REDES INALAMBRICAS ENMALLADAS METROPOLITANAS

DIANA MARGARITA ACUÑA MARTINEZ

RAFAEL JULIO RONCALLO KELSEY

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA ELECTRONICA

COMUNICACIONES Y REDES

CARTAGENA DE INDIAS

2007

REDES INALAMBRICAS ENMALLADAS METROPOLITANAS

DIANA MARGARITA ACUÑA MARTINEZ

RAFAEL JULIO RONCALLO KELSEY

Monografía

Minor de Telecomunicaciones

Para optar al titulo de

Ingeniero Electrónico

Director

Margarita Upegui Ferrer

Magíster en Ciencias Computacionales

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA ELECTRONICA

COMUNICACIONES Y REDES

CARTAGENA DE INDIAS

2007

Cartagena de Indias, 8 de Agosto de 2007

Señores
Comité curricular de Ingeniería Eléctrica y Electrónica
Universidad Tecnológica de Bolívar
L. C.

Respetados señores:
Por medio de la presente nos permitimos informarles que la monografía titulada **"Redes Inalámbricas Enmalladas Metropolitanas"** ha sido desarrollada de acuerdo a los objetivos y justificaciones establecidas con anterioridad.

Como autores de la monografía consideramos que el trabajo investigativo es satisfactorio y merece ser presentado para su evaluación.

Atentamente,

_____ _____

Diana M. Acuña M. Rafael J. Roncallo K.

Cartagena de Indias, 8 de Agosto de 2007

Señores
Comité curricular de Ingeniería Eléctrica y Electrónica
Universidad Tecnológica de Bolívar
L. C.

Respetados señores:

Cordialmente me permito informarles, que he llevado a cabo la dirección del trabajo de grado de los estudiantes Diana Acuña Martínez y Rafael Roncallo Kelsey, titulado **"Redes Inalámbricas Enmalladas Metropolitanas".**

Atentamente,

_____

Margarita Upegui Ferrer
Magíster en Ciencias Computacionales

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Cartagena de Indias 8 de Agosto de 2007

AUTORIZACIÓN

Cartagena de Indias D.T Y C. Noviembre de 2006

Yo Rafael Julio Roncallo Kelsey, identificado con la cedula de ciudadanía numero 7.570589 de Valledupar (Cesar), autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catalogo online de la biblioteca.

_____

Rafael Julio Roncallo Kelsey
C.C # 7.570.589 de Valledupar

AUTORIZACIÓN

Cartagena de Indias D.T Y C. Noviembre de 2006

Yo Diana Acuña Martinez, identificado con la cedula de ciudadanía numero 75.276.354 de Cartagena (Bolívar), autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catalogo online de la biblioteca.

_____

Diana Acuña Martinez
C.C # 75.276.354 de Cartagena

DEDICATORIA

Esta monografía se la dedico a todas las personas que creyeron en mí, a todas esas personas que han sido luz en mi camino.

Diana Margarita Acuña Martínez

Esta investigación es dedicada a nuestro señor Dios por darme la fe y la fuerza necesaria para que hiciera posible este logro muy importante en mi vida, además de todo eso, a mi madre y padre que fueron el pilar de esta proeza ya que hicieron de mí una persona llena de valores para que yo progresase.

Rafael Julio Roncallo Kelsey

AGRADECIMIENTOS

Le agradezco a Dios por brindarme la posibilidad de alcanzar una educación superior por medio del esfuerzo y el apoyo económico de mis padres.
Les agradezco a mis profesores por compartir sus conocimientos conmigo y por demostrarme que los buenos resultados son obtenidos por medio del esfuerzo y dedicación.

Diana Margarita Acuña Martínez

Le agradezco a mi padre y a mi madre por el duro esfuerzo que han hecho toda su vida por hacer de su hijo una persona de bien y servil para la sociedad y por el apoyo incondicional a todos los profesores que lograron que me esmerara para alcanzar mis objetivos y hacer de mi una persona integral y valiosa para la sociedad.

