrecido.

Si disponemos el tanto por ciento de la población que cae por encima del tráfico ofertado podremos comprobar que tiende a establecerse en un valor límite cercado al 17 por ciento. Por tanto, como regla aproximada, la distribución de canal debe de tener un 17 por ciento de su distribución de probabilidad por encima del tráfico ofertado. En una asignación clásica secuencial con distribución simétrica, la distribución de canal debería tener el 50 por ciento por encima y el cincuenta por debajo. En cambio, ahora el máximo tráfico cursable se sitúa por encima del tráfico nominal de forma que deje a su derecha un 17 por ciento de la distribución. La figura 5.12 muestra de forma gráfica la mejora de las prestaciones de forma general y definitiva.

6. ESTUDIO PRÁCTICO SOBRE CANAL VARIANTE

6.1 Introducción

En la presente sección se mostrarán los resultados de simulación obtenidos en los escenarios de trabajo caracterizados por las distribuciones de tráfico comentadas en

la sección 4 y por las diferentes distribuciones de calidad de canal expuestas en la sección 3. Debido a que el sistema posee un único servidor para atender a los diferentes usuarios (ya que el servidor simula el canal móvil), su parámetro tiempo de servicio será variable en función del usuario que el algoritmo M-LWDF haya escogido para transmitir en un cierto instante. Este tiempo de servicio será calculado como el inverso del rate instantáneo de ese usuario, pues la generación estadística finalmente será llevada a cabo sobre el parámetro rate o velocidad de transmisión.

De esta forma, cada escenario de simulación queda definido por dos parámetros:

o Distribución de generación de tráfico de entrada

- Exponencial (Poisson), IPP, On-Off

o Distribución de calidad de canal (SNR)

- Exponencial (entorno urbano o *indoor*)
- Rayleigh (entorno semi-urbano)

El criterio será caracterizar un escenario por el tipo de generación de tráfico de entrada que utiliza, y dentro de ese escenario se simulará para los dos tipos de distribuciones de canal consideradas, observándose así el impacto de la calidad de la transmisión en el sistema. Una vez seleccionado el escenario según el tráfico de entrada, se realizarán simulaciones en función del número de usuarios que acceden al sistema, con valores habituales de 2, 4, 6, 10 y 14 usuarios, permitiéndonos comprobar la evolución del sistema a medida que aumenta su número de usuarios. Por otro lado es importante indicar que fijada la capacidad media del sistema a 10 kbps, la generación de tráfico ha sido configurada para que siempre ofrezca una tasa de tráfico igual a la tasa máxima que puede admitir un sistema monousuario (M / M / 1). De este modo, denotando como m a la tasa de salida, la generación de tráfico se ha fijado a un valor de $r = \lambda / m = \mu / m = 1$. Obviamente, la simulación de este sistema monousuario mostraría que éste se encuentra en saturación, puesto que su parámetro de utilización es de:

$$r = \lambda / m = \mu / m = 1$$

A medida que se vaya aumentando el número de usuarios, la política a seguir será la misma, generar para cada usuario una tasa de tráfico de manera que la suma para todos los usuarios se convierta en un tráfico total de tasa $\lambda_{total} = \mu$. A diferencia del caso monousuario que se ha comentado anteriormente, en este nuevo caso a pesar de recibir el servidor la misma tasa de tráfico de entrada, la respuesta del sistema será mejor cuantos más usuarios disponga, pues a mayor número de usuarios, mayor variedad de rates/tiempos de servicio instantáneos con los que

Over	1	1.1	1.2	1.3	1.4	1.5	1.6	1.7
Varianza mínima	1	4	6	12	20	30	42	56
Tráfico ofrecido	10	11	12	13	14	15	16	17
Porcentaje población	50	30.85	20.7	19.32	18.55	18	17.27	17.47

Tabla. 5.1 Varianza mínima exigida en función del incremento de tráfico



analizar cuál es el que mejor se ajusta a sus necesidades de maximización de throughput. Ello hará que la tasa media de salida sea superior a su valor teórico, por lo que será posible aumentar ligeramente la tasa de tráfico que le será ofrecida al sistema. Para ello se ha definido un parámetro denominado como "over", el cual será utilizado en las simulaciones para comprobar la sobrecarga de tráfico de entrada que puede soportar el sistema respecto al caso monousuario.

En el caso monousuario el sistema no tendría más remedio que utilizar siempre el valor de rate/tiempo de servicio instantáneo que obtiene el único usuario que hay, obteniendo a veces valores buenos, pero otras veces valores muy malos que irremediablemente tendría que aceptar. A medida que aumenta el número de usuarios, es lógico que por muy bajos que sean las realizaciones de los rates aparezca haya al menos alguna realización que sea comparativamente mejor que el resto, y por tanto pueda ser aprovechada para transmitir en ese instante y aumentar así en media, la tasa de salida.

Recordemos por otro lado que la ponderación M-LWDF tiene en cuenta no sólo el rate instantáneo sino también el número de elementos en cola, por lo que un aumento considerable de este número dará prioridad a ese usuario, a pesar que su rate no sea comparativamente el mejor.

Finalmente comentar que los principales parámetros del sistema que serán analizados en cada una de las simulaciones serán el retardo medio en el sistema, el rate medio conseguido por el servidor, y la evolución del número de elementos en cola.

6.2 Escenario con tráfico exponencial

Este escenario se caracteriza por la utilización de una generación de tráfico de entrada de tipo exponencial o Poisson, repartiéndose la tasa de llegada entre los diferentes usuarios de manera que la tasa global que se ofrezca al servidor sea la máxima permitida por el sistema. De esta forma se pretende analizar el comportamiento en saturación del sistema, pues así se obtendrá una idea de las prestaciones máximas que pueden conseguirse en comparación con un sistema normal.

Para cada número de usuarios, el procedimiento consiste en simular diferentes puntos de trabajo, a partir de la tasa global máxima equivalente para un sistema $M/M/1$. De este modo, como ya se comentó anteriormente, siendo m la tasa de salida de paquetes servidos (el tiempo de servicio es pues de media λ/μ), la máxima tasa de entrada será de $\lambda = \mu$, ya que supondremos un caso de colas infinitas para centrar nuestro problema en el algoritmo de asignación de recurso y no en el desbordamiento de las colas (aunque siempre se intentará trabajar en puntos de trabajo en donde el número de elementos en cola permanezca estable).

Partiendo de una tasa global de entrada $\lambda = \mu$, con m igual a la capacidad estadística media del canal, ésta será

repartida de manera equitativa entre los N usuarios. Tras realizar una primera simulación con el Algoritmo M-LWDF, se puede apreciar cómo a pesar de recibir una tasa de paquetes de entrada igual a la que teóricamente en media puede servir, la utilización del servidor disminuye a medida que aumenta el número de usuarios debido a que existe mayor diversidad estadística con la que el Algoritmo M-LWDF puede trabajar.

Ello es lógico si se tiene en cuenta que el Algoritmo M-LWDF aprovecha los mejores instantes del canal para transmitir, haciendo que la tasa real de servicio de paquetes sea superior a la tasa media que teóricamente habíamos calculado. De esta forma, es posible incrementar el tráfico de entrada en un cierto porcentaje, y volver a simular para ver cómo evoluciona la ocupación del servidor. Mientras ésta se encuentre por debajo del valor inestable de 0.99, el sistema será capaz de procesar más tráfico de entrada. Es por este motivo que se ha definido el parámetro *OVER* con el cual sobrecargar el tráfico individual de entrada de cada usuario. Este parámetro nos permitirá analizar la mejora en términos de incremento de tráfico de entrada que el Algoritmo M-LWDF consigue.

Cabe mencionar que el aumento de tráfico de entrada no será directamente proporcional a la disminución producida en la utilización del sistema, ya que éste posee un algoritmo de asignación de canal que puede modelarse como un sistema no lineal, por lo que el efecto del tráfico que finalmente puede introducirse debe observarse mediante simulación.

Este hecho es el que muestran las figuras 6.2a y 6.2b, donde se presenta la evolución del rate medio que ha conseguido el Algoritmo M-LWDF para diferentes sobrecargas de tráfico de entrada y en función de diferentes números de usuarios. Como puede comprobarse, se consigue incrementar el tráfico de entrada total hasta en un 25 % para el caso de distribución de SNR exponencial.

El efecto que el rate medio aumente a medida que aumenta la sobrecarga de tráfico introducido al sistema es lógico,

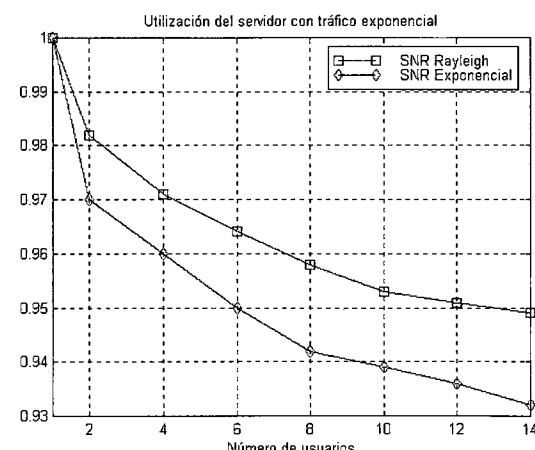


Fig. 6.1. Reducción de la utilización del servidor con $\lambda=\mu$ gracias al algoritmo M-LWDF.

ya que a más tasa de entrada de paquetes mayor debe ser también la tasa de salida para evitar que se saturen las colas del sistema. De hecho, las simulaciones se han llevado a cabo hasta conseguir saturar el sistema, observando la evolución del número de elementos en cola. Como puede verse, cuantos más usuarios existen en el sistema mayor es el punto de trabajo que se consigue antes de llegar a saturación, lo cual es coherente con la gráfica 6.1 que muestra una disminución de la utilización del servidor con el número de usuarios.

Por lo que respecta a las gráficas 6.2a y 6.2b que acaban de presentarse, se aprecia claramente el impacto que produce el tipo de distribución de canal que se utiliza. De esta forma, los mejores resultados tanto en términos de sobrecarga de tráfico de entrada como de rate medio conseguido se obtienen para la distribución exponencial, pues su mayor varianza respecto la distribución de tipo Rayleigh hace que el Algoritmo M-LWDF disponga de mayor variedad de valores estadísticos en donde buscar los mejores instantes de transmisión. En el caso de la distribución de tipo Rayleigh, sin embargo, su menor varianza hace que los rates medios conseguidos posean una dispersión bastante menor, tal y como se observa en la gráfica 6.2b donde los valores conseguidos apenas varían en función del número de usuarios en el sistema.

Este mismo hecho fue ya adelantado en la sección 5, donde se abordó estudio teórico del impacto de la varianza de la distribución del canal sobre la tasa de transmisión conseguida con M-LWDF, el cual cobra ahora sentido.

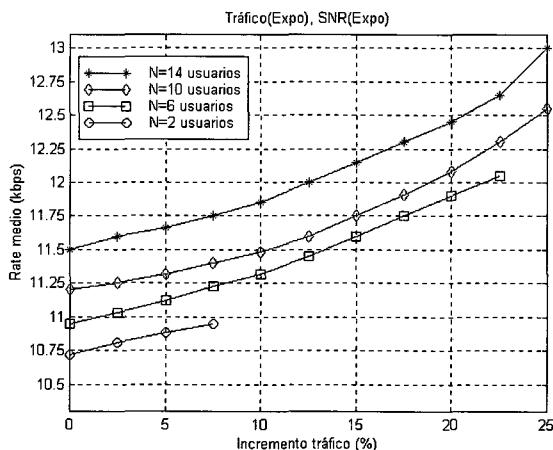


Fig. 6.2a. Rate medio conseguido por el servidor en función de la sobrecarga de tráfico de entrada para SNR exponencial.

Otro aspecto interesante a evaluar es la evolución del tiempo medio de espera en el sistema a que han de hacer frente los paquetes de entrada. Este parámetro es de gran importancia al permitir definir un criterio de QoS fijando un umbral máximo permitido sobre el retardo en el sistema a partir del análisis de los resultados obtenidos. En las figuras 6.3a y 6.3b se presenta la evolución de este retardo para las dos distribuciones de SNR bajo estudio.

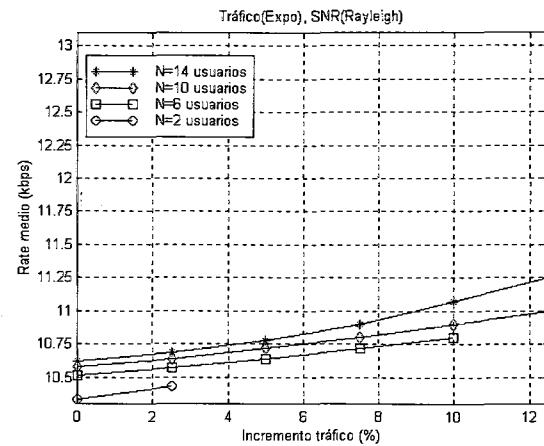


Fig. 6.2b. Rate medio conseguido por el servidor en función de la sobrecarga de tráfico de entrada para SNR Rayleigh.

A partir de la observación de las gráficas de retardo medio puede concluirse que no todos los valores de rates medio presentados en las gráficas 6.2a y 6.2b son posibles si se busca mantener un criterio de QoS basado en garantizar un cierto retardo máximo en sistema. En efecto, para valores pequeños de incremento de tráfico puede conseguirse una zona de trabajo con retardo en sistema aproximadamente constante para diferente número de usuarios, pero que aumentando en exceso la sobrecarga de tráfico (a medida que el sistema se acerca a su estado de saturación o de inestabilidad), el retardo comienza a crecer de manera exponencial.

Al igual que ocurría con la evolución de los rates medios, el escenario con distribución de SNR de tipo Rayleigh presenta las peores prestaciones, ya que consigue llegar a un estado de inestabilidad en cuanto a retardo medio en sistema, en un margen menor de sobrecarga de tráfico de entrada que en el caso exponencial. Así por ejemplo, para el caso de N=14 usuarios, el escenario Rayleigh comienza a ser inestable a partir de una sobrecarga del 7.5 % mientras que en el escenario Exponencial esto no ocurre hasta aproximadamente el 22 %.

6.3 Escenario con tráfico IPP

Como comparativa respecto al escenario con generación de tráfico exponencial, se ha simulado un nuevo escenario de trabajo basado en generación de paquetes IPP la cual, tal y como se ha visto en la sección 4, se caracteriza por ser un tráfico a ráfagas con generación exponencial durante el periodo de actividad.

Siguiendo el mismo enfoque que se ha dado para el análisis del Algoritmo M-LWDF para tráfico exponencial, en este nuevo caso el tráfico total de entrada también parte del caso límite para M / M / 1, esto es $I_{total} = m$. Para ello la generación de ráfagas se ha configurado de manera que la tasa media de generación total de paquetes sea la misma que en el caso del escenario contemplado en el apartado



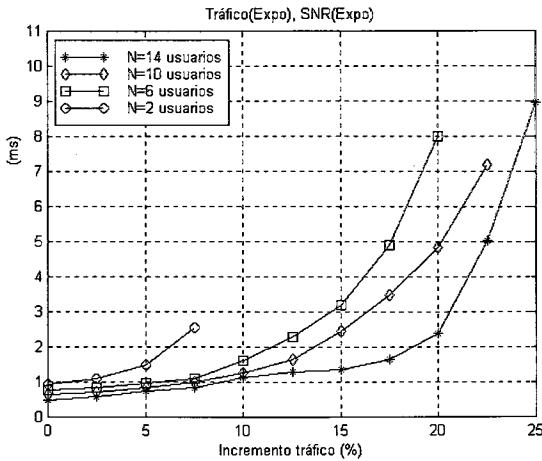


Fig. 6.3a. Retardo medio en sistema en función de la sobrecarga de tráfico de entrada para SNR exponencial.

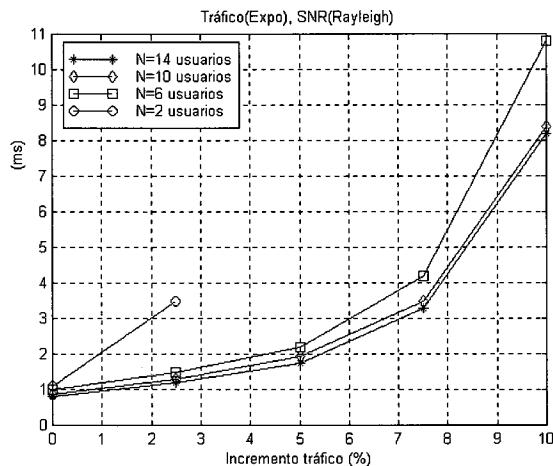


Fig. 6.3b. Retardo medio en sistema en función de la sobrecarga de tráfico de entrada para SNR Rayleigh.

6.2, siendo la tasa individual de llegada durante el periodo de actividad igual a 51. De este modo se pretende evaluar el impacto que supone el cambiar de una naturaleza de tráfico exponencial, a una de tipo a ráfagas, siendo el tráfico ofrecido medio el mismo en ambos casos.

En las figuras 6.4a y 6.4b se muestran los resultados obtenidos para el rate medio de salida en función del incremento de tráfico a la entrada, para las habituales distribuciones de SNR de tipo exponencial y Rayleigh.

La primera observación que puede hacerse es que, al igual que en el escenario de tráfico exponencial, las prestaciones del algoritmo son peores cuanta menor es la varianza de la distribución de SNR que se posee. Esto se aprecia en la figura 6.4b, donde los rates medios conseguidos por el servidor experimentan una leve mejora respecto la media estadística del canal de 10 kbps, y además la evolución para un número mayor de usuarios tampoco ofrece mejoras importantes.

Respecto la figura 6.4a para distribución de SNR exponencial, la mejora en rate medio es apreciable en función del incremento de tráfico ofrecido, pero un fenó-

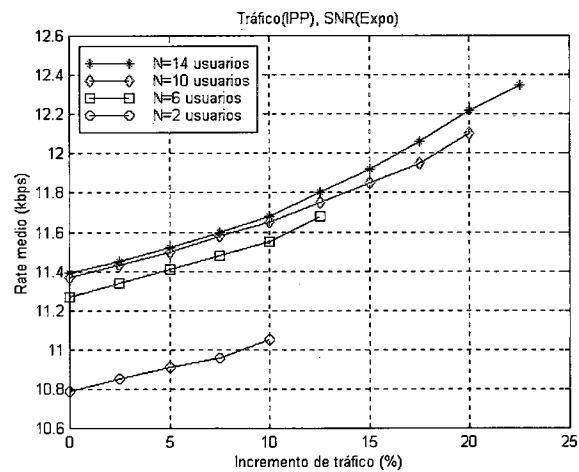


Fig. 6.4a. Rate medio conseguido por el servidor en función de la sobrecarga de tráfico de entrada para SNR exponencial.

