Estudio de viabilidad de la utilización de redes inalámbricas Ad-Hoc en edificios departamentales

Autor
Francisco Javier Hidalgo Pastor

Directores
Juan Carlos Cano Escribá
Carlos T. Calafate

Máster de Ingeniería de Computadores - Orientación Profesional
Universidad Politécnica de Valencia

Valencia, Diciembre de 2008

INDICE

AGRADECIMIENTOS

Dedicado a mis padres y a mis hermanas por todo el interés y apoyo demostrado durante la realización del Máster.

También quiero dar las gracias a Jorge Hortelano, por las dudas que me ha ido aclarando a medida que se desarrollaba el trabajo.

Y evidentemente a los profesores y directores del proyecto: Juan Carlos Cano Escribá y Carlos T. Calafate. Ellos me dieron la oportunidad de dirigirme la tesis del Máster de Ingeniería de Computadores y como profesores han sabido indicarme correctamente las pautas para realización de este proyecto, además de prestarme todo su ayuda y apoyo para que este trabajo se haya hecho de la mejor manera posible.

A todos ellos, muchas gracias.

MOTIVACIÓN Y OBJETIVOS

Cuando se precisa movilidad en las comunicaciones, depender de cables supone una restricción para conseguir plena libertad de movimientos. Para salvar las restricciones impuestas por el cable, las comunicaciones inalámbricas se convierten en una alternativa a los sistemas de comunicación tradicionales.

No cabe duda de que las comunicaciones inalámbricas están en auge y han alcanzado en los últimos años la robustez, madurez y estandarización necesarias para convertirse en una verdadera alternativa a las redes cableadas. También podríamos destacar en los últimos años un acusado descenso del coste económico del hardware necesario para las comunicaciones inalámbricas. Es por esto por lo que usuarios o futuros usuarios de esta tecnología están interesados en evaluar cuales son realmente las prestaciones de estos dispositivos, para así poder optar o no por su utilización.

Existen dos tipos de redes inalámbricas: Aquellas que están constituidas, además de dispositivos inalámbricos, por una infraestructura formando una parte más o extensión de la misma (Redes con infraestructura), y las que carecen de esta parte y están constituidas por un conjunto de dispositivos móviles inalámbricos, los cuales pueden conectarse dinámica y arbitrariamente entre ellos, encargándose además del encaminamiento de todos los mensajes de control e información (Redes Ad-Hoc).

Las redes inalámbricas tienen muchos usos, como la oficina portátil: profesionales que se desplazan continuamente en su trabajo y necesitan usar sus dispositivos electrónicos para enviar y recibir llamadas de teléfono, faxes, correo electrónico, acceder a computadores remotos, leer y modificar ficheros en estos computadores. Todo esto en tierra, mar o en un avión. Igualmente se aplican en flotas de camiones, autobuses, taxis y otros vehiculos. También son muy valiosas en lugares en los que las redes con infraestructura se han destruido por alguna catástrofe o por su ausencia debido al alto coste de instalarlas en sitios de difícil acceso o por la orografía del terreno.

El objetivo de este estudio es comprobar la viabilidad del uso de redes inalámbricas Ad-Hoc en un edificio departamental típico de la Universidad Politécnica de Valencia (aunque es extrapolable a otros edificios de características físicas o estructurales de la misma universidad), y compararlas con las redes inalámbricas propias de la UPV. Evaluaremos las prestaciones de estas redes Ad-Hoc usando dos protocolos de encaminamiento: AODV (Ad-Hoc On-Demand Distance Vector) como representante de los protocolos reactivos, y OLSR (Optimized Link State Routing) como representante de los proactivos.

El trabajo realizado se ha organizado en 4 capítulos. El Capítulo 1 presenta una introducción a las redes inalámbricas, sus configuraciones y problemas. En el Capítulo 2 se introducen los protocolos de encaminamiento, haciendo un estudio de OLSR y AODV. El Capítulo 3 explica los detalles relativos a la instalación y configuración de la red Ad-Hoc utilizada para las pruebas. En el Capítulo 4 se presentan los detalles del estudio de prestaciones realizado. En el Capítulo 5 se muestran las conclusiones del trabajo y para finalizar, se presenta la Bibliografía consultada.

1. INTRODUCCIÓN A LAS REDES INALÁMBRICAS

Dentro del horizonte de las comunicaciones sin cables y la informática móvil, las redes inalámbricas van ganando rápidamente adeptos al ser una tecnología madura y fiable, que permite resolver los inconvenientes derivados de la propia naturaleza del cable como medio físico de transmisión de datos. Es difícil renunciar a un tipo de comunicación que libera del pesado lastre que supone acarrear cables de un lado para otro y, sobre todo, estar siempre pendiente de la existencia de un punto de conexión. En la Tabla 1 se muestra la comparación de estas redes con las tradicionales.

Tabla 1. Comparación entre tecnologías.

	Redes con cable	Redes inalámbricas
Ventajas	Tecnología Madura Altas velocidades de transmisión Confiabilidad Cumple con varios estándares de industria Resistencia a las interferencias externas	Buenas características de desempeño Bajo coste de operación Facilidad de instalación Facilidad en el mantenimiento y detección de fallos Imprescindibles en ciertas circunstancias geográficas Menor tiempo instalación Buen nivel de integración en redes tradicionales existentes
Limitaciones	El tiempo de reparación es mayor Dificultad para el tendido del cableado o reutilización de éste. Mayor tiempo de instalación	Potencia y distancias limitadas Velocidad de transmisión limitada Tecnología relativamente nueva.

Las redes de área local sin cables, más conocidas por el nombre de Wireless Local Area Networks (WLANs), surgieron una vez visto el potencial que esta clase de redes podía llegar a alcanzar.

Actualmente, existen varias soluciones de redes inalámbricas, con distintos niveles de estandarización e interoperabilidad. Dos soluciones que hoy por hoy lideran el sector son HomeRF y Wi-Fi™ (IEEE 802.11b/g). De estas dos, la tecnología 802.11 [1] dispone de una mayor aceptación en el mercado y está destinada a solucionar las necesidades de las redes locales inalámbricas para zonas empresariales, domésticas y públicas.

1.1 Comunicación inalámbrica

Cuando nos referimos a una red de estaciones móviles entendemos como tal a cualquier tipo de red de comunicación donde al menos uno de sus componentes cambia su ubicación relativa en el tiempo. A medida que las estaciones se desplazan por la red, la comunicación puede continuar o puede ser suspendida, dependiendo de las características de la red y la naturaleza de la comunicación.

Las ventajas de utilizar redes inalámbricas pueden verse en los siguientes casos:

- Imposibilidad de instalar cables: por ejemplo en zonas geográficas de difícil acceso o en zonas en las que su normativa municipal lo dificulten o tenga un gran coste.
- Redes temporales o de rápida implantación: por ejemplo en empresas con gran movilidad de sus trabajadores. Otro ejemplo puede ser dar soporte a convenciones, estar ocupando sedes provisionales o sufrir con relativa frecuencia cambios en la organización de la red. El coste es menor y las posibilidades de ampliación son mayores, además de que se instalan con rapidez.
- Domótica: las redes domésticas inalámbricas son un campo en auge. Pueden ser capaces de automatizar una vivienda con aplicaciones como el control de la luz, riego, ahorro energético, etc

Los usuarios móviles, cuyo número crece día a día, acceden a las redes inalámbricas con equipos portátiles y tarjetas de red inalámbricas. Esto permite al usuario viajar a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) sin perder el acceso a la red. Fuera del ámbito empresarial, también hay redes inalámbricas públicas en aeropuertos, restaurantes, estaciones de tren, etc. Sin el acceso inalámbrico, el usuario tendría que llevar consigo cables y disponer de conexiones de red.

En todos estos escenarios, las redes locales inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años. El acceso del usuario normalmente supera los 11 Mbits/s, de 30 a 100 veces más rápido que las tecnologías de acceso telefónico o de las redes WAN inalámbricas estándar. Este ancho de banda es adecuado para que el usuario pueda trabajar sin problemas con varias aplicaciones o servicios a través del PC o dispositivos móviles. Además, los avances en curso de estos estándares inalámbricos continúan aumentando el ancho de banda.

1.2 Redes locales inalámbricas (WLAN)

El concepto de WLAN, acrónimo de Wireless Local Area Network, surge ante la idea de un sistema de comunicación de datos flexible, utilizado como alternativa a la red local cableada o como extensión de esta. Este tipo de redes se diferencia de las convencionales principalmente en la capa física y de enlace de datos según el modelo de referencia OSI. Muy superficialmente, la capa física indica cómo son enviados los bits de un nodo a otro, mientras que la capa de enlace, denominada MAC, se encarga de describir como se empaquetan nuevamente los datos y el modo de verificación de los

bits para que no contengan errores. Evidentemente, al cambiar el medio físico, la tecnología inalámbrica reemplaza el cable por otros métodos de naturaleza similar pero muy bien diferenciados en su comportamiento, como son la transmisión por radiofrecuencia o la luz infrarroja.

La mayoría de las estaciones móviles utilizan conexiones inalámbricas para comunicarse con el resto de la red.

1.3 Revisión del Standard 802.11

Dentro de las redes inalámbricas, hemos centrando este proyecto en el estándar IEEE 802.11, el que utilizan las WLAN. Fue un consorcio, el Wi*reless Ethernet Compatibility Alliance (WECA),* formado por un grupo de grandes empresas, el que creó una nueva línea de productos de mayores prestaciones y de plena compatibilidad que garantizan la interoperatividad entre distintos fabricantes.

En general los sistemas 802.11 usan la banda de frecuencias de 2,4 Ghz debido a que en esta zona del espectro magnético no se requiere el uso de licencias.

El Standard IEEE 802.11 es una tecnología cuyo propósito es proporcionar acceso inalámbrico a redes de área local (WLANs). Usando esta tecnología, las estaciones acceden al medio inalámbrico usando Point Coordination Function (PCF) o Distributed Coordination Function (DCF). Point Coordination Function es un modo de acceso centralizado opcionalmente usado cuando hay disponible un point coordinator (PC). La tecnología CSMA/CA reparte el acceso al medio entre todas las estaciones, haciendo a cada estación responsable de asegurar la entrega de unidades de datos en la capa MAC y reaccionar ante las colisiones. El esquema CA se usa para reducir la probabilidad de colisiones entre diferentes estaciones.

1.3.1 Arquitectura de red

Hay tres posibles configuraciones de red disponibles en el standard IEE 802.11: IBSS, BSS y ESS.

- IBSS (Independent Basic Server Set), también conocida como red Ad-Hoc, es una red establecida de un conjunto de estaciones sin ninguna clase de infraestructura.
- BSS (Basic Server Set), también conocida como red con infraestructura, se crea mediante un punto de acceso que normalmente tiene una conexión cableada. Cada nodo móvil se comunica directamente con el punto de acceso.
- ESS (Extended Service Set): permite formar redes más complejas que se caracterizan por la existencia de multiples puntos de acceso cuya cobertura se solapa parcialmente.

1.3.2 Nivel Físico

Los anchos de banda definidos por el standard operan hoy en día de 1 a 54 Mbps, pero se están desarrollando en la familia 802.11 otros standards que ofrecerán anchos de banda mayores. El Standard 802.11 define tres capas físicas. Dos de ellas fueron diseñadas para operar en la banda de frecuencias de la ISM (Industria, Científica y Médica) a 2.4 GHz; éstas son las técnicas Frequency-hopping (FH) y Direct-sequency (DS) spread-spectrum frequency. Se definió también una capa física que usa luz infrarroja (IR). La tecnología 802.11a es un anexo a la capa física de IEEE 802.11 que opera en la frecuencia de radio de 5GHz y soporta velocidades entre 6 y 54 Mbit/s.

- La tecnología IEEE 802.11a permite alcanzar buenos resultados soportando aplicaciones multimedia en entornos con varios usuarios. El único inconveniente es que se requieren más puntos de acceso para cubrir un área similar que con las tecnologías IEEE 802.11b o IEEE 802.11g.
- La especificación IEEE 802.11b mejora la capa física de IEEE 802.11 para alcanzar mayores ratios de datos en la banda de los 2.4 GHz, combinando la técnica DSSS (Direct Sequence Spread Spectrum) basada en Complementary Code Keying (CCK) con la modulación QPSK (Quadrature Phase Shift Keying), que es la clave para alcanzar ratios de datos de 5.5 y 11 Mbit/s.
- IEEE 802.11g es la especificación más reciente disponible para la capa física de IEEE 802.11. La principal ventaja de 802.11g es que mantiene la compatibilidad con más de 11 milllones de productos Wi-Fi vendidos con tecnología IEEE 802.11b.
- IEEE 802.11n es el standard 802.11 para redes de area local inalámbricas. El ratio de datos real se estima que alcanza teóricamente 600 Mbit/s. IEEE 802.11n se construye sobre el Standard 802.11 añadiéndole MIMO (multiple-input multiple-output) y orthogonal frequency-division multiplexing (OFDM).

1.4 Problemas en la comunicación Inalámbrica

Las comunicaciones inalámbricas presentan una menor calidad de comunicación debido a los siguientes factores: menor ancho de banda, mayor cantidad de errores en el intercambio de paquetes, y mayor número de fallos en la conexión que la cableada. Todo esto provoca una mayor latencia en la comunicación debido a la retransmisión de datos perdidos y a los protocolos de control de errores entre otros factores.