Rafael Julio Roncallo Kelsey

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

Backhaul (red de retorno): Conexión de baja, media o alta velocidad que conecta a computadoras u otros equipos de telecomunicaciones encargados de hacer circular la información. Los backhaul conectan redes de datos, redes de telefonía celular y constituyen una estructura fundamental de las redes de comunicación. Un Backhaul es usado para interconectar redes entre sí utilizando diferentes tipos de tecnologías cabledas o inalámbricas.

Bluetooth: es el nombre común de la especificación industrial IEEE 802.15.1, que define un estándar global de comunicación inalámbrica que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura, globalmente y sin licencia de corto rango.

Broadcast: es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Frame Relay: es una técnica de comunicación mediante retransmisión de tramas, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("*frames*") para datos, perfecto para la transmisión de grandes cantidades de datos.

Gateway: es una puerta de enlace entre dos redes distintas. Esto significa que se usa como puente, también tiene este significado, entre una red local, LAN, y una extensa, WAN. El significado más empleado actualmente es para designar al dispositivo hardware software o, más usualmente, una combinación de ambos, que controla el tráfico entre Internet y el ordenador o la red local de ordenadores de una empresa.

Half-dúplex: modo de transmisión de datos que se realiza en ambos sentidos, pero de forma alternativa, es decir solo uno puede transmitir en un momento dado, no pudiendo transmitir los dos al mismo tiempo.

Last Mile: Se refiere al último tramo de una línea de comunicación (línea telefónica o cable óptico) que da el servicio al usuario.

Multi-Point (Multipunto): tipo de red en la cual cada canal de datos se puede usar para comunicarse con diversos nodos. En una red multipunto solo existe una línea de comunicación cuyo uso esta compartido por todas las terminales en la red. La información fluye de forma bidireccional y es discernible para todas las terminales de la red.

Multiplexacion: es la combinación de dos o más canales de información en un solo medio de transmisión usando un dispositivo llamado multiplexor. El proceso inverso se conoce como demultiplexación.

Multiradio: consiste en el manejo de la comunicación en cualquier frecuencia: desde teléfonos celulares hasta UWB. Los dispositivos tienen la capacidad de activar y desactivar radios según se necesite administrar energía, administrar la conexión y aumentar la comunicación con una pila de software de conexión mixta en red. La multiradio ofrece un conjunto de innovaciones que proporcionan los beneficios que representa una conexión permanente y óptima, sin importar dónde esté el dispositivo.

Point-To-Point (punto a punto): tipo de red en las que se usa cada canal de datos para comunicar únicamente a 2 nodos. En una red punto a punto, los dispositivos en red actúan como socios iguales, o pares entre sí.

Throughput: En redes de comunicaciones, el rendimiento de procesamiento es la cantidad de datos digitales por la unidad del tiempo que se entrega sobre

un acoplamiento físico o lógico, o que está pasando con cierto nodo de red. Por ejemplo, puede ser la cantidad de datos que se entreguen a un cierto Terminal de la red u ordenador huésped, o entre dos computadoras específicas. El rendimiento de procesamiento se mide generalmente en pedacito por segundo (bit/s o los BPS), de vez en cuando en paquetes de los datos por los paquetes del segundo o de los datos por time slot. El término corresponde a la consumición digital de la anchura de banda. El rendimiento de procesamiento de sistema o el rendimiento de procesamiento del agregado es la suma de las tarifas de datos que se entregan a todos los terminales en una red.

VoIP (Voz sobre IP): es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol). Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla en forma de circuitos como una compañía telefónica convencional.

Wi-Fi (Wireless Fidelity): La expresión que se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, *Wireless Local Area Netwoks*).

Wimax (Interoperabilidad Mundial para Acceso por Microondas): es un estándar de transmisión inalámbrica de datos (802.16 MAN) que proporciona accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base.

