DESARROLLO DE UN INTERFAZ WEB EDUCATIVO PARA LA DEFINICIÓN Y MONITORIZACIÓN DE UNA RED AD HOC CON ENCAMINAMIENTO AODV

D. CRUZADO HERRERA, E. CASILARI, J. M. CANO GARCÍA, A. TRIVIÑO CABRERA.
Dpto. de Tecnología Electrónica. ETSI de Telecomunicación. Universidad de Málaga. España.

En este documento, se describe un interfaz basado en web para la monitorización didáctica del funcionamiento del protocolo de encaminamiento AODV en el establecimiento de una red ad hoc entre varios PC. A su vez se repasan brevemente las redes ad hoc, sus características y aplicaciones, así como las características y funcionalidades del interfaz web desarrollado y las tecnologías en él empleadas. Por último se comentan las pruebas realizadas y las futuras ampliaciones del sistema.

1. Introducción

El objetivo de este trabajo se centra en las redes ad hoc o MANET (*Mobile Ad hoc Networks*). Una red inalámbrica ad hoc está compuesta por dispositivos móviles de computación que usan la transmisión inalámbrica para comunicarse sin tener ningún tipo de infraestructura fija y previa, esto es, sin dispositivos de administración centralizada, tales como las estaciones base de las redes inalámbricas celulares o los puntos de acceso de las redes inalámbricas de área local. Los dispositivos móviles o nodos que forman la red además deben realizar funciones de encaminamiento debido al limitado rango de cobertura de la transmisión inalámbrica, es decir, todo nodo de la red deberá ser capaz, en principio, de encaminar ciertos paquetes antes de que lleguen a su destino final. Este tipo de redes pueden ser desplegadas de forma muy rápida en cualquier sitio debido a que no precisan el empleo de ninguna infraestructura y, por tanto, presentan un tremendo potencial de uso en situaciones tales como las comunicaciones militares (se puede establecer un sistema de comunicaciones entre un grupo de soldados en operaciones tácticas en zonas donde la utilización de una infraestructura de comunicaciones es imposible, como en territorio enemigo o terreno inhóspito) o los sistemas de emergencia (por ejemplo, para el establecimiento de comunicaciones entre el personal de rescate en caso de catástrofes). También presentan un enorme potencial en computación distribuida, redes inalámbricas de sensores y redes híbridas inalámbricas (redes que integran sistemas celulares y ad hoc).

A lo largo de este trabajo, se comenta el funcionamiento de las redes ad hoc inalámbricas, con especial interés en el problema que presenta la resolución del encaminamiento en estas redes. Tras ello se opta por uno de los protocolos propuestos por la comunidad científica, el protocolo de encaminamiento AODV (*Ad Hoc Distance Vector*, o protocolo de encaminamiento ad hoc por vector distancia), definido por el IETF (*Internet Engineering Task Force*) en la recomendación RFC 3561 [1], para configurar una red de este tipo en el laboratorio. Se emplea para ello una implementación del protocolo realizada en la universidad de Uppsala (Suecia), AODV-UU [2]. Una vez conseguido esto, se desarrolla una herramienta didáctica para la comprensión del modo de operación del mencionado protocolo a través de la visualización de su funcionamiento. Esta herramienta se encarga de la presentación al usuario de la tabla de encaminamiento de cada nodo de la red, así como de información sobre los paquetes AODV que circulen por él y el estado de los nodos cercanos.

Este artículo se organiza del modo siguiente: la sección 2 describe sumariamente las particularidades el funcionamiento de las redes ad hoc y del protocolo AODV en particular. La sección 3 resume las tecnologías empleadas en el desarrollo del interfaz Web, cuyas funcionalidades básicas se exponen en la sección 4. La sección 5 retrata las pruebas software realizadas mientras que la 6 extracta algunas conclusiones y propone ciertas líneas de trabajo futuras.

2. Redes Ad Hoc inalámbricas con encaminamiento AODV

El principal concepto que subyace bajo las redes ad hoc es el multisalto, esto es, la posibilidad de que los nodos se retransmitan entre sí los datos buscando alcanzar su destinatario. Durante toda la década de 1980 fueron muy importantes las investigaciones militares realizadas para crear un sistema de comunicaciones multisalto inalámbrico que pudiera operar en una extensa área geográfica, como se menciona en [3]. Con el objetivo de establecer estándares abiertos en esta área emergente, el IETF creó el grupo de trabajo de redes ad hoc móviles (MANET, *Mobile Ad Hoc Networks* [4]), para estandarizar protocolos y las especificaciones funcionales de las redes ad hoc inalámbricas.

En estas redes, la topología de las conexiones puede variar en cualquier momento de forma aleatoria. Los protocolos de encaminamiento son aquellos que encuentran la ruta que deben seguir los paquetes de datos para llegar desde el nodo fuente de los mismos hasta el destino deseado. Los utilizados en las redes cableadas tradicionales no pueden ser directamente aplicados aquí, debido a la topología altamente dinámica, la ausencia de elementos centralizados de administración como los Puntos de Acceso de IEEE 802.11 así como por las restricciones en el ancho de banda de los enlaces inalámbricos y en las baterías de los nodos. Por los motivos expuestos, en los últimos años han aparecido varias propuestas de protocolos de encaminamiento para redes ad hoc, que pueden clasificarse siguiendo diferentes criterios. Según el mecanismo de actualización de la información de encaminamiento, podemos clasificar estos protocolos en tres categorías principales:

Protocolos Proactivos. En los protocolos de este tipo, cada nodo mantiene la información sobre la topología parcial o completa de la red en unas tablas de encaminamiento que se intercambian periódicamente entre ellos. La información sobre el encaminamiento se suele difundir por toda la red. Cuando un nodo necesita un camino hacia un destino en concreto, ejecuta un determinado algoritmo de búsqueda de caminos utilizando la información que tiene guardada sobre la topología, y generalmente, la ruta estará disponible inmediatamente. Como ejemplos de protocolos de encaminamiento proactivos se pueden citar el protocolo de encaminamiento DSDV (*Destination Sequence Distance Vector*), el protocolo OLSR (*Optimized Link State Routing*) y el protocolo WRP (*Wireless Routing Protocol*).

