Localización en redes WLAN 802.11: desarrollo e implementación de una solución basada en traps SNMP

Eduard Garcia Villegas, Rafael Vidal Ferré
Departament d'Enginyeria Telemàtica. Universitat Politècnica de Catalunya.
EPSC, Avda. del Canal Olímpic, sn. 08860 Castelldefels
Teléfono: 934 137 055 Fax: 934 137 007
E-mail: eduardg@entel.upc.es, rafael.vidal@entel.upc.es

***Abstract**. The growth of WLANs and hence, the increase of mobile data terminals, bring about a visible proliferation of location-based services. This scenario also carries the need for location management systems that are device independent. In this paper, after an overview of several different solutions, we present a location discovery system for WLANs 802.11, based on SNMP traps. As a result of our work, two location aware applications have been implemented. One of these applications is a web service for location discovery that can be used to suggest the nearest points of interest (noteworthy tourist spots, shops, libraries, etc.). The other is a centralized application proposed for WLAN administrators to localize mobile users on their current position or to track those users on the past. The bulk of location-based services don't have the need of a big granularity, therefore our solution simply identifies to which AP a mobile user is currently connected to.*

1 Introducción

Durante el curso 2001/02, a iniciativa del grupo de comunicaciones inalámbricas del Departamento de Ingeniería Telemática, se llevo a cabo el despliegue de una red WLAN con tecnología IEEE 802.11b en la EPSC (Escuela Politécnica Superior de Castelldefels) formada en una primera fase por tres puntos de acceso (APs) conectados a la red de la Escuela [1]. El objetivo del despliegue era doble. Por un lado se pensaba en ofrecer a toda la comunidad que forma la EPSC de un acceso sin hilos de calidad a su red y, por extensión, a la de la UPC y a Internet. Por otro, se buscaba disponer de una plataforma sobre la que desarrollar y probar soluciones para el soporte de la movilidad, como por ejemplo Mobile IP y Cellular IP, aplicaciones que sacarán provecho de ella, además de desarrollar herramientas que permitiesen una fácil monitorización de la propia red WLAN y sus usuarios. Es precisamente en este último punto donde se centra el presente artículo.

1.1 Localización en redes móviles

Para la monitorización de la red WLAN se tomo como punto de partida el protocolo SNMP (*Simple Network Management Protocol*) [2] y la información contenida en las MIBs (*Management Information Base*) de los APs utilizados. A partir de esta información se desarrolló una web de acceso restringido que permite monitorizar el correcto funcionamiento de la red a través de estadísticas actualizadas de determinados parámetros de la misma y la visualización de las alarmas producidas en ella. Todo ello mediante la utilización de MRTG (*Multi Router Traffic Grapher*) [3].

El siguiente paso era la monitorización de los usuarios y en concreto de su localización. La motivación para conseguir este objetivo era constatar cómo el acceso a la información de localización supone un valor añadido de cara a la gestión de una red con usuarios móviles, a la vez que abre las puertas al desarrollo de nuevos servicios como ya se está comprobando para el caso de las redes de comunicaciones móviles celulares de segunda generación. Algunos ejemplos de estos nuevos servicios son: el control de flotas, las campañas de marketing vía mensajes cortos dirigidas a zonas concretas de especial interés o la búsqueda de un determinado servicio (restaurantes, farmacias, hospitales, museos,...) en función a la posición del usuario. Aunque la precisión con que se conoce la posición de un usuario no es comparable a la de sistemas de localización vía satélite, es suficiente para el desarrollo de muchas aplicaciones. Además, las redes celulares presentan algunas ventajas muy significativas respecto a las de satélite. En primer lugar superan en cobertura a los sistemas satélite en entornos urbanos y muy especialmente en el interior de edificios; y sobretodo, el usuario de la red celular no necesita de ningún hardware ni software adicional a su terminal telefónico para ser localizado.

En el momento de plantearse una solución para la localización en redes WLAN se ha tomado precisamente este último aspecto como condición irrenunciable: para localizar un usuario de la red WLAN no se necesitará más hardware que su tarjeta de red ni ningún software adicional más allá de los controladores de ésta. En el segundo capítulo del artículo se clasifican y comparan las diferentes soluciones de localización en redes WLAN existentes, a la vez que se introduce la desarrollada por los autores basada en el envío y tratamiento de *traps* SNMP. La arquitectura funcional de esta solución se describe con detalle en el tercer capítulo.