RESUMEN

Las redes inalámbricas enmalladas metropolitanas 802.11s están siendo utilizadas para ofrecer acceso a los ciudadanos en las denominadas municipalidades WI-FI. Son muchas las ciudades que están usando esta tecnología como es el caso de Londres, Nueva York y San Francisco ya que son auto configurables, auto reparables y muy seguras. Además no operan de manera singular ni aislada, sino que trabajan en conexión con otras redes. Un aspecto fundamental del funcionamiento de las redes en malla es que la comunicación entre un nodo y cualquier otro puede ir más allá del rango de cobertura de cualquier nodo individual. Esto se logra haciendo un enrutamiento multisaltos, donde cualquier par de nodos que desean comunicarse podrán utilizar para ello otros nodos inalámbricos intermedios que se encuentren en el camino. Esto es importante si se compara con las redes tradicionales Wi-Fi, donde los nodos deben de estar dentro del rango de cobertura de un AP y sólo se pueden comunicar con otros nodos mediante los AP que, a su vez, necesitan de una red cableada para comunicarse entre sí. Con las redes en malla no es necesario tener AP, pues todos los nodos pueden comunicarse directamente con los vecinos dentro de su rango de cobertura inalámbrica y con otros nodos distantes. Además sus propiedades de autoconfiguracion y reconfiguracion son posibles gracias a los sofisticados protocolos que permiten el descubrimiento automático de rutas y el redescubrimiento de las mismas en caso de falla en algunos nodos. Dada esta capacidad de reconfiguración, las redes en malla también resultan ser flexibles y robustas, pues la falla de uno o más nodos no impide el funcionamiento de la red y no se presenta un punto crítico de falla. En la actualidad son muchos los fabricantes y vendedores de productos que soportan redes Mesh como son Tropos Network, Belair, Firetire, Skypilot entre otros., pero aun se continua estudiando y mejorando el estándar 802.11s ya que presenta problemas que se necesitan resolver.

En esta monografía se mencionaran cada una de las características de las redes Mesh, así como sus protocolos, aplicaciones y fabricantes.

INTRODUCCION

Las redes Mesh son un conjunto autónomo y espontáneo de routers móviles, conectados por enlaces inalámbricos que no precisan de una infraestructura fija. Se proyectan para operar en ambientes hostiles e irregulares, y sus aplicaciones son extensas tales como redes de área personal, entornos militares, entornos ciudadanos y operaciones de emergencia. Estas redes plantean grandes retos técnicos y funcionales debido a la hostilidad del medio inalámbrico que representan un gran avance tecnológico de los últimos tiempos.

Esta monografía inicia con una fundamentación de las redes Mesh, primero se exponen los conceptos generales tales como FDMA, OFDM y multiplexación en frecuencia, luego se hace referencia a las tecnologías inalámbricas comúnmente usadas en las WMNs como son Wi-Fi y Wimax. También se muestran los sistemas enmallados de primera, segunda y tercera generación. Por ultimo se habla sobre el futuro de las redes Mesh y las nuevas tecnologías que se avecinan.

El capitulo 2 trata de la infraestructura de las WMNs, aquí se tocan temas relacionados con las topologías de las redes inalámbricas, entre estas están las basadas en infraestructura, Ad-Hoc e Hibridas. También se habla acerca de la estandarización de las redes Mesh 802.11s. Además se hace referencia a la operación de las WMNs, se explican sus características, funcionamiento y alcance.

El capitulo 3 trata de la arquitectura de las WMNs, se exponen sus problemas funcionales entre los cuales están la capacidad, confiabilidad, manejo de recursos, entre otros. También se habla de los diferentes tipos de protocolos según su clasificación que puede ser basada en topología, posición o hibrido.

En el capitulo 4 se hace una descripción de las tecnologías de seguridad en una red Mesh, también se habla del uso de las capas del modelo OSI en las WMNs, y se hace mucho énfasis en la capa Mac, se habla de los protocolos, antenas usadas, tablas de ruteo entre otras. Y por ultimo se hace referencia a los fabricantes que hoy en día están comercializando equipos para las WMNs, entre estos están las compañías Troposnetwork y Firetire que son unas de las que mas se han expandido en el mundo debido a la rentabilidad y buen funcionamiento de sus productos.

1. FUNDAMENTACION DE WMN

El importante desarrollo y avance de las telecomunicaciones ha tenido varios factores para ayudas de su progreso y una de ellas es la modulación de frecuencia.