Los factores ambientales juegan un papel muy importante, no sólo limitando la distancia entre dos estaciones, sino añadiendo ruido, interferencias y variedad de escenarios que obstruyen la señal. Este tipo de comunicación también se puede ver degradada por la movilidad de sus estaciones. Es decir, los usuarios pueden entrar y salir de áreas de mayor interferencia, o alejarse repentinamente de una zona de cobertura de otra estación con la cual han establecido comunicación. Además, contrariamente a las redes cableadas, el número de integrantes en una determinada área puede variar dinámicamente, pudiendo llegar a saturar dicha red.

A continuación se muestran brevemente algunos de los problemas comunes de las redes inalámbricas:

Desconexiones Frecuentes. Los diseñadores de redes inalámbricas prestan mayor atención a los fallos de red que los diseñadores tradicionales ya que los fallos de red son muy comunes en comunicaciones inalámbricas, y no tanto en las realizadas utilizando fibra óptica, coaxial o UTP. Ante esta situación tienen que prevenir las desconexiones, o permitir que puedan recuperarse sin problemas.

Ancho de Banda Limitado. El ancho de banda que proporciona una conexión inalámbrica con respecto a una conexión cableada es mucho menor. Inicialmente los productos con interfaces inalámbricas que se podían encontrar en el mercado operaban a velocidades de hasta 11 Mbps. Paulatinamente la tecnología inalámbrica ha ido evolucionando y se ha pasado de tener en el mercado productos con tecnología 802.11g a 54 Mbps a los últimos con tecnología 802.11n que alcanzan los 300 Mbps (con un máximo teórico de hasta 600 Mbps).

Heterogeneidad de la Red inalámbrica. Los ordenadores de una red inalámbrica son susceptibles de encontrar múltiples tipos de conexiones. Cuando una estación móvil se aleja de su grupo, o punto de acceso, este se puede conectar con el contiguo, donde puede experimentar cambios en la calidad de la conexión o en los servicios prestados. O quizás pueda estar situado en un lugar donde se solapen varios con frecuencias diferentes. Esta heterogeneidad hace que el diseño de redes inalámbricas sea más complejo que el de las redes tradicionales cableadas.

Riesgos de Seguridad. La seguridad en redes inalámbricas está más comprometida que en las cableadas, especialmente si la comunicación cubre un área muy extensa.

Se puede garantizar comunicaciones seguras sobre canales inseguros mediante el uso de encriptación, la cual puede ser realizada por software, o más rápidamente mediante hardware especializado. La seguridad depende de las claves de encriptación, que solo pueden ser conocidas por las partes que la componen y, opcionalmente, por una autoridad que garantiza la autenticidad de la clave.

La especificación 802.11 proporciona algunos mecanismos de seguridad básicos. Por ejemplo, los puntos de acceso (o conjuntos de puntos de acceso) 802.11 se pueden configurar con un identificador del conjunto de servicios (SSID). La tarjeta también debe conocer este SSID para asociarlo al punto de acceso y así proceder a la transmisión y recepción de datos en la red. Esta seguridad es muy débil debido a las siguientes razones:

- Todas las tarjetas y todos los puntos de acceso conocen perfectamente el SSID.
- El SSID se transmite de manera transparente (incluso es señalizado por el punto de acceso).
- La tarjeta o el controlador pueden controlar localmente si se permite la asociación en caso de que el SSID no se conozca.
- No se proporciona ningún tipo de cifrado a través de este esquema.

La especificación 802.11 proporciona seguridad adicional mediante el algoritmo WEP (Wired Equivalent Privacy) dotándole de servicios de autenticación y cifrado. El

algoritmo WEP define el uso de una clave secreta de 40 bits para la autenticación y el cifrado.

Movilidad. La posibilidad de las estaciones móviles de cambiar de lugar mientras continúan conectadas a la red disminuye el tiempo de vida útil de cierta información.

Cuando un usuario o una estación se desplaza de un punto de acceso a otro punto de acceso, se debe mantener una asociación entre la tarjeta y un punto de acceso para poder mantener la conectividad de la red. Esto puede plantear un problema especialmente complicado si la red es grande y el usuario debe cruzar límites de subredes (que pueden ocasionar problemas con el direccionamiento IP) o dominios de control administrativo (que pueden ocasionar además problemas de permisos de acceso).

La configuración puede ser un problema para el usuario móvil, por lo que la estación inalámbrica del usuario debe tener capacidad para configurarse automáticamente.

1.5 Configuraciones de las redes inalámbricas 802.11

Las redes locales inalámbricas se despliegan utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, con infraestructura y Ad-Hoc. Durante la tesina se utilizan los términos “con infraestructura” y “Ad-Hoc”. Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

1.5.1 Redes con infraestructura

Una topología de red inalámbrica con infraestructura es aquella que extiende una red local con cable existente para incorporar dispositivos inalámbricos mediante estaciones base, denominadas puntos de acceso. En este tipo de redes existen dos clases de estaciones o dispositivos: fijos y móviles El punto de acceso une la red local inalámbrica y la red local con cable y sirve de controlador central de la red local inalámbrica; su comportamiento es fijo, es decir, que no presenta cambios en su ubicación relativa.

El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

Cuando una estación móvil se encuentra dentro del área de influencia de un punto de acceso, ésta se comunica normalmente, como si se tratara de una estación fija. Pero cuando se sale del radio de acción de su estación base, tendrá la necesidad de comunicarse con una estación foránea (un nodo de otra red que cumple esta función).

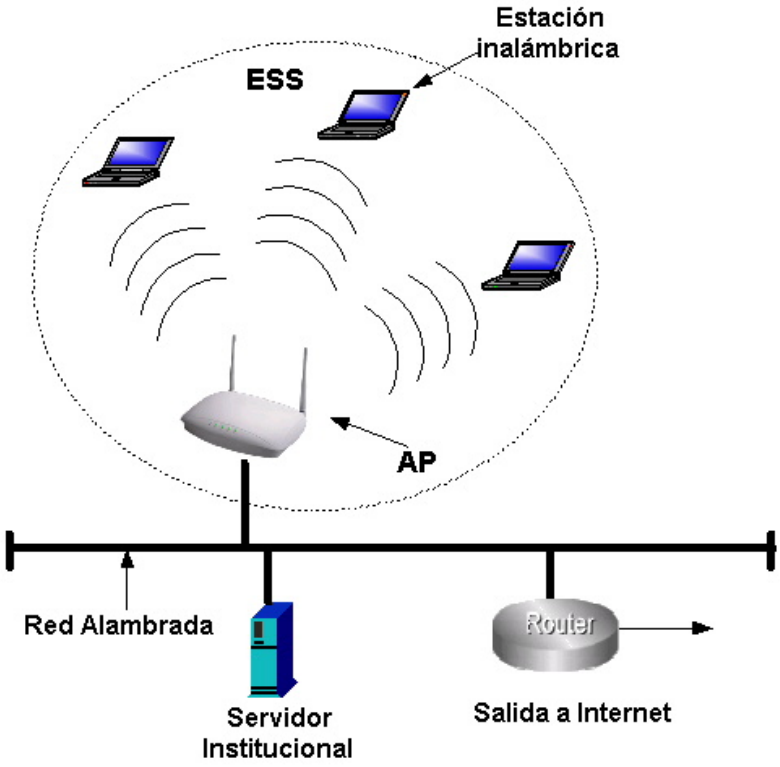

Figura 1. Ejemplo de red con infraestructura.

1.5.2 Redes Ad-Hoc

Las redes sin infraestructura, comúnmente conocidas como redes Ad-Hoc (Mobile Ad-Hoc Network o MANET [2]), no poseen elementos fijos o administración centralizada de ningún tipo. Todas las estaciones son capaces de moverse y conectarse dinámicamente de una manera arbitraria con otras estaciones de la red, definiendo diferentes topologías que cambian con frecuencia. Cada estación es autónoma y puede actuar como router encaminando los distintos paquetes entre los diferentes terminales, sin la necesidad de que exista un alcance directo entre la fuente y el destino. Estas estaciones pueden estar ubicadas en aviones, barcos, camiones, autos o pueden ser transportadas por personas (pequeños dispositivos).

Figura 2. Red Ad-Hoc.

Las estaciones de una MANET utilizan tablas de encaminamiento para organizar las rutas y así poder enviar los paquetes. Estas tablas de encaminamiento se deben actualizar con mucha frecuencia ya que la red es móvil y las estaciones van cambiando de posición constantemente.

El objetivo de las redes Ad-Hoc es el de soportar comunicaciones robustas y eficientes en redes móviles inalámbricas mediante la incorporación de funciones de encaminamiento en las estaciones móviles. Tales redes deberán disponer de tecnologías multisalto, que se adapten rápida y dinámicamente a los cambios de topología que las estaciones describen, siempre teniendo en cuenta las limitaciones en los consumos de energía.

Las estaciones de las redes Ad-Hoc están equipadas con transmisores y receptores inalámbricos que típicamente utilizan antenas omnidireccionales (broadcast), aunque también pueden ser direccionales (punto-a-punto). Dependiendo de la posición de las estaciones, las potencias de recepción y transmisión, y las interferencias que puedan existir en un canal, se forma entre las estaciones una conectividad inalámbrica dinámica en forma de grafo y con características aleatorias. La topología de la red Ad-Hoc, debido a la movilidad, varía con el tiempo ya que las estaciones modifican su posición relativa, y por consiguiente sus parámetros de recepción y transmisión, dificultando así poder lograr buenas prestaciones.

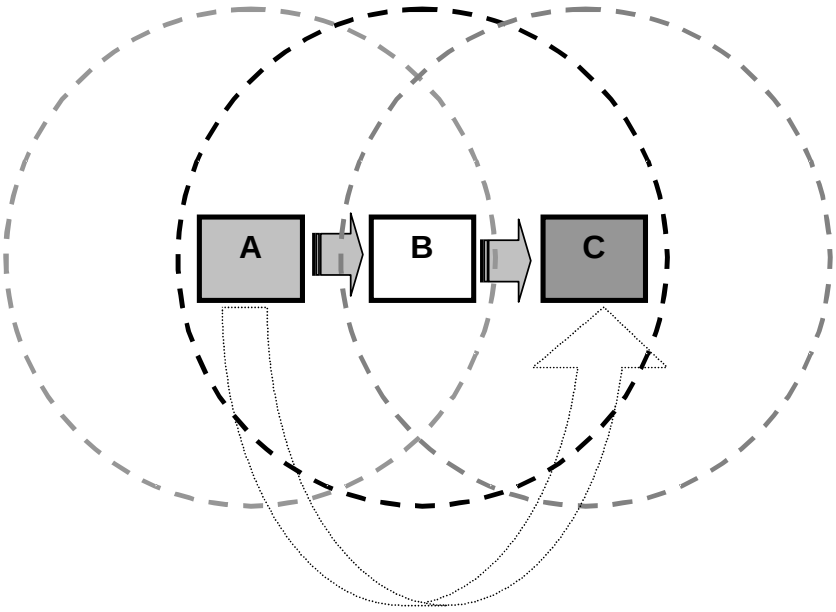

Figura 3. Modelo de red Ad hoc.

Dado que el radio de transmisión es limitado, no se permite a las estaciones establecer una comunicación punto-a-punto con el resto de estaciones de la red. Si dos estaciones se quieren comunicar y están fuera de su radio de alcance, deberá haber otras estaciones (pertenecientes a la red) que se comporten como routers, encaminado los paquetes hasta el nodo destino.

En la Figura 3 se muestra una red Ad-Hoc sencilla compuesta por tres estaciones. Las circunferencias representan los radios de transmisión ideales de cada una de ellas. En este ejemplo, la estación A desea enviarle una serie de paquetes a la C. Pero esto no es posible, ya que C se encuentra fuera del radio de A, por lo que la estación B, se convierte en un enrutador, recibiendo los paquetes de A y redirigiéndolos (enrutándolos) a C.

Gracias a que este tipo de redes no necesita infraestructura, se han visto muchas aplicaciones del uso de las mismas en lugares en los que la infraestructura de red es insuficiente o inexistente. Estas redes se forman temporalmente y en lugares donde no sería posible imaginar un despliegue de cables ni elementos fijos que gestionen la comunicación.

Los inicios de estas redes fueron puramente militares, pero ya se le ha visto la gran utilidad en lugares donde la concentración de gente es elevada (hotspots) como aeropuertos, cafeterías, bibliotecas, universidades o en lugares que han sufrido una catástrofe natural (terremotos, incendios, inundaciones, huracanes, etc.) y la infraestructura existente se haya visto gravemente dañada.

Actualmente se están realizando investigaciones paralelas para solventar toda la problemática que supone el uso de este tipo de redes. Veamos algunos de los desafíos existentes en el diseño e implementación de redes Ad-Hoc.

- **Encaminamiento de paquetes.** La constante movilidad de los terminales supone un continuo cambio de la topología de la red e implica una nueva configuración de las tablas de encaminamiento de los nodos a la hora de encaminar los paquetes de información. En este estudio se abordará con detalle el encaminamiento de los paquetes y se explicarán y utilizarán los algoritmos AODV y OLSR.
- **Calidad de Servicio.** Se ha de tener en cuenta que hay aplicaciones (como las de tiempo real) a las que se les debe garantizar un cierto nivel de QoS (Quality of Service, calidad de servicio). La topología dinámica hace variar constantemente las tablas de encaminamiento y hace que la provisión de QoS resulte compleja y se deban fijar unos parámetros (niveles de ruido, niveles de potencia,…) para las diferentes líneas de estudio.
- **Seguridad.** Una red con cable está dotada de una seguridad inherente ya que un posible hacker necesita un acceso físico al cable. Sobre este acceso físico se pueden superponer otros mecanismos de seguridad. En una red inalámbrica la transmisión de los datos se hace por el aire y está expuesta a diferentes ataques de hackers. Es posible que entidades no autorizadas se conecten a redes privadas si no se utilizan mecanismos de seguridad adecuados. Los tres aspectos claves de seguridad que deberían cubrirse en las redes Ad-Hoc son los Sistemas de detección de intrusos (SDI), la Seguridad de los protocolos de encaminamiento y los Servicios de gestión de claves y autentificación de claves
- **Consumo de potencia.** Es un asunto importante debido a que los terminales de las redes Ad-Hoc son ligeros y de poca capacidad. Se debe buscar una optimización en los diseños para reducir al máximo el consumo de potencia y así alargar la duración de las baterías.