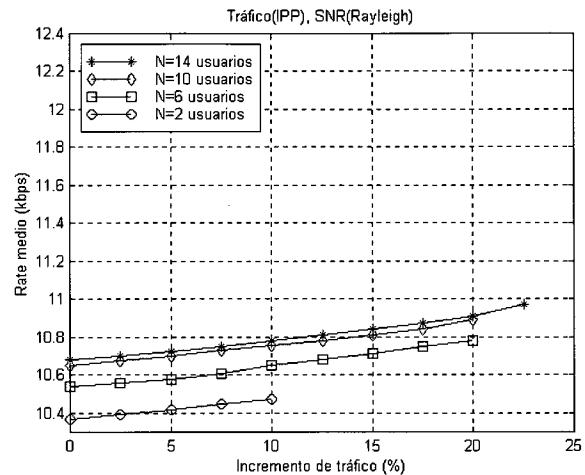


Fig. 6.4b. Rate medio conseguido por el servidor en función de la sobrecarga de tráfico de entrada para SNR Rayleigh.

meno curioso es que los resultados no siguen aumentando a medida que aumenta el número de usuarios sino que a partir de N=6, el incremento de usuarios no mejora sustancialmente el rate medio conseguido, a diferencia de lo que ocurría en el escenario de tráfico exponencial.

Como se indicó en el apartado 6.3, el incremento en número de usuarios es beneficioso para el Algoritmo M-LWDF en términos de mejorar la diversidad estadística de rates instantáneos entre los que elegir el mejor. Entonces la mejora era clara, pues de los dos parámetros que pondera el algoritmo de decisión, esto es, el número de elementos en cola N_i y el rate instantáneo $r_i(t)$ (ver apartado 2.3), el número de elementos en cola se mantiene más o menos constante para el conjunto de usuarios considerados, siendo el rate instantáneo prácticamente el que fija la decisión final. Recordemos que para la realización de este estudio práctico se ha tomado como criterio el análisis del sistema a partir de usuarios con igual tasa de llegada de paquetes, aunque un escenario de simulación mucho más general podría considerar usuarios con tasas de llegadas independientes.

En el caso generar tráfico a ráfagas, a pesar que la tasa media de llegadas para cada uno de los usuarios es la misma, los instantes en los que se producen los períodos de actividad son independientes, por lo que el número de elementos en cola de cada usuario sufrirá grandes variaciones de manera independiente entre los diferentes usuarios. De este modo, el cálculo M-LWDF posee ahora dos variables de gran variabilidad: el rate instantáneo y el número medio de elementos en cola, proveniente éste último como consecuencia de la llegada de paquetes durante el periodo de actividad a una tasa de $5l_i$.

Como resultado, las prestaciones del algoritmo presentan un efecto de saturación a partir de $N=6$ usuarios, pues ahora cuantos más usuarios posea, mayor será también la posibilidad que dos usuarios puedan recibir una ráfaga de paquetes en instantes cercanos. Cada vez que se produce una ráfaga, el número de paquetes en cola crece de manera desmesurada por lo que el algoritmo, en los instantes siguientes, debe prestar la mayor parte de su tiempo a la atención de la ráfaga de ese usuario para disminuir su gran número de elementos en cola, a pesar que su rate instantáneo de transmisión no sea el mejor del sistema.

Ello provoca que, si mientras el servidor intenta atender al usuario que ha recibido una ráfaga, otro recibe una nueva ráfaga, la prioridad del sistema se convierte en la reducción del número de elementos en cola, dejando a un lado la maximización del rate de salida. Es por este motivo por lo que especialmente en la gráfica 6.4a no se observan mejoras importantes en el rate medio de transmisión conforme se aumenta el número de usuarios. El impacto sobre el retardo medio en el sistema se muestra en las gráficas 6.5a y 6.5b.

En tráfico a ráfagas, el efecto de saturación con el número de usuarios puede ahora apreciarse también en las gráficas de retardo medio en sistema. Mientras en la gráfica 6.5a de retardo medio en sistema para distribución de SNR exponencial, a medida que aumenta el número de usuarios disminuye el tiempo en sistema, lo cual es coherente con el hecho que a medida que se aumenta el número de usuarios, esa misma distribución de canal consigue mejorar el rate medio de salida.

Sin embargo, para el caso de la distribución Rayleigh, el hecho que el rate medio apenas mejore a medida que se aumenta el número de usuarios perjudica las prestaciones del sistema. En efecto, a medida que se aumenta el número de usuarios en un escenario con ráfagas mayores son los requerimientos en términos de rate de salida, pues en caso que se coincidan en el tiempo la llegada de varias ráfagas a diferentes usuarios, se necesitará unos buenos rates de transmisión para dar salida a las respectivas acumulaciones de paquetes. Como esto no es posible en una distribución de SNR de tipo Rayleigh, el sistema sufre más para dar salida a los paquetes acumulados cuantos más usuarios posee. Ello se aprecia en la gráfica 6.5b, donde el retardo en sistema disminuye progresivamente para $N=2$,

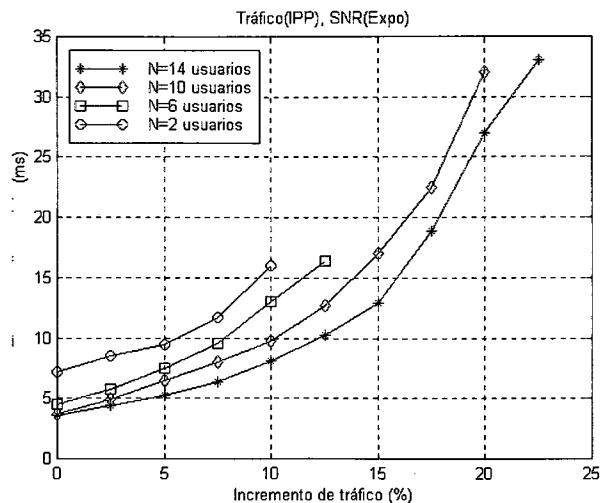


Fig. 6.5a. Retardo medio en sistema en función de la sobrecarga de tráfico de entrada para SNR Exponencial.

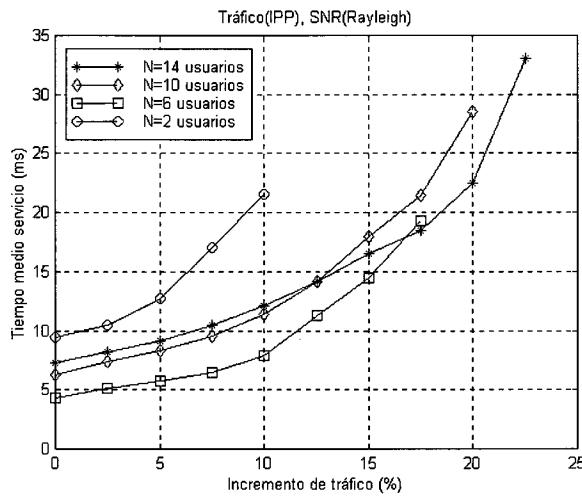


Fig. 6.5b. Retardo medio en sistema en función de la sobrecarga de tráfico de entrada para SNR Rayleigh.

6 usuarios, pero para $N=10$ y 14 usuarios el retardo medio aumenta al no ser capaz el sistema de conseguir rates proporcionalmente buenos respecto el número de usuarios como para seguir la disminución del retardo experimentada para $N=2$ y 6 usuarios.

BIBLIOGRAFÍA

- [1] M. Andrews et al., “Providing Quality of Service over a Shared Wireless Link”, IEEE Communications magazine, February 2001.
- [2] Ana Pérez Neira y Gregori Vázquez, “Sincronització i mòdems d’alta velocitat”, Apuntes de la asignatura optativa de SMAV (ETSETB-UPC), CPET 2000.
- [3] Grup de Comunicacions Ràdio, Dpt. TSC - UPC, “Transparències de Comunicacions Mòbils”, Apuntes de la asignatura de Radiocomunicaciones (ETSETB-UPC), CPET 2000.
- [4] Josep Paradells, “Comunicaciones Móviles de 3ª Generación”, Apuntes de la asignatura optativa de CM3G (ETSETB-UPC), CPET 2001.



YUFORIC'2001

Vicente Esbrí González

Miembro de la Rama de Estudiantes del IEEE de Valencia

YUFORIC'01

YOUTH FORUM IN COMPUTER
SCIENCE AND ENGINEERING

Los pasados días 29 y 30 de Noviembre se celebró en la ETSIT de la Universidad Politécnica de Valencia la YUFORIC '01, que reunió a profesores, empresarios y alumnos de ambos lados del Atlántico.

"La YUFORIC hace especial hincapié en las investigaciones más actuales y prometedoras"

Dicho evento es la punta del iceberg de un programa de la Computer Society del IEEE, cuya primera y más destacada finalidad es la de reunir a estudiantes y profesionales de las nuevas tecnologías en un foro internacional donde intercambiar ideas y compartir experiencias. La YUFORIC hace especial hincapié en las investigaciones más actuales y prometedoras que estudiantes, catedráticos y nuevos profesionales de la industria están desarrollando; con el objetivo de potenciar la creación y el progreso tecnológico. Con este horizonte, se pretende favorecer el debate y la colaboración entre los sectores académico y empresarial, así como animar a los profesionales a que se impliquen con la comunidad universitaria en dos planos básicos: la motivación de los estudiantes y la orientación de éstos en sus intereses de investigación. Como consecuencia, los universitarios obtendrán una visión más amplia y práctica del «mundo real» en general y de la comunidad profesional en concreto.

"La Sociedad de la Información ha devenido en el principal motor del desarrollo tecnológico en Europa"

Respecto a sus contenidos, la YUFORIC parte de la base de que la Sociedad de la Información ha devenido en el principal motor del desarrollo tecnológico en Europa. Dicho desarrollo ha sido espe-

cialmente importante en el terreno de las tecnologías informáticas, que han abierto el camino a nuevas formas de hacer negocios, trabajar y aprender. Como una aplicación clave de Internet se erige el Comercio Electrónico, sin duda el punto que más interés ha despertado hasta la fecha en empresarios, usuarios y desarrolladores de software; pero a su lado comienzan a florecer otras aplicaciones como el Trabajo o Aprendizaje Electrónico. Por tanto, son materias de especial interés todas aquellas relacionadas de manera directa o indirecta con el *E-Commerce*: tecnologías Web y Java, interfaces de usuario, seguridad (certificado digital, PKI, criptografía), autenticación de usuarios, certificados de calidad para el comercio electrónico, métodos electrónicos de pago, plataformas multidispositivo (WAP, set-top box), servicios intermediarios orientados al comercio (CORBA, DCOM, J2EE), etc.

"Los países de Asia Oriental, es donde el desarrollo tecnológico es netamente superior a la media mundial"

La YUFORIC lleva varios años celebrándose en todo el mundo. Aunque su cuna fueron los países de Asia Oriental, donde el desarrollo tecnológico es netamente superior a la media mundial, se ha ido desplazando a grandes capitales de América, Asia y Europa en sus sucesivas convocatorias. Hace cuatro años se celebró en la UPC, y este año la ETSIT de Valencia tuvo el honor de ser su sede en la primera YUFORIC del siglo veintiuno, con el patrocinio de la UPV, la sección Española del IEEE y la Computer Society.

Como hemos indicado, la YUFORIC se dividió en dos días, y cada uno de estos se estructuró en dos sesiones. A su vez, cada sesión consistió en un ciclo de conferencias cortas (ninguna superó los 25 minutos) centradas en un tema relacionado con el

Comercio Electrónico, comenzando en el primer ciclo con una visión bastante general del panorama actual para terminar en el cuarto y último ciclo con el estudio concreto de distintos sistemas de seguridad y pago.

"Por unos motivos u otros quedó la sensación de que la relación entre inversión en investigación-participación en el foro estuvo desequilibrada"

La totalidad de las conferencias se impartieron en inglés; éstas corrieron a cargo de antiguos alumnos y profesores de la UPV prácticamente en la mitad de los casos, el resto de los ponentes pertenecían en su mayoría a otras universidades de España, Alemania, Singapur o Taiwan. Por tanto, pese al carácter empresarial de que se quería dotar al foro, el 75% de las charlas corrieron a cargo de personas relacionadas de manera directa o indirecta con la universidad, echándose en falta una mayor representación de la comunidad profesional independiente. Grandes multinacionales como Nokia estuvieron representadas, pero por unos motivos u otros quedó la sensación de que la relación entre *inversión en investigación-participación en el foro* estuvo desequilibrada. Además, el apretado programa dificultó el establecimiento de un verdadero debate o comunicación entre los asistentes y los conferenciantes, contrariamente a lo que decretaban las premisas del evento.

"YUFORIC '01 donde se estudió la aplicación del PHP a los servicios de acceso WAP"

Las cuatro sesiones en que se dividió la YUFORIC 2001 fueron:

SESSION I: «Case Studies and Architectures», donde se presentaron y analizaron algunos modelos actuales, prestando especial atención a las redes de Banda An-

cha, aprendizaje on-line y modelos de referencia para los e-Business.

"Queda un largo camino por recorrer si se pretende crear un verdadero foro internacional de empresarios y universitarios"

SESSION II: «Application Development and Tools», donde entre otras cosas se estudió la aplicación del PHP a los servicios de acceso WAP.

SESSION III: «Web and network technology», ciclo que se centró en XML, routers para Linux y Protocolos Consistentes para Bases de Datos Replicadas.

SESSION IV: «Security and Payment», sesión basada en las firmas digitales, sistemas de encriptación caóticos y transferencias seguras y anónimas.

El programa del jueves se completó con una visita turística guiada por Valencia en la que se visitó el centro histórico de la ciudad, y una cena para el comité organizador y los conferenciantes.

"YUFORIC '01 fue un éxito"

En resumen, la YUFORIC '01 fue un éxito en cuanto a organización e interés de sus contenidos. Pese a ser también un éxito de participación con respecto a otras convocatorias, sesenta asistentes entre ponentes, organizadores y auditorio parece todavía un registro demasiado corto para el atractivo real del foro y el esfuerzo de organización que éste supone. Tal vez la solución resida en una mayor promoción, no sólo en el ámbito local. Por tanto, aunque el sentimiento general de organizadores y asistentes es profundamente positivo, queda un largo camino por recorrer si se pretende crear un verdadero foro internacional de empresarios y universitarios que fomente la investigación y el desarrollo de las nuevas tecnologías, que hoy por hoy son financiados en su mayor parte por capital privado. Aparentemente la voluntad existe, pero ahora hay que potenciarla.





LA BABEL DE LOS SISTEMAS DE MEDIDA

La unificación del sistema de medida dimensional es imitado por la unificación del sistema monetario

Josep M. Torrents

*Departamento de Ingeniería Electrónica
Universitat Politècnica de Catalunya*

INTRODUCCIÓN

Los 7'1" o "7-foot-1" de Pau Gasol no sorprenden a los entusiastas de la NBA si navegan por internet. El común de aficionados al baloncesto transformamos esa cifra a 216 cm antes de asumir a que altura corresponde. Pies, pulgadas, mills, libras, galones, pintas, etc. son muchas de las unidades de medida a las que no estamos habituados y que nos encontramos por ejemplo si vamos de vacaciones a países de habla inglesa.

Por suerte para los ingenieros del continente europeo, este problema se solucionó no hace tanto tiempo y hoy disfrutamos de un Sistema Internacional (SI) de aceptación global que nos facilita el trabajo. En cambio, si trabajamos en EE.UU. pensaremos en "SI" para investigación o desarrollo pero en "sistema alternativo" para gestión, contacto con proveedores o vida social.



Figura 1. Fotomontaje con Pau Gasol y una moneda de 1 Euro.

Sin ir tan lejos, 1 billete verde son 6 Euros, pero no es suficiente conocer la equivalencia para contar con una unidad u otra eficientemente. Sabemos la teoría pero deberemos practicar a destajo hasta asumir que un bolígrafo "Bic" es barato si nos cuesta 25 céntimos y caro si 50 céntimos. Siempre queda el recurso de traducir a la unidad conocida y decidir después, pero esta estrategia es poco o nada eficiente.

Este artículo curioseaba como se unificó o globalizó, terminó muy en boga, los sistemas de medida dimensionales. Al igual que vivimos la unificación progresiva de monedas a Euro, la aceptación al SI fue

lenta, pero a la larga, beneficio a todo el mundo. Además, los gobiernos protagonistas son casi los mismos (franceses, alemanes, escandinavos e ingleses) y con papeles similares (optimista, dinamizador, retrasado, retraído, etc.). Quizá aprendamos algo de la historia del SI aplicable al presente del sistema monetario. El grueso de la historia parte de la época de la Revolución Francesa inconsciente de cómo se resolviera; y la "evolución" de la moneda en nuestra época de "globalización" no sabemos como se recordará.

LA EVOLUCIÓN

1660, la "Royal Society" de Londres propone la longitud de un péndulo que oscila en un segundo como unidad de longitud. Proposición que suscriben ilustres franceses como Jean Picard y La Condamine, holandeses como Christian Huygens, ingleses y norteamericanos como John Miller y Jefferson.

1670, el abad Gabriel Mouton propone la milésima parte de la milla náutica (una milla es un minuto de meridiano) como unidad de longitud. Esta unidad (1,85 m) es quizás demasiado grande para ser práctica.

1672, Richer descubre que la longitud del péndulo es función de la latitud del emplazamiento y en vez de buscar un lugar "nominal", se rechaza la idea de esta unidad.

1790, 8 de mayo, Talleyrand propone en la Asamblea Constituyente francesa la creación de un sistema de medida simple y unificado. Se encarga el estudio a una comisión de la Academia de Ciencias que incluye, entre otros, a Lagrange, Laplace, Monge, Borda y Lavoisier. Se elige la medida del péndulo que oscila en un segundo.

1791, 26 de marzo, la comisión asesora a la Asamblea Constituyente para que elija como unidad de longitud la diezmillonésima parte de un cuarto de meridiano terrestre (entre el polo y el ecuador). Charles Borda le da el nombre de metro atendiendo a la etimología griega (metron=medida). ¡Ya solo falta medirlo!