Protocolos Reactivos o bajo demanda. Bajo estos protocolos los nodos no intercambian información topológica periódicamente entre sí. En lugar de ello, buscan el camino al destino deseado sólo cuando lo necesitan y, por ello, sufrirán cierto retardo en el establecimiento de la conexión con respecto a los proactivos. La búsqueda de rutas implica alguna clase de inundación de la red con la petición de la ruta. Algunos ejemplos son TORA (*Temporary Ordered Routing Algorithm*), DSR (*Dynamic Source Routing*), AODV (*Ad Hoc on Demand Distance Vector*) o DYMO (*Dynamic MANET On Demand*). Los protocolos DSR y AODV usan el envío *unicast* para hacer llegar la respuesta a la petición de ruta a quién la originó, a través del camino inverso al que siguió la petición para llegar al destino.

Protocolos de encaminamiento Híbridos. Combinan las mejores características de los dos tipos anteriores. Los nodos que estén a cierta distancia del nodo en cuestión o dentro de una zona geográfica definida en particular se dice que están dentro de la zona de encaminamiento del nodo dado. Para encaminar a un nodo que esté dentro de esta zona, se utilizará un algoritmo proactivo, mientras que para nodos fuera de dicha zona, se utilizarán mecanismos reactivos. El protocolo de encaminamiento de zona ZRP (*Zone Routing Protocol*) es un ejemplo de esta solución híbrida.

El protocolo de encaminamiento AODV es un protocolo especialmente diseñado para redes ad hoc inalámbricas que utiliza una estrategia "bajo demanda" para establecer las rutas, es decir, sólo se establece una ruta cuando es requerida por una fuente para alcanzar el destino de los paquetes que desea transmitir. Por ello, como en los demás protocolos de encaminamiento ad hoc reactivos, no se mantiene información relativa a aquellas rutas que no se utilizan ni se intercambia periódicamente información relativa al encaminamiento con los demás nodos de la red. AODV utiliza sólo enlaces simétricos entre nodos vecinos, pero no depende de ningún otro aspecto particular del medio físico a través del cual se envían los paquetes, por lo que es capaz de operar en medios cableados también.

AODV incorpora la técnica de los números de secuencia de destino del protocolo DSDV. Así, cada nodo mantiene un contador propio de número de secuencia, el cual se incrementa monótonamente para identificar las rutas obsoletas que conducen hacia él. De este modo, para cada destino del cual se tiene ruta en un nodo, este número se almacena en una tabla de encaminamiento junto con la dirección IP del siguiente salto. Una ruta expira si no es usada o reactivada dentro de un umbral de tiempo determinado.

Si la fuente no posee ruta hacia un destino, difunde a la red un mensaje *multicast* de petición de ruta (RREQ o *Route Request*). El paquete RREQ contiene el último número de secuencia conocido del destino, además del número de secuencia actual del nodo fuente. Cualquier nodo que recibe el RREQ actualiza su tabla del siguiente salto con respecto al nodo fuente. Un nodo que mantiene una ruta al destino con un número de secuencia mayor (y más actual, por tanto) que el que se especifica en el RREQ, envía de forma *unicast* un paquete de respuesta de ruta o RREP (*Route Reply*) de vuelta a la fuente, mediante el envío del paquete al siguiente salto hacia el nodo fuente. Conforme el paquete de respuesta RREP se propaga hacia atrás (hacia el origen), cada nodo intermedio a lo largo de la ruta de dicho RREP actualiza su tabla de encaminamiento con respecto al nodo destino, descartando los paquetes RREP redundantes y aquellos con menor número de secuencia de destino que los previamente recibidos. El nodo, independientemente de si es capaz de generar el mensaje de RREP o no, actualiza el número de secuencia de destino en el RREQ eligiendo el valor máximo entre el número de secuencia que transporta el RREQ y el número de secuencia de destino en la tabla de encaminamiento (si existe). Esto asegura que el paquete RREQ siempre lleve el valor más alto conocido del número de secuencia del destino.

Una vez que el nodo fuente recibe el RREP, ya puede utilizar la ruta para enviar paquetes de datos hacia el destino. Si ocurriera que, posteriormente, la fuente recibiera un RREP con un número de secuencia de destino mayor (ruta más actual) o igual que el número de secuencia guardado en la tabla de encaminamiento pero con menor número de saltos, el nodo fuente actualizaría la información de su tabla de encaminamiento y usaría la nueva ruta. En cambio, cuando un nodo intermedio descubre un enlace roto en una ruta activa, difunde por la red un mensaje de error de ruta o RERR (*Route Error*) a sus vecinos, que propagarán a su vez dicho mensaje de error en la dirección de la fuente a todos los nodos que tengan una ruta activa en la que participe el mencionado enlace roto. De ese modo, la fuente afectada podrá comenzar de nuevo un proceso de descubrimiento de ruta si la sigue necesitando.