2. PROTOCOLOS DE ENCAMINAMIENTO

La búsqueda de un protocolo de encaminamiento en redes Ad-Hoc se ha convertido en un importante desafío debido a la complejidad de este tipo de redes. A diferencia de las redes clásicas cableadas, que presuponen que la topología de la red es poco cambiante, en una MANET se utiliza como medio de transmisión el aire y está en constante cambio por la movilidad de sus estaciones. Por ello no se pueden utilizar los algoritmos ya existentes y se deben buscar otros nuevos que soporten estas condiciones, teniendo en cuenta las limitaciones del ancho de banda, la memoria reducida y la saturación por el denso tráfico que han de soportar. Actualmente hay disponibles soluciones, como los protocolos AODV y OLSR, que estudiaremos más adelante y que se han utilizado en esta tesina.

Para que un protocolo ofrezca un encaminamiento eficiente el algoritmo debería de tener las siguientes características: señalización mínima, mínimo tiempo de procesado, que no se produzcan bucles, que sea distribuido, que soporte una topología dinámica, que soporte enlaces unidireccionales y el modo sleep cuando una estación esté inactiva.

Se requiere un protocolo de encaminamiento cuando un paquete debe dar varios saltos para alcanzar una estación destino. Este protocolo es el responsable de encontrar una ruta para el paquete y asegurarse de que va por el camino adecuado.

2.1 Técnicas de Encaminamiento

Independientemente de cómo se clasifique el protocolo de acuerdo con estos criterios, las técnicas de encaminamiento se pueden dividir en tres familias: vector distancia, estado del enlace y encaminamiento fuente. Vamos a ver los principios básicos de estas técnicas.

Vector Distancia. Esta técnica mantiene una tabla para que tenga lugar la comunicación y emplea difusión (no flooding) para el intercambio de información entre vecinos. Todas las estaciones deben calcular el camino más corto hacia el destino utilizando la información de encaminamiento de sus vecinos.

Estado del Enlace. Los protocolos basados en esta técnica mantienen una tabla de encaminamiento con toda la topología de red. La topología se construye encontrando el camino más corto en términos de coste del enlace, coste que es periódicamente intercambiado entre todas las estaciones por medio de flooding. Cada estación actualiza su tabla de encaminamiento usando información recogida sobre su coste del enlace. Esta técnica tiende a originar bucles en redes que cambian rápidamente su topología.

Encaminamiento Fuente. Es una técnica en la que todos los paquetes de datos tienen la información de encaminamiento en sus cabeceras. La decisión de encaminamiento se hace en la estación fuente. Esta técnica evita los bucles, aunque la sobrecarga del protocolo es elevada. Esta técnica puede ser ineficiente en topologías que tienen

movimientos rápidos debido a la invalidez de rutas de un paquete a lo largo de un camino.

2.2 Clasificación de los Protocolos de Encaminamiento

Los protocolos de encaminamiento basados en algoritmos como los de Vector Distancia (por ej. RIP [5]) o Estado del Enlace (por ej. OSPF [6]) han sido diseñados con anterioridad a las redes inalámbricas Ad-Hoc. Estos protocolos de encaminamiento generan periódicamente mensajes de control, procedimiento que no es adecuado para redes de gran tamaño con rutas largas ya que se generaría mucho tráfico de encaminamiento. Todos los protocolos de encaminamiento convencionales asumen rutas bidireccionales con una calidad similar, algo que no es siempre cierto en algunas clases de redes (por ej. redes inalámbricas Ad-Hoc). Los protocolos de encaminamiento pueden clasificarse de acuerdo a tres criterios diferentes:

- **Centralizados o distribuidos:** en los centralizados todas las decisiones se toman en una estación central. Sin embargo, con un protocolo de encaminamiento distribuido, todas las estaciones comparten las decisiones de encaminamiento.
- **Adaptativos o estáticos:** un protocolo de encaminamiento adaptativo puede cambiar su comportamiento de acuerdo al estado de la red, como por ej. congestión en algunas conexiones u otros posibles factores, al contrario que un estático.
- **Reactivos, proactivos o hibridos:** un protocolo de encaminamiento reactivo debe actuar encontrando rutas cuando sea necesario, mientras que un protocolo de encaminamiento proactivo encuentra las rutas antes de que se necesiten. Los protocolos reactivos también se conocen como protocolos de routing *on-demand*. Ya que se ejecutan por petición, la sobrecarga por mensajes de control se reduce considerablemente. Los proactivos mantienen tablas de encaminamiento que se actualizan periodicamente. Los hibridos usan una combinación de los proactivos y los reactivos para alcanzar una solución equilibrada.

2.3 Encaminamiento en Redes Ad-Hoc

Un protocolo de encaminamiento ideal para redes Ad-Hoc debe tener algunas propiedades que lo hagan diferente del resto. Debe ser distribuido para aumentar la fiabilidad: cuando todas las estaciones son móviles, no tiene sentido tener un protocolo de encaminamiento centralizado. Cada estación debe tener la capacidad de tomar decisiones de encaminamiento con la ayuda del resto de estaciones.

Un protocolo de encaminamiento también debe asumir que los enlaces detectados son conexiones unidireccionales. En un canal inalámbrico, una conexión unidireccional puede formarse por factores físicos, por lo que una conexión bidireccional puede resultar imposible. También hay que tener en cuenta características como el consumo de potencia y la seguridad. Las estaciones móviles dependen de

baterías. Un protocolo que minimice el consumo de la red de estaciones sería ideal. Sobre la seguridad, hay que tener en cuenta que el medio inalámbrico es muy vulnerable. En el nivel físico, los ataques de Denegación de Servicio (DoS) pueden evitarse usando saltos de frecuencia o técnicas de code-based Spread Spectrum. En el nivel de routing se requiere la autenticación de vecinos y la encriptación.

Los protocolos de encaminamiento usados en estas redes deben ser, de acuerdo con la clasificación de la sección 2.2, distribuidos y adaptativos.

En cuanto a la tercera categoría (reactivos/proactivos/hibridos), no hay consenso en cual es la estrategia más adecuada.

2.3.1 Protocolos de encaminamiento Proactivos

El concepto de encaminamiento proactivo quiere decir que todas las estaciones intercambian periodicamente información de encaminamiento (o cuando detectan cambios en la topología) para mantener una vista de la red consistente, actualizada y completa. Esto evita retrasos asociados con encontrar rutas on-demand. Las técnicas proactivas usan normalmente algoritmos como el vector distancia o el estado del enlace. Ambas técnicas requieren que las estaciones envien periodicamente información (guardada en tablas) por broadcast y, basándose en esta información, calcular el camino más corto hacia el resto de estaciones. La principal ventaja del encaminamiento proactivo es que no hay un retardo cuando se requiere una ruta. Por otra parte hay mayor sobrecarga y una convergencia de tiempo mayor que en los reactivos, especialmente cuando la movilidad es alta.

Ejemplos de protocolos de encaminamiento que usan técnicas de vector distancia son el Destination-Sequenced Distance Vector (DSDV) [7] y el Wireless Routing Protocol (WRP) [8]. Ejemplos de protocolos basados en el Estado del Enlace son Open Shortest Path First (OSPF) [6], Optimized Link State Routing (OLSR) [4], Topology Broadcast Reverse Path Forwarding (TBRPF) [9], Source Tree Adaptive Routing (STAR) [10], Global State Routing (GSR) [11], Fisheye State Routing (FSR) [12] y Landmark Routing Protocol (LANMAR) [13].

2.3.2 Protocolos de encaminamiento Reactivos

El encaminamiento Reactivo no depende en general del intercambio periódico de información de encaminamiento o de un cálculo de rutas. Cuando se necesita una ruta, la estación debe iniciar un proceso de descubrimiento de ruta. Esto es lo que les ha llevado a conocerse como protocolos bajo demanda. Se optimizan los recursos evitando el envío de paquetes de forma innecesaria. Debe difundir la petición de ruta por la red y esperar una respuesta antes de que envíe paquetes al destino. La ruta se mantiene hasta que el destino es inalcanzable o hasta que la ruta ya no es necesaria. El proceso de descubrimiento de rutas origina un retardo significante en el inicio y da lugar a un considerable desperdicio de recursos. Si la red es lo suficientemente grande, la sobrecarga será similar o superior a la alcanzada con los protocolos de encaminamiento proactivos.

Los algoritmos de encaminamiento más comunes entre los protocolos reactivos son el Vector Distancia y el Encaminamiento Fuente. Ejemplos de protocolos de encaminamiento reactivos son Ad-hoc On-demand Distance Vector (AODV) [14], Dynamic Source Routing (DSR) [15], Associativity Based Routing (ABR) [16], Signal Stability based Adaptive routing (SSA) [17], Temporally Ordered Routing Algorithm (TORA) [18], Relative Distance Micro-discovery Ad-hoc Routing (RDMAR) [19] y Dynamic On-demand MANET routing protocol (DYMO) [20].

Procederemos ahora a describir un protocolo de cada uno de estos grupos ya que los hemos utilizado en el desarrollo de la tesina (el OLSR y el AODV).

2.4 El protocolo OLSR (Optimized Link-State Routing Protocol)

El protocolo Optimized Link State Routing [4] es un protocolo de encaminamiento proactivo especificamente diseñado para redes Ad-Hoc móviles (MANETs). Se basa en la definición y uso de estaciones dedicadas, llamadas multipoint relays (MPRs). Los MPRs son los responsables de reenviar los paquetes de broadcast durante el proceso de flooding. Esta técnica permite reducir la sobrecarga de paquetes en comparación con un mecanismo puro de flooding en el que cada estación retransmite el paquete cuando recibe la primera copia suya. Al contrario que el algoritmo clásico del estado del enlace, apenas se distribuye información parcial del estado del enlace a la red.

2.4.1 Principios Básicos

El protocolo OLSR hereda su estabilidad de los algoritmos de estado del enlace. Debido a su naturaleza proactiva, ofrece la ventaja de que las rutas disponibles pueden usarse inmediatamente.

Los algoritmos de estado del enlace declaran y propagan la lista de vecinos de cada estación a la red. OLSR intenta mejorar esta solución usando diferentes técnicas. Reduce el tamaño de los paquetes de control ya que éstos no se declaran a los vecinos, sólo un subconjunto de ellos llamados Multipoint Relay Selectors. Una estación Multipoint Relay se encarga de retransmitir sus mensajes de broadcast. El uso de MPRs sirve para minimizar la cantidad de retransmisiones de un evento de broadcast o de flooding.

Además de los mensajes de control periódicos, el protocolo no genera tráfico de control adicional para responder a fallos o asociaciones con nuevas estaciones. El protocolo mantiene rutas hacia todos los destinos de la red, siendo útiles en situaciones en las que un gran número de estaciones de la MANET se están comunicando, especialmente cuando los pares fuente/destino cambian con frecuencia. Este protocolo es más adecuado para redes grandes y densas, en las que las optimizaciones alcanzadas introduciendo Multipoint Relays ofrecen importantes beneficios.

El protocolo está diseñado para operar en modo distribuido, por lo que no depende de una entidad central. No requiere una transmisión fiable de sus mensajes de control: cada estación envía periódicamente mensajes de control, siendo tolerante a

pérdidas esporádicas de paquetes de control. El reordenamiento de paquetes, cosa común en las redes Ad-Hoc, no lleva asociado un mal comportamiento de OLSR ya que cada mensaje lleva un número de secuencia diferente.

El protocolo OLSR usa reenvío de paquetes *per-node*, lo que significa que cada estación usa su información más reciente para encaminar un paquete. La capacidad para seguir a una estación puede ajustarse configurando el intervalo entre mensajes de control consecutivos.

2.4.2 Multipoint Relays

El concepto de Multipoint Relay consiste en intentar minimizar el flooding originado por tráfico de broadcast eliminando transmisiones duplicadas en una misma región. Cada estación de la red selecciona un subconjunto de estaciones de su vecindad para retransmitirles paquetes. Las estaciones que pertenecen a este subconjunto son los nodos Multipoint Relays (MPRs). Los vecinos que no forman parte del subconjunto de MPRs de un nodo N todavía recibirán paquetes de él, pero no los retransmitirán. De esta forma, cada estación mantiene una tabla con las estaciones que han sido seleccionadas como MPR.

Cada estación selecciona su propio conjunto de MPRs entre sus vecinos con un criterio que consiste en asegurarse que todas las estaciones que están a dos saltos de una estación dada pueden alcanzarse con un número mínimo de MPRs. La Figura 4 ilustra este concepto.