Antes de desarrollar el tema de la investigación es necesario recordar algunos conceptos claves y además básicos para comprender esta monografía.

En este capitulo se mencionaran algunos conceptos básicos y características de toda red mesh inalámbrica relacionados con las telecomunicaciones. Como es el concepto de FM la cual fue utilizada en un principio por la radiodifusión para crear canales radiofónicos, pero que con el avanzar de los tiempos se ha dado a conocer diferentes métodos de modulación de frecuencia que han aportado un gran desarrollo a las telecomunicaciones.

1.1 CONCEPTOS BASICOS

Características de FM

La frecuencia modulada posee varias ventajas sobre el sistema de modulación de amplitud (AM) utilizado alternativamente en radiodifusión. La más importante es que al sistema FM apenas le afectan las interferencias y descargas estáticas. Las características principales de la frecuencia modulada son: su modulación y su propagación por ondas directas como consecuencia de su ubicación en la banda de frecuencia de VHF.

La modulación en frecuencia consiste en variar la frecuencia de la portadora proporcionalmente a la frecuencia de la onda moduladora (información), permaneciendo constante su amplitud. A diferencia de la AM, la modulación en frecuencia crea un conjunto de complejas bandas laterales cuya profundidad

(extensión) dependerá de la amplitud de la onda moduladora. Como consecuencia del incremento de las bandas laterales, la anchura del canal de la FM será más grande que el tradicional de la onda media, siendo también mayor la anchura de banda de sintonización de los aparatos receptores. La principal consecuencia de la modulación en frecuencia es una mayor calidad de reproducción como resultado de su casi inmunidad hacia las interferencias eléctricas. En consecuencia, es un sistema adecuado para la emisión de programas (música) de alta fidelidad.

Espectro disperso

El espectro disperso es una técnica de comunicación que por los altos costos que acarrea, se aplicó casi exclusivamente para objetivos militares, hasta comienzos de los años noventa. Sin embargo, comienza a surgir lentamente un mercado comercial.

Las LAN (Local Area Networks: Area de redes locales) son redes que comunican ordenadores entre sí a través de cables, lo que hace posible que por ordenador se pueda enviar correo dentro de un edificio determinado, por ejemplo. Actualmente se venden también 'Radio LAN' (RLAN), que constituyen una comunicación inalámbrica entre una cantidad determinada de ordenadores.

Para poder captar un programa radial hay que sintonizar con un emisor que está en una determinada frecuencia. Emisores diferentes están en diferentes frecuencias. Cada emisor ocupa un pequeño trozo de la banda emisora dentro de la cual se concentra la potencia de emisión irradiada. Ese pequeño trozo, también llamado amplitud de banda, tiene que ser lo suficientemente grande como para que los emisores cercanos no sean interferidos. A medida que la amplitud de banda es más angosta, pueden funcionar más emisores en una banda de frecuencia.

La radio-receptora se puede sintonizar siempre en una frecuencia. Esa frecuencia es retransmitida por el emisor con una amplitud de banda lo más pequeña posible, pero lo suficientemente grande como para transmitir la información deseada. Este tipo de receptores se llama receptores de banda angosta (estrecha).

Por el contrario, en Spread Spectrum no se elige por una amplitud de banda lo más pequeña posible, sino justamente por una lo más grande posible. La amplitud de banda es mayor de lo que se necesita estrictamente para la transmisión de la información. Esta mayor amplitud de banda puede obtenerse de dos maneras. La primera es codificar la información con una señal seudo-fortuita (aleatoria). La información codificada se transmite en la frecuencia en que funciona el emisor para lo cual se utiliza una amplitud de banda mucho mayor que la que se usa sin codificación (secuencia directa). La segunda posibilidad es codificar la frecuencia de trabajo con una señal seudo-fortuita (aleatoria), por lo que la frecuencia de trabajo cambia permanentemente. En cada frecuencia se envía un pequeño trozo de información (Frecuencia Hopping).