Para mantener la conectividad local con otros nodos cercanos, cada nodo puede avisar de su existencia a los demás mediante la difusión local (sólo a los nodos situados a un salto) de una baliza denominada mensaje *Hello*, que se transmitirá periódicamente.

3. Tecnologías aplicadas en el desarrollo del Interfaz Web

Se propone la implantación en el laboratorio de una red ad hoc AODV monitorizable a través de una herramienta con interfaz Web. La idea básica era que esta herramienta didáctica presentara al alumno en todo momento toda la información posible sobre el estado del funcionamiento y la actividad del protocolo de encaminamiento AODV. Las especificaciones con las que se construyó la interfaz eran:

-La herramienta debía presentar al usuario la información concerniente a la tabla de encaminamiento AODV conforme esté disponible en la implementación software usada, así como una representación gráfica del estado del vecindario del nodo en el que se ejecute.
-La herramienta presentaría información con diverso grado de detalle sobre todos los paquetes AODV que circulasen por el nodo, ya sean generados por él, destinados a él o retransmitidos por él como nodo intermedio de una comunicación entre otros dos nodos. Dicha información debía ser accesible durante todo el tiempo en que se ejecutara la herramienta.
-Desde la herramienta se podría activar y desactivar el encaminamiento AODV en el nodo donde se estuviera ejecutando, con todas las opciones permitidas por la implementación usada del protocolo de encaminamiento ad hoc.

-La información generada en un nodo de la red ad hoc debía ser accesible desde cualquier otro nodo de su vecindario inmediato (a un solo salto de distancia).
-Los nodos de la red ad hoc serían ordenadores personales, por lo que las tecnologías a utilizar debía adaptarse a este entorno.
-La información se había de presentar de forma compacta, a ser posible, en una única pantalla, a través de un interfaz intuitivo y de fácil utilización, acompañado de un manual *on line* y de un tutorial sobre AODV.

Hoy en día, cuando se habla de redes ad-hoc, casi todos los profesionales implicados en ellas asumen implícitamente que estas redes se deben basar en una de las tecnologías de redes de área local inalámbrica (WLAN) ya existente. La mayoría de los documentos científicos publicados sobre evaluaciones de prestaciones en entornos simulados de protocolos de encaminamiento ad hoc propuestos asumen que debajo del nivel de red IP hay un control de acceso al medio compartido (MAC) y una capa física (PHY) de una WLAN. Recientemente, han aparecido trabajos sobre la posibilidad de sustituir la WLAN por una WPAN, como son los recientes esfuerzos de establecer redes ad hoc malladas que empleen la tecnología Bluetooth [11]. Las redes 802.11 son muy populares entre los investigadores de redes ad hoc debido a que proporcionan un soporte inmediato para sus simulaciones y sus esfuerzos de crear bancos de pruebas en el mundo real. La mayor parte de las herramientas de simulación de redes tienen, ya sea de forma integrada o en módulos realizados por contribuciones externas, librerías que emulan el comportamiento del interfaz IEEE 802.11. Los tres simuladores más usados en el mundo para redes ad hoc, NS2, OPNET y GloMoSim tienen cada uno su propia implementación de los niveles MAC y PHY de IEEE 802.11. Aunque 802.11 fue diseñado teniendo en mente el funcionamiento ad hoc, éste modo de trabajo se limita únicamente a conexiones punto a punto, esto es, podemos interconectar de esta manera un par de ordenadores y configurarlos rápidamente para intercambiar archivos sin tener que contar con un punto de acceso para ello. El trabajo en [5] nos indica, sien embargo, las carencias de las que adolece la capa MAC definida por el IEEE 802.11 para implementar redes ad hoc. Los autores señalan que debido al diseño MAC de las redes 802.11, las redes ad hoc basadas en dicha tecnología no funcionarán adecuadamente, y se reducirán las prestaciones de los protocolos de encaminamiento probados debido a problemas como la inestabilidad de los enlaces entre nodos. Aun así, como nuestra red ad hoc estará formada por ordenadores personales (PC) que harán de nodos, nos basaremos en esta tecnología, ya que se disponen de adaptadores inalámbricos compatibles con la norma IEEE 802.11 sobre la que estableceremos la comunicación ad hoc entre los nodos.

De entre todas las implementaciones propuestas de AODV existentes [6], se eligió la implementación de Uppsala, AODV-UU, por considerar que se trata de la más madura, y la más recomendada por los propios implementadores de AODV en su lista de distribución de correo (AODV Implementors List [7]). Se trata de una implementación muy estable y fácil de instalar que, como se ha mencionado, funciona con IPv4 en un sistema operativo GNU/Linux. Este software necesita un *kernel* 2.4.x o superior, ya que hace uso de *Netfilter* [8] para el encaminamiento de los paquetes. Esta implementación cumple las especificaciones del RFC 3561 y el mismo código funciona tanto para entornos de prueba reales como para el simulador NS-2. AODV-UU ha sido implementado como "demonio" en el espacio del usuario, basándose en la utilidad *Netfilter* para enviar paquetes desde el espacio del *kernel* al espacio del usuario. Aunque las implementaciones en el espacio del *kernel* son más rápidas, los autores decidieron que la estabilidad, que es más fácil de conseguir en un programa en el espacio del usuario, se primaría frente a la rapidez. AODV-UU consiste en un módulo del *kernel* llamado *kaodv* que envía datos al espacio del usuario a través de *Netfilter* siguiendo el esquema de la figura 1, donde se ilustra cómo el paquete es transferido a una aplicación, denominada en la figura "Decisión de Encaminamiento" usando la librería *libipq*. Esto se aplica a los paquetes de datos, mientras que para los mensajes de control AODV, se usa el puerto UDP 654, asignado por IANA [9] a AODV, donde es recibido por un módulo (llamado aodv_socket) para su ulterior procesado.