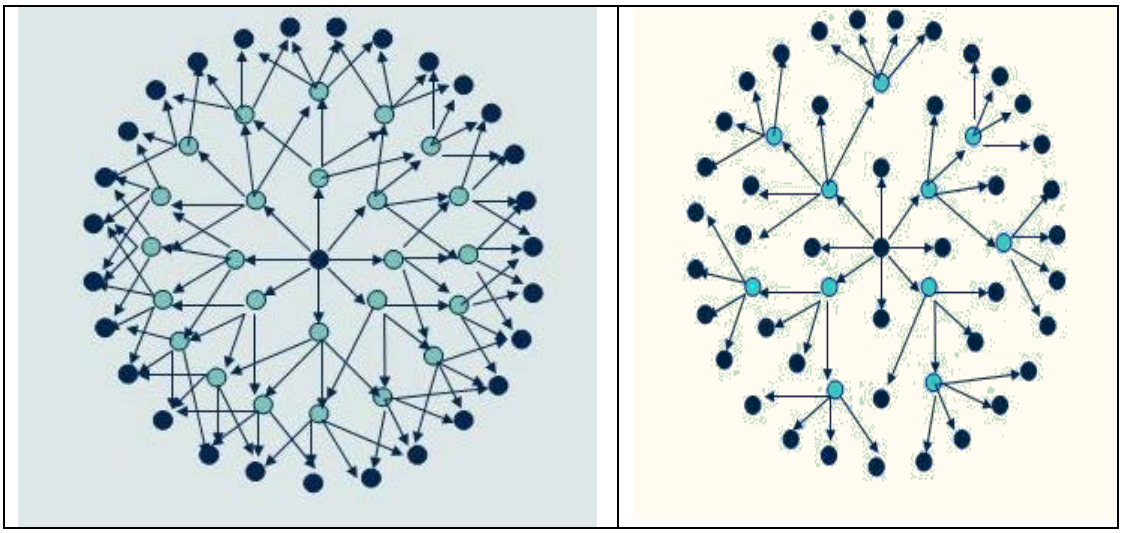

Figura 4. Ilustración del concepto de multipoint relay para N estaciones

OLSR confía en la selección de MPRs para calcular rutas a todos los destinos teniendo a éstas como estaciones intermedias. Esta solución requiere que cada estación envíe por broadcast periodicamente su lista de estaciones vecinas elegidas como sus MPRs. Cuando se recibe esta información, cada vecino actualiza las rutas hacia sus estaciones conocidas.

2.4.3 Detección de vecinos

Cada estación debe detectar las estaciones vecinas hacia las cuales existe una comunicación bidireccional. Para ello, una estación emite periodicamente por broadcast mensajes HELLO que contienen información sobre sus vecinos y el estado del canal hacia ellos. Estos mensajes los reciben todas las estaciones vecinas pero no se retransmiten.

Cada estación mantiene una tabla con una lista de todas las estaciones que puede ver directa o indirectamente. Los enlaces a vecinos que están a un salto se marcan como unidireccionales, bidireccionales o MPR. Cada entrada de la tabla tiene un número de secuencia y un valor de timeout asociados, por lo que las entradas obsoletas pueden eliminarse.

2.4.4 Selección Multipoint Relay

Cada estación de la red escoge su conjunto MPR. Para mantener una lista de vecinos que están a dos saltos tiene que analizar los mensajes HELLO y filtrar todos los enlaces unidireccionales. El conjunto MPR sólo se modifica cuando se detecta un cambio en términos de vecinos a un salto o a dos saltos (sólo conexiones bidireccionales).

2.4.5 Información de Broadcasting MPR

Cada estación debe enviar mensajes de control de topología (TC) para que todas las estaciones mantengan sus bases de datos actualizadas. Estos mensajes se envían por broadcast usando una técnica similar a una usada en los protocolos de encaminamiento de estado del enlace, con la única diferencia que emplea MPRs para mejorar la escalabilidad.

Un mensaje TC se envía periódicamente a cada estación de la red para que declare su conjunto de selectores MPR. Esto significa que el mensaje debe contener una lista con los vecinos directos que lo han seleccionado como su MPR. La lista siempre tiene un número de secuencia asociado.

La lista de direcciones en cada mensaje TC puede ser parcial, pero debe ser completa antes de que acabe el periodo de refresco. Estos mensajes permitirán a cada estación mantener su propia tabla con la topología de la red. Si una estación no ha sido seleccionada de la lista de estaciones MPR, no enviará mensajes TC, por lo que ahorrará consumo y ancho de banda.

El intervalo entre la transmisión de dos mensajes TC depende de si ha habido cambios en una estación del conjunto de selectores MPR. Si ha habido un cambio, el siguiente mensaje TC puede transmitirse antes del tiempo programado, pero respetando el tiempo mínimo entre mensajes.

2.4.6 Cálculo de la Tabla de Encaminamiento

Cada estación mantiene una tabla de encaminamiento con información de cómo acceder a otras estaciones de la red. Cuando las estaciones reciben un mensaje TC almacenan conjuntos de dos direcciones que indican el último salto antes de alcanzar una estación destino, así como la propia estación destino. Combinando la información de estos pares de direcciones la estación es capaz de encontrar cual es el siguiente salto a una estación destino. Debe tenerse en cuenta el criterio de distancia mínima para restringir las opciones de búsqueda.

Las entradas de la tabla de encaminamiento están compuestas de un destino, el siguiente salto y la distancia estimada a la estación destino. En esta tabla sólo se registran las entradas en las que se conoce una ruta hacia un destino. Esto significa que la tabla de encaminamiento debe ser constantemente actualizada de acuerdo con los cambios en la topología de red detectados.

2.5 El protocolo AODV (Ad-Hoc On Demand Distance Vector)

El protocolo Ad hoc On Demand Distance Vector (AODV) es un protocolo de encaminamiento IP que permite a unas estaciones encontrar y mantener rutas hacia otras estaciones de la red. AODV es on-demand, o reactivo, en el sentido de que las rutas se establecen sólo cuando se necesitan (cuando la estación origen quiere transmitir datos a un destino). Las decisiones de encaminamiento se hacen usando vectores distancia, por ej. distancias medidas en saltos a todos los routers disponibles. El protocolo soporta unicast y broadcast. La version que vamos a describer a continuación se basa en el RFC 3561 Internet draft standard [3].

Cada estación mantiene un número de secuencia que guarda un timestamp, y una tabla de encaminamiento que contiene rutas hacia los destinos. Los números de secuencia se usan para determinar si una ruta es actual (cuanto mayor sea el número, más acualizada está la ruta; el más antiguo puede descartarse) y con ellos el protocolo se asegura de que no hay bucles. Cada entrada de la tabla contiene la dirección del siguiente salto (siguiente estación hacia el destino), un contador de saltos (número de saltos hacia el destino) y un destination sequence number. Ya que es un esquema de vector-distancia on-demand, los routers mantienen las distancias de aquellos destinos con los que necesitan contactar o transmitir información. Cada ruta activa se asocia con un tiempo de vida almacenado en la tabla; cuando este tiempo finaliza, la ruta se marca como inválida y después se borra de la tabla para no sobrecargarla. AODV usa dos procedimientos principales, el descubrimiento de rutas y el mantenimiento de rutas, que se describen a continuación.

2.5.1 Descubrimiento de Rutas

Si la estación fuente (sender, que envía datos) necesita una ruta a un destino, envía por broadcast un mensaje ROUTE REQUEST (RREQ). Cada estación también guarda un identificador de broadcast que, junto con la direción IP del origen, identifica unívocamente a un RREQ. Cada vez que el emisor emite un RREQ, incrementa en uno su identificador de broadcast y el número de secuencia. Además, almacena este RREQ

durante un tiempo PATH DISCOVERY TIME (PDT), y así no lo vuelve a procesar si un vecino se lo envía de vuelta. El emisor espera durante un tiempo NET TRAVERSAL TIME (NETT) a que le llegue un mensaje ROUTE REPLY (RREP). Si no se recibe un RREP durante este tiempo, volverá a mandar por broadcast otro RREQ hasta un número de veces RREQ TRIES. Con cada intento adicional, el tiempo de espera (NETT) se duplica.

Cuando una estación recibe un mensaje RREQ que no ha visto con anterioridad, configura una ruta de vuelta a la estación de la que proviene el RREQ. Esta ruta de vuelta tiene un valor de tiempo de vida ACTIVE ROUTE TIMEOUT (ART). La entrada en la tabla correspondiente a la ruta de vuelta se almacena con la información de la dirección de destino requerida. Si la estación que recibe este mensaje no tiene una ruta al destino, reenvía por broadcast el RREQ. Cada estación guarda el número de saltos que ha hecho el mensaje y también qué estación ha reenviado el RREQ. Si una estación recibe un RREQ que ya ha procesado, lo descarta y no lo reenvía.

Si una estación tiene una ruta a un destino, contesta enviando por unicast un mensaje RREP a la estación de la que recibió el mensaje de petición. Como el RREP se propaga de vuelta a la estación fuente, las estaciones configuran punteros hacia el destino. Cuando la estación fuente recibe el RREP, la ruta se ha establecido y los paquetes de datos pueden enviarse al destino. Opcionalmente, la estación origen puede emitir un mensaje RREP-ACK al destino para asegurarse de la fiabilidad del camino bidireccional.

2.5.2 Mantenimiento de rutas

La función del mantenimiento de rutas es proporcionar un feedback al sender en caso de que un router o un enlace se rompa, y así la ruta puede modificarse o redescubrirse. Una ruta puede dejar de funcionar simplemente porque una de sus estaciones se mueva. Si se mueve una estación fuente, debe informar a todos los vecinos que necesiten este salto. Este mensaje se reenvía a todos los otros saltos y la ruta obsoleta se borra. La estación origen debe descubrir una nueva ruta.

Una forma para que una estación guarde información de sus vecinos es usando mensajes HELLO. Estos se envían periódicamente para detectar fallos en los enlaces. Cuando se recibe una notificación de enlace roto, la estación fuente puede reiniciar el proceso de descubrimiento de rutas. Si hay un enlace roto, puede enviarse por broadcast un mensaje ROUTE ERROR (RERR) a la red. Cualquier estación que recibe el RERR, invalida la ruta y reenvía por broadcast los mensajes de error con el destino inalcanzable a todas las estaciones de la red.

3. INSTALACIÓN Y CONFIGURACIÓN DE LA RED AD-HOC

Para la realización de esta tesina sobre la evaluación de redes inalámbricas Ad-Hoc basadas en IEE802.11, se necesita un escenario para tener una red inalámbrica sencilla compuesta por cuatro ordenadores portátiles en un edificio departamental de cinco alturas de la Universidad Politécnica de Valencia. Estos ordenadores se situarán en plantas diferentes del edificio de forma que la comunicación entre ellos se realizará a través de dos protocolos de encaminamiento (AODV y OLSR) y de las redes inalámbricas propias de la Universidad. El objetivo es ver si la red Ad-Hoc es adecuada en un edificio de estas características y se comparará con las redes inalámbricas existentes en la Universidad. Las pruebas realizadas y los resultados obtenidos se describirán con más detalle en el Capítulo 4.

La red es de tipo Ad-Hoc ya que no se dispone de ningún elemento de infraestructura en la red, es decir, se establece una red punto-a-punto entre los ordenadores.

3.1 Planificación de la red Ad-Hoc

La cobertura o el rendimiento que puede ofrecer una red inalámbrica dependen de la distancia que puedan alcanzar las ondas de radiofrecuencia (RF), y está en función de las características técnicas del hardware utilizado y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso personas, afectan a la propagación de la señal. El rango de cobertura de una WLAN oscila entre los 30 y 250 metros, aunque esa distancia puede ampliarse utilizando antenas direccionales.

A diferencia del cable, la conectividad inalámbrica no tiene el problema de que se pueda romper el medio por el que viajan los datos. Sin embargo, las redes inalámbricas suelen experimentar otro tipo de problemas que deterioran e incluso pueden llegar a interrumpir su normal funcionamiento. Fenómenos tales como el desvanecimiento debido a interferencias entre estaciones, la propagación por diferentes trayectorias motivadas por las ondas reflejadas y la atenuación debida a la distancia o a diferentes materiales, son problemas típicos.

Para configurar una red Ad-Hoc, los usuarios de esa red deberán conocer algunos parámetros de configuración. Independientemente de los imprescindibles controladores, a la hora de configurar cada una de las estaciones habrá que asignarle el nombre de cliente inalámbrico “Client Name”.

En segundo lugar habrá que asignar el SSID o Service Set Identification para controlar el acceso a una red Ad-Hoc. El SSID acepta hasta 32 caracteres que distinguen entre mayúsculas y minúsculas. En nuestro caso se definirá un nombre común en los ordenadores que deberá ser igual en el resto de ordenadores que se quieran añadir a la red.

También habrá que tener en cuenta el canal que utilizará la estación cuando esté configurado en una topología Ad-Hoc, como es nuestro caso, ya que todos los equipos

deberán utilizar el mismo canal para poder comunicarse entre si. Según [26] el Standard 802.11 divide la banda de 2.4 Ghz en 11 o en 13 canales (para América y Europa respectivamente). Estos canales tienen una separación de frecuencia de 5 Mhz y una frecuencia de ocupación (ancho de banda del canal) de 22 MHz. El nivel de energía de radiofrecuencia que atraviesa los canales determina las interferencias. Esta energía se expande más allá del límite de la frontera de un canal. El nivel de energía decrece a medida que la señal se expande del centro del canal. El objetivo es que haya la suficiente separación física entre celdas de forma que el nivel de energía en el límite de la celda sea lo suficientemente bajo para que no provoque interferencias. Puede ocurrir que la señal que cruce el canal sea muy baja y no pueda ser decodificada como una señal 802.11 válida, por lo que se consideraría como ruido. En la banda de 2.4Ghz se usan normalmente los canales 1, 6 y 11 sin que se solapen (es recomendable dejar 4 canales sin ocupar entre dos canales ocupados).