La comisión determina las demás unidades a partir de la unidad de longitud, salvo la de tiempo: La unidad de superficie, el área, es el cuadrado de un decámetro. La

unidad de peso, el kilogramo, es el peso del volumen unidad (litro) de agua pura a temperatura de fusión a una atmósfera.

1792-1799, “expedición del meridiano”, en la que participan también los físicos Coulomb, Haüy y Hassenfratz. Se enlaza Dunkerque y Barcelona mediante hitos geodésicos. Un equipo triangula bajo la dirección de los astrónomos Delambre y Méchain. La distancia medida resulta $5,131 \cdot 10^6$ toesa (1 toesa=1,946 m). La Caille, de forma previa y más exacta, había medido $5,129 \cdot 10^6$ toesa. Un segundo equipo establece los patrones en platino y un tercero redacta los manuales de uso como se comenta a continuación.

1793, 1 de agosto, Decreto que decimaliza (múltiplos y submúltiplos siempre en potencias de 10) el sistema monetario y las medidas de longitud, superficie, volumen y peso, cambiando el múltiplo habitual que era la docena.

1795, 7 de abril, la Ley del 18 Germinal, año III, organiza el sistema métrico: Define el metro como fracción de meridiano y fija las unidades y sus múltiplos y submúltiplos. 9 de junio, Lenoir construye el primer patrón métrico legal referido a las medidas de La Caille. 25 de junio, se crea la Oficina de las Longitudes en París.

1799, la Conferencia Internacional de París debate la adopción universal del sistema métrico. Finalmente se concluye como demasiado revolucionario para su implantación. 22 de junio, el segundo equipo antes mencionado construye en platino los prototipos definitivos de metro y de kilogramo y los deposita en los Archivos Nacionales. 10 de diciembre, Ley del 19 Frimario, año VIII que fija las definiciones y patrones definitivos. En teoría, obliga al uso del sistema métrico (empresa difícil por el arraigo de costumbres de medida en sistemas previos).

1840, 1 de enero, entra en vigor la ley de 4 de abril de 1837 que obliga al uso del sistema métrico.

1875, se crea en Sèvres la Oficina Internacional de Pesos y Medidas.

1889, la Conferencia General de Pesos y Medidas, define el metro como la distancia del patrón métrico internacional de platino iridiado.

1960, 14 de octubre. Gracias a los progresos instrumentales se define el patrón óptico de metro como la $1.650.763,73$ longitudes de onda en el vacío de la radiación anaranjada del criptón de peso atómico 86.

1983, 20 de octubre. La XVII Conferencia General de Pesos y Medidas define el metro en función de la velocidad de la luz como el trayecto recorrido por la luz en el vacío durante $1/299.792.458$ segundo. Donde el segundo se define como la duración de $9.192.631.770$ periodos de la radiación de la transición entre dos niveles hiperfinos del átomo de cesio 133. También fija las normas del Sistema Internacional.

CONCLUSIONES

El acuerdo hacia el uso de un sistema de medidas global, el Sistema Internacional, fue un pequeño descubrimiento o una pequeña “revolución” que tardó en imponerse. Si se analiza el resultado, el SI ha sido muy útil porque creó una nomenclatura eficiente para medir y porque proporcionó un código casi universal, adelantándose a su tiempo, para la “aldea global” que vivimos.

Si podemos establecer analogías en la Historia de la humanidad, además de ciclicidad y repetición, debería ser mucho más fácil aprender de errores y aciertos pasados. La dificultad estriba en que el periodo de cada ciclo es una variable pseudoaleatoria y el análisis estadístico no experimental, como en ciencias sociales, resulta incierto.

BIBLIOGRAFÍA Y OTRAS LECTURAS RECOMENDADAS

- [1] <http://nbadraft.net/profiles/paugasol.htm>
- [2] Kowalenko, Kathy, 2001. “Willing to relocate? Try global job market”.
- [3] The Institute, vol. 25, junio, pág. 1 y 12.
- [4] Ifrah, Georges, 1997. Historia universal de las cifras: la inteligencia de la humanidad contada por los números y el cálculo. Editorial Espasa, Madrid, pág. 120-123.
- [5] <http://www.ctv.es/USERS/pmc/>
- [6] <http://physics.nist.gov/Pubs/SP811/cover.html>
- [7] <http://www.unc.edu/~rowlett/units/>
- [8] <http://europa.eu.int/euro/html/home1.html?lang=1>
- [9] La Vanguardia, 2001. Joan Monfort/Sport, 1 de julio.

AUTORES



Josep M. Torrents se graduó y se doctoró en Ingeniería de Telecomunicación en la Universidad Politécnica de Cataluña (UPC) en 1989 y 1996 respectivamente.

Vinculado al Departamento de Ingeniería Electrónica de la UPC desde 1987, actualmente ejerce el cargo de Profesor Titular. Obtuvo una beca postdoctoral del Ministerio de Educación y Cultura durante el curso 98/99. Investigó con el Profesor Thomas O. Mason en la Universidad de Northwestern (Illinois, EE.UU.) en la Escuela de Ingeniería y Ciencias Aplicadas Robert R. McCormick y en el centro para materiales avanzados de base cemento (ACBM) de la Fundación Nacional de Ciencia (NSF). Su interés actual se centra en instrumentación electrónica, sensores, acondicionamiento de señal, calibración y cálculo de incertidumbres y en medida y caracterización de materiales por métodos eléctricos no destructivos (impedancia, tdr). Dr. Torrents es miembro de IEEE desde 1990.

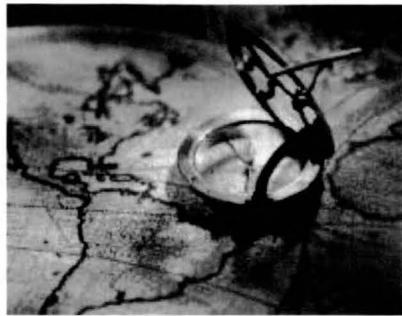




BREVE INTRODUCCIÓN AL SISTEMA DE POSICIONAMIENTO EUROPEO POR SATÉLITE GALILEO

Enric Chillaron i Farré

Estudiante de la ETSETB y Miembro de la Rama de Estudiantes del IEEE de Barcelona
bovera25@casal.upc.es



« Whatever happens, Galileo will be a reality. It might not be a PPP (Public-Private-Partnership); it might be another thing. The important thing is that nothing can stop it now.»

B. H. Andersen, European Commission Directorate General for Transport and Energy (2000).

INTRODUCCIÓN

El espacio ha sido materia de estudio y de reflexión a lo largo del tiempo. Los antiguos filósofos griegos ya concebían el espacio como la oposición entre lo realmente lleno (*pléo*) y el más puro vacío (*kénon*). Platón definió el espacio como el habitáculo de las cosas creadas, y Aristóteles lo hizo como el lugar donde las cosas son particularizaciones. Posteriormente, se adoptó una idea *relacional* del espacio, como la que definió Leibniz, o *absoluta*, como la de Newton y Clark. La Edad Media y la filosofía escolástica adoptaron la doctrina aristotélica del espacio y lo definieron como un receptáculo *real* o *imaginario*. El mundo moderno dividió el concepto de espacio en dos bloques: por una lado, el mundo occidental o *racional* de Descartes y Spinoza; y por otro lado, el mundo insular o *empírico* de Locke y Berkeley. Pero sin duda, las aportaciones de la física contemporánea son fundamentales para la comprensión del concepto de espacio, cuya orientación viene marcada por el espacio tetradimensional de Hermann Minkowski y, en especial, por Albert Einstein y su teoría de la relatividad.

Este artículo presenta una breve introducción al sistema de posicionamiento por satélite de carácter europeo, *Galileo*. Se ha creído oportuno dejar de un lado los tecnicismos en pos de ofrecer una visión global del proyecto y de su futuro alcance (referente a lo económico y a sus aplicaciones).

Al mismo tiempo que se realizarán comparaciones puntuales con el sistema *GPS*, se delimitará el marco de trabajo del sistema *Galileo* así como sus características orbitales y frecuenciales.

Finalmente, se presenta al lector una futura valoración económica del proyecto en lo que refiere a beneficios como a costes de implantación

Galileo aparece como un proyecto europeo potente, delante del ya asentado GPS

El único requisito para seguir plenamente este artículo es tener nociones puntuales sobre GPS.

NECESIDADES DE GALILEO

Galileo aparece como un proyecto europeo potente, delante del ya asentado *GPS*, con cuatro vías de desarrollo bien delimitadas:

- Política.
- Tecnológica.
- Social.
- Económica.

La vía política, subsanada por los miembros de la comunidad europea, la dirigen principalmente los países integrantes. La vía tecnológica se centra en el fuerte

mercado tecnológico europeo en materia aeronáutica e ingeniería. La vía social engloba la necesidad de posicionarse con máxima precisión y de manera autocontenido. Y, finalmente, la vía económica (la más crítica actualmente) depara mucho futuro comercial y poco presente.

FASES DEL PROYECTO	COSTE EN MILLONES DE EUROS
Definición (1999-2000)	80
Desarrollo y validación (2001-2005)	1.000
Despliegue	2.150
Operativo	220 por año

Tabla 1.- Programa de coste de Galileo (incluyendo Egnos).

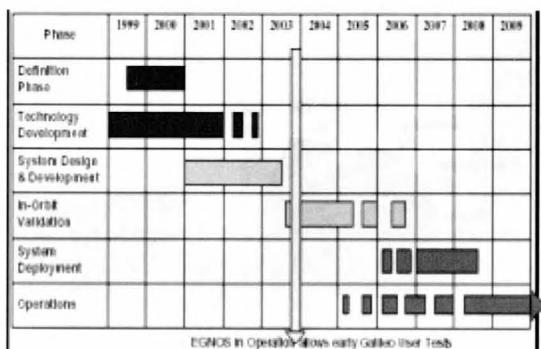


Figura 1.- Planning en el programa de desarrollo de Galileo.

APLICACIONES Y CARACTERÍSTICAS

El sistema de posicionamiento *Galileo* se caracteriza por ser un sistema claramente civil, comercial, seguro e independiente del *GPS* (pero con un futuro muy ligado al de este último). Además de contar con una cobertura total europea, *Galileo* estará dirigido por organismos no militares (como difiere *GPS*).

Galileo, podrá ofrecer servicios en aplicaciones aéreas, terrestres (automóviles y trenes), marítimas, de emergencia, laborales o incluso lúdicas.

Segmento espacial: *Galileo*, que se prevé que opere en el 2008, tendrá una constelación de 30 satélites de órbita media (MEO), además de algunos geoestacionarios (aún por determinar), distribuidos proporcionalmente en tres órbitas.

El sistema utilizará tres frecuencias a E1 (1589MHz), E2 (1561MHz) y E4 (1295MHz).

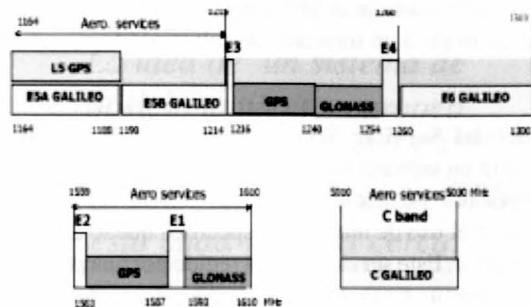


Figura 2.- Localización de las frecuencias de trabajo de Galileo en la banda L y C.

Segmento terrestre: El segmento en tierra estará formado por una estación central (*Navegation Satellite Control Center*) además de otra de *backup*, y por doce estaciones esclavas (*Tracking Stations*) con otras tres de reserva. Su ubicación está aún por determinar.

	Galileo	GPS
# satélites	30+?	27
# órbitas	3	6
# frecuencias	3	2+1 (~2014)
Servicio 100 % garantizado	👍	👎
Incertidumbre en medida (95%)	6-7 metros	10-12 metros ¹
Combinando ambos sistemas se garantizan 3-4 metros.		

Tabla 2.- Tabla comparativa entre un sistema GPS y Galileo.

¹ Caso óptimo sin uso de técnicas diferenciales y sin ningún tipo de degradación como la S/A.



Segmento usuario: Este último bloque lo integra el usuario que se tiene que posicionar con un receptor combinación de receptores GPS+Glonass+Galileo.

SERVICIOS DE NAVEGACIÓN

Galileo ofrecerá tres tipos de servicios de navegación con amplia cobertura.

O.A.S (Open Access Service): Será un servicio libre para todo usuario (similar al SPS que ofrece el GPS) dedicado especialmente a un mercado de aplicaciones.

Comercial Service: Servicio basado en el O.A.S que proveerá un servicio con el valor añadido garantizado de encriptación de datos. El acceso a este servicio será mediante el uso de una clave específica que lo diferencie del anterior. Este servicio estará regido por una política de precios en sus tasas. Cabe decir que el uso del servicio comercial resolverá la ambigüedad en el servicio de tres portadoras (TCAR).

Galileo ofrecerá tres tipos de servicios de navegación con amplia cobertura.

Public Services : Este último servicio se dividirá en dos partes:

. **P.R.S (Public Regulated Service) & S.A.S (Safety of Life Service)** servicio controlado de alta seguridad e integridad que no tolera ninguna disfunción del sistema ni en tiempos de crisis.

. **S.A.R (Search&Recue)**

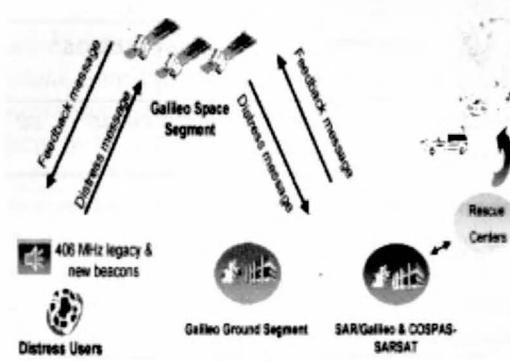


Figura 3.- Servicio S.A.R.

MERCADO EUROPEO

Galileo ofrece un abanico de posibilidades tan diversas como suculentas, comercialmente hablando. En este apartado se ofrecen unos gráficos en los que se puede observar la tendencia al alza del uso del sistema de posicionamiento europeo.

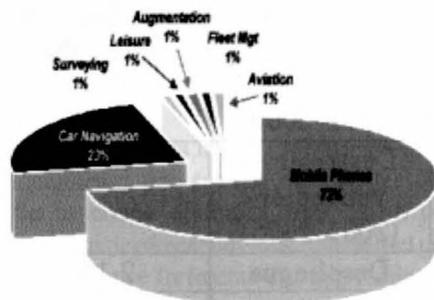


Figura 4.- Estimado mercado europeo en 1999 valorado en •1Bn.

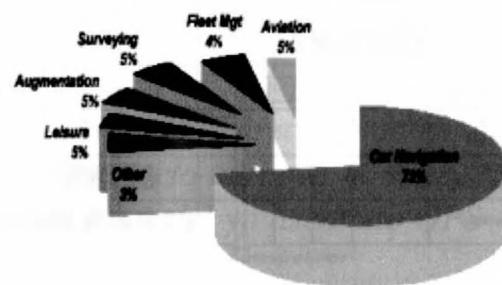


Figura 5.- Estimado mercado europeo en 2005 valorado en •6Bn.

De este modo, para hacernos a la idea de los miles de euros que pueden estar vinculados al uso de *Galileo*, se estima que la industria del sector espacial europeo y el operador *Galileo* tendrán unos beneficios de cerca de •190 M por año con un extra de •740 M durante la fase de despliegue.

Galileo ofrece un abanico de posibilidades tan diversas como suculentas, comercialmente hablando.

Igualmente, se estima que los productores de servicios relacionados con *Galileo* incrementarán sus ganancias en valor de •20M por año (a partir de 2010) hasta llegar a los hipotéticos •80M por año, diez años más tarde.

Se estima que los productores de servicios relacionados con Galileo incrementarán sus ganancias en valor de •20M por año hasta llegar a unos hipotéticos •80M por año.

Estos beneficios económicos estarán ligados a los sociales, reduciendo así las congestiones de tráfico e incrementando la seguridad.

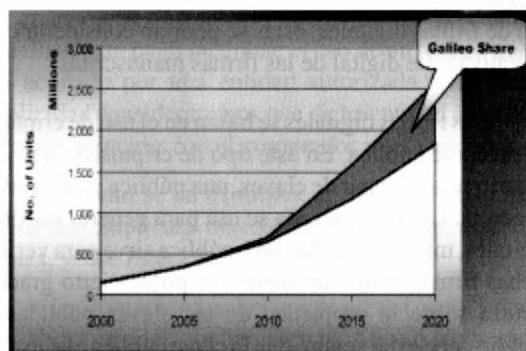


Figura 6.- Tamaño estimado del mercado de Galileo.

Finalmente, en la siguiente tabla se puede observar un análisis de los beneficios correspondientes entre 2000 y 2020.

ANÁLISIS DE BENEFICIOS 2000-2020	
Beneficios económicos	€62Bn
Beneficios Sociales	€12Bn
Total de Beneficios	€74Bn
Total de costes (€3.25Bn + operaciones)	€6Bn
Ratio interno recibido del	75%

Tabla 3.- Análisis de beneficios.

CONCLUSIONES

El sistema de posicionamiento *Galileo* surge en un mundo donde posicionarse llega a ser tan necesario como consultar la hora. Las facilidades que este sistema nos puede ofrecer son tan diversas como tentativas para los futuros ingenieros que vean en el proyecto un sínfín de posibilidades laborales.

La idea de un sistema de posicionamiento europeo gobernado por los 15 y rivalizando el aposentado GPS está cada vez más cerca.

A pesar de lo dicho, *Galileo* padece de una agravante de carácter político-financiero más que tecnológico, que frenará su desarrollo inmediato. Aún así, la idea de un sistema de posicionamiento europeo gobernado por los 15 y rivalizando el aposentado GPS está cada vez más cerca.

REFERENCIAS

- [1] <http://www.galileo-pgm.org/>
- [2] <http://www.genesis-office.org/>
- [3] Martínez, J. A.; Fuster, J.M. «*El Sistema de Posicionamiento Global (GPS)*».

AUTOR



Enric Chillaron i Farré nació en Lleida el 23 de agosto de 1979. Estudió Ingeniería Técnica de Telecomunicación, especialidad en Sistemas de Telecomunicaciones, en la Universidad de Vic. Titulado en el año 2000, realizó su Proyecto de Final de Carrera sobre GPS. Actualmente es estudiante de Ingeniería de Telecomunicación en la Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona. Desde el año 2001 pertenece a la Rama de Estudiantes del IEEE de Barcelona.