Netfilter es una arquitectura de manejo de paquetes, no incluida en el interfaz estándar de Berkeley *socket*, que se incluye en los *kernels* de Linux a partir de la versión 2.4. *Netfilter* proporciona un sistema muy flexible para la construcción de protocolos de encaminamiento ad hoc.

Gracias a *Netfilter* los paquetes de salida pueden ser examinados por AODV antes de que se tomen las decisiones de encaminamiento en la capa IP. Por tanto, el protocolo de encaminamiento puede observar los paquetes para cuyos destinos no exista ruta e iniciar su mecanismo de descubrimiento de caminos enviando un RREQ. De la misma forma, examinando todos los paquetes salientes se puede determinar si una ruta en particular está siendo usada y así actualizar su temporizador asociado en la tabla de encaminamiento AODV. Al permitir también analizar los paquetes entrantes antes de ser reencaminados, el protocolo de encaminamiento ad hoc puede saber si está recibiendo un paquete para retransmitirlo a otro nodo para el que no existe el siguiente salto, con lo que se podrá enviar un RRER a la fuente de dicho paquete. Para hacer uso de todas estas funcionalidades, la implementación de AODV debe definir un módulo del *kernel* donde estarán las funciones que requieren de los ganchos de *Netfilter*.

Para la creación de esta herramienta, se parte de nodos en los que se instalará AODV-UU. A tal efecto se emplearán equipos con sistema operativo GNU/Linux con *kernel* con soporte a *Netfilter* (2.4 o superior). Para la captura de los paquetes AODV se utilizará una herramienta denominada *ULOG* [10] (*User Logging target*), que añade un nuevo "target" al subsistema *iptables* de *Netfilter*. *Iptables* son un sistema de reglas que definen el comportamiento de *Netfilter*. Los denominados "targets" de *iptables* determinan la acción a tomar sobre cierto paquete (por ejemplo, si el paquete bajo ciertas condiciones se descarta, se acepta o se encola). *ULOG* es un "target" añadido a *iptables* que copia los paquetes que se le envían al espacio del usuario. Así, los paquetes cuyo destino sea *ULOG* se pasan a un servicio denominado *ulogd*, que incluye parches para diversos intérpretes de paquetes. De esta manera *ulogd* puede registrar en un archivo los paquetes recibidos por ULOG en el formato de los mensajes del *kernel* (*syslog*), en bases de datos SQL o en el formato de la librería *libpq* de captura de paquetes, que es el formato empleado por el analizador *Ethereal* [11].

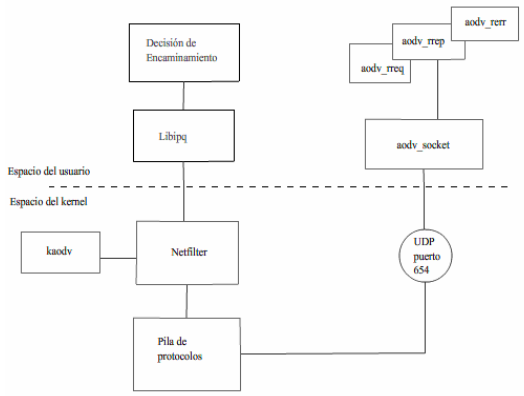

Figura 1. Módulos de AODV-UU.

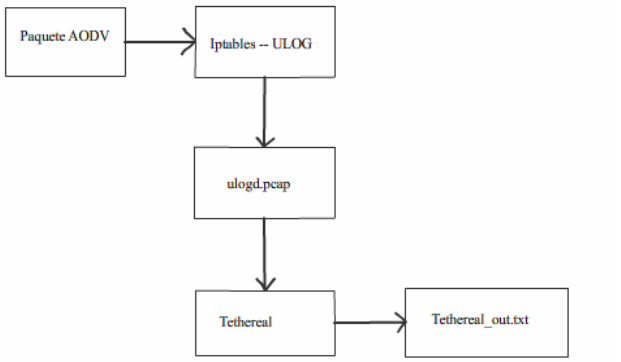

Figura 2. Esquema de la solución propuesta.

El esquema básico de la captura de paquetes que se realizó es el descrito en la figura 2. Se ve en ella que cuando llega un paquete AODV al sistema, pasa por las reglas *iptables* que lo destinan al *target ULOG*, que, a su vez, lo reenvía a *ulog*d para que éste haga una copia en formato de la librería de captura de paquetes *libpq* en un fichero denominado *ulogd.pcap*. Este fichero será posteriormente traducido por *Ethereal* a un formato amigable para el usuario mediante la herramienta *tethereal* (*Ethereal* en modo texto), que nos devolverá un fichero de texto con información sobre los paquetes capturados. Toda vez que se tienen los paquetes capturados en un fichero de texto, y ya que la red ad hoc con encaminamiento AODV está formada por ordenadores personales, se decidió que la aplicación a realizar sería un interfaz web, esto es, cada nodo de la red ad hoc ejecutaría un servidor HTTP (*HiperText Transfer Protocol*) donde presentaría la información requerida mediante una serie de páginas HTML programadas en el lenguaje PHP (*Hypertext Preprocessor*), las cuales interpretarían y procesarían los ficheros de texto generados por *tethereal*, volcando en pantalla cada cierto tiempo el contenido de los mismos. La información de cada nodo es accesible desde los demás a través de un cliente HTML (un navegador web cualquiera) que accede al nodo a través de su URL. La información concerniente a la topología del vecindario ad hoc y a la tabla de encaminamiento se