En configuraciones Ad-Hoc existen dos funciones que sólo afectan a esta topología. En primer lugar, el parámetro "Beacon Period" especifica la duración entre los paquetes de aviso que utilizan los sistemas 802.11 para sincronizar los saltos o cambios de frecuencias. El paquete de aviso contiene información sobre los patrones de saltos que se emite a través de las ondas radiofónicas. Toda estación que reciba el paquete de aviso podrá sincronizar su temporizador interno para que se pueda efectuar los saltos de frecuencia en el mismo instante que el resto de estaciones que forman la red. El valor predeterminado del período de aviso es la mitad del período de espera para que así se transmitan dos avisos por periodo de espera de salto. El parámetro "Wake duration" establece la cantidad de tiempo por periodo de espera de salto que el adaptador permanece activo a la espera de recibir paquetes de datos pasando después al modo de ahorro energético.

Para seleccionar los dos canales en el estudio, uno poco congestionado y otro muy congestionado, se ha utilizado el software "Wi-Spy" [22]. Se trata de un analizador del espectro en la banda de los 2.4 GHz que lleva asociado una antena interna en un dispositivo USB. Podemos identificar las interferencias que hay en una zona con dispositivos Wi-Fi, microondas, Bluetoth, Zigbee y otros dispositivos que operan en la banda de 2.4 GHz. Este software funciona en entorno Windows (2000, XP o Vista con .Net 2.0). Entre sus funcionalidades podemos destacar el rastreo de las frecuencias actuales, medias y máximas, marcas de frecuencia/amplitud, etiquetas de frecuencia/canal y guardar y reproducir trazas.

Se ejecutó Wi-Spy en un ordenador portátil en diferentes dias de una semana y a distintas horas del dia con el fin de escoger el canal más y el menos congestionado del espectro. En las diferentes pruebas se vió que el canal menos congestionado era el 7 y el más congestionado el 11, por lo que se eligieron estos dos canales para la obtención de los datos de esta tesina.

En la Figura 5 podemos ver el uso de los canales en un instante temporal:

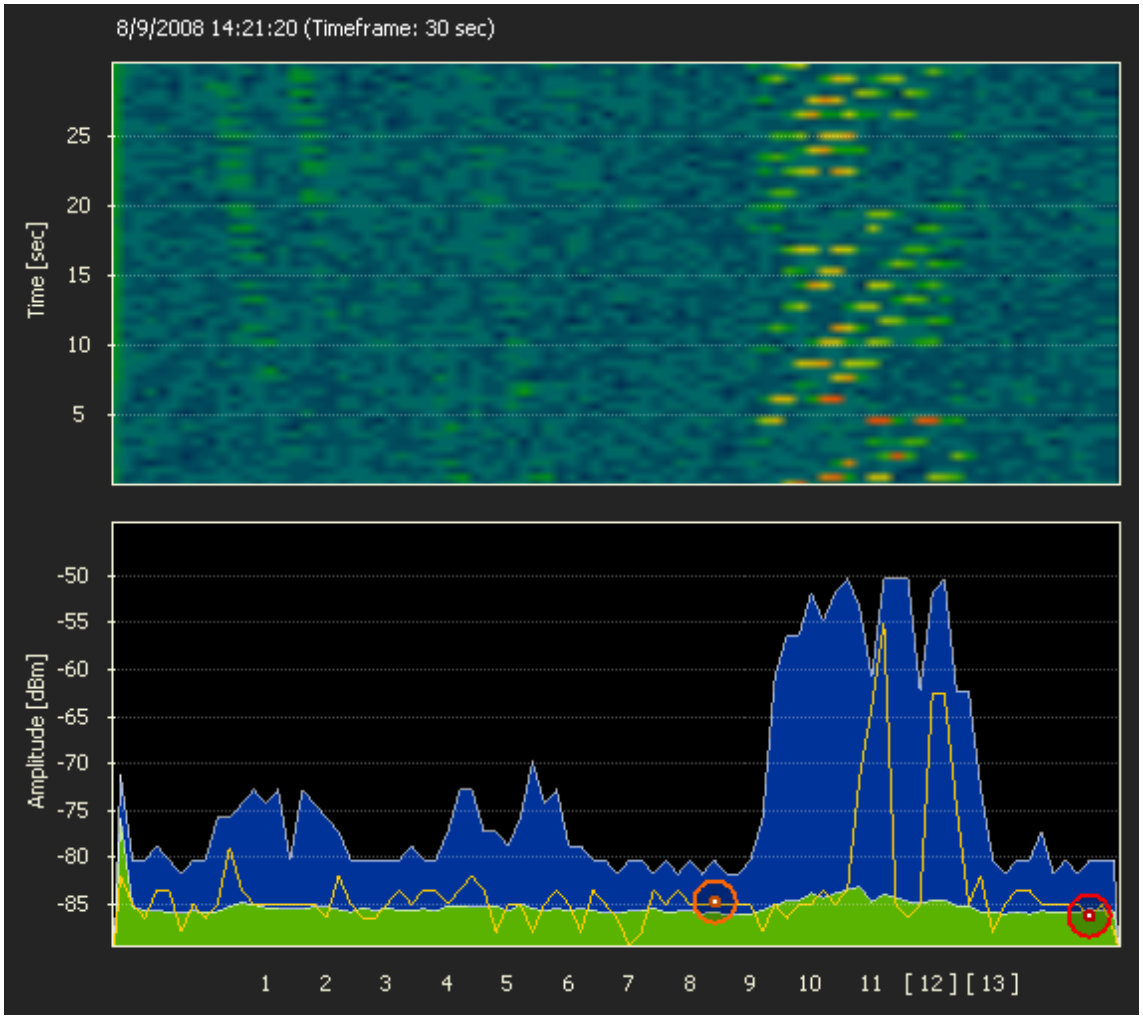

Figura 5. Espectro de la utilización de los canales de la red

En la Figura 6 podemos ver la potencia de la señal asociada a cada canal. Podemos observar que los canales menos ocupados tienen el valor de pico medio con menor valor (poco ruido o interferencias) y los canales con más interferencias tienen este valor más alto.

Figura 6. Potencia de la señal en cada canal

La elección de los canales se basará en dos parámetros: el ***Average Peak*** es la señal inalámbrica más fuerte que va a recibir el ordenador y el ***Duty Cycle***, que es junto al movimiento de las estaciones una de las causas más frecuentes de desconexión en entornos inalámbricos, y que podriamos definir como el porcentage del tiempo en el cual la estación está activa (no en estado sleep) o que le llega señal inalámbrica.

Se observa claramente que los canales 10, 11 y 12 son los que más ocupados están. Un canal que se puede elegir para hacer las pruebas es el 13 ya que ninguna red inalámbrica de las que hay instaladas en la Universidad lo usa, pero no es recomendable porque algunos dispositivos tienen problemas al usar este canal. Para la realización de las pruebas elegiremos los canales 7 y 11 como canales menos y más saturados, respectivamente. El canal 7 tiene los menores Average Peak y Duty Cicle. Por el contrario, el canal 11 tiene los mayores valores para estos parámetros, lo que justifica nuestra selección.

3.2 Localización geográfica del escenario

Para la realización del estudio se escogió un edificio de la Universidad Politécnica de Valencia. Se trata de un edificio departamental de cinco alturas. Cada planta de este edificio puede tener una superficie aproximada de 730 m². Está dedicado a un entorno de oficinas o despachos en el que hay ordenadores portátiles, de sobremesa, PDA´s, teléfonos móviles, impresoras, etc. que pueden provocar interferencias en nuestra red Ad-Hoc. Están también presentes las redes inalámbricas propias de esta Universidad: UPVNET, UPVNET2G y EDUROAM. En el estudio se hará una comparación de la red Ad-Hoc instalada con UPVNET y UPVNET2G.

Se ha procedido a separar en el interior del edificio los portátiles que hacen el papel de cliente y servidor FTP hasta el punto que no tienen conectividad a través de su tarjeta inalámbrica, y además se han localizado dos portátiles en un punto intermedio entre los dos extremos que actuarán como enrutadores cuando se usen los protocolos AODV y OLSR.

La Figura 7 muestra el escenario del trabajo con todos los elementos que intervienen: los cuatro portátiles ubicados en plantas diferentes del edificio (el cliente FTP, el servidor FTP y los dos enrutadores). En las mismas plantas también hay otros ordenadores (de sobremesa o portátiles), además de PDAs y puntos de acceso de las redes inalámbricas propias de la Universidad, que generan interferencias.

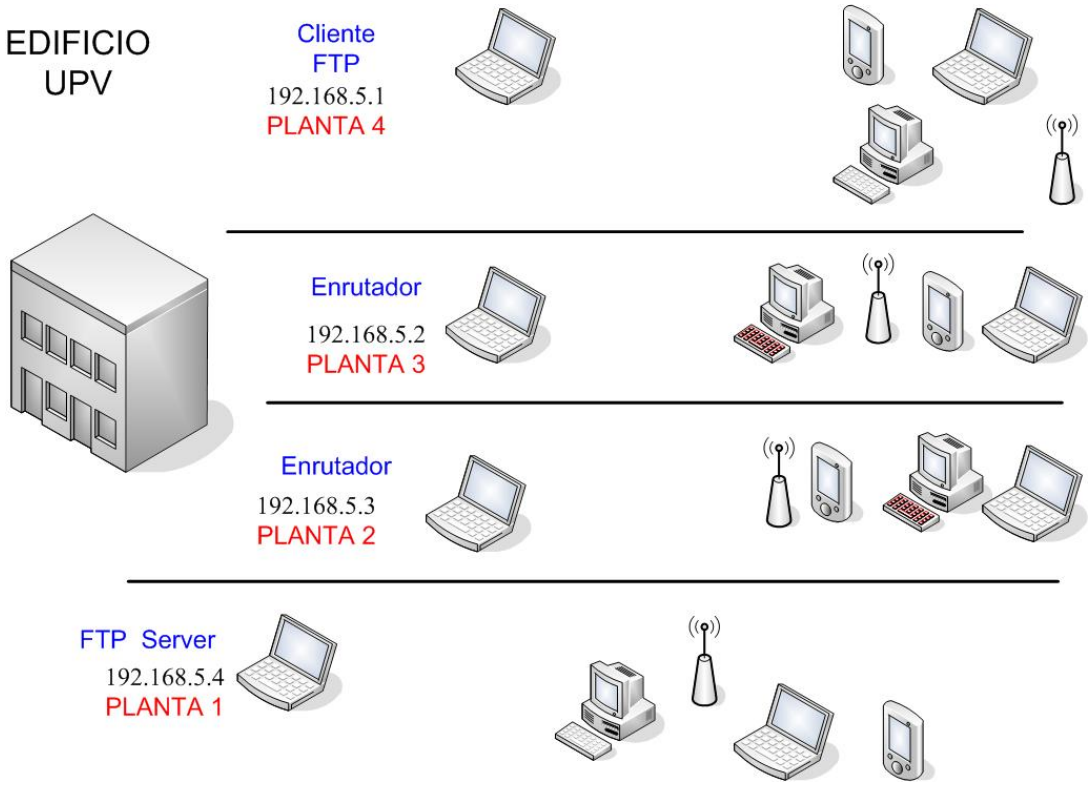

Figura 7. Escenario del trabajo

3.3 INSTALACIÓN DEL ESCENARIO

Una vez se ha seleccionado la ubicación física del escenario es necesario disponer de ordenadores portátiles con el software adecuado para la realización del estudio.

3.3.1 Hardware utilizado

Para la realización del trabajo se dispone de cuatro ordenadores portátiles con las siguientes características Hardware:

- AIRIS
  Intel Centrino Duo T2050 1.6 GHz
  1 Gb RAM
  120 GB HD
  Intel PRO/Wireless 3945 ABG Network Connection MAC 00 13 60 7E 48 A0

- MAXDATA
  Intel Pentium IV M 2.2 GHz
  1 Gb RAM
  30 GB HD
  Wistron NeWeb 802.11B Wireless Lan MAC 00 01 24 D0 5B DB

- ACER TravelMate 4020
  Intel Pentium M 1.6 GHz
  1 Gb RAM
  50 GB HD
  Intel PRO/Wireless 2200 BG MAC 00 12 F0 D5 F3 75

- SAMSUNG R40
  Intel Core 2 Duo T5600 1.83 Mhz
  120 GB HD
  Atheros Wíreles Network Adapter MAC 00 16 E3 B2 EE 88

El escenario ideal se hubiera dado con todos los portátiles idénticos (con las mismas características Hardware), aunque esto fue imposible de conseguir por cuestiones de logística. De todas formas, consideramos que las prestaciones de los distintos ordenadores involucrados es suficiente para impedir que se conviertan en un cuello de botella en las comunicaciones.

3.3.2 Instalación del SW

Una vez conseguido el Hardware necesario, era necesario elegir un Sistema Operativo. Se optó por una SUSE 10.3 para Linux (disponible en [23]) por los siguientes motivos: en primer lugar, por su facilidad de instalación y posibilidad de tener un entorno gráfico (aunque esto hoy en día es una característica de casi todas las

distribuciones Linux); en segundo lugar, porque SUSE reconoce una gran variedad de dispositivos, y en la realización del trabajo esta era una fuente de posibles problemas debido a la heterogeneidad de los ordenadores portátiles. En tercer y último lugar, por su potencia y estabilidad.

Sobre esta plataforma se han instalado los 2 protocolos de encaminamiento analizados: el AODV y el OLSR.

3.3.2.1 Instalación de los protocolos de encaminamiento.

AODV. Hay dos tipos de implementaciones de este protocolo: user space daemons y kernel modules. La primera requiere mantener una tabla de encaminamiento propia y su primera implementación fue la de Fredrik Lilieblad et al., funcionando en un Linux con kernel 2.2, pero no tenía soporte multicast. La Universidad de Upsala también publicó una implementación de user space daemon para un Linux con kernel 2.4. La única implementación de la variante basada en kernel modules fue hecha por el NIST, Department of Commerce's Technology Administration U.S., Wireless Communications Technologies Group, funcionando en un Linux con kernel 2.4.