Salto en frecuencia (FHSS: FREQUENCY HOPPING SPREAD SPECTRUM)

FHSS de banda estrecha consiste en que una trama de bits se envía ocupando ranuras específicas de tiempo en diversos canales de radio-frecuencia. FHSS de banda ancha consiste en que durante el intervalo de 1 bit se conmutan diversos canales de radio-frecuencia.

Al igual que Ethernet los datos son divididos en paquetes de información, solo que estos paquetes son enviados a través de varias frecuencias, esto es conocido como "Hopping Pattern", la intención de enviar la información por varias frecuencias es cuestión de seguridad, ya que si la información fuera enviada por una sola frecuencia sería muy fácil interceptarla

Además, para llevar acabo la transmisión de datos es necesario que tanto el aparato que envia como el que recibe información coordinen este denominado "Hopping Pattern". El estandard IEEE 802.11 utiliza FHSS, aunque hoy en dia la tecnologia que sobresale utilizando FHSS es Bluetooth

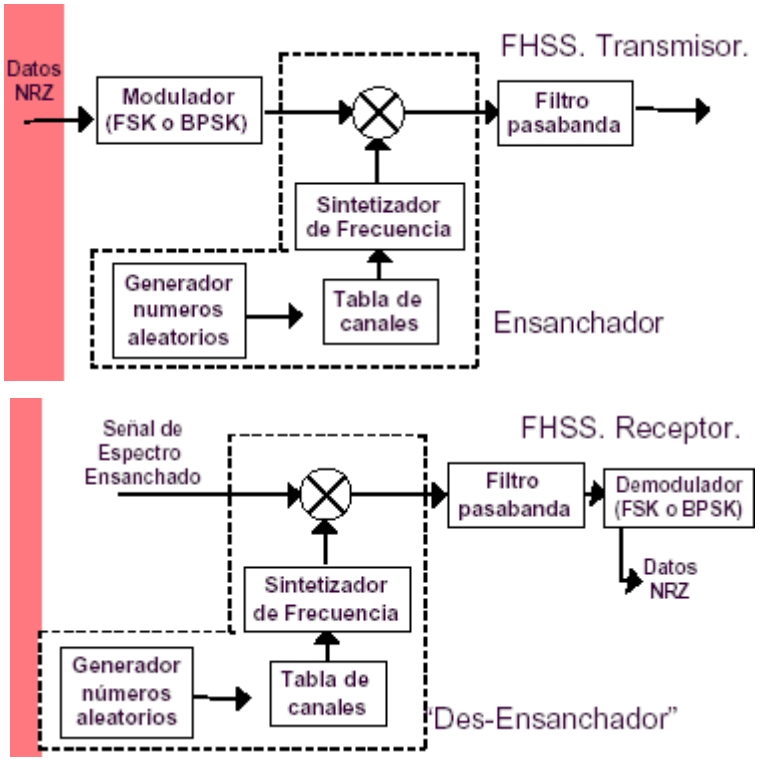


Fig 1.1Transmisión y Recepción en FHSS

Acceso inalámbrico

El acceso inalámbrico es aquél en que los usuarios obtienen su servicio mediante un enlace óptico o de radio-frecuencias.

Para tener acceso, se han creado protocolos que garantizan que el acceso obedezca a algún criterio acordado: acceso justo, dar prioridad a la información sensible a retardos, ofrecer garantías de transporte confiable, etc.

El acceso puede ser mantenido indefinidamente o ser asignado temporalmente por demanda de cada usuario:

FAMA (Fixed Assigned Multiple Access)

DAMA (Demand Assigned Multiple Access)

Por lo general, estas modalidades se utilizan en enlaces satelitales, aunque también es factible encontrarlo en enlaces terrestres.

El acceso inalámbrico en modo de asignación dinámica puede presentar diversas variantes, cada una de las cuales se adapta mejor a la aplicación específica.

FDMA

FDMA es una tecnología de acceso múltiple por división de frecuencias, que corresponde a una tecnología de comunicaciones usado en los teléfonos móviles de redes GSM.