El trabajo realizado culmina con la implementación de esta arquitectura en la WLAN de la EPSC y el

desarrollo de aplicaciones que pudiesen mostrar las posibilidades de esta solución. En el momento de buscar utilidades a la información de localización en redes WLAN es necesario observar que estas redes presentan algunas particularidades respecto a las celulares, que hacen pensar en otras aplicaciones. En primer lugar, su ámbito de explotación es privado en cuanto a sus usuarios y reducido en cuanto a cobertura. En nuestro caso, por ejemplo, el acceso se limita a la comunidad de alumnos, profesores y personal de servicios que forma la Escuela y la cobertura al edificio donde ésta se ubica. En segundo lugar, los dispositivos utilizados, típicamente portátiles y PDAs (*Personal Digital Assistants*), disponen de mayores capacidades de proceso, almacenamiento y multimedia. Y finalmente, la velocidad de acceso es mucho más elevada, con 802.11b, entre 1 y 11Mbps. Mientras que las mayores prestaciones de los terminales y la mayor velocidad de acceso permitirán el desarrollo de aplicaciones más sofisticadas que podrán enviar y/o recibir volúmenes de datos más elevados en un menor tiempo, las limitaciones de su ámbito de explotación nos llevaran a pensar en soluciones a medida de las necesidades de los administradores y usuarios de una determinada red WLAN. Por ejemplo: museos, campus universitarios, edificios de oficinas,...

Todo esto se ha tenido en cuenta en la implementación del sistema que se ha realizado y que se describe en el cuarto capítulo. Esta implementación se ha traducido en dos aplicaciones. Una de ellas dirigida a los administradores de red permite rastrear y localizar a los usuarios de ésta. La otra, ofrece a los usuarios información a medida según su localización mediante un servicio vía web. Respecto a esta última aplicación, en el quinto capítulo se comentan las posibles causas de error en la localización que puede introducir el sistema y se describen las pruebas realizadas para estudiar como afectan a los usuarios. Finalmente, se cierra el artículo con las conclusiones en las que se comentan los principales logros conseguidos y las líneas futuras de trabajo que piensan seguirse.

2 Localización en redes 802.11

Las estrategias de localización de dispositivos móviles en redes WLAN 802.11 se pueden agrupar en dos grandes bloques: las que sólo utilizan información de nivel de enlace y superiores y las que también se fijan en parámetros de nivel físico, en concreto en el de potencia de señal recibida.

Las soluciones del primer tipo permiten determinar el AP al que un nodo móvil se encuentra asociado. Es decir, tienen una resolución igual al área de cobertura del AP. Esta resolución puede mejorarse completándolas con soluciones del segundo bloque, es decir, con estrategias basadas en la medida de niveles de potencia. Básicamente, estas soluciones, realizan conversiones de niveles de señal, medidos desde diferentes puntos, en longitudes, a partir de las cuales, mediante un algoritmo, el sistema devuelve las coordenadas x, y, z del dispositivo [4]. De hecho, muchas de las soluciones existentes proponen métodos más sencillos en dos dimensiones, haciendo la (falsa) suposición de que los APs y el cliente se encuentran en un mismo plano [5][6][7]. Para la conversión nivel de señal/distancia, la teoría dice que hay una relación $1/r^2$, pero los resultados empíricos ponen de manifiesto que la respuesta real es difícil de describir con ecuaciones. En entornos diferentes a espacios abiertos, las conversiones de potencias a distancias pueden resultar engañosas debido a la atenuación producida por paredes de hormigón, ficheros metálicos, ascensores, etc. Por este motivo se usan modelos empíricos de propagación particulares que no son válidos de un entorno a otro.

La complejidad introducida por las soluciones basadas en medidas de señal es en muchos casos injustificable, pues como ocurre en el caso de las redes celulares, conocer la zona de cobertura en la que se encuentra un usuario puede ser más que suficiente para muchos servicios de localización. Por este motivo, nos centraremos en el estudio del primer bloque de soluciones basadas en la información de nivel de enlace y superiores.

A priori, la forma más evidente de realizar una localización de este tipo, sería utilizar la información que el dispositivo cliente conoce, pues éste sabe al instante la identidad del AP al que se conecta, es más, lo sabe con antelación ya que debe mantener estadísticas a partir de medidas de potencia para decidir el traspaso de un AP a otro. El problema de esta solución es que no es independiente del sistema operativo (SO) o de la arquitectura del dispositivo al servirse de ciertas llamadas a sistema.

Otra posibilidad sería aprovechar que normalmente los APs trabajan haciendo de *bridge* transparente, por lo que mantienen una tabla (*bridge learn table*) con información de los dispositivos que han estado asociados al AP recientemente. Una consulta periódica a estas tablas mediante el protocolo SNMP, proporciona la información necesaria para el funcionamiento de otro sistema para localizar usuarios [8]. Un inconveniente importante es que el AP mantiene dicha información sobre un usuario durante un periodo entre 15 y 30 minutos después de que éste se haya desconectado o se haya asociado a otro AP, por eso, se debe buscar la información más reciente de entre todos los APs y mantener, un fichero *log* con el resultado de las consultas SNMP a los diferentes APs. Otro inconveniente es que para obtener una medida más precisa, se deben realizar consultas con más frecuencia, lo que supone un aumento significativo del tráfico en la red.