construye de la misma forma a través del proceso que ejecutan las páginas PHP a partir de los ficheros de texto que genera como ficheros de trazas (*logs*) el propio programa AODV-UU. Así, este programa devuelve cada cierto tiempo (que será programable) dos ficheros denominados *aodvd*.log, con los mensajes generados por la ejecución del protocolo de encaminamiento, y *aodvd.rtlog*, donde se guarda la tabla de encaminamiento. PHP es un lenguaje de programación que se ejecuta en el servidor, al contrario que *javascript*, que se ejecuta en el navegador del cliente. Así, *aodvWeb* (llamaremos así al interfaz web AODV desarrollado) se ejecuta simultáneamente en cada nodo de manera que cuando desde un nodo se quiera acceder a la información de otro, el código PHP se ejecuta en el servidor HTTP del que se requiere información, el cual enviará al navegador cliente exclusivamente la información relativa a cómo presentar la página HTML ya procesada.

Ya que tanto *ULOG* como *Ethereal* y el sistema operativo Linux son libres y se distribuyen bajo licencia GNU (*General public license*), se utilizaron herramientas libres con licencia GNU: Apache como servidor HTTP, el cual lleva integrado un intérprete de PHP, Mozilla Firefox como cliente HTTP y el editor HTML Bluefish para diseñar las páginas.

4. Estructura y funcionalidades del Interfaz Web

Aparte de una botonadura en la página Web principal que permite arrancar y detener la aplicación así como revisar el historial de ejecuciones anteriores u ofrecer un tutorial sobre AODV, la aplicación desarrollada incluye un menú de acciones donde aparecen cuatro cuadros (o *frames*) de información:

-*Cuadro de equipos próximos:* Este cuadro, representado en la figura 3, presenta un hiperenlace que abre una nueva página en una nueva ventana a pantalla completa, de modo que bajo ésta aparece la misma página mencionada mediante un IFRAME, que es un método que permite a los desarrolladores de páginas web insertar un marco en cualquier punto de la página cuyo contenido es independiente del resto del documento. Con ello se consigue insertar la representación gráfica del vecindario ad hoc en la página principal. Se ofrece un icono de un ordenador representando el nodo donde se ejecuta el interfaz con su dirección IP debajo, y bajo él, aparece en forma de árbol un nuevo icono por cada vecino que se detecte, también con su dirección IP debajo. La información sobre la topología se recoge de los mensajes de información recopilados en el archivo *aodvd.log* generado por AODV-UU. En la representación gráfica cada icono que representa a un nodo es también un hipervínculo, que lleva a una página idéntica a la actual pero correspondiente al nodo al cual representa. Cuando se accede a estos hipervínculos, se accede a un fichero que informa sobre los vecinos del nodo en cuestión, y se compara con el que a tal fin tiene nuestro nodo. Esta operación permite buscar vecinos del nodo investigado que no estén en el área de transmisión radio del nodo original. Si se encuentra alguno, se dibuja junto al nodo vecino un icono representativo de un nodo no alcanzable con su dirección IP debajo, que será un hipervínculo a una página (*ping.php*), encargada de enviar un mensaje *ping* controlado a un nodo no alcanzable directamente, con el objeto de establecer una ruta hacia él para que el alumno pueda visualizar cómo se comunican los nodos mediante multisalto, estableciendo una ruta y la consiguiente entrada en la tabla de encaminamiento.

-*Cuadro de detalle de los paquetes:* Este cuadro tiene como objetivo fundamental la presentación mediante un IFRAME de una página, que presenta información reducida sobre los paquetes AODV que se capturan. También aparece en este cuadro un hipervínculo que nos muestra en una ventana nueva a pantalla completa la salida íntegra de la lectura de la captura de paquetes que hace *ethereal*. Bajo este hiperenlace, se obtiene un formulario en el que es posible escoger el tiempo de refresco de la representación de los paquetes e indicar si se desea filtrar los paquetes *Hello* procedentes de los demás nodos o los nuestros propios, para que el alumno pueda distinguir mejor entre aquellos paquetes que participen en el establecimiento de una ruta multisalto y aquellos que no lo hacen. En esta página, se ejecuta la traducción mediante *tethereal* de los ficheros de captura de paquetes creando dos ficheros de texto, uno denominado *tethereal.out* con la información más relevante de los paquetes, y otro llamado *tethereal.out_2*, con la información más detallada que será utilizada para presentar información sobre los paquetes con varios niveles de detalle. La información que se presenta sobre los paquetes es un hipervínculo para cada uno de ellos a una página, donde se presentará información personalizada para

cada paquete, dividiendo la pantalla verticalmente en dos partes. A la izquierda, se presenta un IFRAME con una página que representa una animación del tránsito del paquete en el vecindario ad hoc. A la derecha, se presenta la información sobre el paquete relativa únicamente a AODV. La figura 4 ver aporta una vista de esta página.