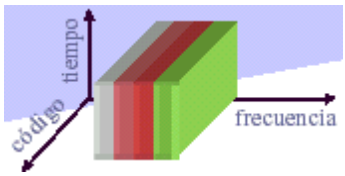


Fig 1.2 Representación grafica de la tecnología FDMA

FDMA es la manera más común de acceso truncado. Con FDMA, se asigna a los usuarios un canal de un conjunto limitado de canales ordenados en el dominio de la frecuencia. Los canales de frecuencia son muy preciados, y son asignados a los sistemas por los cuerpos reguladores de los gobiernos de acuerdo con las necesidades comunes de la sociedad. Cuando hay más usuarios que el suministro de canales de frecuencia puede soportar, se bloquea el acceso de los usuarios al sistema. Cuantas más frecuencias se disponen, hay más usuarios, y esto significa que tiene que pasar más

señalización a través del canal de control. Los sistemas muy grandes FDMA frecuentemente tienen más de un canal de control para manejar todas las tareas de control de acceso. Una característica importante de los sistemas FDMA es que una vez que se asigna una frecuencia a un usuario, ésta es usada exclusivamente por ese usuario hasta que éste no necesite el recurso. FDMA utiliza un filtro RF para evitar las interferencias con canales adyacentes.

(FDM) MULTIPLEXACIÓN POR DIVISIÓN EN FRECUENCIA

El empleo de técnicas de multiplexación por división en frecuencia requiere el uso de circuitos que tengan un ancho de banda relativamente grande. Este ancho de banda se divide luego en subcanales de frecuencia.

Cuando una portadora usa FDM para la multiplexación de conversaciones de voz en un circuito ordinario, el paso-banda de 3 Khz de cada conversación se traslada hacia arriba en la frecuencia según un incremento fijo de frecuencia. Este cambio de frecuencia coloca la conversación de voz en un canal predefinido del circuito multiplexado de FDM.

En el destino, otro FDM demultiplexa la voz, cambiando el *spectrum* de frecuencia de cada conversación hacia abajo con el mismo incremento de frecuencia que se hizo al principio hacia arriba.

El principal uso de FDM es para permitir a las portadoras llevar un gran número de conversaciones de voz simultáneamente en un único circuito común enrutado

Las técnicas de multicanalización son formas intrínsecas de modulación, permitiendo la transición de señales múltiples sobre un canal, de tal manera que cada señal puede ser captada en el extremo receptor. Las aplicaciones de la multicanalización comprenden telemetría de datos, emisión de FM estereofónica y telefonía de larga distancia.
FDM es un ambiente en el cual toda la banda de frecuencias disponible en el enlace de comunicaciones es dividida en subbandas o canales individuales. Cada usuario tiene asignada una frecuencia diferente. Las señales viajan en

paralelo sobre el mismo canal de comunicaciones, pero están divididos en frecuencia, es decir, cada señal se envía en una diferente porción del espectro. Como la frecuencia es un parámetro analógico, por lo regular el uso de esta técnica de multicanalización es para aplicaciones de televisión. Las compañías de televisión por cable utilizan esta técnica para acomodar su programación de canales.

(OFDM) ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING

OFDM es una tecnología de modulación digital, una forma especial de modulación multi-carrier considerada la piedra angular de la próxima generación de productos y servicios de radio frecuencia de alta velocidad para uso tanto personal como corporativo. La técnica de espectro disperso de OFDM distribuye los datos en un gran número de carriers que están espaciados entre sí en distintas frecuencias precisas. Ese espaciado evita que los demoduladores vean frecuencias distintas a las suyas propias.

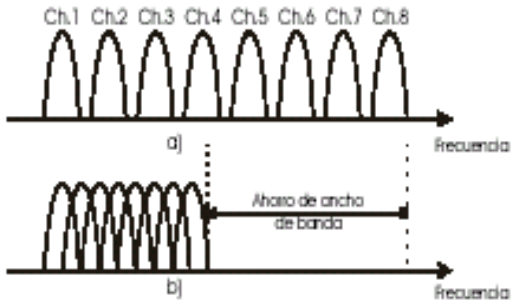


Fig 1.3 a)Técnica Multiportadora convencional b)Modulación con portadoras ortogonales

OFDM[1] tiene una alta eficiencia de espectro, resistencia a la interfase RF y menor distorsión multi-ruta. Actualmente OFDM no sólo se usa en las redes inalámbricas LAN 802.11a, sino en las 802.11g, en comunicaciones de alta

[1] http://en.wikipedia.org/wiki/OFDM

velocidad por vía telefónica como las ADSL y en difusión de señales de televisión digital terrestre en Europa, Japón y Australia.