SISTEMAS DE PAGOS ELECTRÓNICOS



Josep Pegueroles Vallés

Profesor Asociado del Departamento de Ingeniería Telemática
Universitat Politècnica de Catalunya

josep.pegueroles@entel.upc.es

1. INTRODUCCIÓN.

Inmersos en la denominada Sociedad de la Información, nuestra forma de relacionarnos está cada vez más ligada a las redes de ordenadores y en particular a Internet. La tecnología basada en el uso de computadoras está transformando nuestra forma de acceder, guardar y distribuir la información. Uno de los campos que ya ha sufrido un cambio importante debido a la introducción de estas tecnologías es el comercio.

La realización de transacciones financieras a través de información electrónica sobre líneas de telecomunicaciones es lo que se denomina comúnmente Comercio Electrónico. Un punto clave para el éxito del comercio electrónico es el uso de sistemas de pago seguros y eficientes. La necesidad de seguridad en este tipo de transacciones se ve incrementada si se tiene en cuenta que se estima que la mayoría de dichos intercambios se realizarán a través de Internet (ya sea mediante el uso de ordenadores personales o teléfonos móviles).

Existen distintos sistemas de pago electrónicos: cheques digitales, tarjetas de crédito, tarjetas de débito, tarjetas prepago... Los servicios de seguridad requeridos usualmente para este tipo de sistemas son privacidad (protección frente a escuchas), autenticación (identificación de usuario e integridad del mensaje) y no repudio (protección frente a negaciones de servicio prestado).

El sistema de pago electrónico menos extendido, debido en gran medida a la dificultad de su implementación, es la moneda electrónica o *Electronic cash*. Tal como su nombre indica, los sistemas de moneda electrónica pretenden ofrecer un sistema de pago con las mismas características que presenta la moneda tradicional o papel moneda.

La moneda electrónica deberá ser: universal, es decir, deberá poderse utilizar en cualquier lugar y a través de cualquier medio electrónico; segura, de difícil falsificación y duplicación; anónima, deberá poder utilizarse sin que su propietario sea identificado, de la misma forma que es posible efectuar el pago de servicios o productos mediante la moneda corriente sin que los billetes utilizados puedan por lo general identificar al comprador; autentifiable, su validez deberá poder ser comprobada sin necesidad de acudir a una entidad de verificación, de la misma forma que la autenticidad de los billetes en curso

puede ser reconocida por lo general sin acudir al banco; transferible, ha de ser posible intercambiar bits de un monedero electrónico a otro, de la misma forma que es posible hacerlo con los billetes; divisible, debe ser posible hacer cambios de un valor a valores inferiores, lo mismo que un billete analógico de un determinado valor es equivalente al conjunto de otros de valor más pequeño.

La mayoría de estudios sobre moneda electrónica se centran en garantizar las características de no trazabilidad y anonimato. En general, los esquemas de moneda electrónica consiguen estos servicios de seguridad mediante el uso de firmas digitales, éstas se podrían considerar como el equivalente digital de las firmas manuscritas.

Las firmas digitales se basan en el uso de criptografía de clave pública. En este tipo de criptosistemas, cada usuario posee un par de claves, una pública y otra privada o secreta. La clave privada se usa para generar las firmas digitales, mientras que la clave pública sirve para verificar dichas firmas. Este mecanismo requiere cierto grado de certeza sobre la propiedad de las claves públicas (un usuario debe estar seguro que la clave pública que usa para verificar al firmante realmente pertenece al firmante), esto introduce un problema de gestión de claves y su solución pasa por crear una cierta infraestructura para la autenticación, esto es, existencia de organismos notarizadores de la propiedad de esas firmas. Además, estos sistemas deben presentar seguridad física y de red suficiente para garantizar la privacidad de las claves secretas.

En este artículo se da una visión general del estado del arte en los mecanismos de pagos electrónicos, haciendo especial hincapié en los sistemas de pagos anónimos y aproximaciones a sistemas de moneda electrónica. En primer lugar se presentan las definiciones de los conceptos y la terminología básica usada en el campo así como los criterios de clasificación más comúnmente usados. Seguidamente se presenta las herramientas básicas usadas para prestar servicios de seguridad a los sistemas de pagos electrónicos. A continuación, partiendo de un modelo clásico sencillo de transacción electrónica segura sin anonimato ni no trazabilidad, se discutirá sus ventajas y carencias, y se irán presentando protocolos más sofisticados para finalmente exponer el modelo que cumpla las características de moneda electrónica. Finalmente se describen a alto nivel algunos de los protocolos propuestos en la

literatura, clasificados según sus características de trazabilidad y on/off-line.

2. DEFINICIONES.

Antes de adentrarnos en los protocolos de pagos electrónicos haremos un breve repaso a la nomenclatura y definiciones más comúnmente usados.

2.1 Comercio Electrónico vs Pagos Electrónicos.

El término Comercio Electrónico se refiere a cualquier transacción financiera que implique transmisión de información de forma electrónica. Los paquetes de información que se transmiten se denominan testigos electrónicos o Electronic tokens. No se debe confundir el testigo, que es una secuencia de bits, con su soporte físico, este soporte físico se denomina comúnmente tarjeta, ya que la mayoría de veces toma la forma de una tarjeta de plástico del tamaño de un monedero (un ejemplo serían las tarjetas de crédito); de cualquier forma también puede ser, por ejemplo, la memoria de un ordenador.

Un caso particular de comercio electrónico es el pago electrónico. Un protocolo de pago electrónico consiste en una serie de transacciones al final de las cuales se ha realizado un pago mediante el uso de un testigo que ha sido acuñado por una entidad autorizada. Para mayor simplicidad consideraremos que dicha entidad autorizada no puede coincidir con el comprador ni el vendedor.

Tal como se ha expuesto, el esquema de un pago electrónico implicará necesariamente el concurso de 3 agentes, véase figura 1:

- Un comprador, aquel que realiza el pago, y que de ahora en adelante llamaremos Alice o Comprador.
- Un vendedor, aquel que recibe el pago, y que de ahora en adelante llamaremos Bob o Vendedor.
- Una entidad financiera, de la cual Alice retira el dinero de su cuenta y a la cual Bob deposita el dinero en su cuenta. A dicha entidad la denominaremos a partir de ahora Banco, y para mayor simplicidad, de momento, sólo consideraremos el caso en que Alice y Bob tienen cuenta en el mismo banco.

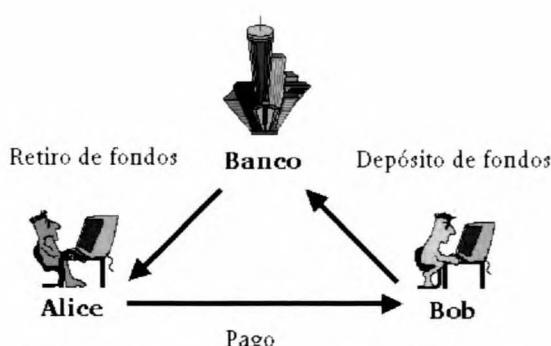


Figura 1. Esquema básico de pago electrónico

Adicionalmente, en esquemas más complejos, puede aparecer la figura del intermediario, que se encargaría de funciones propias del Banco, pero lo haría transparente a Comprador y Vendedor. Más adelante nos encargaremos de esta figura.

2.2 Seguridad en los pagos electrónicos.

Los pagos electrónicos, expuestos en el apartado anterior, pueden realizarse a través de medios de transmisión abiertos o cerrados. Con el auge de las telecomunicaciones y el éxito de la red Internet, cada vez es más frecuente que dichas transacciones electrónicas se realicen sobre medios de transmisión inseguros (pensemos que hasta hace muy poco la mayoría de transacciones electrónicas se realizaban a través de EDI sobre circuitos propietarios o mediante líneas dedicadas). Este escenario hace especialmente importante la seguridad de los mensajes que se envían a través de esas redes.

Los servicios básicos de seguridad requeridos para que se confíe en las transacciones económicas sobre este tipo de medios electrónicos son:

- Privacidad, o protección frente a escuchas. Este servicio es especialmente importante para transacciones en las que los números de tarjetas de crédito se envían a través de la red.
- Identificación de usuario o protección frente a suplantación de personalidad. Cualquier intercambio o transacción económica debe asegurar que los participantes en esa transacción sepan con quien están tratando.
- Integridad o protección frente a sustitución del mensaje original. Se debe asegurar que la copia del mensaje que se recibe es la misma que la que se envió.
- Repudio, o protección frente a posteriores negaciones de servicio prestado o recibido.

Normalmente, los tres últimos servicios se engloban en un único término: Autenticación. Estos servicios de seguridad se pueden conseguir de muy distintas formas, la técnica más empleada se fundamenta en Infraestructuras de Autenticación.

En dicho esquema, la privacidad se consigue mediante el cifrado del mensaje con una clave secreta conocida únicamente por el emisor y el receptor. La autenticación se consigue mediante sistemas de distribución de claves. Los sistemas de distribución requieren autoridades de certificación, o agentes de confianza que son los responsables de garantizar la identidad de usuario. Cada integrante en una transacción económica debe tener su identidad garantizada (incluyendo los bancos) mediante un certificado. Este certificado se puede usar cada vez que el usuario quiera identificarse frente a otro usuario.

Aunque la infraestructura de autenticación no se puede considerar parte integrante del esquema de comercio electrónico, los servicios de seguridad que proporciona son esenciales en dicho esquema. En todos los modelos

propuestos en este informe se asume la existencia de una infraestructura de autenticación que proporciona dichos servicios, de esta forma, en la exposición de los protocolos, nos centraremos en la parte referida a la transacción.

2.3 Anonimato y concepto de Moneda Electrónica.

Los servicios de seguridad expuestos anteriormente se consideran los mínimos necesarios para depositar confianza en un sistema de pago electrónico pero distan mucho de tener todas las propiedades expuestas por Okamoto en [Oka92].

Pensemos que el término Dinero Electrónico se usa normalmente para designar cualquier tipo de pago electrónico que de alguna manera hace pensar al usuario que dispone de "efectivo", aunque en realidad, dicho término sólo hace referencia a un sistema específico de pago que viene muy acotado por ciertas propiedades criptográficas.

Hasta el momento, dentro de la definición de seguridad, sólo nos hemos referido a la privacidad como protección frente a escuchas, pero existe un concepto mucho más amplio de privacidad, introducido por David Chaum en 1992 [Cha92]. En dicha definición Chaum afirma que no existe privacidad completa mientras las entidades financieras puedan confeccionar historiales de compras susceptibles de ser analizadas no sólo por ellos sino también por el gobierno.

Para conseguir esta privacidad en sentido más amplio, no sólo se requiere el uso de las técnicas tradicionales que proporcionaban protección frente a escuchas sino que además se necesita anonimato en las transacciones.

En particular aparece la necesidad de dos nuevos servicios:

- Anonimato del comprador durante el pago.
- No trazabilidad del pago, de forma que el banco no pueda averiguar "el dinero de quien" se ha usado para realizar un determinado pago.

Las tarjetas de crédito convencionales no proporcionan este tipo de seguridad, por esta razón Chaum introdujo el concepto de Moneda Electrónica, *electronic cash* o *digital cash*, como un sistema de pago electrónico que garantice, además de los servicios básicos expuestos los de anonimato y no trazabilidad antes mencionados. Como también se aprecia en la figura 1, cualquier esquema de pago electrónico debe seguir los siguientes pasos:

- Retiro de fondos o en inglés *withdrawal*. Donde Alice transfiere parte de su dinero desde su cuenta en el banco a una tarjeta propia.
- Pago en donde Alice traspasa el dinero de su tarjeta a la de Bob.
- Depósito de fondos en el cual Bob transfiere el dinero que ha recibido de Alice a su cuenta en el banco.

Estos pasos se pueden realizar de dos distintas formas:

- On-line, si Bob contacta con el banco para verificar la validez del testigo de Alice antes de aceptar el pago y enviarle el producto, es decir, durante el proceso de compra se contacta con el Banco. Este mecanismo es el más usado hoy en día en sistemas basados en tarjeta de crédito.
- Off-line, Bob realiza el depósito del dinero que le ha dado Alice, para que el Banco lo verifique y lo ingrese en su cuenta, cierto tiempo después de que le haya aceptado el dinero y enviado el producto. Es decir, Bob no contacta con el banco durante el proceso de compra-venta.

Existen otras formas de clasificar los pagos electrónicos, atendiendo al momento en que se realiza el retiro de dinero de la cuenta del comprador. En este sentido, los pagos electrónicos se pueden clasificar en:

- Sistemas pre-pago. Si el comprador ve decrementada su cuenta bancaria antes de realizar la compra. Este método se correspondería con los sistemas de monedero electrónico y tarjetas telefónicas. Éste sería el sistema más análogo al papel moneda tradicional.
- Sistemas de pago instantáneo. Cuando al comprador se le realiza el cargo en cuenta justo en el momento de realizar la compra. Se correspondería con los sistemas actuales de pagos con tarjeta de débito (Visa Electron, 6000, ...).
- Sistemas a crédito. Cuando Alice realiza la compra, el Banco asegura al vendedor que se le hará efectiva la cantidad acordada, pero Alice sólo verá decrementada su cuenta cierto tiempo después de haberse realizado la compra.

Otro criterio habitual es la cantidad implicada en la transacción, de esta forma se clasifican los pagos electrónicos como:

- Macropagos, cualquier pago superior a 10 euros.
- Pagos, aquel que la cantidad está comprendida entre 1 y 10 euros.
- Micropagos, cualquier pago inferior a 1 euro.

Los pagos superiores a 10 euros se realizan mayoritariamente entre dos empresas, es por esto que también reciben la denominación global de pagos B2B (*Business to Business*).

Normalmente los pagos inferiores a 10 euros, tanto si son pagos como micropagos, se realizan entre empresa y usuario o entre usuario y usuario, por esto, este tipo de pagos también se denominan B2C (*Business to Consumer*) o C2C (*Consumer to Consumer*) dependiendo del caso. Estos últimos sistemas presentan el problema añadido del coste de implementación, ya que no tendría sentido utilizar un sistema de pago cuyo coste económico sea del orden de magnitud o superior al importe de la transacción.

Finalmente, la prestación o no de los servicios de seguridad añadidos presentados por Chaum en [Cha92] (Anonimato y trazabilidad) también sirven para clasificar los pagos electrónicos como Anónimos o No Anónimos, Trazables o No Trazables.

Atendiendo a estas clasificaciones, el sistema electrónico análogo al papel moneda descrito por Okamoto debería ser Off-line, Pre-pago, Micropago, Anónimo y No trazable.

Llegados a este punto se podría plantear que las características extendidas que serían deseables en un sistema de pago electrónico entran en conflicto con las características básicas que se les pedía a los sistemas de pago electrónicos, la identificación de usuario frente al anonimato, por ejemplo, o el no repudio frente a la trazabilidad.

Una reflexión profunda sobre el significado de dichas características llevaría a la interpretación de los servicios clásicos de Identificación de usuario, Integridad y No Repudio como garantía de legitimidad de usuario. En otras palabras, que garanticen que el participante en la transacción es un individuo autorizado y competente para realizar la transacción, aunque no se sepa realmente quien es. Visto esto, podríamos reformular las características generales de cualquier sistema de pago electrónico como:

- Secreto
- Legítimo

La necesidad de distintas características: Anonimato o Identificación, Trazabilidad o No Repudio, Pagos Grandes o Pagos Pequeños... darán lugar a distintas creaciones de pagos electrónicos, una de las cuales será la Moneda Electrónica.

2.4 Nuevas Amenazas.

La introducción de las nuevas características de anonimato y no trazabilidad que dan lugar al concepto de Moneda Electrónica propician la aparición de nuevas amenazas de uso indebido de la misma que debemos evitar o detectar. Análogamente a lo que ocurre con la falsificación del papel moneda tradicional, existen dos riesgos de uso ilícito en los sistemas de moneda electrónica:

- Falsificación de testigo o *Token forgery*. Que consiste en la creación de una moneda electrónica aparentemente válida sin la realización del correspondiente retiro de fondos.
- Pago múltiple, en inglés *Multiple spending, re-spending, double spending o repeat spending*. Que consiste en el uso de la misma moneda electrónica para realizar distintos pagos, de modo que un único retiro de fondos cubriría múltiples compras. Esta amenaza toma gran relevancia ya que debe tenerse en cuenta que la moneda electrónica no es más que información digital, y por tanto, reproducible tantas veces como se quiera.

Existen dos filosofías de protección frente a estas amenazas: protección a priori, o intentar prevenir que las amenazas se materialicen en ataques, y a posteriori, que consiste en la posibilidad de detección del ataque y su correspondiente penalización, de esta forma no se toma ninguna medida para que no se realice el ataque, pero se garantiza que un ataque será detectado, y consecuentemente, penalizado.

3 PROTOCOLOS

Seguidamente se presentarán los protocolos genéricos básicos para conseguir los distintos sistemas de pago según las características expuestas en la sección anterior. Partiendo de un modelo clásico sencillo de transacción electrónica segura sin anonimato ni no trazabilidad se irán presentando protocolos más sofisticados para finalmente exponer el modelo que cumpla las características de moneda electrónica.

3.1 Pagos electrónicos trazables.

Los pagos electrónicos trazables son aquellos en que es posible saber qué individuo ha realizado una determinada compra o transacción.

3.1.1 Pago electrónico on-line.

En todos los sistemas on-line la acción de pago y la de depósito coinciden ya que la conexión obligada para la comprobación de la validez del token se aprovecha para ingresar el token en la cuenta del receptor. Los sistemas on-line son los de más fácil solución frente a problemas de *double-spending* pero a su vez son los que generan mayor tráfico en las redes, debido precisamente a la necesidad de realizar una conexión con el Banco para cada realización de pago.

La serie de acciones implicadas en el proceso son las que se describen a continuación.

Retiro de fondos:

- Alice envía una petición de retiro de fondos al Banco.
- El Banco prepara una moneda electrónica y la firma digitalmente.
- El Banco envía una moneda a Alice y la carga en su cuenta.

Pago y depósito de fondos.

- Alice envía la moneda a Bob.
- Bob contacta con el Banco y le envía la moneda.
- El Banco verifica la firma digital del Banco.
- El Banco verifica que la moneda no ha sido ya gastada.
- El Banco consulta su registro de retiro de fondos para confirmar el retiro de fondos de Alice (opcional).
- El Banco introduce la moneda en la base de datos de monedas gastadas.
- El Banco ingresa la cantidad en la cuenta de Bob y le informa.
- Bob da a Alice la mercancía.