Otra solución es el uso de RADIUS (*Remote Authentication Dial-In User Service*) [9], que, junto con EAP (*Extensible Authentication Protocol*) [10][11], aparte de proporcionar control de acceso a los APs, puede usarse para mantener información sobre la situación de usuarios de una red WLAN. Cada AP actúa como un cliente RADIUS que comprobará la autenticación de los usuarios dentro de

su área de cobertura. Si la autenticación es correcta, se guarda la información (hora, identidad del AP y MAC de cliente) en un fichero log que luego se inspecciona para obtener el AP al que un determinado usuario, conocida su dirección física MAC, está conectado [8]. El principal problema de esta solución es el hecho de que, aunque el uso de EAP (sobre 802.1x) está ampliamente aceptado en equipos fijos (AP, *switch*, etc.), no todos los fabricantes de tarjetas cliente 802.11 apuestan por ese método para realizar un control de acceso seguro en redes sin cables [12].

Finalmente, el método que se quiere exponer en este artículo, se basa en una funcionalidad del protocolo de gestión de redes SNMP diferente a la vista hasta ahora. Sin los inconvenientes de las consultas periódicas a las tablas de todos los APs, se obtienen mejores resultados que con la solución RADIUS (ver tabla 1), ya que no se requiere una autenticación previa tipo cliente-AP-RADIUS, solución más costosa en términos de tiempo y tráfico. Este método se basa en el envío de *traps* SNMP para la gestión de eventos. Un *trap* (o *notification*, como se rebautiza en SNMPv2) es un mensaje enviado por una entidad SNMP a otra, para indicar la ocurrencia de un evento significativo, como una condición definida específicamente, o un umbral que ha sido alcanzado. Esto significa que, ante ciertos eventos, el dispositivo no espera a que hagan una consulta SNMP para mostrar la información de dicho evento, lo que hace es informar inmediatamente de éste a un determinado nodo de la red. En el caso que nos atañe, cuando un AP detecta la conexión o desconexión de un cliente, automáticamente envía un *trap*. De esta manera, en cuanto un usuario se conecta a la WLAN o cambia su punto de acceso, se dispone de la información sobre su localización, es decir se sabe en todo momento, a qué AP está conectado el cliente, sabiendo su dirección física MAC.

Una vez descartada la solución basada en medidas de potencia, ampliando los datos de [8], en la tabla 1 podemos ver las ventajas del último método sobre los demás:

- Se trata de un sistema rápido
- Genera poco tráfico adicional
- No requiere software adicional en terminales
- Independiente del SO y de la arquitectura del cliente

Como contrapunto, el sistema estará limitado a redes cuyos APs sean capaces de generar *traps* al detectar asociaciones de usuarios.

3 Arquitectura del sistema

La arquitectura del sistema de localización basado en *traps* SNMP, versiones uno, dos y/o tres, se compone de cinco entidades lógicas:

- **Usuario móvil**: dispositivo con interfaz de red 802.11 cuya dirección física se conoce y que se desplaza por el área de un ESS (*Extended Service Set*).
- **AP**: punto de acceso de los usuarios móviles a la red de área local. Estos dispositivos deben ser capaces de generar *traps* SNMP ante eventos de conexión o desconexión de usuarios.
- **Servidor de localización (SLOC)**: proceso que recibirá *traps* SNMP y que guardará su información en un fichero log o en una base de datos.
- **Log**: fichero o base de datos donde se almacena la información recibida de los *traps* SNMP.
- **Servidor de aplicaciones (SAP)**: proceso que lee e interpreta la información del log para mostrarla a los usuarios de la aplicación de localización.

En la figura 1 puede verse un ejemplo de la interrelación de estos elementos. En primer lugar el AP1 informa al servidor de localización mediante el envío de un *trap* sobre la asociación del usuario con MAC 1. SLOC guarda esta información y le añade la hora en que llegó el mensaje. A continuación, el usuario se mueve y pasa a asociarse a un nuevo AP, AP2. Esto provoca el envío de un nuevo *trap* por parte del AP2 a SLOC, que lo procesa tal como se ha comentado.

Tabla 1: comparación entre sistemas de localización en WLANs

	En cliente	RADIUS	SNMP	Traps SNMP
Servicios de red adicionales	NO	Cliente RADIUS en AP	AP con SNMP	AP con SNMP y generación de traps
Señalización adicional	NO	Queries RADIUS cada asociación	Consultas periódicas	Traps SNMP por cada asociación
Software adicional en cliente	Sí	No	No	No
Independiente de S.O.	No	Sí	Sí	Sí
Independiente de hardward	No	Si	Si	Si
Dificultad de implementación	Alta	Baja	Media	Baja
Tiempo de respuesta	Inmediato después de asociación	3 a 5 segundos	10-30 segundos (según periodo consulta)	1 a 2 segundos