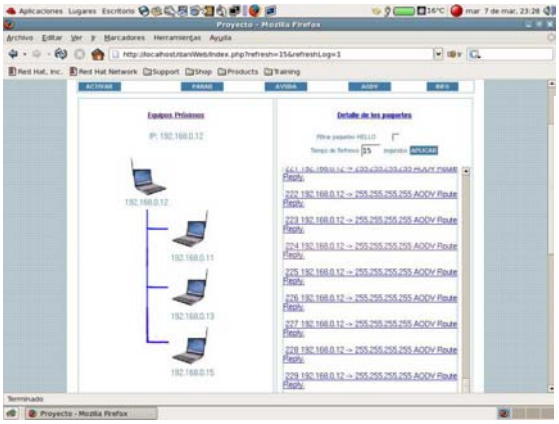

Figura 3. Cuadro de equipos próximos

Figura 4. Información del paquete AODV.

-*Cuadro de tabla de encaminamiento:* En este cuadro se presenta una página, mediante un IFRAME, que lee la información contenida en el fichero *aodvd.rtlog*, la procesa y la presenta al alumno.

-*Cuadro de fichero de 'trazas' (logs) del programa*: Esta página se encarga de presentar la salida de *aodvd* registrada en el fichero *aodvd.log*. Para ello se lee el fichero línea a línea y se le presenta al usuario.

5. Pruebas realizadas

Para comprobar el funcionamiento de la aplicación se configuró una red ad hoc (véase la Figura 5) con encaminamiento AODV formada por tres nodos (PC1, PC2 y PC3), cuyas configuraciones se detallan a continuación: Los nodos PC1 (dirección IP 192.168.0.10) y PC2 (IP 192.168.0.13) eran equipos PC con microprocesadores AMD Athlon +1500, con 256 Mb de memoria RAM e Intel Pentium III 350MHz con 128 Mb de memoria RAM, respectivamente. Ambos nodos se equiparon con adaptadores PCI/PCMCIA para la inserción de una tarjeta inalámbrica Cardbus Proxim ORINOCO 802.11 b/g silver. El nodo PC3 (IP 192.168.0.11) consistía en un ordenador portátil con procesador Intel Pentium Mobile M740 (1.743 GHz) con 1 Gb de memoria RAM y un adaptador inalámbrico integrado, Intel ProWireless 802.11 b/g Wireless LAN IPW2200. En todos los nodos se instaló la distribución de GNU/Linux Fedora Core 4, con *kernel* 2.6.11-1.1369_FC4, compilado con *Netfilter*. Esta distribución incluye por defecto el analizador de paquetes *Ethereal* 0.10.11, compilado con la librería lib*pcap* 0.8.3, con soporte para paquetes AODV. También incluía el servidor HTTP Apache 2.0.54 y el intérprete de PHP 5.0.4. Se instaló además *Ulogd* 1.23 y AODV-UU 0.9.1, por ser ambas las versiones más recientes de las herramientas en el momento de la realización de este trabajo. Tanto PC1 como PC2 son equipos voluminosos y sin batería, por lo que se mantuvieron estacionarios dentro de la misma sala. Para poder emular la movilidad de los nodos (y la posible ruptura de enlaces), en ambos nodos se introdujo, en su caso, una regla de *iptables* según la cual se rechazarían los paquetes de entrada pertenecientes a un nodo en concreto, ya que, de otro modo, siempre estarían dentro del área de cobertura del otro.

Para simular esta falta de conectividad y evitar que los nodos PC2 y PC1 pudieran comunicarse directamente, se inserta en cada uno de los dos nodo la regla de *iptables* pertinente para descartar los paquetes provenientes de la dirección MAC correspondiente.

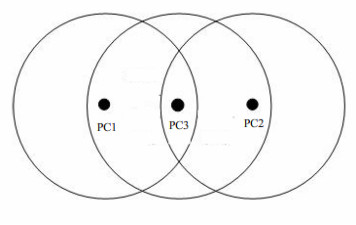

Figura 5. Topología de las pruebas (los círculos indican las zonas efectivas de coberturas de cada nodo)

Tras el montaje de la red de prueba, se realizaron pruebas de funcionalidad básica consistentes en comprobar botón a botón y enlace a enlace si las páginas realizadas responden a los eventos tal y como se esperaba. Estas pruebas se realizaron página a página conforme estas eran programadas durante el proceso de depuración de las mismas. Posteriormente se realizaron pruebas de ciertos aspectos funcionales del código realizado. Así, se comprobó el comportamiento del interfaz en condiciones de movilidad simulada de los nodos, comprobando también cómo se establece una ruta multisalto mediante el intercambio de los ficheros de vecinos y la ejecución de la instrucción *ping*. La primera de todas las pruebas que tuvo lugar para comprobar el funcionamiento de la utilidad gráfica fue conectar los tres nodos en el laboratorio, de forma que estuvieran los tres en el mismo vecindario y activar *aodvd* en los tres nodos. Se comprobó cómo el interfaz reflejaba esta topología de conectividad total de modo que los nodos aparecían uno debajo de otro en la representación gráfica, tal y como se aprecia en la figura 6.

Se procedió entonces a realizar sucesivas desconexiones y reconexiones de uno y otro vecino del nodo para comprobar que la página no sufría de ningún problema a la hora de reconocer nodos que salían o entraban en el vecindario. El resultado, tras las pruebas, fue el deseado.

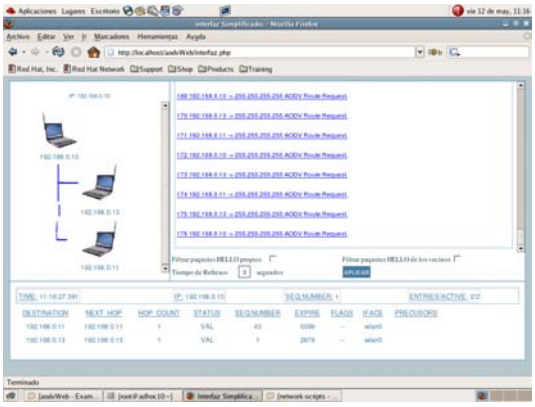

Figura 6. Interfaz en un nodo con dos vecinos.