3.1.2 Pago electrónico off-line

Para minimizar la cantidad de tráfico generado en la red de los sistemas on-line se propusieron sistemas fuera de conexión u off-line. En ellos no es necesaria la conexión con el Banco para cada transacción pero es preciso utilizar mecanismos mucho más robustos de detección de doble uso, ya que el uso de la moneda sólo se podrá detectar al llegar de nuevo a la entidad financiera. Esta dificultad se supera con la característica de trazabilidad, como es posible “seguir la pista” de quién ha realizado un determinado pago, cuando se detecte un uso fraudulento de las monedas electrónicas, se podrá penalizar a posteriori.

Además, la acción de pago difiere de la acción de depósito de fondos. Por ejemplo, Bob contactará con el Banco sólo una vez al día para ingresar todos los tokens recibidos en ese día.

La serie de mensajes enviados en dicho sistema es la que se describe a continuación.

Retiro de fondos

- Alice envía al Banco una solicitud de retiro de fondos.
- El Banco prepara una moneda electrónica y la firma digitalmente.
- El Banco envía la moneda a Alice y la carga en su cuenta.

Pago

- Alice entrega la moneda a Bob
- Bob verifica la firma digital del Banco (opcional)
- Bob da a Alice la Mercancía

Depósito de fondos

- Bob envía la moneda al banco
- El Banco verifica su firma digital.
- El Banco verifica que la moneda no ha sido ya gastada
- El Banco consulta su registro de retiro de fondos para confirmar el retiro por parte de Alice (opcional)
- El Banco introduce la moneda en la base de datos de la moneda gastada
- El Banco ingresa el dinero en la cuenta de Bob

Los dos protocolos anteriores usan firmas digitales para conseguir autenticidad. La autenticidad se puede conseguir por otros métodos pero se necesita el uso de firmas digitales para añadir los mecanismos que proporcionaran anonimato.

3.2 Pagos electrónicos no trazables.

En este apartado se describen las modificaciones que se realizan sobre los protocolos básicos ya presentados con el fin de impedir que los pagos sean trazables. Para esto es necesario que el banco no sea capaz de relacionar un determinado retiro de fondos con un ingreso en cuenta concreto. Habitualmente esta característica se consigue mediante el uso de un determinado tipo de firmas denominadas firmas ciegas o *blind signatures*.

En las firmas convencionales, el firmante conoce el contenido del documento digital que firma - tanto si lo ha generado él como si no - y lo cifra con su clave privada. En las firmas ciegas, sin embargo, el firmante no llega a conocer el contenido del mensaje que cifra ni lo genera él, por lo tanto se necesitan como mínimo 2 participantes para generar un documento firmado ciegamente, supongámoslos Alice y el Banco.

La encargada de generar el documento a firmar será Alice, ésta, antes de enviar el documento digital que el Banco debe firmar, modifica el mensaje que envía al Banco mediante el uso de un número aleatorio. Este paso se denomina “cegar el mensaje” y al número aleatorio *blinding factor* o factor de cegado. Despues del proceso de cegado el banco firma el mensaje aparentemente aleatorio y se lo devuelve a Alice. Finalmente Alice, que es capaz de “deshacer” el cegado, lo recupera.

A partir de este momento Alice posee un mensaje válido (que en nuestro caso puede ser una moneda electrónica) firmado por el Banco sin que éste se haya percatado de su contenido. El Banco será capaz de leer el contenido del mensaje cuando se le retorne en el proceso de depósito de fondos - téngase en cuenta que a partir del momento en que se retira el factor de cegado el mensaje viaja “en claro” y firmado - pero no podrá asociar dicho mensaje al usuario que se lo ha hecho firmar, Alice, en nuestro caso.

Nótese que en el primero de los pasos a seguir el Banco no sabe qué es lo que está firmando, este hecho introduce la posibilidad que el Banco firme una cantidad distinta a la que Alice le “dice” que está firmando. Para subsanar este problema el banco podría disponer de distintas “claves de firma”, de forma que, por ejemplo, use la clave K1 para firmar los mensajes supuestamente de importes no superiores a 10 euros, K2 para los mensajes entre 10 y 50 euros etc...

3.2.1 Pago electrónico on-line no trazable.

En los sistemas de pago no trazables la moneda la emite (o acuña) el comprador, y el Banco sólo se encarga de firmarla. Como la entidad financiera no es consciente de los “números de serie” de los billetes que están en circulación, ya que sólo los podrá ver cuando se le hayan devuelto, y por tanto, ya se hayan gastado, es crucial la prevención del doble uso. La solución es trivial en el sistema on-line (ya que la comprobación es en tiempo real) pero es de vital importancia en los sistemas off-line. De cualquier modo, para poder detectar quien es el defraudador, Alice debe identificarse frente a Bob, haciendo el sistema no trazable, pero tampoco anónimo.

La secuencia de mensajes intercambiados en el sistema on-line no trazable es la que se describe a continuación.

Retiro de fondos

- Alice crea una moneda electrónica y la ciega.

- Alice envía la moneda cegada al Banco con una petición de retiro de fondos de su cuenta.
- El Banco la firma digitalmente.
- El Banco devuelve a Alice la moneda firmada y la carga en su cuenta.
- Alice quita el factor de cegado de la moneda.

Pago/depósito de fondos

- Alice envía a Bob la moneda.
- Bob contacta con el Banco y envía la moneda.
- El Banco verifica la firma digital de la moneda.
- El Banco comprueba que la moneda no se haya utilizado con anterioridad.
- El Banco introduce la moneda en la base de datos de monedas gastadas.
- El Banco ingresa la cantidad en la cuenta de Bob y le informa.
- Bob entrega a Alice la mercancía comprada.

3.2.2 Pago electrónico off-line no trazable

El método de pago off-line no trazable es equivalente al on-line con la salvedad de la distinción de los procesos de pago e ingreso en cuenta. Como ya se comentó, para prevenir el doble uso, el comprador debe identificarse frente al vendedor. Así, aunque el Banco no puede trazar las compras, si el comprador realiza un doble uso, éste puede ser denunciado por el vendedor.

La secuencia de mensajes intercambiados son los que se describen a continuación.

Retiro de fondos

- Alice crea una moneda electrónica y la ciega
- Alice envía la moneda cegada al Banco junto con la petición de retiro de fondos.
- El Banco firma digitalmente la moneda cegada.
- El Banco devuelve la moneda cegada a Alice y la carga en su cuenta.
- Alice retira el factor de cegado de la moneda

Pago

- Alice entrega a Bob la moneda.
- Bob verifica la firma digital del Banco (opcional).
- Bob entrega a Alice la mercancía.

Depósito de fondos.

- Bob envía la moneda al Banco.
- El Banco comprueba su firma digital.
- El Banco comprueba que la moneda no haya sido ya gastada.
- El Banco introduce la moneda en la base de datos de monedas gastadas.
- El Banco ingresa la cantidad en la cuenta de Bob.

3.3 Protocolo de pago electrónico anónimo.

Finalmente, se le añadirán las modificaciones oportunas a los protocolos anteriores para garantizar anonimato en el pago. La condición ideal, desde el punto de vista de anonimato, sería que ni el Banco ni el Vendedor (Bob) conocieran la identidad del Comprador (Alice). Esto haría

las transacciones electrónicas totalmente anónimas: nadie sabe donde Alice ha gastado su dinero y quién le ha dado ese dinero.

De cualquier modo, los protocolos usados hasta el momento sólo garantizan anonimato de comprador, es decir, el Banco sabe que Alice ha retirado dinero de su cuenta pero no sabe donde lo ha gastado y Bob sabe que el dinero proviene de un Banco en concreto pero no sabe quien es el comprador. Así decimos que se produce anonimato dos a dos. Si los pagos se realizan on-line el protocolo on-line no trazable ya garantiza dicha propiedad.

En el mecanismo off-line no trazable, sin embargo, como no deseamos que Alice desvele su identidad frente al Vendedor, aparecen nuevas dificultades. Si Bob quiere ingresar en su cuenta una moneda que ha sido gastada previamente no podrá, ya que el banco se lo impedirá, y además, nunca podrá saber quien ha gastado múltiples veces esa moneda, ya que se pretende que sea anónima.

Se ve la necesidad de un mecanismo mediante el cual el banco sea capaz de identificar un uso múltiple de una moneda y que a su vez garantice el anonimato de los usuarios de la moneda "legal" (no usada más de una vez).

En el momento en que se realice el pago, Alice deberá revelar cierta información a Bob, de esta forma se asegura que sólo Alice puede haber gastado la moneda ya que sólo ella conoce esa información.

Este procedimiento se realiza mediante lo que se denomina un protocolo de respuesta a desafío. En este tipo de protocolos, Bob envía a Alice un mensaje de desafío y Alice, como respuesta, le envía cierta información de identificación.

En el momento del depósito de fondos, Bob envía al Banco tanto la moneda como la respuesta al desafío. Si todos los participantes han actuado de buena fe, la información de identificación de Alice nunca desvelará su identidad. Si Alice, en cambio, decide gastar la moneda dos veces, deberá responder a dos desafíos (en principio) distintos. Cuando las dos monedas con los dos desafíos regresen al Banco la unión de las respuestas a los dos desafíos revelará la identidad de Alice. Mediante este procedimiento sólo los que deciden gastar la moneda dos veces serán identificados ya que el conocimiento de una única respuesta a un desafío no desvela ninguna identidad.

3.3.1 Pago electrónico no trazable anónimo.

Con todo lo expuesto anteriormente, el mecanismo de pago electrónico no trazable y anónimo queda descrito a continuación.

Retiro de fondos

- Alice crea una moneda electrónica que incluye información de identificación.
- Alice ciega la moneda.
- Alice envía la moneda cegada al banco con la petición de retiro de fondos.
- El Banco verifica que la información de identificación esté presente.



- El Banco firma la moneda cegada.
- El Banco devuelve la moneda firmada a Alice y la carga en su cuenta.
- Alice retira el factor de cegado de la moneda.

Pago

- Alice envía la moneda a Bob.
- Bob comprueba la firma digital del banco.
- Bob envía a Alice el desafío.
- Alice envía a Bob la respuesta (le revela una parte de su información de identificación).
- Bob comprueba la respuesta.
- Bob entrega a Alice el producto comprado.

Depósito

- Bob envía la moneda, el desafío y la respuesta al banco.
- El Banco verifica su firma digital.
- El Banco verifica que la moneda no se haya gastado previamente.
- El Banco guarda la moneda, el desafío y la respuesta en la base de datos de monedas gastadas.
- El Banco ingresa la cantidad en la cuenta de Bob.

Téngase en cuenta que en este procedimiento Bob puede comprobar la firma digital del banco antes de entregarle la mercancía a Alice, de esta forma Bob puede asegurar que o le ingresarán la cantidad en su cuenta o podrá saber quien ha gastado dos veces la misma moneda.

3.4 Características adicionales de los pagos electrónicos.

3.4.1 Transferibilidad.

La transferibilidad es una característica inherente en el papel moneda y que permite a su usuario gastar una moneda que acaba de recibir de otro usuario sin necesidad de contactar con el banco. Una transferencia, por tanto, será un pago en que el receptor puede usar la moneda en un pago posterior sin haber contactado con el Banco. Un sistema de pago es transferible si admite como mínimo una transferencia por moneda. En la figura 2 se puede ver el recorrido máximo de una moneda que permite dos transferencias.

La transferibilidad es una característica deseable en sistemas off-line porque requerirá menos conexiones con el banco. Un sistema de pago electrónico transferible es off-line por definición ya que los pagos on-line requieren conexión con el banco durante la transacción o transmisión del token.

Los sistemas transferibles no han recibido mucha atención por parte de la literatura académica. Cualquier sistema de pago electrónico transferible tiene el inconveniente que la moneda electrónica deberá "crecer de tamaño" cada vez que se gaste. Esto se debe a que la moneda debe añadir información de cada uno de los participantes en las distintas transferencias de forma que el banco pueda identificarlas en caso en que se produzca un uso doble de

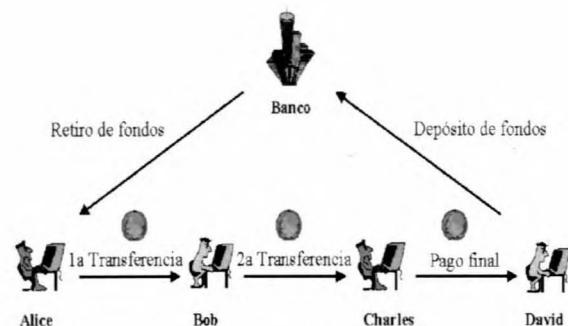


Figura 2. Esquema de pago transferible.

la misma. Este incremento de tamaño hace inviable un sistema de transferencias de número indeterminado y limita el máximo de transferencias permitidas a la capacidad de los sistemas informáticos que realizan la transacción.

Existen otros aspectos por los cuales los sistemas transferibles no han tenido demasiado éxito, incluso limitando el número de transacciones y no garantizando anonimato de los participantes. Hasta que la moneda no vuelve a ser depositada en el Banco, la entidad financiera sólo posee la información de quién ha realizado el retiro de fondos. Cualquier otra transacción sólo revelará la identidad de los participantes con la colaboración de éstos. Esto presenta el mismo problema que el papel moneda y su dificultad para detectar operaciones de blanqueo de dinero o evasión de impuestos: no existen registros de las transferencias realizadas.

Además, cada transferencia retrasa la detección de dobles usos o falsificaciones. Los usos múltiples de una moneda electrónica no se descubrirían hasta que como mínimo dos copias de la misma moneda se depositen en el banco. Por entonces, puede que sea demasiado tarde para detener al infractor y posiblemente muchos usuarios habrán recibido monedas electrónicas falsas. Esto pone de manifiesto que no es suficiente la detección del delito para sistemas de pago electrónico transferibles, sino que serán necesarios mecanismos de prevención del delito o a priori.

3.4.2 Divisibilidad.

Supongamos que Alice es una de las participantes de un pago electrónico no transferible y off-line, y quiere comprar a Bob un producto por valor de 4.5 euros. Si por casualidad tiene un conjunto de monedas electrónicas que juntas reúnen exactamente dicho valor no se presenta ningún problema, simplemente las entrega a Bob. De cualquier modo, a menos que Alice tenga una gran cantidad de monedas electrónicas y de distinto valor, es bastante improbable que reúna la cantidad exacta de "cualquier" compra.

Una posible opción sería que Alice retire del banco una cantidad exacta cada vez que quiera realizar una

compra, pero eso requiere interacción con el banco, convirtiendo al pago en on-line desde el punto de vista de Alice. La tercera opción sería que Bob “pagase” a Alice la diferencia entre lo que le ha entregado y el valor del producto, pero esta solución únicamente traslada al plazo de Bob el hecho de disponer de monedas de una determinada cantidad y además requeriría que Alice contactase con el banco para “ingresar” el cambio.

Una solución a estos inconvenientes es el uso de monedas divisibles. Las monedas divisibles son monedas que pueden fragmentarse en partes cuyo valor total es igual al valor del original. Esto permitiría pagos off-line por una cantidad exacta sin la necesidad de acuñar monedas de distintas cantidades. Esta propiedad tal como aquí está planteada no la presenta el papel moneda, pero esta falta de divisibilidad se contrarresta con su transferibilidad.

4. EJEMPLOS DE IMPLEMENTACIONES Y PROTOCOLOS REALES.

En este apartado se presentan los que se consideran los ejemplos más significativos de propuestas e implementaciones reales. La exposición se estructura según la clasificación de protocolos expuesta anteriormente. Para cada uno de los sistemas se detalla las empresas o instituciones que lo propusieron, las herramientas criptográficas en las que se basa, su modo de funcionamiento en cuanto a transacciones de mensajes se refiere y referencias donde encontrar más información.

Para entender los mecanismos aquí propuestos deberemos realizar una generalización del esquema básico de pago electrónico presentado en la figura 3.

En el nuevo esquema no se exige que comprador y vendedor tengan la misma entidad financiera, sino que ésta se desdobra en dos organismos: el Emisor de la moneda (o *Issuer* en inglés) y el Receptor del dinero (*Acquirer* en inglés). Así, el comprador retira su dinero del Emisor de moneda electrónica, efectúa un pago al vendedor quien a su vez deposita la moneda al Receptor. El flujo “real” de dinero se realiza entre *issuer* y *acquirer*.

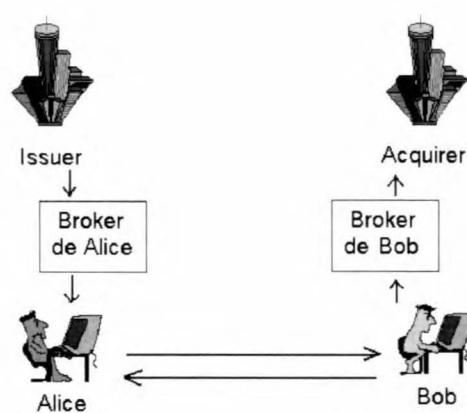


Figura 3. Esquema general de pago electrónico.

Adicionalmente puede aparecer la figura del *broker* o agente que, no siendo propiamente una entidad financiera, actuará como intermediario entre el Comprador o Vendedor y sus respectivos Bancos.

4.1 Sistemas on-line trazables.

Como ya se comentó cuando se expuso el procedimiento general de los sistemas trazables on-line, éstos son los de más fácil implementación; ésta es la razón por la que el número de implementaciones propuestas ha sido elevado. Aunque ya en desuso, se presentan First-Virtual, Cyber-Cash e iKP como ejemplos de propuestas anteriores al estándar SET. Este último, aunque con ciertas dificultades frente a sistemas de pago con tarjeta mediante SSL, pretende establecerse como estándar mundial de pagos on-line y trazables basados en tarjetas de crédito.

El problema más patente de los sistemas on-line es su elevado coste económico para la realización de pagos pequeños. La última parte de esta sección la dedicamos a exponer tres sistemas de micropagos on-line: NetBill, Millicent y MiniPay que pretenden subsanar dicho problema.

4.1.1 First - Virtual

Aunque ya totalmente en desuso, se presenta el sistema First-Virtual como uno de los primeros intentos de acomodar la infraestructura de comunicaciones existente a los protocolos de pago electrónico.

First Virtual Holdings Inc. propuso un sistema de pago que aprovechaba el correo electrónico para intercambiar mensajes entre el Vendedor y First-Virtual y el Comprador y First-Virtual. Esto eliminaba la necesidad de software y protocolos específicos y permitía a la empresa First-Virtual desarrollar su sistema a través de la infraestructura de Internet existente.