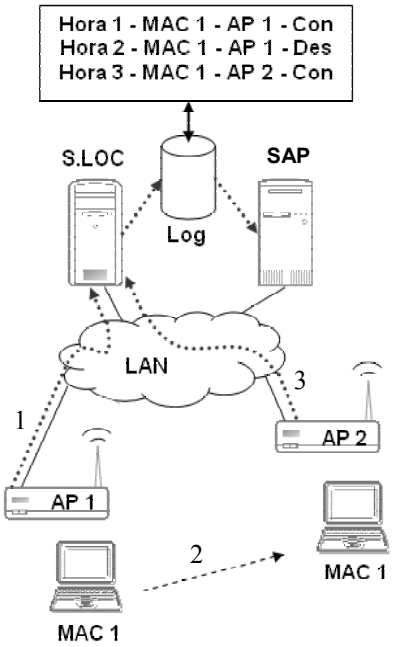

Figura 1: Arquitectura del sistema de localización

4 Aplicaciones desarrolladas

Sobre la arquitectura descrita en el apartado anterior se han desarrollado dos aplicaciones que sacan partido a la información de localización de los usuarios en una red 802.11 desde dos puntos opuestos:

- **XLOC**. Herramienta para administrador que permite, desde un punto central de la red, conocer el área de cobertura donde se encuentra un determinado usuario y rastrear sus movimientos.
- **Servicio de páginas web inteligente**. Las páginas servidas son personalizadas según la localización del usuario que hace la petición.

En los siguientes subapartados se explicará el detalle del funcionamiento de estas aplicaciones, realizadas y probadas sobre la red WLAN 802.11b de la EPSC.

4.1 Implementación

Los *traps* SNMP no están estandardizados y el formato de la información varía según el fabricante del AP. La aplicación ha sido implementada con soporte para los *traps* SNMPv1 de los APs 3COM AirConnect, y los *traps* SNMPv1 y SNMPv2 de los APs Cisco Aironet 340/350, pero puede ser modificada fácilmente para admitir formatos de otros APs. En ambos casos, cuando un AP detecta un evento de tipo ***MU state change*** (cambio de estado de una unidad móvil), ya sea provocado por la asociación de un nuevo usuario al AP o por la pérdida de un usuario que estaba asociado, envía un trap SNMP al servidor de localización.

La información que incluyen los *traps* SNMP que recibe el servidor de localización consta de:

- Dirección IP del AP que ha detectado el evento
- Dirección física (MAC) del AP que ha detectado el evento
- Dirección física (MAC) del cliente, el estado del cual ha cambiado
- Nuevo estado del cliente (asociado, desasociado, perdido, etc.)

El trato dado a la información contenida en el trap es dependiente de la implementación. En nuestro caso, por sencillez, se guarda en un fichero de texto que reside en el mismo servidor de localización, pero una vez obtenida, la información puede almacenarse en cualquier tipo de base de datos, lo que facilitaría su posterior análisis y el poder ser accedida desde cualquier tipo de aplicación (PHP, servlet, JSP, etc.).

Así pues, lo único que conocen los APs sobre un cliente asociado es su dirección MAC. Por este motivo, en las dos aplicaciones se realiza una búsqueda basada en direcciones MAC para saber en qué AP está asociado y así conocer el área donde se encuentra el usuario. Esta idea se recoge en el diagrama de la figura 2, donde se puede ver el funcionamiento simplificado del sistema. Por un lado, hay un proceso continuamente esperando la llegada de *traps* SNMP, cuando eso sucede, se limita a añadir esa información al sistema de **log**. Dejando de lado temas de concurrencia, el esquema es válido para representar los procesos que siguen las dos aplicaciones. Ambas esperan una petición de búsqueda por parte del usuario. Partiendo de una situación en que el usuario a localizar está registrado, es decir, conocemos el mapeo IP → MAC, se obtiene del sistema de almacenamiento de *traps* la información sobre el AP al que está asociado. El último paso consiste en generar la información personalizada según la localización y mostrarla al usuario. Si, de entrada, no se tiene información sobre el cliente a localizar o sobre el AP al que se ha asociado un cliente, la aplicación mostrará un error.

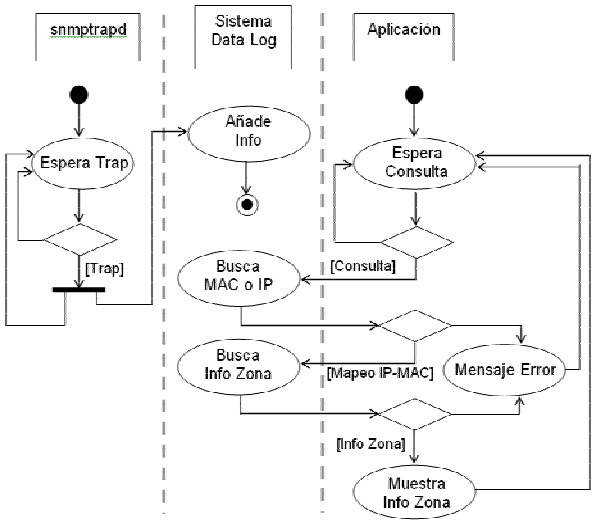

Figura 2: Diagrama de actividad del sistema

La importancia del mapeo IP → MAC se comentará en los siguientes apartados.