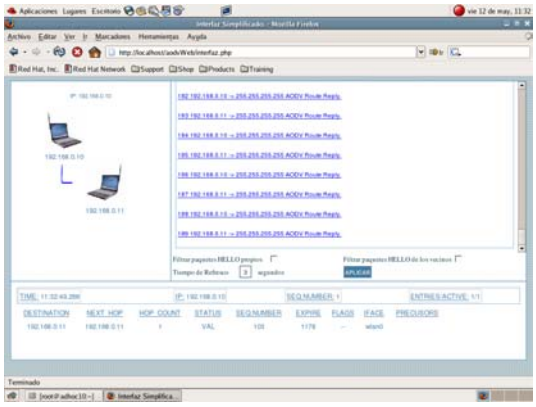

Figura 7. Interfaz en PC1 con PC3 de vecino único

La Figura 7, en cambio, nos muestra el interfaz del nodo PC1 cuando se monta la topología de la figura 5 (en la que PC1 y PC2 no pueden conectarse directamente). La figura indica cómo PC1 sólo tiene de vecino a PC3 tiene. Si se pulsa en el icono representativo de PC3, se abre una ventana con su interfaz simplificado, tal y como se muestra en la figura 8. En ella se aprecia cómo el nodo PC3 de dirección IP 192.168.0.11 tiene dos vecinos, el propio PC1, y un nuevo nodo, de dirección IP 192.168.0.13, que corresponde a PC2. Se comprueba así el funcionamiento de los hipervínculos en la representación de nodos y la accesibilidad de la información de un nodo desde un vecino en la red ad hoc. En dicha figura, se ilustra también cómo el equipo PC2 tiene dos rutas activas a sus dos vecinos en la representación de su tabla de encaminamiento.

Si se cierra esta ventana, en el interfaz de PC1 (que será consciente de la posición de PC2) aparecerá ahora el nodo PC2 como un nodo no perteneciente al vecindario, pero que sí está al alcance de PC3. El nodo no alcanzable aparece con un icono “desenfocado”, para indicar el estado que no se encuentra a un solo salto. Si hubiera más nodos no alcanzables directamente, además de PC2, aparecerían en la misma línea del grafo junto al que aparece. Si se pulsa en el icono correspondiente

sobre dicho nodo no alcanzable, se abrirá una nueva ventana con la página *ping.php*, donde se observa cómo aparece un mensaje que indica "El nodo 192.168.0.13 es accesible desde 192.168.0.11 pero no tenemos una ruta hacia él", ya que ambos nodos (PC2 y PC3) son vecinos. Debajo de este mensaje hay un botón que indica "*PING* 192.168.0.13", junto con la leyenda, "Pulse el botón para buscar una ruta". Al pusarlo se modifica esta ventana para ejecutar el *ping* tal y como se muestra en la figura 9. En ella se ve cómo se ha enviado un *ping* al nodo no alcanzable, registrando la ruta que ha seguido dicho mensaje. Podemos ver cómo el *ping* ha ido de 192.168.0.10 a 192.168.0.11 y de ahí a 192.168.0.13, y ha seguido el camino inverso a la vuelta. Se puede observar también cómo en la tabla de encaminamiento del nodo con dirección IP 192.168.0.10 aparece una nueva ruta a 192.168.0.13, pero en lugar de tener esa misma dirección en el campo "NEXT_HOP" como ocurre con su vecino 192.168.0.11, aparece como siguiente salto de la ruta la dirección 191.168.0.11, que es el siguiente salto al que se le deben entregar los paquetes para alcanzar el destino deseado.

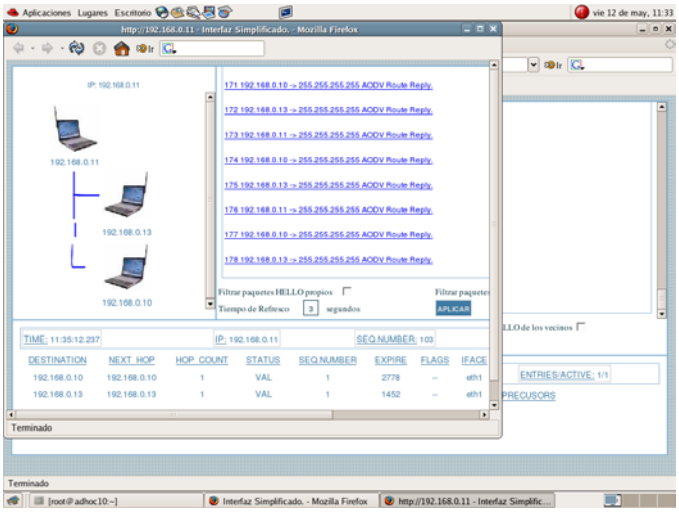

Figura 8. Vecinos de PC2 vista desde PC1

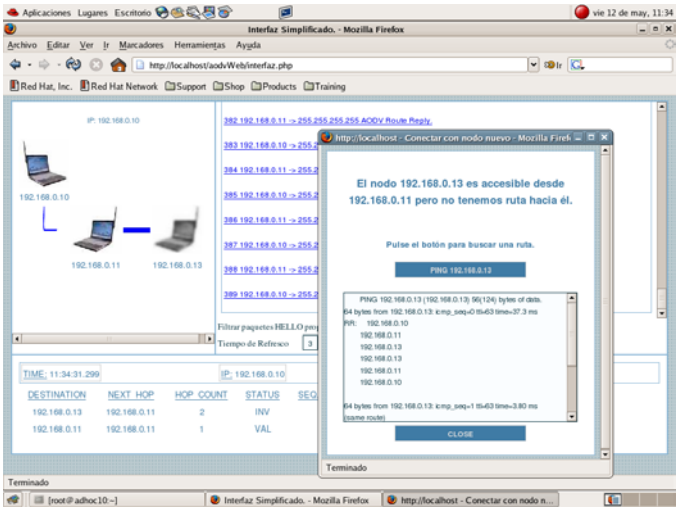

Figura 9. *Ping* a nodo no alcanzable.