El sistema ofrecía anonimato del comprador frente al vendedor, pero la empresa First-Virtual, que actuaba como Broker, disponía de todos los datos, tanto del comprador como del vendedor. Uno de los aspectos que se presentaba como ventajoso era el hecho que ningún dato bancario “real” viajaba a través de la red, de esta forma se protegía frente a escuchas de terceros. Por el contrario, esto requería la existencia de un Identificador Virtual o y era necesario que tanto comprador como vendedor se diesen de alta (o hayan abierto una cuenta) en el Broker.

El protocolo seguía los siguientes pasos, véase figura 4:

- (1) Alice inicia el proceso de compra de la forma habitual, pero en vez de enviar sus datos bancarios al vendedor, le envía su Virtual-PIN.
- (2) Bob envía un correo a First Virtual (el broker) con la información del PIN de Alice,



el suyo propio, y una descripción de la compra.

(3) El Broker envía un correo a Alice con la información que le ha mandado Bob solicitando su confirmación.

(4) Alice envía por correo electrónico la confirmación al Broker.

(5) El Broker usa las redes financieras existentes para procesar la transacción mediante tarjetas de crédito (que dispone gracias a la base de datos, ya que tanto Alice como Bob están dados de alta en su servicio).

(6) En cuanto se ha realizado la transacción, el Broker envía un identificador de autorización a Bob.

Se puede encontrar más información sobre First Virtual en [Sir97].

4.1.2 CyberCash.

El sistema propuesto por CyberCash Inc. es muy similar al ya expuesto First Virtual en cuanto los dos utilizan las redes financieras existentes para realizar las transacciones reales de fondos y actúan a través de intermediarios o brokers.

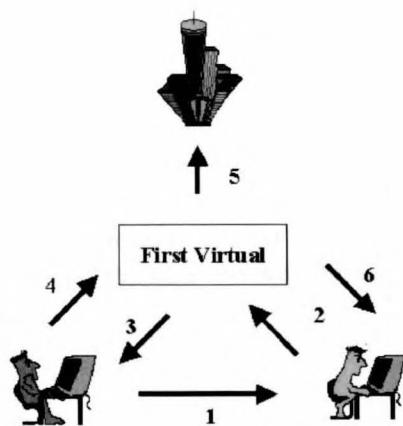


Figura 4. Transacciones de datos implicadas en el sistema First-Virtual.

El sistema básico CyberCash no es más que una pasarela que une a los vendedores en Internet con los sistemas de pago electrónico por tarjeta de crédito existentes. CyberCash simplemente integra el software del vendedor en las redes financieras existentes como si fuera un TPV (terminal punto de venta) más.

El sistema sigue los pasos descritos a continuación, véase figura 5:

- (1) Alice realiza una orden de compra a Bob.
- (2) Bob le contesta con una petición de pago.
- (3) Alice genera un "pago cifrado" mediante el monedero CyberCash y se lo envía a Bob.
- (4) Bob recorta el "pago cifrado" del mensaje que le ha enviado Alice, lo firma digitalmente y lo reenvía al servidor CyberCash.

(5) El servidor CyberCash traspasa la transacción de Internet a la red financiera, usa hardware específico para descifrarlo, formatea el mensaje de pago adecuadamente a la red financiera y lo envía al Banco de Bob.

(6) El Banco de Bob transfiere el mensaje de pago al Banco de Alice.

(7) El Banco de Alice confirma o deniega el pago y envía el resultado al Banco de Bob.

(8) El Banco de Bob envía el código de aprobación o denegación al servidor CyberCash.

(9) El Servidor CyberCash envía la aprobación o denegación a Bob.

Los 4 primeros pasos y el último se realizan a través de redes abiertas (Internet) mediante la combinación de criptografía de clave pública y simétrica. Los pasos 5,6,7 y 8 utilizan las redes financieras existentes. CyberCash estima que se puede realizar la transacción completa en un tiempo de 20 segundos aproximadamente. El sistema es atractivo para los bancos ya que sólo interactúan con ellos a través de sus redes financieras ya existentes.

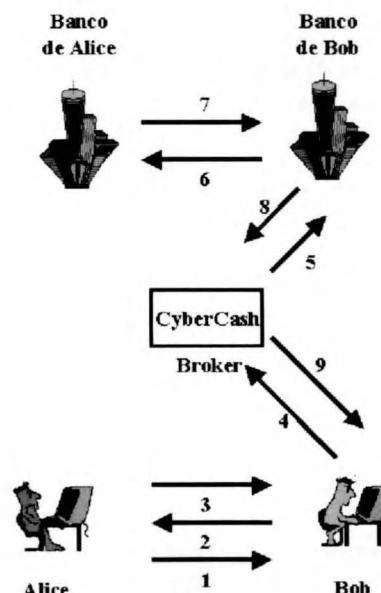


Figura 5. Transacciones de datos implicadas en el sistema Cyber-Cash

Cybercash también ha desarrollado mejoras de este sistema denominados CyberCoin, que consiste en un sistema on-line y trazable pero que soporta pagos pequeños (25 céntimos como mínimo) y CyberCheque. Todos estos sistemas son no anónimos y trazables. Puede encontrarse más información sobre CyberCash en [HREF1]

4.1.3 iKP

iKP o Internet Keyed Payment Protocols es una familia de protocolos desarrollado por IBM Research Group. Todos los protocolos de la familia se basan en criptografía de clave pública pero se diferencian en el número de participantes que se autentifican en el procedimiento de pago, este número es el indicado en el índice i:

- 1KP Sólo el Broker tiene clave pública y certificado.
- 2KP El Broker y el Vendedor disponen de herramientas de autenticación.
- 3KP Todos los participantes tienen certificado y clave.

El procedimiento de pago es análogo al de CyberCash, véase figura 5, aunque el formato de los mensajes implicados en la transacción es diferente. Al igual que en CyberCash, también existe una variante de este protocolo para la realización de micropagos denominado m-KP.

MasterCard, IBM, Netscape y CyberCash desarrollaron conjuntamente un sistema práctico de este protocolo, denominado Secure Electronic Payments Protocol (SEPP) considerado uno de los predecesores del SET. Puede encontrarse más información sobre iKP en [HREF2].

4.1.4 SET

SET o Secure Electronic Transactions es un estándar de pago seguro mediante tarjeta de crédito a través de Internet. Fue propuesto por MasterCard y Visa y auspiciado por la mayoría de entidades financieras y fabricantes de tecnología. Este sistema se basa en propuestas muy similares, entre las cuales están iKP de IBM, STT propuesto por Visa y Microsoft y SEPP desarrollado entre otros por MasterCard, IBM y Netscape.

Al ser un sistema basado en iKP y CyberCash, el diagrama de mensajes implicados en la transacción es muy parecido al de éstos aunque difiere en que, al pretender ser un estándar, no es necesaria la intervención de un broker sino que el mismo Banco del vendedor es quien ejerce esas funciones. Los pasos más detallados del sistema SET son los que se describen a continuación, véase figura 6.

- (1) Alice realiza la orden de compra.
- (2) Bob, el vendedor, envía al monedero de Alice, la compradora, la clave pública de su Banco, certificada por VISA/MC.
- (3) Alice usa la clave pública de Bob para cifrar el número de su tarjeta de crédito. Emite la orden de pago firmada por ella misma, y la envía a Bob.
- (4) Bob reenvía la orden de pago a su Banco.
- (5) El Banco de Bob usa la red financiera existente para cursar la orden de pago hasta el Banco de Alice. Este procedimiento sólo se diferencia de una transacción por tarjeta de crédito convencional en que se indica que se trata de una operación SET.
- (6) El Banco de Alice confirma el pago al Banco de Bob.
- (7) El Banco de Bob envía un recibo de pago firmado a Bob.
- (8) Bob envía el recibo firmado a Alice.

Aunque actualmente es el sistema de pago estándar, se deben hacer algunas consideraciones sobre el sistema SET. Debido a que la clave pública del banco de Bob debe estar firmada por VISA/MC, sólo los bancos autorizados por dichas firmas comerciales podrán integrarse dentro del sistema SET. En segundo lugar, cuando los mensajes de transacción se introducen dentro de la red financiera existente pierden la firma del comprador, es decir, la orden de pago no viaja firmada por el comprador, careciendo entonces de la propiedad de no repudio, aunque a nivel práctico existan suficientes pistas como para trazar el mensaje y garantizar cierto nivel de no repudio.

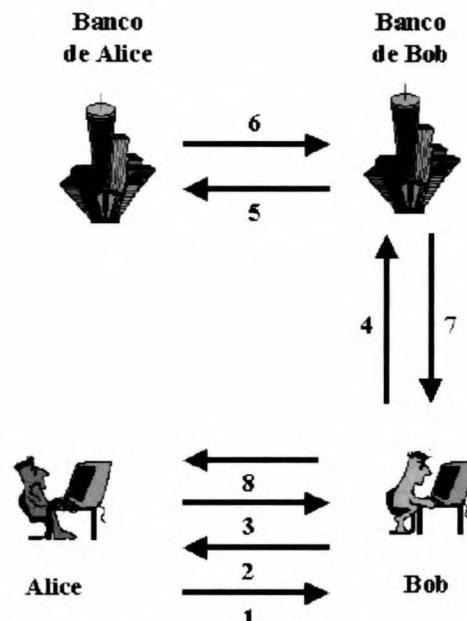


Figura 6. Transacciones de datos implicadas en el sistema SET

Finalmente, apuntar que el sistema SET entra en competencia con los sistemas de pagos mediante tarjetas de crédito tradicionales con transmisión segura de datos bancarios sobre el protocolo SSL, que es hoy en día el mecanismo más extendido, aunque no se trate de un protocolo de pago propiamente dicho.

Puede hallarse información más detallada sobre el sistema SET en [HREF3].

Sistemas on-line trazables para micropagos.

Los pagos con tarjeta de crédito tienen un coste muy elevado en cuanto a comisiones por servicio se refiere, alrededor de un 2% con tasas mínimas del orden de 25 céntimos de euro. Además, el proceso de autorización implica retardos considerables en el tiempo de compra. Estos dos problemas son los más significativos a la hora de realizar pagos de pequeñas cantidades.

4.1.5 NetBill.

La Universidad de Carnegie Mellon junto con la empresa CyberCash desarrollaron en 1997 un sistema de pago basado en cheques electrónicos denominado NetBill.



Dicho sistema usa tanto criptografía de clave pública como simétrica para garantizar los servicios de seguridad requeridos. Al igual que el sistema de pagos y macropagos First Virtual, NetBill requiere que tanto vendedor como comprador dispongan de una cuenta abierta en una central (o broker) de NetBill. El sistema está pensado para la venta de productos electrónicos (música, vídeo a través de internet, documentos...)

El mecanismo de funcionamiento consta de 6 pasos y se describe a continuación, véase figura 7:

- (1) Alice realiza una petición de compra "pay-per-click".
- (2) Bob envía a Alice el producto electrónico cifrado junto con una función resumen del producto cifrado.
- (3) Alice, mediante el hash, comprueba que el producto cifrado se ha recibido de forma correcta y devuelve un mensaje de verificación a Bob.
- (4) Bob envía el mensaje de verificación, la información de la cuenta NetBill de Alice y la clave de descifrado del producto comprado al servidor NetBill.
- (5) NetBill comprueba la existencia de fondos en la cuenta de Alice, realiza la transferencia entre cuentas y lo notifica a Bob.
- (6) Bob envía la clave de descifrado del producto a Alice. Si Bob no envía la clave de descifrado, Alice puede pedírsela al servidor NetBill directamente.

Se puede obtener más información sobre este sistema de micropago en [HREF4].

4.1.6 Millicent.

Millicent es un "Sistema de Microcomercio Digital" propietario, desarrollado por la empresa Digital Inc. Se basa en el uso de bonos o *scrips*, que consisten en un determinado tipo de tokens que sólo son válidos para un vendedor en particular y un broker concreto. Este hecho elimina la necesidad de conectarse a un determinado emisor o *issuer* para comprobar la validez de los tokens reduciendo por tanto el tráfico ofrecido a la red.

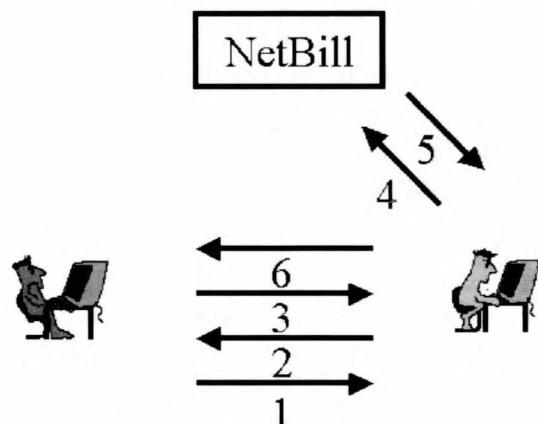


Figura 7 Esquema de transacciones en el sistema NetBill.

El sistema se descompone en los siguientes pasos, figura 8:

- (1) Alice obtiene una determinada cantidad de bonos del broker.
- (2) Alice solicita bonos de un determinado vendedor a su broker.
- (3) El Broker obtiene los bonos de Bob.
- (4) El Broker vende los bonos de Bob a Alice.
- (5) Alice compra los productos de Bob pagándole con sus bonos.
- (6) Bob le devuelve el cambio a Alice mediante bonos de Bob.

Se puede obtener más información sobre este sistema de micropagos en [HREF5].

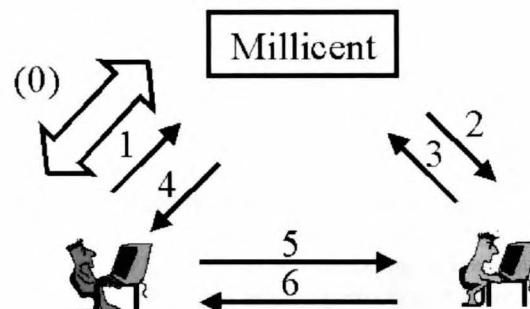


Figura 8. Transacción según Millicent

4.1.7 MiniPay.

MiniPay es un mecanismo de pago desarrollado por IBM que pretende superar los problemas presentados por sistemas anteriores para la realización de micropagos: ofrece bajo coste (menos de un céntimo de euro por transacción) y retardo despreciable.

Los mecanismos de seguridad que utiliza son firmas digitales, certificados y hashes. MiniPay minimiza el tráfico ofrecido a la red ya que la validación de los tokens se realiza semi on-line, es decir, sólo se contacta con la entidad emisora o receptora una vez al día o en caso de detectarse un gasto superior a cierto valor.

La idea básica es que issuer y acquirer son los respectivos Proveedores de Acceso o Servicios de Internet de Alice y Bob, así que están on-line si sus respectivos clientes están on-line. Cada comprador obtiene un "límite de gasto" autenticado de su respectivo Proveedor de acceso. Cada comprador acepta compromisos de pago de los usuarios autenticados de manera off-line, y sólo realiza la comprobación on-line si la cantidad comprometida supera un determinado valor.

El esquema en sí consta sólo de 3 pasos, aunque una vez al día se produzcan las transacciones periódicas correspondientes, o eventualmente se realicen comprobaciones on-line, véase figura 9.

Puede encontrarse más información de este sistema en [HREF6]

Otros sistemas de micropagos.

Existen otros sistemas de micropagos, se ha presentado un ejemplo de sistema de micropagos basado en cadenas de hash invertidas, otro basado en bonos y finalmente otro basado en tarjetas de débito. Además de éstos también existen variaciones de los mismos denominados Netcard [HREF7], Payword [HREF8], Agora [HREF9] entre otros...

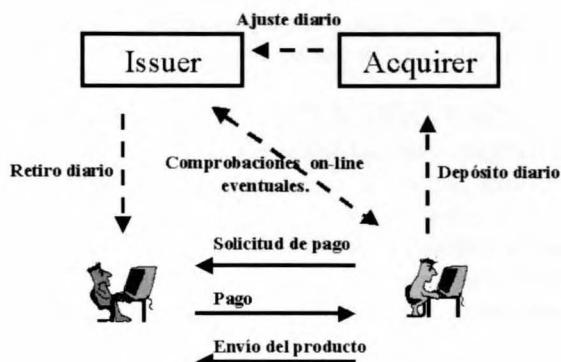


Figura 9. Transacciones en MiniPay.

4.2 Sistemas off-line trazable.

Un paso más hacia las características que apuntábamos que debía tener la moneda electrónica era su condición de off-line, evitar la comprobación de la validez del token durante el proceso de transacción. Recordemos que el mayor peligro que presentaban este tipo de sistemas era la amenaza de *double spending*.

En esta sección presentamos dos propuestas de sistemas prácticos off-line aunque trazables. El primero se protege frente al doble uso mediante el uso de tarjetas inteligentes o smartcards. Es decir, evita la duplicación del token basándose en la dificultad de duplicar un dispositivo hardware; en última instancia, este es el mismo método que se utiliza en el papel moneda tradicional en los que la falsificación de papel moneda, aunque no imposible con suficientes medios, es técnicamente muy costosa. Este tipo de tarjetas se denomina en la literatura *tamper proof devices* o dispositivos a prueba de copia.

El segundo de los sistemas que se presenta se basa en la emisión de cheques electrónicos, mecanismo análogo a los cheques tradicionales, en este sistema no se puede evitar que un usuario "emita" el mismo cheque varias veces o que éstos no tengan fondos, pero como se trata de un sistema trazable, el delito es detectable y punible.

En los sistemas off-line, retiro de fondos, pago y depósito se realizan en instantes temporalmente diferenciados. El pago sólo implica a Alice y Bob, y

normalmente sólo consta de 3 pasos: solicitud de compra, solicitud de pago y envío de token. En este tipo de sistemas no tiene tanta importancia la secuencia de mensajes generados como las técnicas empleadas y su robustez.

4.2.1 Mondex.

Mondex es un sistema propuesto por MasterCard en 1995. Proporciona un sistema de pago mediante el uso de tarjetas inteligentes. Es un sistema propietario del cual se conocen muy pocas especificaciones técnicas. Concebido principalmente para la realización de micropagos, existe una versión que adapta el sistema para realizar pagos a través de Internet, aunque es necesario el uso de lectores de tarjetas en los PC's involucrados.

La ventaja de Mondex es que no necesita verificación on-line generando mucho menos tráfico que en las transacciones off-line. En cambio, el sistema no proporciona anonimato y el banco puede trazar todas las transacciones y construir perfiles de usuario.