4.2 Servidor de localización

En nuestra maqueta, el servidor de localización se monta sobre un PC Pentium con sistema operativo (SO) Linux Red Hat 7.3 (*kernel* 2.4.18). Para recibir correctamente los *traps* que envían los APs se requiere la instalación del demonio ***snmptrapd***. Este demonio forma parte del paquete *ucd-snmp* [13]. En nuestra maqueta se ha instalado la versión 4.2.4-3 del paquete, incluida en la distribución del SO instalado, aunque cualquier versión posterior, actualmente bajo el nombre de *net-snmp*, es válida.

Los mensajes que el demonio ***snmptrapd*** recibe, pueden guardarse directamente en un fichero o ser enviados al demonio ***syslogd*** de la misma máquina o de otra diferente. ***Syslogd*** es el encargado de tratar los mensajes del sistema.

En nuestro caso, el servidor de localización, además de ser la máquina preparada para recibir los *traps* SNMP que envían los AP, es donde se ejecuta un CGI para la aplicación de páginas web personalizadas y donde se ejecuta la aplicación del administrador. Por ello, además de lo anterior, se ha instalado la versión 1.3.23 del servidor HTTP ***Apache*** [14] para atender las peticiones de clientes de la aplicación de páginas web personalizadas. Para compilar y ejecutar la aplicación de administrador **XLOC**, es necesario instalar las librerías GTK+ [15], versión 1.2.0 o superior, y *gnome* [16], versión 1.0.0 o superior.

4.3 Páginas web inteligentes

Como ya se ha comentado, la información que sobre un cliente móvil lleva un *trap* SNMP se limita a su dirección MAC. Sin embargo, a nivel HTTP, para distinguir usuarios sólo podremos usar direcciones IP. Por ello, es necesario conocer el mapeo IP – MAC de los usuarios del sistema y tener guardada esa información en una base de datos o en un fichero de configuración. En nuestro caso, se utiliza un fichero de configuración donde, además, se guarda información de los APs y de las zonas que éstos cubren.

Para que un cliente pueda hacer uso de la aplicación, bastará con que haga una petición web al servidor de localización, pidiendo el ejecutable CGI. Si el cliente está registrado en el sistema (conocemos su mapeo IP – MAC), verá una página HTML como la que se muestra en la figura 3, donde se puede ver cuál es el área donde se encuentra en ese momento, información sobre el AP al que está asociado, fecha y hora de su asociación e información sobre la zona donde se encuentra (tiendas, restaurantes, bibliotecas, etc.)

Para mostrar siempre la información sobre la localización actualizada, se puede provocar que la página se refresque de manera automática con más o menos frecuencia, haciendo uso del *Meta Tag* [17] "Refresh", que, aunque en un principio sólo era válido para navegadores Netscape, actualmente es interpretado correctamente por la inmensa mayoría de los navegadores existentes.

4.4 Aplicación Administrador (XLOC)

Se trata de una aplicación programada en C, que hace uso de las librerías GTK+ 1.2 y *gnome-libs* para proporcionar una interfaz gráfica amigable. Está pensada para ser ejecutada en la misma máquina donde se guarda la información sobre los *traps*, es decir, el servidor de localización. Si se desea ejecutar esta aplicación en cualquier otra máquina, se puede configurar el *demonio* ***snmptrapd*** o el ***syslogd*** para

Figura 3: Aplicación de web personalizada

redirigir los *traps* hacia ella.

Como en el caso de la aplicación de páginas web personalizadas, se necesita un fichero de configuración donde guardar información de los APs y de los clientes. Dicho fichero es prácticamente igual al fichero de la aplicación CGI.

La ejecución del programa hará aparecer la ventana que se muestra en la figura 4. En la parte superior de ésta aparece una entrada de texto para escribir la dirección física del cliente a localizar o seleccionarla del menú desplegable donde aparecen las direcciones que la aplicación lee del fichero de configuración. La parte inferior está ocupada por un plano de la Escuela en el que se marcan las diferentes zonas de cobertura, para facilitar la ubicación espacial de los usuarios.