Para las pruebas realizadas se escogió la última versión (0.9.5) de la Universidad de Upsala (AODV-UU) [21]. Esta funciona en los kernels de Linux 2.4 y 2.6, por lo que cumplimos este primer requisito ya que la versión de SUSE instalada tiene el 2.6. AODV-UU cumple la RFC3561 y fue desarrollado en C para plataforma Linux. Está implementado como un demonio de espacio de usuario usando funcionalidad del kernel. Además soporta múltiples Gateways por medio de tunneling.

Esta implementación nos facilita el estudio ya que almacena en archivos de texto toda la información relativa a todos los movimientos de paquetes para cada estación.

Otras versiones son: AODV-UU con soporte multicast de la Universidad de Maryland, AODV-UU para IPv6, ns-2 2.26 con AODV-UU y Integración móvil IP y AODV-UU con ETX en ns-2: SIPAODV-UUETX.

Para que la compilación de los protocolos de encaminamiento sea correcta, es necesario realizar las siguientes acciones sobre el Sistema Operativo:

1. Instalar Kernel Sources, kernel headers y GCC
2. Actualizar el sistema operativo mediante las actualizaciones On-line

Para instalar el protocolo en los ordenadores hay que ejecutar los siguientes comandos:

1. # tar –xzvf aodv-uu-0.9.5.tar.gz (extrae el software del protocolo)
2. # make
3. # make install
4. # insmod kaodv.ko
5. # aodvd (demonio que lanza el protocolo de encaminamiento)

Llegados a este punto el protocolo instalado está instalado y listo para iniciar las pruebas. El protocolo ofrece la posibilidad de guardar los resultados de todos los

mensajes que se envían en el archivo *aodvd.log* y de todas las tablas de encaminamiento para cada uno de las estaciones, en el archivo *aodvd.rtlog.* Estos dos archivos generados por el protocolo están en el directorio /var/log.

Sintaxis: Aodvd [-dghjlouwxLDRV] [-i if0 , if1,…] [-r N] [-n N] [-q THR]

Algunos de los parámetros más significativos son:

-*i interface*. Indicamos por cual de las interfaces inalámbricas se tiene que arrancar aodvd. Por defecto se arranca en la primera que esté activa.
-*j hello-jitter*. Por defecto puesto a ON
-*n n-hellos* Indica el número de HELLOs que un nodo debe recibir de un host para considerarlo un vecino
-*w gateway-mode.* Es una funcionalidad experimental. Permite que se puedan enviar paquetes hacia una estación que hace de Gateway dentro de la red Ad-hoc.
-*R rate-limit*. Limita el número de paquetes RREQ y RREP transmitidos en un periodo de tiempo para no colapsar la red con paquetes de control. (por defecto a ON)

El comando que se usa para iniciar el protocolo es el siguiente:

aodvd –d –l –r 1 –i eth0

-*d*: lanza el protocolo en background.
-*l*: guarda los log´s en los cuales podemos ver todos los paquetes (RREQ, RERR, RREP, HELLO) que se envían las estaciones.
-*r*: guarda las tablas de cada estación. Se especifica con un valor (en segundos) la frecuencia con la que se refresca la tabla.
-*i*: se utiliza para especificar la interface que debe utilizar para ver al resto de estaciones.

OLSR. Se escogió la última versión: olsrd-0.5.5, el cual es además más estable y corrige algunos errores de la 0.5.4. El protocolo funciona en las siguientes plataformas: Windows (XP y Vista), Linux, OS X, VxWorks, NetBSD, FreeBSD, OpenBSD, Linux wifi phones (WIP). Cumple con RFC3626 y fue diseñado para funcionar como un proceso standalone.

El protocolo está disponible en [22]. Para su instalación y funcionamiento en los ordenadores es necesario hacer los siguientes pasos:

1. Instalar con el YAST
   Bison
   Flex (un corrector sintáctico)
2. Compilar con make en /src/cfgparser para ver las dependencias
3. Extraer el software del protocolo con el siguiente comando:
   # tar –xzvf olsrd-0.5.5.tar.gz
4. # make
5. # make install

6. Editar el fichero /etc/olsrd.conf. Aquí residen todos los parámetros configurables del daemon olsrd. De las múltiples opciones que podemos configurar, hemos seleccionado dos: **Interface "nombre"** (siendo nombre wlan0 ó eth1, dependiendo del portátil) y **UseHysteresis** que le hemos asignado el valor "No" (la Hysteresis añade más robustez al link sensing pero retrasa el registro de vecinos). El link sensing es la capacidad de una estación de detectar enlaces entre su interface y las interfaces de las estaciones vecinas.
7. Ejecutar olsrd (demonio que lanza el protocolo de encaminamiento)

Sintaxis: Olsrd [-f <configfile>] [-i interface1 interface2…] [-d <debug_level>] [-ipv6] [-multi <IPv6 multicast address>] [-lql <LQ level>] [-lqw <LQ winsize>] [-lqnt <nat threshold>] [-bcast <broadcastaddr>] [-ipc] [-dispin] [-dispout] [-delgw] [-hint <hello interval (secs)>] [-tcint <tc interval (secs)>] [-midint mid interval (secs)>] [-hnaint <hna interval (secs)>] [-T <Polling Rate (secs)>] [-nofork] [-hemu <ip_address>] [-lql <LQ level>] [-lqw <LQ winsize>]

Con este comando se aprecia como las estaciones empiezan a calcular la topología enviandose mensajes a otras estaciones vecinas. Se puede almacenar esta información en un archivo de texto de la siguiente forma:

olsrd –d 0 > archivo.txt.

-d: lanza el protocolo en background.

3.3.2.2 Otras consideraciones del software

Para el correcto funcionamiento de la práctica, es necesario desactivar el Firewall del sistema Operativo. En SUSE, esto se hace desde el YAST (centro de control).

Se necesita un servidor de ficheros instalado en un portátil y un cliente FTP en otro para obtener los datos del tiempo consumido para descargar los archivos. Como servidor se instala el vsftp por su sencillez de configuración y como cliente, el Filezilla por su sencillez de uso e interfaz gráfico (disponible en [24]).

En XINETD (Network Service Configuration del YAST), hay que activar el FTP con los siguientes comandos que se lanzan desde un script:

```
# /etc/init.d/xinetd    stop
# /etc/init.d/vsftpd    start
```

3.3.3 Esquema de direccionamiento del escenario

Cada portátil debe tener una dirección IP y las 4 deben estar en el mismo rango de direccionamiento para que puedan intercambiar información.

El primer paso es asociar los 4 portátiles a un mismo SSID (cualquier nombre y para el trabajo se ha elegido master) por el mismo canal (7) y que trabajen en modo Ad-Hoc:

 # iwconfig eth1 essid "master" mode ad-hoc channel 7

Se puede verificar que están asociados a la misma celda de nuevo usando el comando *iwconfig*.

Después es necesario asignar a cada portátil una dirección IP fija. Se ha elegido el siguiente esquema:

```
# ifconfig eth1 192.168.5.1 netmask 255.255.255.0
# ifconfig eth1 192.168.5.2 netmask 255.255.255.0
# ifconfig eth1 192.168.5.3 netmask 255.255.255.0
# ifconfig eth1 192.168.5.4 netmask 255.255.255.0
```

Finalmente, con un Ping se puede probar la conectividad de los portátiles entre sí.

4. ESTUDIO DE PRESTACIONES

En este capítulo se analizan diferentes escenarios con el fin de ver el comportamiento de los dos protocolos estudiados: AODV y OLSR. También se hará una comparación de estos dos protocolos con las redes UPVNET y UPVNET2G de la Universidad Politécnica de Valencia.

Las redes inalámbricas UPVNET y UPVNET2G permiten conectar un equipo WiFi a la red de la UPV de manera rápida y directa, ofreciéndo acceso a Internet y a los recursos informáticos propios de esta universidad.

Los requisitos de la red UPVNET2G son dos: que el equipo disponga de una tarjeta inalámbrica 802.11b u 802.11g con tecnología WPA, y que el sistema operativo soporte el estandar 802.1x. La velocidad máxima de conexión es de 54 Mbps desde distancias muy cercanas al punto de acceso.

Desde el punto de vista de la seguridad, la autenticación se basa en el estándar 802.1x y el cifrado de datos en WPA. Técnicamente hablando, el cifrado se realiza mediante TKIP y la autenticación del usuario mediante PEAP, utilizándose certificados para garantizar la identidad de los servidores RADIUS. Una vez el usuario se valida mediante su usuario y contraseña, estará autorizado para acceder a la red y dispondrá de una dirección IP pública con la que se puede navegar directamente por Internet, si bien el equipo no podrá ofrecer ningún servicio público a Internet.

4.1 Escenario I. Impacto del número de saltos en el retardo de la red

El primer escenario se usa para evaluar el impacto que tiene el aumento de número de saltos entre estaciones en el retardo de la red. Se trata de separar geográficamente los portátiles que hacen el papel de cliente y servidor FTP hasta el punto que no tienen conectividad a través de su tarjeta inalámbrica, y poner portátiles en puntos intermedios entre los 2, que sean los que actúen de enrutador.

Para llevar a cabo las mediciones se ha utilizado el siguiente comando:

ping dir_destino –c 10 → hace un ping de 10 paquetes al nodo destino

Con este comando ping se envían paquetes de la estación fuente (o nodo 1, ya que se ha elegido uno de los extremos) al resto de estaciones para ver los retardos que se producen. Esta operación se ha repetido 3 veces y se ha hecho una media de los resultados.

Las pruebas se realizan con los protocolos de encaminamiento iniciados antes de realizar el ping, para así poder ver cual de ellos tarda más tiempo en llegar. Esto se hace con el siguiente script que se lanza en cada portátil:

```
# ifconfig eth0 192.168.5.1 netmask 255.255.255.0
# iwconfig eth0 essid “master” mode ad-hoc channel 7
# aodvd –d –l –r 1 –i eth0
```

Al script se le da permiso de ejecución con el comando # chmod 744 nombre_script. Con la primera linea se inicia la tarjeta inalámbrica del portátil para conseguir una dirección IP. Con la segunda se configura la red inalámbrica (proporcionando el mismo essid, modo de conexión y canal en los portátiles) y con la tercera se lanza el protocolo. Los comandos lanzados para cada protocolo se han detallado en la sección 3.3.2.1

Los resultados obtenidos utilizando el canal 7 (canal poco saturado) fueron los mostrados en la Figura 8.

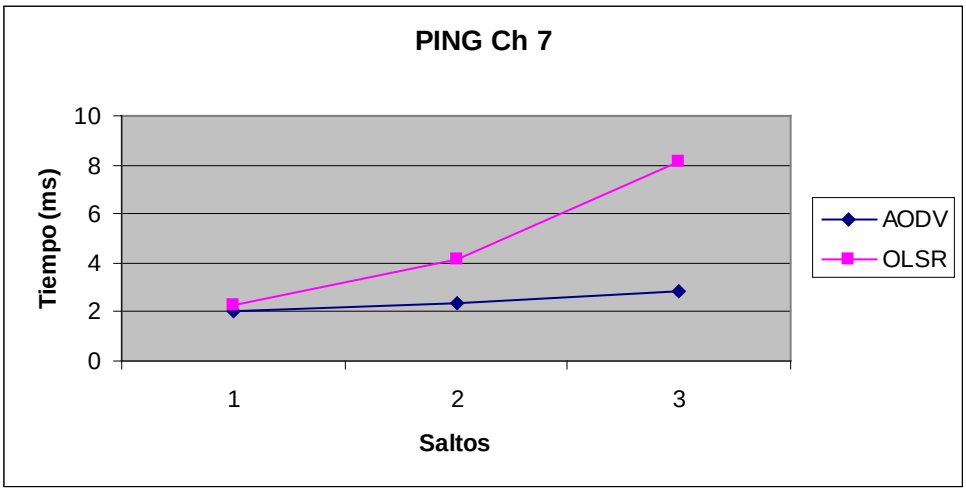

Figura 8. Tiempos de Ping obtenidos en el Canal 7

Analizando la Figura 8 se puede ver cómo OLSR se comporta peor que AODV. De hecho, para una distancia de un salto, hay un incremento de un 15.08 %. Para dos saltos el retardo aumenta hasta un 75.21 %, y con tres saltos se dispara a un 186.94%. También se aprecia cómo va creciendo el retardo en función del número de saltos que hay que dar para llegar a las estaciones.

A continuación se repitió la prueba usando un canal saturado como el 11. Los resultados obtenidos fueron los mostrados en la Figura 9.

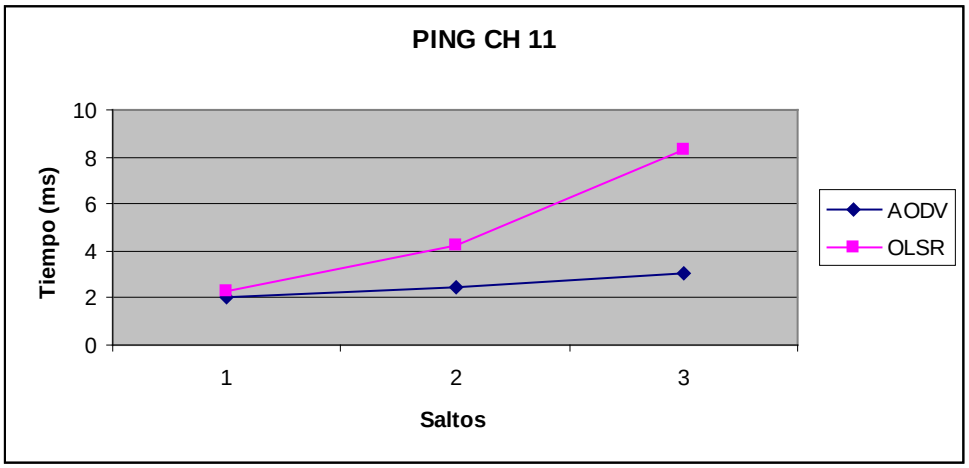

Figura 9. Tiempos de Ping obtenidos en el Canal 11

Analizando la Figura 9 se puede ver cómo OLSR se comporta peor que AODV. Para una distancia de un salto, hay un incremento de un 14.96 %. Para dos saltos el retardo aumenta hasta un 71.78 %, y con tres saltos se dispara a un 173.95%. También se aprecia cómo va creciendo el retardo en función del número de saltos que hay que dar para llegar a las estaciones.