Puede encontrarse más información sobre Mondex en [HREF10].

4.2.2 FSTC Electronic Check Project

FSTC o Financial Services Technology Consortium propuso en 1997 un sistema off-line trazable basado en la idea de cheques electrónicos. La propuesta forma parte del proyecto BIPS, que se centra en el estudio de un modelo general de integración de las infraestructuras financieras existentes en los pagos a través de Internet.

En los cheques convencionales la entidad financiera da "permiso" al usuario para que "emita" un documento similar al papel moneda, para que a posteriori se lo cargue en su cuenta y lo abone al "portador" de ese cheque. Como el cheque está identificado, el fraude se puede detectar y penar. El sistema FSTC sigue la misma idea pero de forma electrónica.

Alice firma digitalmente el cheque para garantizar autenticación y Bob, a su vez, también lo firma para garantizar no repudio. Es necesaria la existencia de certificados de comprador, vendedor y cuenta bancaria para realizarse la transacción. El Cheque, una vez emitido, puede enviarse por cualquier medio existente, e-mail, por ejemplo.

Aunque en principio no son necesarias las tarjetas inteligentes o cualquier otro dispositivo hardware, se recomienda el uso de éstas para generar las firmas de los participantes en la transacción sin comprometer la privacidad de su clave secreta. Puede encontrarse más información sobre FSTC en [HREF11].



Otros Sistemas Off-line trazables.

En [Com97] se apunta la existencia de otras propuestas de sistemas off-line trazables, la mayoría basados en dispositivos tamperproof del tipo tarjetas monederos, denominados CLIP, CEN Intersector Electronic Purse, EMV Electronic Purse, aunque las referencias a hipertexto allí indicadas ya no estaban disponibles.

4.3 Sistemas on-line no trazables.

Otro paso intermedio hacia los sistemas de moneda electrónica son los sistemas on-line no trazables, en ellos la comprobación del token se realiza justo en el momento de la transacción pero la confabulación de Vendedor y Banco no desvela el rastro de las compras de Alice.

Es difícil conseguir un anonimato total, más incluso en sistemas on-line, donde como mínimo se revela la conexión que se realiza (IP del host de emisión y recepción por ejemplo). La mayoría de sistemas que dicen que ofrecen esta garantía lo hacen desplazando la responsabilidad de unir datos bancarios (o dinero) y producto comprado a un tercer agente, supuestamente de confianza, que aunque capaz de trazar todas las compras, se compromete a no desvelar dichos datos.

4.3.1 NetCash.

NetCash es un sistema propuesto en 1996 por G. Medvinsky y B.C. Neuman del *Information Sciences Institute* de la Universidad de California del Sur. Está orientado a micropagos.

Ofrece un sistema de pago seguro y anónimo en tiempo real. Como técnicas criptográficas utiliza certificados, firmas digitales y control de doble uso mediante base de datos. No necesita hardware especial ni redes seguras, y está especialmente pensado para su uso en Internet.

El sistema de detección de doble uso o doble gasto implementado en NetCash es inverso al empleado normalmente por las otras propuestas. NetCash guarda una base de datos con el número de serie de billetes emitidos y no de billetes gastados, como es habitual, y los borra de su base de datos cuando se han gastado. Se pretende así no tener que mantener indefinidamente una base de datos de billetes usados. La comprobación de la validez del token se realiza on-line.

La no trazabilidad ofrecida por NetCash es una no trazabilidad reducida ya que aunque el Banco no será capaz de seguir el rastro del comprador ni construir perfiles de usuario, ésta amenaza se traspasa al Servidor NetCash. Puede encontrarse más información sobre NetCash en [HREF12].

4.3.2 Anonymous Credit Cards (ACC).

ACC pretende ofrecer un sistema de tarjetas de crédito no asociado a una determinada persona física. Fue propuesto en 1994 por D. Kristol, S. Low, M. Maxemchuk y S. Paul de los Laboratorios AT&T Bell y está concebido para la realización de compras de bienes tangibles en centros comerciales de forma presencial.

La idea básica es separar la información necesaria para la transacción económica en distintas partes según sean datos requeridos por cada uno de los integrantes de la transacción. Una vez esté separada dicha información se usan técnicas criptográficas para ocultar a cada participante la información que no requiere.

Con el sistema ACC Alice se encuentra físicamente en el centro comercial donde realiza la compra y la realiza de forma presencial, en cambio, su identidad no le es revelada a Bob. El protocolo tiene una versión extendida para la realización de compras en internet denominada AIMP (*the Anonymous Internet Mercantile Protocol*). Puede encontrarse más información en [HREF13].

4.4 Sistemas off-line no trazables.

Los sistemas off-line no trazables son los de más difícil realización, y es por esto que son los que menos propuestas han recibido en la literatura. En ellos se unen todos los inconvenientes de los sistemas off-line y todos los de los sistemas no trazables. Como solución a los problemas off-line se opta por el uso de tarjetas inteligentes y como solución a los problemas planteados por la no trazabilidad se optó por no asociar ninguna cuenta bancaria ni dato personal al dispositivo hardware, sino “depositar” el dinero en el mismo dispositivo, de forma que si se pierde o deteriora la tarjeta, se perderá o deteriorará el dinero real. Esta última característica es completamente análoga al papel moneda.

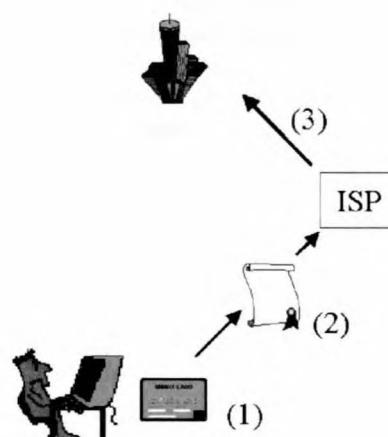


Figura 10. Esquema del sistema off-line no trazable propuesto por S. Brands.

4.4.1 Brands Cash.

Uno de los primeros sistemas off-line no trazables fue propuesto por Stefan Brands en [Bra93] y [Bra95]. El sistema se basa en dispositivos hardware para evitar el doble uso, en concreto en tarjetas PCMCIA y en criptografía de clave pública y firmas digitales para evitar repudio. Un esquema simplificado del mismo se puede ver en la figura 10.

En la tarjeta inteligente existe un contador que actualiza el saldo del usuario. El sistema se basa en criptografía de clave pública, existe una clave pública y otra secreta que sólo conoce la Smartcard. El PC actúa como interfaz entre la tarjeta e Internet (1). El sistema emite un cheque electrónico con la firma de la tarjeta (o de su propietario) sobre la cantidad expresada en el cheque y lo envía al Proveedor de Servicios de Internet (2), el cual transcribe el pago hasta el banco o la entidad financiera (3). Este sistema se considera el padre de CAFE.

4.4.2 CAFE

CAFE o Conditional Access For Europe fue propuesto por la Union Europea, la universidad de Leuven y un grupo de empresas entre las que se encuentran DigiCash, CWI y Siemens. Es un sistema off-line de moneda electrónica con garantía de anonimato. Puede encontrarse más información sobre este sistema en [HREF14].

Otros sistemas

El mayor inconveniente de este tipo de sistemas es que necesitan de tarjetas inteligentes o smartcards para su implementación, y éstas presentan aun varios problemas. En [Cha99] se exponen los inconvenientes de la utilización de tarjetas inteligentes: falta de movilidad, ya que al depender de un lector de tarjetas, la movilidad también depende de éste, y además, al no existir un único estándar de lector, cualquier PC debería disponer de todos los posibles lectores para garantizar movilidad absoluta; elevado coste tanto del lector como de la tarjeta para el montante que habitualmente implicará dicho tipo de pagos; e ineficiencia de cálculo, ya que en algunas implementaciones de tarjetas inteligentes se han detectado tiempos de cómputo superiores a implementaciones basadas en software. Estos inconvenientes se presentan como los motivos principales por los cuales no ha tenido éxito dicha tecnología.

5. CONCLUSIONES

En este artículo se ha realizado una introducción a los sistemas de pagos electrónicos, su evolución, situación actual y retos futuros. En primer lugar se

presentó la nomenclatura y definiciones básicas usadas en el campo del comercio electrónico para facilitar la comprensión de los siguientes apartados y dar una uniformidad de lenguaje al documento. Igualmente se expuso el conflicto existente a la hora de caracterizar los sistemas de pago electrónico, especialmente la dicotomía planteada entre sistemas autenticados o anónimos y trazables o repudiables. Asimismo, se planteó una posible vía de solución, se introdujo el concepto global de legitimidad y se trasladaron las características antes mencionadas a un plano más concreto dependiente del método de pago electrónico usado.

A continuación se presentaron los protocolos genéricos capaces de proporcionar cada una de las características mencionadas, se destacó la especial dificultad de proporcionar sistemas anónimos off-line y no trazables. Finalmente se expusieron los sistemas reales que implementaban los protocolos expuestos de forma genérica.

Del estudio de la evolución de los sistemas reales presentados se deduce que el éxito o el fracaso de un determinado esquema depende en gran medida del esfuerzo estandarizador y el apoyo de las grandes entidades financieras, que serán las principales "clientes" de dichos sistemas, así como de los estados, que son los responsables actuales de "emitir" el dinero en circulación, y que ven con cierto recelo la aparición de dinero "acuñable" por entidades no controladas por ellos.

De todos modos, ejemplos como el SET ponen de manifiesto que, a parte de la necesidad de estandarización y apoyos de entidades financieras, es preciso no perder de vista soluciones técnicas baratas, abiertas y compatibles con infraestructuras ya existentes, como el pago con numeración de tarjetas de crédito sobre HTTP seguro. En ese sentido Schneier apunta en [Sch99] la importancia que tiene en criptografía el hecho de "no ser diferentes".

Por otro lado, existen sistemas de pago menores basados en bonos, en cheques o en terceras partes (brokers) emisoras de moneda, que aunque no lleguen a escalas de universalidad comparables con los ya mencionados si pueden ofrecer soluciones a casos

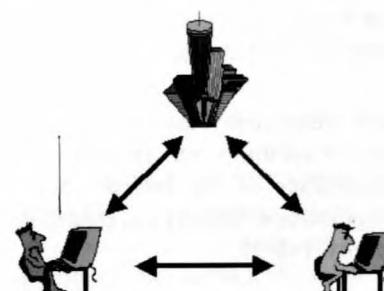


Figura 11. Esquema circular de pago electrónico.



concretos. Este tipo de sistemas, en cambio, presenta la dificultad de integración (necesidad de infraestructura y acuerdos) con las redes financieras existentes.

Otro punto que se ha puesto de manifiesto es la relación casi unívoca entre las características requeridas por un sistema con las herramientas criptográficas usadas para conseguir dichas características. Así, por ejemplo, el gasto doble en sistemas anónimos se evita principalmente mediante el uso de hardware tamperproof, y no se han encontrado estudios que presenten alternativas a dicha tecnología. Como el uso de tarjetas inteligentes presenta muchos inconvenientes, tal como expone Chadwick en [Cha99b], se prescinde de sistemas reales anónimos y así se aseguran la detección del infractor.

Si a lo expuesto anteriormente se le añade la precaución que suscita el anonimato en las transacciones electrónicas debido a la potencialidad de fraude y uso ilícito que de él se deriva, concluiremos que, aunque técnicamente viable, no existe voluntad de impulsar los sistemas de pago anónimos, y los pretendidamente existentes son fácilmente rastreables.

De igual forma, se observa que la totalidad de los sistemas expuestos depositan la responsabilidad en el vendedor. Es decir, el vendedor es quien toma la iniciativa en cuanto a transacción de mensajes válidos, y por tanto, el comprador adopta un papel pasivo y más indefenso frente a posible fraude por parte del vendedor.

En todos los esquemas presentados existe una estructura común cerrada, véase figura 11, que además de pasividad en el comprador, favorece la confabulación de Banco y Vendedor.

REFERENCIAS

- [Bra93] Brands, S. An Efficient Off-line cash system based on the representation problem} Centrum voor Wiskunde en Informatica(CWI) Technical Report CS-R9323. March 93
- [Bra95] Brands, S Electronic Cash on the Internet Centrum voor Wiskunde en Informatica (CWI) Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security. Feb 95.
- [Cha92] Chaum, David. Achieving Electronic Privacy, Scientific American, August 1992, p. 96-101.

- [Cha99] Chadwick D. Smart Cards Aren't Always the SmartChoice}, IEEE Computer. December 1999
- [Leo98] Leong, Anthony. Paper, Plastic, and Now, Electronic: A survey of Electronic Payment Systems 1998.

- [Oka92] Okamoto, T., Ohta k. Universal Electronic Cash. Advances in Cryptology, CRYPTO'91 Springer Verlag, 1992, pp324-337

- [Sch99] Schneier B. Cryptography: the Importance of not Being Differet. IEEE Computer March 1999

- [Sir97] Sirbu, Marvin. Credits and debits on the internet. IEEE Spectrum. Feb 97

- [Com97] VV.AA The state of the art in electronic payment systems. IEEE Computer Sept 97.

REFERENCIAS A HIPERTEXTO

[HREF1] <http://www.cybercash.com>

[HREF2] <http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.html>

[HREF3] <http://www.dlib.org/dlib/january98/ibm/01herzberg.html>

[HREF4] <http://www.netbill.com>

[HREF5] <http://www.millicent.digital.com>

[HREF6] <http://www-4.ibm.com/software/webservers/commerce/payment/mpay/index.htm>

[HREF7] http://www.cl.cam.ac.uk/~cm213/Project/project_publ.html

[HREF8] <http://theory.lcs.mit.edu/~rivest/RivestShamirmpay.ps>

[HREF9] <http://www.bell-labs.com/user/eran/agora.html>

[HREF10] <http://www.mondex.com>

[HREF11] <http://www.fstc.org>

[HREF12] <http://www.isi.edu/gost/info/netcash/>

[HREF13] <http://portal.research.bell-labs.com/lateinfo/projects/ecom.html>

[HREF14] <http://www.cwi.nl/cwi/projects/cafe.html>



MODELADO DE EXPRESIONES PARA UNA CARA ROBÓTICA

Oscar Déniz Suárez

Licenciado en Informática. Estudiante de doctorado
Universidad de Las Palmas de Gran Canaria.

INTRODUCCIÓN

En el marco del desarrollo de interfaces hombre-máquina cada vez más flexibles y sencillos de utilizar, se ha realizado en los últimos años un esfuerzo considerable en dotar de características y habilidades humanas a dispositivos físicos destinados a estar en íntimo contacto con personas, como por ejemplo los robots móviles. Obviamente, si el aspecto del robot, sus movimientos, y sus capacidades de más alto nivel se asemejan hasta cierto punto a las humanas, la respuesta de las personas que interactuarán con él será más positiva. Éstas se sentirán más atraídas por el dispositivo, se despertará su curiosidad, y la comunicación será más fluida. Escenarios típicos en los que este tipo de robots resultaría muy adecuado serían museos, puestos de atención al público, juguetes, etc.

De todas las partes del cuerpo humano, la que mayor información aporta en el proceso de comunicación persona-persona es sin duda la cara (la cabeza es la única parte del cuerpo donde se encuentran los cinco sentidos). Las posibilidades de comunicación que nos aporta la cara son realmente destacables, y todos somos capaces de comprobarlo en nuestras relaciones diarias con otras personas. En la mayoría de las ocasiones las expresiones que adopta la cara permiten complementar de forma significativa la información que se transmite con el habla. Otras veces, las expresiones «lo dicen todo». No es de extrañar por tanto, que una gran parte del esfuerzo investigador arriba mencionado se haya dedicado al estudio y desarrollo de caras de aspecto humano o animal. En unos casos se ha optado por emplear gráficos de ordenador, con la ventaja principal de no tener prácticamente limitaciones de tipo físico. En otros casos se han diseñado y construido dispositivos físicos, que si bien presentan limitaciones, aportan una componente no despreciable: las personas perciben con mayor interés al dispositivo que es físico, real. El dispositivo físico puede además ser observado desde diferentes ángulos. Por muy complejos que sean los gráficos, el parecido a la cara humana debe completarse con esa existencia física. En adelante nos centraremos en esta última opción.

En este artículo se presenta la descripción de un esquema de modelado de expresiones para una cara robótica. El software que lo implementa constituye uno de los módulos

de un proyecto actualmente en curso denominado CASIMIRO (*Cara Expresiva y Procesamiento Visual Básico para Robots Interactivos*). Por modelado de expresiones se entiende el proceso por el cual un diseñador define, de una forma más o menos sencilla, cuáles serán las expresiones que podrá presentar la cara, las posiciones asociadas de los distintos motores y cómo se realiza el paso de una expresión a otra. El modelado de expresiones debe emplear el mayor nivel de detalle posible, con el fin de dotar de más flexibilidad y posibilidades a la cara. No obstante, es fundamental que el modelado no se convierta en un proceso excesivamente complejo y sobre todo que pueda hacerse de forma interactiva, es decir, comprobando con el robot físico el aspecto de las distintas expresiones, las transiciones entre ellas, etc. En el siguiente apartado se describen brevemente otros trabajos relacionados, para a continuación presentar el marco de modelado. Por último, se describirá el software desarrollado y se discutirán posibles ampliaciones futuras.

TRABAJOS RELACIONADOS

Una cara robot muy simple es la del robot móvil Minerva¹. La cara tiene cuatro grados de libertad, uno para cada una de las cejas y dos para la boca. Las cejas se mueven rotando sobre su centro. La boca está constituida por una banda elástica roja. Cada extremo de la banda se halla enganchado a un brazo del servomotor, y el movimiento está limitado por tres pins. A pesar de la simplicidad del hardware, la cara de Minerva es capaz de producir un efecto significativo sobre el observador. Minerva podía adoptar cuatro expresiones básicas: neutral, sonrisa, tristeza y enfado.