Hay dos modalidades de búsqueda, la primera, mediante el botón ***Histórico***, permite hacer un seguimiento de los *traps* que han llegado al servidor de localización referentes a un determinado cliente. Las flechas permiten avanzar o retroceder en el tiempo y así conocer los movimientos realizados por el cliente. Dicha modalidad nos facilita la información retenida a lo largo del tiempo en el fichero de *traps*, pero no nos asegura si el cliente que buscamos está conectado en ese mismo instante. Para ello se utiliza la otra modalidad, botón ***Localiza***, con la que se fuerza el envío de mensajes *ICMP echo request* (ping) al cliente, de esta manera, si se recibe respuesta, podemos estar seguros de que el cliente está conectado y ver en qué AP.

5 Pruebas de campo

Las pruebas que se explican en este apartado fueron realizadas para determinar el grado de fiabilidad que tienen los datos sobre localización que muestran las aplicaciones. Entendemos como error cuando, sabiendo nuestra posición, es decir, a qué AP estamos asociados, la aplicación nos muestra unos datos incorrectos.

El error puede ser debido a tres causas, pudiendo presentar las dos primeras una varianza significativa. Como primera causa aparece el tiempo que transcurre desde que el cliente decide asociarse a un determinado AP hasta que se genera el *trap*. El tiempo de asociación (o des-asociación) del cliente al AP puede variar de 100 a 600 ms dependiendo de la combinación de modelo de dispositivo cliente con diferentes modelos de AP [18]. La segunda causa es el tiempo de envío y recepción del *trap*. Estos tiempos dependerán de la capacidad del AP para generar el *trap* en el momento que se produzca el evento que lo provoca y de la red para transportarlo. En cualquier caso se trata de valores de ms dentro de una red LAN. Finalmente, la tercera fuente de error es el tiempo de refresco de la página en el navegador del cliente que es del orden de segundos.

Las zonas donde hay cobertura de más de un AP, y por tanto, los traspasos son frecuentes, son las zonas donde el comportamiento del sistema puede ser más conflictivo y donde, por tanto, se han realizado las pruebas. Dichas zonas se representan en la Fig. 5 mediante líneas numeradas (de la forma X-Y) en el punto donde se detectan traspasos del AP X al AP Y.

Para determinar la máxima exactitud del sistema las pruebas de error se han realizado minimizando la influencia de las fuentes de error controlables:

- Refresco de la página con la máxima frecuencia posible. El cliente recibe la

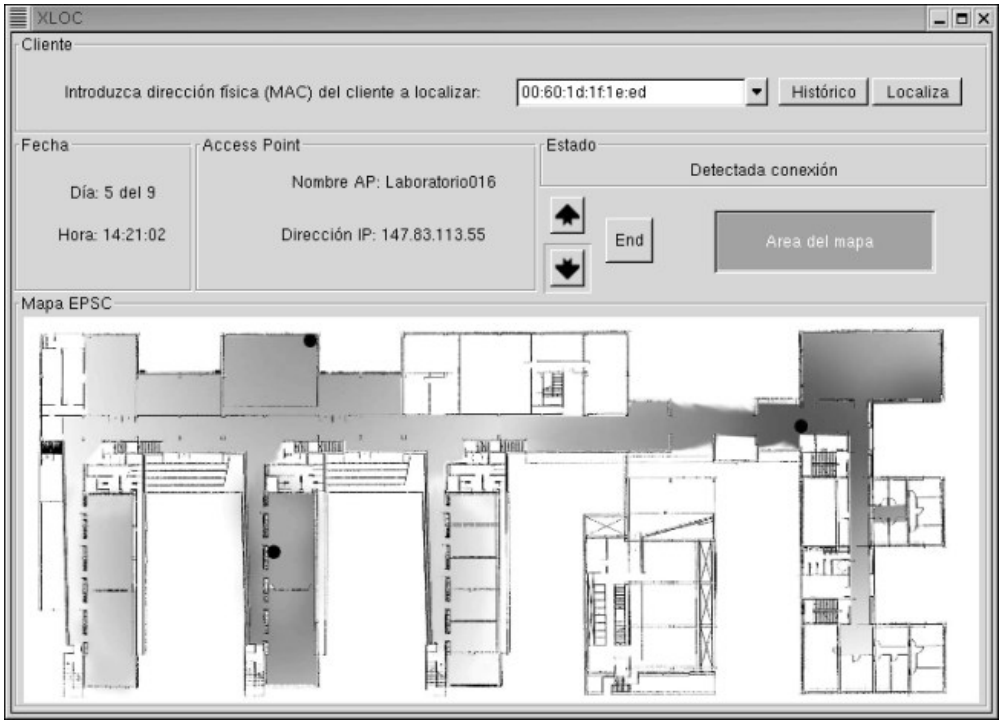

Figura 4: Apariencia de la aplicación de administrador

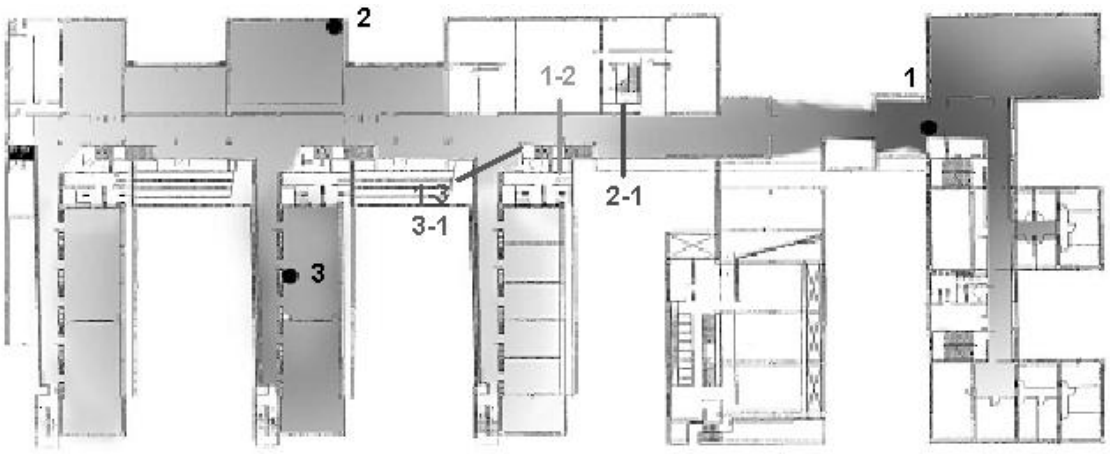

Figura 5: detalle de los límites entre las áreas de cobertura de los tres APs

información cada segundo, i.e. la precisión de la medida está limitada a 1s.

- Versión reducida de la página web (4KB). El tiempo que dura la transferencia de los datos no es significativo ya que a la velocidad mínima (1Mbps), representa tan sólo un retardo de unos 30 ms.
- Red con poca carga. No tendremos tampoco en cuenta el retardo entre el AP que genera un trap y el servidor que lo recibe (orden de ms), ya que no influye en la medida si trabajamos con valores dentro de un orden de magnitud de segundos.

La información obtenida de la aplicación es comparada con la obtenida de las utilidades incluidas con los controladores de las tarjetas 802.11, gracias a las cuales, se puede conocer de manera instantánea la información del AP al que el cliente está asociado.

Por norma general, el cliente recibe la información actualizada con un retardo de alrededor de 1s. Sin embargo, en el peor caso, es decir, cuando el traspaso se realiza justo después de la última actualización de la página CGI, el error es cercano a los 2 segundos. Ello es debido a que la información se actualiza en el servidor de localización dentro del primer segundo después del traspaso y la primera actualización de la página CGI llega aún con la información antigua, por lo que, para tener la nueva información deberá esperar un segundo más. Ese retardo puede suponer, traducido en longitud, un error de entre 1 y 2 metros dentro de una área de cobertura adyacente a la que muestra la aplicación como situación del cliente, suponiendo una velocidad pedestre típica (unos 4 ó 5 km/h).

Finalmente, debe añadirse, que al enviarse los *traps* SNMP sobre UDP (modo datagrama, sin acuse de recibo), podría llegar a producirse la pérdida de un *trap*. En esta situación, el usuario recibiría información errónea hasta que volviera a asociarse a otro AP. De todos modos, para un sistema de localización basado en *traps* SNMP instalado en una red de área local sin congestión y con pocos saltos entre APs y servidor, la probabilidad de perder un paquete pequeño, como un trap SNMP, es prácticamente nula, no habiéndose producido ni una sola vez en las pruebas realizadas.

6 Conclusiones y trabajo futuro

En este artículo se ha descrito una solución que permite localizar usuarios de una red WLAN 802.11 sin que sea necesario hardware o software adicional en los dispositivos móviles. Dicha solución depende solamente del soporte, por parte de los APs, al envío de *traps* SNMP relacionados con la asociación de usuarios.

Para demostrar la utilidad del sistema, se han implementado dos aplicaciones: una orientada a administradores de redes WLAN y otra a los usuarios de éstas. Las aplicaciones han sido probadas y actualmente están en funcionamiento en la red WLAN de la EPSC. Las pruebas realizadas y aquí expuestas, demuestran que el tiempo de respuesta del sistema, concretamente para el caso del servicio de páginas web inteligentes, es adecuado para usuarios que se desplazan dentro del área de cobertura de la red a velocidades pedestres.

Como contrapunto, el sistema presenta un punto débil al depender de UDP para el transporte de los *traps* entre APs y servidor de localización, ya que la pérdida de un *trap* puede resultar en que las aplicaciones muestren información errónea a la hora de ubicar el usuario que provocó el envío del *trap* perdido. Tal pérdida se produce con una probabilidad prácticamente nula cuando el sistema se utiliza en una LAN, pero es un asunto muy a tener en cuenta si se pretende implantar en una WAN, caso que puede ser muy interesante como se comenta más adelante. Este contrapunto puede resolverse a medida que el uso de SNMPv2 se normalice y los fabricantes doten a los APs de la capacidad de enviar mensajes *inform* en lugar de *traps*. Aunque también viajan sobre UDP, su recepción debe ser confirmada por el destinatario.