En la Tabla 2 se muestran los porcentajes de aumento del retardo del protocolo OLSR respecto a AODV. Teniendo en cuenta el comportamiento de ambos protocolos, consideramos que el aumento asociado al protocolo OLSR se debe esencialmente a la generación periódica de mensajes de control de la red, algo que no ocurre con el protocolo AODV (on-demand) ya que al tratarse de un protocolo reactivo, sólo genera mensajes de control cuando hay que establecer una nueva ruta o cuando se pierde una ruta que ya está siendo utilizada.

Tabla 2. Porcentaje de aumento del retardo con OLSR respecto a AODV.

	Número de saltos		
	1	2	3
Canal Libre	15,08 %	75,21 %	186,94 %
Canal Saturado	14,96 %	71,78 %	173,95 %

En la Tabla 3 se puede ver cómo para el canal ocupado se obtienen tiempos de Ping ligeramente más elevados, tal y cómo se esperaba.

Tabla 3. Retardo adicional en el canal ocupado respecto al canal libre

Protocolo	Número de saltos		
	1	2	3
AODV	0,75 %	4,77 %	7,47 %
OLSR	0,65 %	2,60 %	2,72 %

Para poder contrastar los resultados obtenidos con las prestaciones ofrecidas por la infraestructura de red inalámbrica de la UPV, se ha ampliado este conjunto de experimentos para incluir también las redes UPVNET y UPVNET2G.

En la Tabla 4, se pueden ver los tiempos del Ping a través de la red UPVNET y UPVNET2G. Se puede apreciar que UPVNET es un poco más rápida que UPVNET2G ya que no requiere cifrado AES (WPA2), aunque si requiere la creación de un tunel VPN.

Tabla 4. Tiempos de Ping obtenidos en UPVNET y UPVNET2G

PING	UPVNET	UPVNET 2G
min (ms)	1,211	2,018
avg (ms)	4,259	4,524
max (ms)	13,906	14,323

Para finalizar, en la Figura 10 se pueden ver los tiempos de Ping a 1 salto de los protocolos AODV y OLSR, comparándolos con los tiempos que nos dan las redes inalámbricas de la UPV (UPVNET y UPVNET2G). Todos los valores representados son para canales saturados.

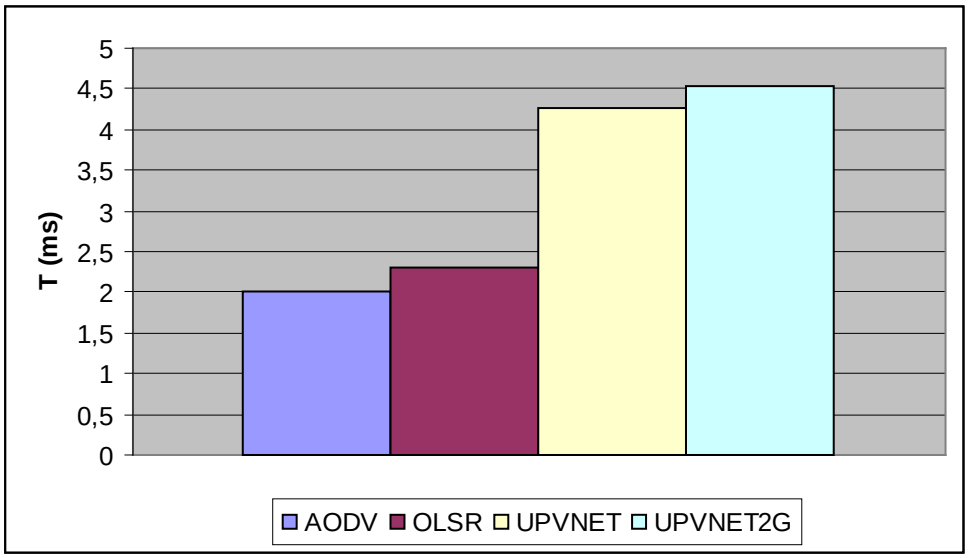

Figura 10. Tiempos de Ping (ms) a 1 salto en los 4 casos de estudio

Como se puede comprobar, el uso de redes Ad-Hoc no supone una penalización en términos de rendimiento, verificándose que por el contrario la latencia media se reduce con respecto al uso de la infraestructura de la UPV, aunque es cierto que no se está aplicando ningún tipo de cifrado en la red ad-hoc. En caso de que cifraramos todo el tráfico se esperaría valores similares a los obtenidos con infraestructura. Si el número de saltos se incrementara de forma significativa con un mayor número de estaciones, posiblemente se obtendrían valores mayores para la red Ad-Hoc que los obtenidos en las redes de la UPV

4.2 Escenario II. Ancho de banda conseguido

En este escenario, el objetivo es cuantificar el ancho de banda que se logra al descargar un fichero de 15 Mbytes con un cliente FTP usando 2 protocolos de encaminamiento (el AODV y el OLSR) y comparar el rendimiento de cada uno de ellos. En la segunda parte se realizará una comparativa con la infraestructura de la UPV.

Como ya se dijo en la sección 3.3.2.2, se ha elegido el servidor vsftp y el cliente Filezilla.

De la misma forma que antes, se hicieron varias mediciones: unas en un canal libre (el 7) y otras en un canal más saturado (el 11). En la Figura 11 se puede ver el rendimiento en Mbits/s para cada uno de los protocolos en el canal 7.

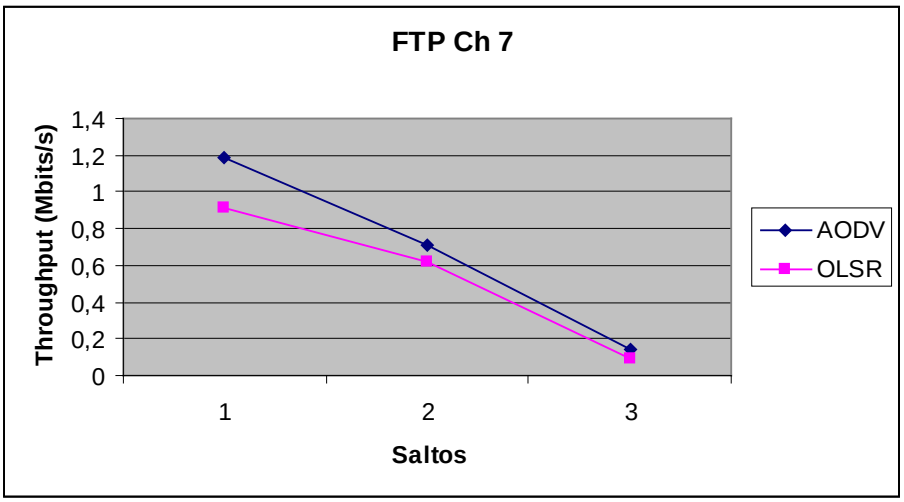

Figura 11. Rendimiento del FTP en el Canal 7 en los dos protocolos

Analizando la Figura 11 se puede ver cómo el Throghput disminuye con el número de saltos tanto para AODV como para OLSR. También se aprecia que OLSR tiene peor rendimiento que AODV. Para una distancia de un salto es un 31.1 % menor. Para dos saltos es un 13.46 %, y para tres saltos un 63.68%.

Del mismo modo que en el caso anterior, en la Figura 12 se aprecia cómo el Throghput disminuye con el número de saltos cuando se utiliza el canal más saturado. De nuevo se verifica que con AODV se obtiene un rendimiento más alto que con OLSR: para un salto es un 96.9 % mejor, para dos saltos un 125.97 % y para tres saltos un 70.75%.

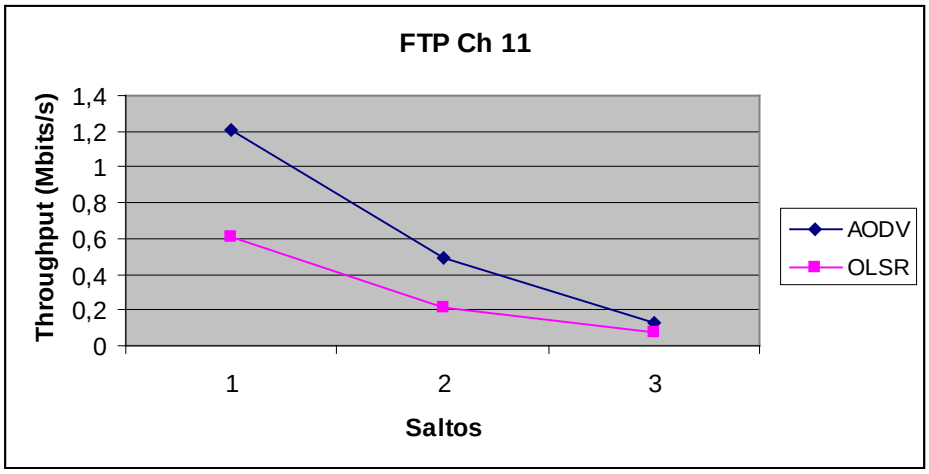

Figura 12. Rendimiento del FTP en el Canal 11 en los dos protocolos

Si se compara un mismo protocolo en los dos canales utilizados (uno libre y otro ocupado), se ve que en el canal libre el rendimiento es mayor tanto para AODV como para OLSR. La única anomalía es en el caso de AODV a un salto, que tiene un valor ligeramente superior en el canal ocupado al del canal libre (1,2098 frente a 1,1919) y que se aprecia en el la Figura 13. Esta anomalía se constató repitiendo la toma de datos varias veces pero como la diferencia es mínima no se le da importancia. Posiblemente se debió a una interferencia provocada por algún dispositivo cercano. Para dos saltos el rendimiento en el canal libre es un 43.49% mayor y para tres saltos es un 13.04% mayor.

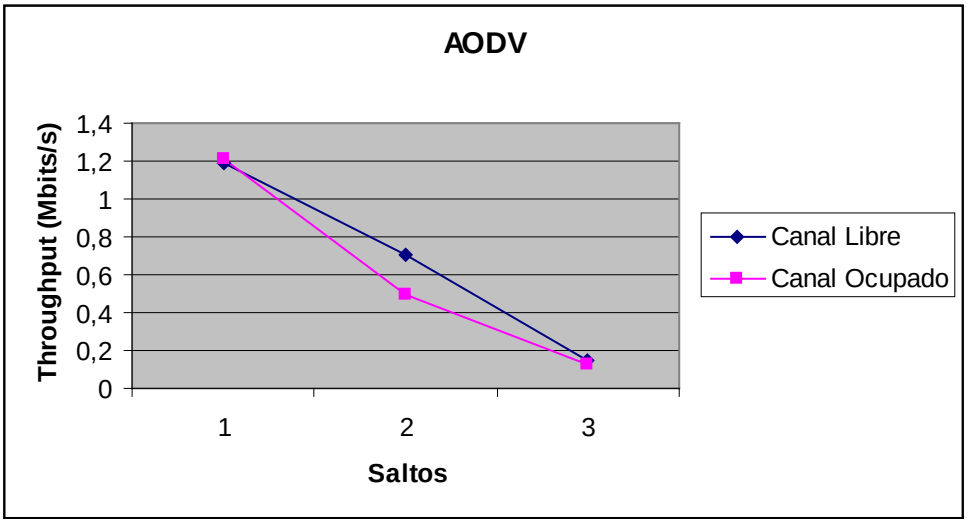

Figura 13. Rendimiento de AODV en los dos canales utilizados

La Figura 14 nos muestra el rendimiento de OLSR. Se verifica que con este protocolo el uso de un canal saturado tiene un mayor impacto en las prestaciones. Para un salto es un 47.96% menor en el canal saturado, para dos saltos es un 185.79 % menor y para tres saltos es un 17.91% menor siendo las diferencias muy superiores a AODV para uno y dos saltos.

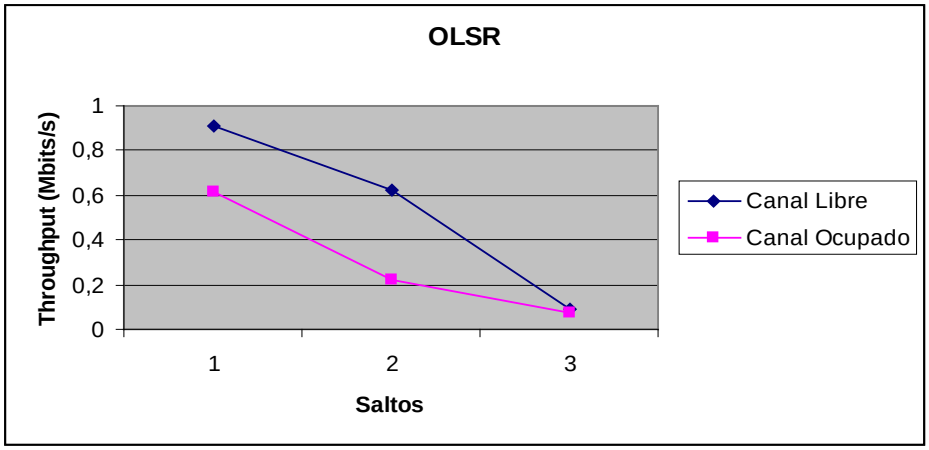

Figura 14. Rendimiento de OLSR en los dos canales utilizados

Si comparamos los dos protocolos, se ve cómo OLSR tiene unas diferencias muy superiores en porcentaje a AODV en uno y dos saltos, tal y como se ve en la Tabla 5.