6. Conclusiones

El interfaz web que se ha propuesto en este trabajo se ha diseñado como un interfaz didáctico para la comprensión del funcionamiento *on line* del protocolo de encaminamiento ad hoc AODV, y no como analizador de paquetes de alta capacidad. Su funcionamiento básico supone que el alumno va a activar *aodvd* desde el interfaz web, y va a aprender su funcionamiento mediante la observación de su modo

de operación y sus tablas de encaminamiento principalmente. Las pruebas al sistema han sido principalmente dirigidas a comprobar la funcionalidad de las páginas que lo componen y a un número reducido de casos concretos. Esta herramienta ha sido diseñada para la monitorización didáctica en entornos académicos. Por ello, en cuanto a las posibles limitaciones de escalabilidad, no se había pensado en esta herramienta para la monitorización de redes altamente densas. Su ajuste en este sentido es posiblemente una de las líneas futuras en la que continuar este trabajo, ya que podría realizarse una aplicación que, empleando la librería *pcap*, tradujera los paquetes capturados uno a uno según se pida información de alguno en concreto, con lo que ya no tendríamos las limitaciones debidas al sistema de traducción usado. De la misma manera, la captura de paquetes se podría realizar directamente en una base de datos, ya que lo permite la herramienta *ulog* utilizada. Dicha base de datos es muy fácilmente accesible desde una web programada en PHP, con lo que ganaríamos en velocidad de acceso a la información, y por tanto en escalabilidad.

Como futuras mejoras del interfaz web AODV, se puede pensar en un sistema de descubrimiento de *gateways*, en el que el nodo configurado como tal avise a sus vecinos, o un sistema que dibuje un gráfico con la topología de la red en un número de saltos definido por el usuario mediante el intercambio de los ficheros o, por último, la ampliación del filtrado en la presentación de los paquetes.

El interfaz web desarrollado, básicamente, se limita a interpretar los archivos de texto generados por la ejecución del protocolo de encaminamiento y la captura de paquetes que circulan por el sistema, por lo que es fácilmente ampliable a otros protocolos de encaminamiento. Se podría por tanto, usar una implementación diferente de AODV o incluso de otros protocolos de encaminamiento y adaptar la herramienta a sus particularidades. Incluso sería deseable la coexistencia de varias implementaciones elegibles a través del interfaz, con lo que tendríamos una valiosa herramienta multiprotocolo para el aprendizaje de los diferentes modos de operación del encaminamiento en redes ad hoc inalámbricas que permitiría establecer comparaciones. Así, por ejemplo, sería muy fácil en un futuro adaptar la herramienta para la reciente implementación del protocolo de encaminamiento DSR realizada por el mismo equipo de la universidad de Uppsala, ya que sigue el mismo esquema básico de funcionamiento, generando el mismo tipo de ficheros de traza (*logs*) que la herramienta interpreta. De la misma forma, al estar programada como interfaz web en PHP, se podría ampliarla a entornos Windows si se obtuviese alguna implementación para dicho sistema de algún protocolo de encaminamiento ad hoc.

Referencias

[1] C. E. Perkins, E. M. Royer.. "Ad Hoc On-Demand Distance Vector Routing Protocol", IETF RFC 3561, Octubre 2003. Disponible en línea: http://www.rfc-archive.org/getrfc.php?rfc=3561.

[2] Portal de implementación de protocolos ad hoc de la universidad de Uppsala (Suecia). http://core.it.uu.se/AdHoc/AodvUUImpl.

[3] J. A. Freebersyser, B. Leiner, "A Department of Defense Perspective on Mobile Ad Hoc Networks". Publicado en *"Ad Hoc Networking"*, Editor Charles E. Perkins, pp. 29-51. Addison Wesley ISBN 0-201-30976-9. 2ª Ed. Marzo 2004.

[4] "IETF MANET Working Group Information", http://www.ietf.org/html.charters/manet-charter.html

[5] S. Xu y T. Saadawi, "Does the IEEE802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?", *IEEE Communications Magazine*, vol. 39, no. 6, pp. 130-137, Junio 2001.

[6] Wikipedia, the free encyclopedia. "Ad Hoc Routing Protocol List". Disponible en línea en : http://en.wikipedia.org/wiki/Ad_hoc_protocols_implementations

[7] Lista de correo pública de implementadores de AODV. http://sourceforge.net/mailarchive/forum.php?forum=aodvimpl-public.

[8] Proyecto *Netfilter*. http://www.*Netfilter*.org.

[9] IANA, Internet Assigned Numbers Authority http://www.iana.org/assignments/port-numbers

[10] *Netfilter-Ulog*. http://www.sunbeam.franken.de/projects/*ulog*d/

[11] Analizador de paquetes Ethereal. http://www.ethereal.com