La proliferación de redes WLAN abiertas y organizadas sin ánimo de lucro así como la figura de los WISP (*Wireless Internet Service Providers*), con acuerdos de *roaming* incluidos, está rompiendo con

la idea de que las redes WLAN son de ámbito reducido y para usuarios privados. Una sola organización puede controlar un número significativo de redes y usuarios con lo que la información de localización aumenta de valor, acercándose más al modelo de negocio de los operadores celulares. Este modelo pasa por separar los datos de localización de los servicios que pueden ser prestados por otras empresas. Para conseguir este propósito y manteniendo la arquitectura descrita en el tercer capítulo, se está modificando la implementación presentada de manera que el servidor de localización escriba la información de localización en una base de datos SQL residente en otro equipo, mediante una modificación del código de ***snmtrapd***. Esta información podría ser recuperada por red desde cualquier otro equipo en el que se quisiera ofrecer un servicio basado en localización y tratada en local para generar estadísticas de uso de la red asociadas a localización de sus usuarios.

Otro aspecto a resolver es el mapeo MAC-IP. Este par puede ser conocido de antemano como en el caso de la WLAN de la EPSC o el de un museo con WLANs en sus salas que alquile PDAs a sus visitantes para que obtengan, vía web, información actualizada según la sala en que se encuentren, por citar un posible caso de aplicación comercial. Sin embargo, en el escenario descrito en el párrafo anterior, la asignación de direcciones suele ser dinámica por lo que se hace necesario obtener información de los servidores que realizan la asignación de direcciones para poder utilizar la función **localiza** de **XLOC** y el servicio de páginas web inteligentes**.**

Finalmente, comentar que se está trabajando en una versión web de **XLOC** que permita su integración en la web de monitorización de la WLAN de la EPSC para facilitar su utilización desde cualquier equipo con el único requisito de que disponga de un navegador.

Agradecimientos

El trabajo presentado en este artículo se enmarca dentro del proyecto TIC2000-1041-C03-01 financiado por Comisión Interministerial de Ciencia y Tecnología (CICYT)

Referencias

[1] X.Bordoy, R.Vidal. “Despliegue de una WLAN en la EPSC”. Buran (pendiente de publicación.)

[2] J. Case, et. al. “A Simple Network Management Protocol (SNMP)”. IETF RFC 1157. Mayo 1990.

[3] MRTG: The Multi Router Traffic Grapher: http://www.mrtg.org

[4] Alois Ferscha, Wolfgang Beer, Wolfgang Narzt. “Location Awareness in Community Wireless LANs”. GI/ÖGC-Jahrestagung, pp. 190-195, vol. 1. 2001

[5] P. Bahl, N. Padmanabhan. “RADAR: An In-Building RF-based User Location and Tracking System”. INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, pp. 775-784, vol. 2. Marzo 2000.

[6] Bhasker, Ezekiel. Griswold, Bill. Location Detection in a Wireless 802.11b Network Environment. 2001

[7] “A Practical Approach to Identifying and Tracking Unauthorized 802.11 Cards and Access Points”. Interlink Networks White Paper, URL: http://www.interlinknetworks.com. 2002.

[8] Koo, Simon, et. al. “Location Discovery in Enterprise-based Wireless Networks: Implementation and Applications”. Second IEEE Workshop on Applications and Services in Wireless Networks (ASWN 2002), Paris. Julio 2002.

[9] C. Rigney, et. al. “Remote Authentication Dial In User Service (RADIUS). IETF RFC 2865. Junio 2000.

[10] L. Blunk, et. al. “PPP Extensible Authentication Protocol (EAP)”. IETF RFC 2284. Marzo 1998.

[11] L.Blunk, et. al. “Extensible Authentication protocol (EAP)”. Internet Draft. Enero 2003.

[12] Erik Dobbelsteijn. “WLAN authentication and authorisation methods”. 2nd Mobility Meeting, Amsterdam. Octubre 2002.

[13] The NET-SNMP Project Home Page: http://net-snmp.sourceforge.net/

[14] The Apache HTTP Project: http://httpd.apache.org/

[15] GTK+ - The Gimp Tool Kit: http://www.gtk.org

[16] GNOME: http://www.gnome.org

[17] Dave Ragget. “HTML 3.2 Reference Specification”. W3C Recommendation. URL: http://www.w3.org/TR/REC-html32.html. Enero 1997.

[18] Arunesh Mishra, Minho Shin, William Arbaugh. “An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process”. 2002. CS Tech Report Number CS-TR-4395. UMIACS Tech Report Number UMIACS-TR-2002-75.