Tabla 5. Diferencia en porcentaje de AODV y OLSR

	Número de saltos		
	1	2	3
AODV	0	43,49	13,04
OLSR	47,96	185,79	17,91

En la Tabla 6 se ven las tres mediciones hechas y la media (en segundos) cuando se hace la transferencia por medio de las redes UPVNET y UPVNET2G.

Tabla 6. Tiempo en segundos del FTP a través de UPVNET y UPVNET2G

FTP	UPVNET	UPVNET2G
medición 1	21	25
medición 2	21	24
medición 3	18	25
media (seg)	20	24,66
Throughput Mbits/s	0,78	0,63

De nuevo se observa una consistencia con los resultados anteriores, observándose que el rendimiento en UPVNET2G es peor debido a que aplica una técnica de cifrado más compleja para el tráfico.

Para finalizar, la Figura 15 muestra el Throughput en Mbits/s de la trasferencia FTP a 1 salto para los protocolos AODV y OLSR, comparándolos con el Throughput que se obtiene mediante las redes inalámbricas de la UPV (UPVNET y UPVNET2G). Todos los resultados son relativos a canales saturados.

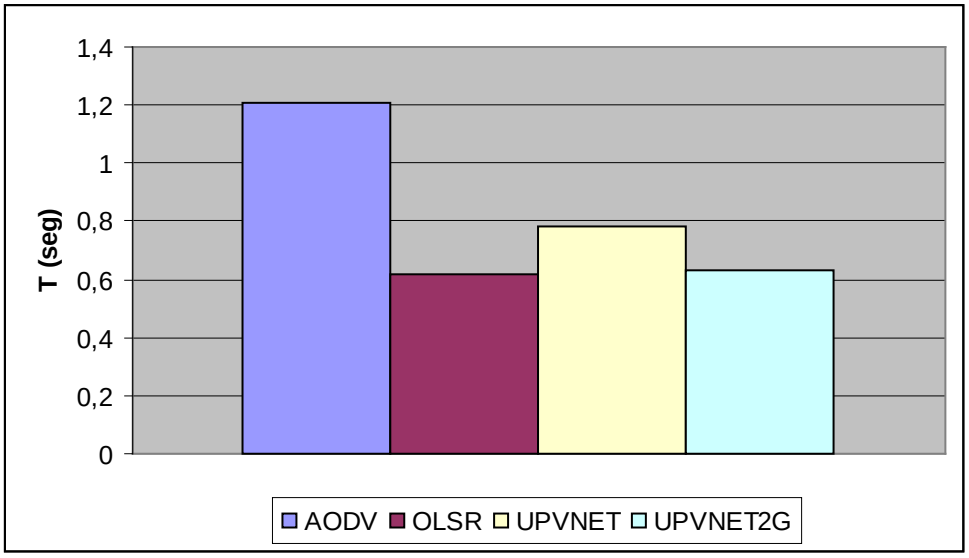

Figura 15. Throughput (Mbits/s) a 1 salto en los 4 casos de estudio

Los resultados muestran que el protocolo AODV permite lograr valores de throughput algo superiores. Incluso con OLSR se logran niveles similares a los obtenidos con UPVNET2G.

4.3 Escenario III. Movilidad de una estación

En el último escenario propuesto se dispone de una red Ad-Hoc ya establecida formada por tres ordenadores, y con un protocolo funcionando en estado estable (o sea, que el transitório inicial ya se ha superado).

El objetivo es cuantificar el tiempo que un cuarto ordenador que se mueve dinámicamente en una de las plantas del edificio de estudio (y que actuará como extremo) tarda en configurarse e integrarse plenamente en la red. Para estimar este tiempo se calcula el retardo inicial en establecer la conexión (mediante el envío de paquetes ping al ordenador que está en el otro extremo).

Para medir este tiempo, se utilizará el software Wireshark [27]. Wireshark es uno de los analizadores de protocolos de red más famosos utilizados, aunque antiguamente se conocía como Ethereal. Esta herramienta es multi-plataforma (se puede ejecutar en Windows, Linux, OS X, Solaris, FreeBSD, NetBSD y otros) y permite analizar cientos de protocolos. Los datos se pueden obtener desde Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI y otros.

Los tiempos de configuración y conexión iniciales se presentan en la Tabla 7. Se observa que con OLSR este retardo inicial es un poco superior respecto a AODV.

Tabla 7. Tiempo de conexión a la red en ambos canales.

Canal utilizado	AODV	OLSR
Canal 7 (libre)	3.332 s	3.755 s
Canal 11 (ocupado)	1.917 s	2.197 s

Se midieron además los tiempos (medido en segundos) que tarda un ordenador en conectarse a cada una de las 2 redes (UPVNET y UPVNET2G), tal y como se ve en la Tabla 8:

Tabla 8. Tiempo de conexión a UPVNET y UPVNET2G

Tiempo de conexión	UPVNET	UPVNET 2G
T (s)	13,3	14,1

En la Figura 16 se puede ver la comparación para cada uno de los dos protocolos estudiados del tiempo de estabilización, tanto para el canal libre como para el canal saturado.

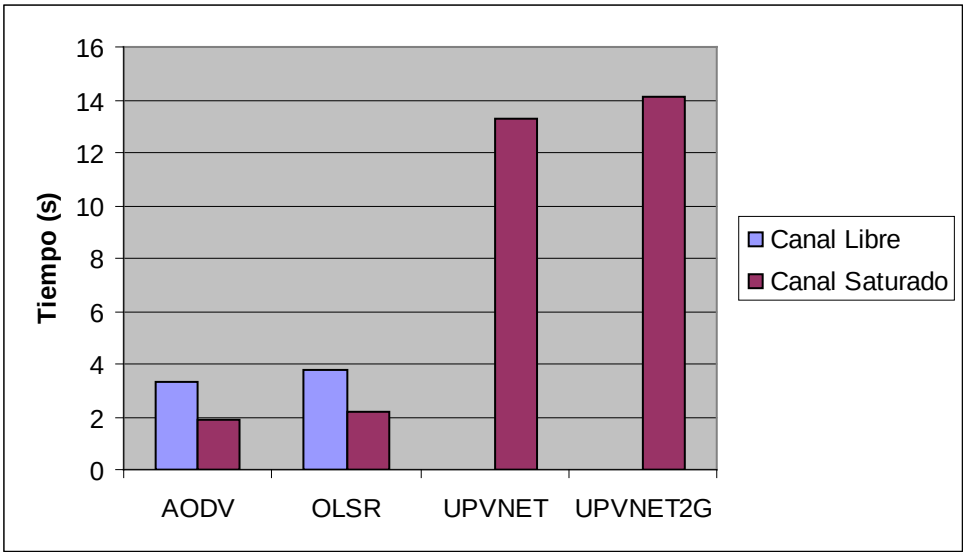

Figura 16. Tiempo de estabilización de los 2 protocolos

Como se puede verificar, aún en el peor caso (3 saltos de distancia), el tiempo inicial de configuración del dispositivo y de la red Ad-Hoc es bastante inferior a los tiempos asociados al proceso de conexión para las redes UPVNET y UPVNET2G, lo que es un resultado bastante sorprendente.

5. CONCLUSIONES

En esta tesina se ha analizado la viabilidad de reemplazar una red de infrastructura por una red Ad-Hoc en un edificio de la UPV en términos de prestaciones de red y latencia percibida por el usuario.

La red Ad-Hoc propuesta se basó en dos protocolos muy utilizados en redes Ad-Hoc: el AODV y el OLSR.

Para realizar las pruebas ha sido necesario hacer un estudio de cada protocolo y configurar los puestos de trabajo adecuadamente. A la hora de seleccionar los protocolos se han podido encontrar muchas implementaciones de las que se han seleccionado las más probadas.

Con la utilización de diferentes escenarios se ha podido ver cómo los resultados cambian según se trate de un protocolo proactivo o reactivo. Los escenarios han servido para calcular el tiempo que se tarda en el envío de pings, el tiempo de transferencia de un fichero de 15 MBytes de un extremo a otro de la red y el tiempo que tarda una estación en hacer un ping a otra que ya está en una red Ad-Hoc con un protocolo ya estabilizado.

AODV se ha comportado mejor al necesitar menos tiempo para reencaminar los paquetes. Se podrían obtener resultados ligeramente diferentes en escenarios concretos ajustando algunos parámetros. Por otra parte, el protocolo OLSR tarda más tiempo en detectar la rotura de enlaces y continúa enviando paquetes por la misma ruta, congestionando los buffers.

También se ha visto cómo la red inalámbrica UPVNET2G es ligeramente más lenta que la UPVNET por la encriptación que realiza.

Los resultados obtenidos muestran que, utilizando el protocolo de encaminamiento más eficiente (AODV) se logran prestaciones superiores a las ofrecidas por la infraestructura de red, lo que viabiliza la aplicación de tecnologías de red Ad-Hoc como un substituto de dicha infraestructura en los casos en que sea necesario.

En escenarios en los que no se dispone de infraestructura, las redes Ad-Hoc permiten aunmentar la cobertura con niveles de prestaciones aceptables siempre que las aplicaciones no demanden un excesivo ancho de banda.

Como posible trabajo futuro sería de destacar la necesidad de validar los resultados obtenidos a mayor escala, empleando un mayor numero de estaciones y más saltos entre fuente y destino. Sería también interesante probar otros protocolos de encaminamiento, y la posibilidad de integrar la tecnología IPv6 de forma transparente.

BIBLIOGRAFÍA

[1] The Institute of Electrical and Electronics Engineers, Inc. Ieee/iec std 802.11, wireless LAN medium access control (MAC) and physical layer (PHY) specifications, August 1999.

[2] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic. Mobile ad hoc networking. IEEE Press, 2004.

[3] Elizabeth M. Belding-Royer, and Ian Chakeres. "Ad Hoc On Demand Distance Vector (AODV) Routing." *IETF Internet draft*, draft-perkins-manet-aodvbis-00.txt, Oct 2003 (Work in Progress)

[4] T. Clausen and P. Jacquet. Optimized link state routing protocol (OLSR). Request for Comments 3626, MANET Working Group, http://www.ietf.org/rfc/rfc3626.txt, October 2003. Work in progress.

[5] G. Malkin. RIP Version 2. IETF RFC 2453, November 1998.

[6] J. Moy. OSPF Version 2. IETF RFC 2328, April 1998.

[7] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM Computer Communication Review, 24(2):234 244, October 1994.

[8] Shree Murthy and J. J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. Mobile Networks and Applications, 1(2):183-197, 1996.

[9] R. Ogier, F. Templin, and M. Lewis. Topology dissemination based on reverse-path forwarding (TBRPF). Request for Comments 3684, MANET Working Group, http://www.ietf.org/rfc/rfc3684.txt, February 2004. Work in progress.

[10] J. J. Garcia-Luna-Aceves and Marcelo Spohn. Source-tree routing in wireless networks. In ICNP, pages 273-282, 1999.

[11] X. Chen, L. Qi, and D. Sun. Global and superlinear convergence of the smoothing Newton method and its application to general box constrained variational inequalities. Mathematics of Computation, 67(222):519-540, 1998.

[12] Guangyu Pei, Mario Gerla, and Tsu-Wei Chen. Fisheye state routing: A routing scheme for ad hoc wireless networks. In ICC (1), pages 70-74, 2000.

[13] G. Pei, M. Gerla, and X. Hong. Lanmar: Landmark routing for large scale wireless ad hoc networks with group mobility, 2000.

[14] Charles E. Perkins and Elizabeth M. Royer. Ad hoc On-Demand Distance Vector Routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pages 90-100, February 1999.

[15] David B. Johnson, David A. Maltz, and Yih-Chun Hu. The dynamic source routing protocol. Internet Draft, MANET Working Group, draft-ietf-manet-dsr-10.txt, July 2004. Work in progress.

[16] C. K. Toh. Associativity-Based Routing for Ad-Hoc Mobile Networks. Wireless Personal Communication, 4(2):1-36, March 1997.

[17] Rohit Dube, Cynthia D. Rais, Kuang-Yeh Wang, and Satish K. Tripathi. Signal stability based adaptive routing (ssa) for ad-hoc mobile networks. Technical report, 1996.

[18] V. Park and S. Corson. Temporally-ordered routing algorithm (TORA) version 1 - functional specification. Internet Draft, MANET Working Group, draft-ietf-manet-tora-spec-03.txt, November 2000. Work in progress.

[19] George Aggelou and Rahim Tafazolli. RDMAR: A bandwidth-efficient routing protocol for mobile ad hoc networks. In Proceedings of the WOWMOM, pages 26-33, 1999.

[20] I. D. Chakeres and C. E. Perkins. Dynamic MANET on-demand routing protocol. IETF Internet Draft, June 2006.

[21] Uppsala Universitet. AODV-UU. Disponible en http://core.it.uu.se/core/index.php/AODV-UU

[22] “Wi-Spy” de Crownhill Associates

[23] www.opensuse.org

[24] http://filezilla-project.org/

[25] www.olsr.org

[26] http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.html

[27] http://www.wireshark.org/