El trabajo más relacionado con el proyecto CASIMIRO es Kismet². Kismet es una cara robótica desarrollada en el MIT que consiste de un sistema de visión activa estéreo y de características faciales que dotan al robot de un aspecto parecido al de un animal. Las características faciales que incluye son cejas (cada una con dos grados de libertad), orejas (cada una con dos grados de libertad), párpados (un grado de libertad) y boca (un grado de libertad). En versiones recientes se han incluido nuevos grados de libertad en partes como la boca. El robot es capaz de adoptar expresiones de enfado, fatiga, temor, disgusto, excitación, felicidad, interés, tristeza y sorpresa, todas



fácilmente interpretables para el observador humano. El sistema motor de Kismet se dividió en tres niveles. En el nivel más bajo se encuentran procesos que controlan cada motor. En el nivel siguiente, existen procesos que coordinan el movimiento de las características faciales. Por último, en el tercer nivel existen procesos que se encargan de disponer las características faciales para conformar las distintas expresiones. La ventaja de este esquema es evidente: la descomposición del trabajo de modelado de una forma natural y fácilmente escalable. Es por ello que en el modelado de expresiones de CASIMIRO se ha empleado este mismo esquema básico. En Kismet también se emplea el concepto de intensidad de la expresión. La intensidad no es más que un grado en que se adopta una expresión, con respecto a una pose que se considera neutral (que no parece conformar ninguna expresión). Los niveles superiores del sistema serán los encargados de suministrar la intensidad con la que se quiere adoptar determinada posición.

Las expresiones básicas que puede adoptar son: neutral, felicidad, enfado, sorpresa, tristeza, temor, disgusto, «bebido» y vergüenza.

El robot WE-3RIV (Waseda Eye Nº 3 Refined IV)³ presenta un hardware avanzado constituido por un total de 26 grados de libertad y multitud de sensores. La cara presenta nada menos que 21 grados de libertad: 4 para los globos oculares, 4 para los párpados, 8 para las cejas, 4 para los labios y 1 para la mandíbula. Las expresiones básicas que puede adoptar son: neutral, felicidad, enfado, sorpresa, tristeza, temor, disgusto, «bebido» y vergüenza. Al igual que en Kismet, se utiliza una medida de intensidad (de 50 grados) para las expresiones. La intensidad se emplea para hacer una interpolación de la expresión, con respecto a la expresión neutral.

ESQUEMA DE MODELADO

Para modelar las expresiones en el robot CASIMIRO, se emplea la jerarquía de tres niveles explicada en el apartado anterior. Se definen grupos de motores que constituyan una característica facial concreta. Por ejemplo, se agrupan dos motores determinados para el control de una ceja. Para cada uno de los grupos de motores definidos, se especifican las poses que se desea presente la característica facial. Por ejemplo, ceja derecha neutral, ceja derecha levantada, ceja derecha hacia el interior, etc. Por defecto, se realiza la transición entre esas poses en línea recta (en el espacio de valores de consigna de los motores), pero se debe dar al modelador la oportunidad de modificar de alguna forma la trayectoria descrita en las transiciones, porque algunas pueden resultar no naturales. En nuestro

caso particular, se optó por dar la oportunidad de introducir puntos intermedios en la trayectoria de transición. Adicionalmente, se otorga la posibilidad de especificar una velocidad entre cada dos puntos de la trayectoria. Se analizó la posibilidad de emplear interpolación no lineal (splines), pero se llegó a la conclusión de que no resultaría necesaria para un modelado aceptable. Una de las poses introducidas (la primera) es la pose neutral. Las poses introducidas son las de grado máximo (por ejemplo 100, si se usa el rango 0-100). El grado de la pose (que se especifica solo en ejecución) se utiliza para interpolar linealmente los puntos de la trayectoria, con respecto a la pose neutral. Con respecto al tercer nivel de la jerarquía comentada, las expresiones hacen referencia a poses de los diferentes grupos, cada una con un grado determinado. Por ejemplo, la expresión «Sorpresa» podría representarse simplificadamente por los siguientes datos:

Expresión: "Sorpresa"		
Grupo	Pose	Grado
Boca	Abierta	90
Ceja derecha	Levantada	90
Ceja izquierda	Levantada	90
Oreja derecha	Levantada	100
Oreja izquierda	Levantada	100
Párpado derecho	Levantado	80
Párpado izquierdo	Levantado	80

A su vez, la expresión a adoptar puede especificarse en ejecución acompañada de un grado. Este grado permite, mediante multiplicación, obtener el grado concreto a aplicar a las poses de los distintos grupos. Para obtener un mayor control, se permite especificar un tiempo de comienzo de cada grupo. De esta forma, podría por ejemplo conseguirse que al adoptar la expresión de sorpresa, primero se levantarán las cejas y después se abra la boca. En este punto es fácil ver que el empleo de la jerarquía de tres niveles comentada permite realizar movimientos de partes individuales, como por ejemplo guiñar un ojo, parpadear, mover la boca para hablar, etc. Con respecto a este último caso, puede además combinarse el movimiento de la boca con otras poses de otras características faciales, dando lugar a combinaciones como hablar con expresión de sorpresa, de enfado, etc.

TRANSICIONES ENTRE EXPRESIONES

En el apartado anterior se indicó que en tiempo de ejecución las poses de los grupos de motores podían adoptarse en un cierto grado, mientras que las poses que se introducían correspondían al grado máximo. Queda pues por resolver la cuestión de obtener la trayectoria de transición de una pose A con un grado cualquiera G_i a una pose B con un grado cualquiera G_f . En otras palabras, en un momento determinado el grupo se encuentra en la pose A con grado

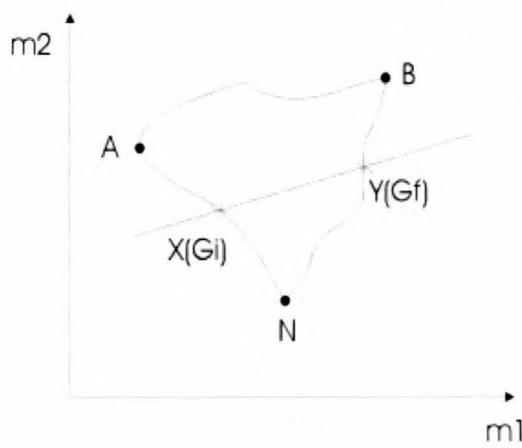
Gi, y se desea adoptar la pose B con grado Gf. Para un grupo de dos motores, el escenario sería el representado en la figura siguiente, donde N representa la pose neutral, X el punto correspondiente al grado inicial e Y el punto correspondiente al grado final. Para obtener la expresión que nos dará la trayectoria buscada, fijamos las siguientes condiciones extremo:

- Si Gi=0 -> T=XNY
- Si Gf=0 -> T=XNY
- Si Gi=1 -> T=(1-Gf)·XNY + Gf·XABY
- Si Gf=1 -> T=(1-Gi)·XNY + Gi·XABY

La ecuación que cumple estas restricciones es:

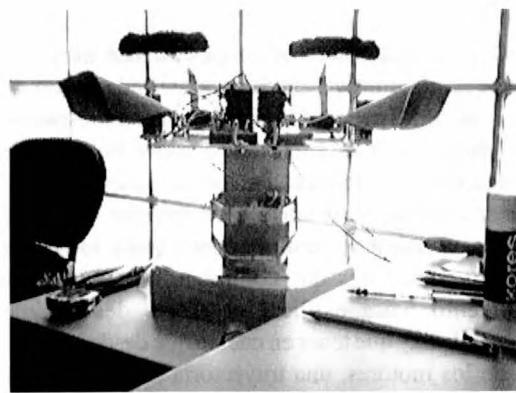
$$T = [1 - ((Gi >= Gf) ? Gf : Gi)] \cdot XNY + ((Gi >= Gf) ? Gf : Gi) \cdot XABY$$

Donde los símbolos ? y : corresponden a la instrucción IF-THEN-ELSE. Puede observarse además que la ecuación de trayectoria es continua en los valores de Gi y Gf. La misma relación se utiliza para hallar las velocidades de la trayectoria.

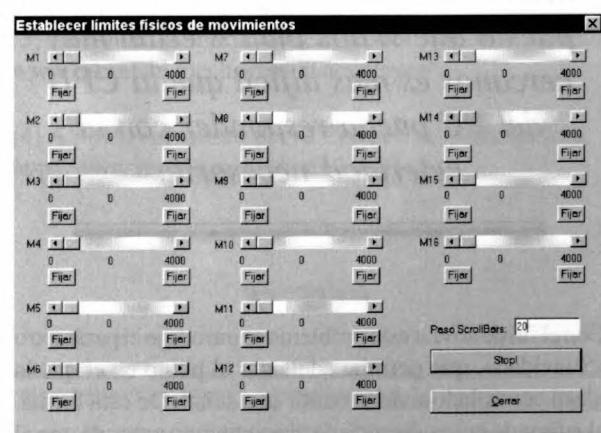


SOFTWARE IMPLEMENTADO

El esquema de modelado descrito se implementó en un programa de ordenador que se denominó «editor de poses». El cometido del editor de poses es proporcionar al modelador una forma sencilla e interactiva de definir las poses, transiciones, etc. La cara robot con la que se probó el software desarrollado es una versión inicial de CASIMIRO. El aspecto de la cara aparece en la figura siguiente. La cara robot está dotada de 9 motores: uno para la boca, 2 para la ceja izquierda, 2 para la ceja derecha, uno para la oreja derecha, uno para la oreja derecha y dos para los párpados. Todos los motores empleados son servomotores del mismo modelo, conectados a una placa controladora ASC16 de Medonis⁴, que es a su vez gobernada desde un PC mediante una conexión serie.



En una primera fase del desarrollo se elaboró una librería de bajo nivel con el fin de proporcionar una forma de enviar comandos a la placa controladora de motores. El editor de poses se basa en esta librería. La filosofía que sigue el editor de poses es la de dar la oportunidad al modelador de especificar una serie de datos sobre la cara y sus movimientos, y grabar todos estos datos en un fichero de poses. Este fichero será posteriormente lo único que se necesite para reproducir (y generar) los movimientos. El editor de poses está pues pensado para funcionar tanto en tiempo de modelado como en tiempo de ejecución, y puede controlarse por otras aplicaciones. Los pasos que seguiría el modelador para empezar el diseño serían: conectar con la placa ASC16, establecer los límites físicos de movimiento y especificar poses y transiciones. Los límites físicos de movimiento son los valores máximos y mínimos que pueden tomar los motores. Estos valores se introducen por el modelador y quedan guardados en el fichero de poses. La siguiente figura muestra la ventana de especificación de límites de movimiento.



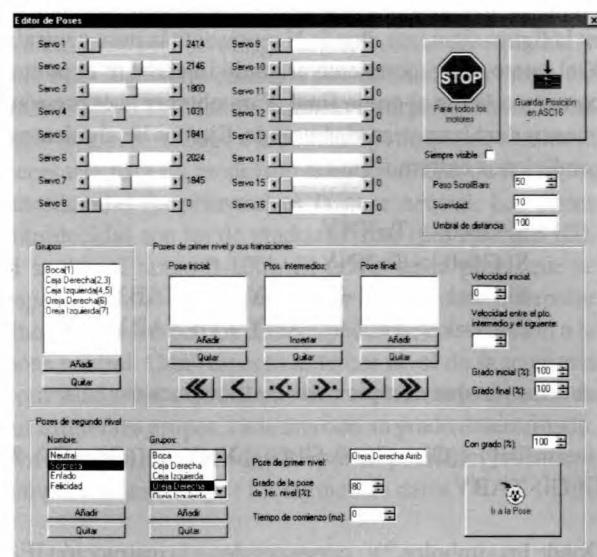
La parte fundamental del programa es la que permite definir los grupos de motores, poses y transiciones. La ventana de esta parte del editor de poses se muestra a continuación. En la parte superior izquierda se encuentran las barras de desplazamiento que permiten mover los



motores. En la parte central izquierda se definen los grupos de motores. En la parte central derecha se definen las poses del grupo seleccionado, y las transiciones entre ellas. Para modelar las transiciones pueden introducirse puntos intermedios y velocidades en cada punto de la trayectoria. En la parte inferior de la ventana se especifican las expresiones. Todos los datos especificados por el modelador se graban en el fichero de poses. En la parte superior derecha de la ventana se dispone de un botón STOP que permite parar al momento todos los motores, así como parámetros que controlan la continuidad del movimiento. Para explicar el efecto del parámetro «Suavidad» hay que tener en cuenta que desde el punto de vista de los motores, una trayectoria es un conjunto de puntos en el espacio motor que los motores siguen en línea recta. Cada tramo de la trayectoria puede tener una velocidad distinta, y además las velocidades definitivas de los motores se modifican para que todos acaben en el mismo instante, aunque el recorrido sea distinto (las velocidades de los servos empleados no son lineales, con lo que hubo de crearse una tabla de conversión). Cada grupo de motores es controlado por una línea de ejecución separada (*thread*), y todos los accesos al puerto serie han de sincronizarse. La placa controladora de motores emite una señal cuando un motor ha alcanzado un punto de la trayectoria. En ese momento, el editor de poses debe enviar a la placa el comando para que el motor se desplace al punto siguiente, con la velocidad asociada al tramo. Desde que se recibe la señal de la placa controladora hasta que se envía el comando de desplazamiento al punto siguiente pasa un tiempo (que dependerá de la carga de la CPU del PC) en el que el motor estará parado, lo cual hace que el movimiento no sea continuo.

El objetivo es también evitar discontinuidades en el movimiento, puesto que si dos puntos están muy cercanos es más difícil que la CPU del PC pueda responder con la celeridad necesaria.

Con el fin de aliviar este problema se introdujo el parámetro «Suavidad», que permite adelantar el punto en el que la placa controladora debe emitir una señal. De esta forma, el editor de poses dispone de cierto tiempo antes de que el motor llegue realmente al punto de parada. Por otro lado, el parámetro «Umbral de distancia» sirve para eliminar de las trayectorias los puntos consecutivos que estén muy cercanos. El objetivo es también evitar discontinuidades en el movimiento, puesto que si dos puntos están muy cercanos es más difícil que la CPU del PC pueda responder con la celeridad necesaria.



Para que el editor de poses pueda funcionar adecuadamente en tiempo de ejecución se incluyó un buffer de peticiones, que se encarga de mantener momentáneamente las peticiones de «Ir a pose X en grado Y» que vengan de otras aplicaciones. El buffer de peticiones es necesario porque las peticiones tardan un cierto tiempo en completarse. El buffer de peticiones comprueba en todo momento las peticiones en espera. Aquellas que sean compatibles con la que actualmente se está ejecutando (no tienen ningún motor en común) son lanzadas a ejecución, pero siempre respetando el orden en que se hizo las peticiones.

El parpadeo se implementaría con el esquema descrito mediante dos comandos consecutivos: uno para mover el párpado izquierdo y otro para mover el derecho.

Un caso especial a mencionar es el del parpadeo. El parpadeo se implementaría con el esquema descrito mediante dos comandos consecutivos: uno para mover el párpado izquierdo y otro para mover el derecho. No obstante, el parpadeo requiere de un tratamiento particular: los párpados han de volver a su posición original, sea cual sea. Además, el movimiento ha de hacerse siempre a la máxima velocidad posible. Por consiguiente, de forma automática los dos comandos de movimiento se convierten en cuatro, y se emplea la máxima velocidad. En el caso de solo querer guiñar un ojo, un comando de movimiento se

convierte en dos. Por otro lado, debido a que en la implementación desarrollada el movimiento de los párpados se ejecutará por dos *threads* distintos y a que el desplazamiento es muy corto y a gran velocidad (lo cual como hemos visto puede provocar que el PC no responda con la celeridad deseable), se impone la siguiente restricción: solo se puede parpadear cuando no hay ningún otro motor de la cara funcionando. De esta forma podemos asegurar la sincronía en el movimiento de los dos párpados. Esta restricción se considera razonable pues los movimientos de la cara para cambiar de expresión duran relativamente poco. La restricción implicaría que la cara no podría hablar (mover la boca) y parpadear al mismo tiempo, pero igualmente se considera aceptable en tanto en cuanto CASIMIRO no está destinado a realizar monólogos, y en cualquier caso, siempre hay pausas en el discurso que permitirían parpadear. El parpadeo no puede iniciarse desde el editor de poses, ha de hacerse con otra aplicación.

La restricción implicaría que la cara no podría hablar (mover la boca) y parpadear al mismo tiempo, pero igualmente se considera aceptable en tanto en cuanto CASIMIRO no está destinado a realizar monólogos, y en cualquier caso, siempre hay pausas en el discurso que permitirían parpadear.

CONCLUSIONES Y TRABAJO FUTURO

En este trabajo se ha descrito un programa de modelado de expresiones para una cara robótica. Un software que permita modelar de forma sencilla e interactiva los movimientos de una cara electromecánica constituye una herramienta muy útil sobre todo en las primeras fases del desarrollo de la misma, cuando se añaden o eliminan motores o piezas. El repertorio de poses es fácilmente escalable con el número de motores que se empleen. El software siempre puede dotarse de una mayor flexibilidad, pero hay que tener en cuenta que el objetivo no debe ser otro que el de conseguir que la cara se mueva lo mejor posible, desde el punto de vista de un observador humano. Quiere esto decir que no debe faltar flexibilidad pero tampoco debe hacerse el programa excesivamente complejo.

Aunque el esquema de modelado presentado es en sí mismo muy flexible, existen posibilidades que la versión

actual aún no contempla. Es particular, la «mezcla» de expresiones sería un aspecto a tener en cuenta. Por mezcla de expresiones se entiende la posibilidad de que la cara adopte simultáneamente dos o más expresiones, dando lugar a casos como por ejemplo presentar un aspecto de sorpresa a la vez que de felicidad. Dadas las posibilidades actuales del hardware disponible de la cara de CASIMIRO, se consideró que la expresividad de la misma no era suficiente para justificar el desarrollo de la mezcla de expresiones, aunque en un futuro debería ser tenida en cuenta.

Dadas las posibilidades actuales del hardware disponible de la cara de CASIMIRO, se consideró que la expresividad de la misma no era suficiente para justificar el desarrollo de la mezcla de expresiones, aunque en un futuro debería ser tenida en cuenta.

BIBLIOGRAFÍA

- [1] Minerva: Carnegie Mellon's Robotic Tourguide Project. <http://www-2.cs.cmu.edu/~minerva/>
- [2] Kismet: <http://www.ai.mit.edu/projects/humanoid-robotics-group/kismet/kismet.html>
- [3] An Anthropomorphic Head Robot WE-3RIV. <http://www.takanishi.mech.waseda.ac.jp/eyes/>
- [4] ASC16: Advanced Servo Controller, Medonis Eng. <http://www.medonis.com/asc16.html>

AUTOR



Oscar Déniz Suárez: Licenciado en Informática. Estudiante de doctorado y becario de investigación adscrito al Departamento de Informática y Sistemas de la Universidad de Las Palmas de Gran Canaria. Sus intereses investigadores se centran en robótica, interfaces percepto-efectores, y reconocimiento de caras.