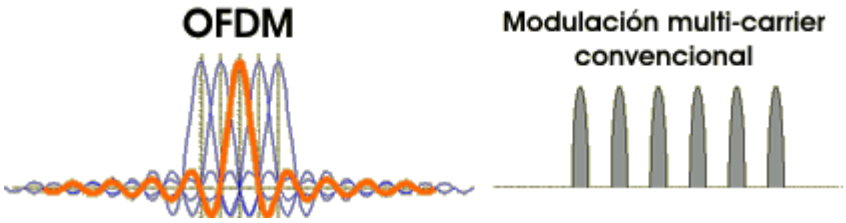


Fig 1.4.Espectro de OFDM traslapado

WDM

Esta técnica conceptualmente es idéntica a FDM, excepto que la multicanalización y involucra haces de luz a través de fibras ópticas. La idea es la misma, combinar diferentes señales de diferentes frecuencias, sin embargo aquí las frecuencias son muy altas ($1x10^{14}$ Hz) y por lo tanto se manejan comúnmente en longitudes de onda (wavelenght). WDM[2], así como DWDM son técnicas de multicanalización muy importantes en las redes de transporte basadas en fibras ópticas.

En resumen, los multicanalizadores optimizan el canal de comunicaciones, son pieza importante en las redes de transporte y ofrecen las siguientes características:

- Permiten que varios dispositivos compartan un mismo canal de comunicaciones
- Útil para rutas de comunicaciones paralelas entre dos localidades
- Minimizan los costos de las comunicaciones, al rentar una sola línea privada para comunicación entre dos puntos.

[2] http:// alegsa.com.ar/Dic/**wdm**.php

- Normalmente los multicanalizadores se utilizan en pares, un mux en cada extremo del circuito.
- Los datos de varios dispositivos pueden ser enviados en un mismo circuito por un mux. El mux receptor separa y envía los datos a los apropiados destinos
- Capacidad para compresión de datos que permite la eliminación de bits redundantes para optimizar el ancho de banda.
- Capacidad para detectar y corregir errores entre dos puntos que están siendo conectados para asegurar que la integridad y precisión de los datos sea mantenida.
- La capacidad para administrar los recursos dinámicamente mediante con niveles de prioridad de tráfico.

1.2 TECNOLOGIAS INALAMBRICAS ORIENTADAS A LAS WMNs

1.2.1 Uso de wi-fi para el acceso de áreas metropolitanas

WI-FI es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI. A este estándar se le han hecho modificaciones a través del hardware y software que permiten que los productos Wi-Fi se conviertan en una opción de instalación de acceso para áreas metropolitanas. Estas dos modificaciones más importantes tratan dos modelos de uso diferentes:

• Uso de acceso fijo o last mile (801.11 con Antenas de Alta Ganancia)
• Uso de acceso portátil o hot zone (redes de malla 802.11)

Los productos Wi-Fi asociados con la opción de instalación de acceso para áreas metropolitanas usan estas frecuencias de radio diferentes:

• El estándar 802.11 usa 5 GHz en un inter-enlace AP a AP.
• Los estándares 802.11b y 802.11g usan 2.4 GHz[3].

Los estándares 802.11a, 802.11b y 802.11g usan bandas de frecuencia; los dispositivos basados en estos estándares no se interfieren mutuamente. Por otro lado, los dispositivos en bandas diferentes no se comunican; por ejemplo, un radio 802.11a no puede conversar con un radio 802.11b.
A la fecha, las instalaciones más comunes de WISPs para acceso para áreas metropolitanas son los estándares 802.11b y 802.11g debido a la interoperabilidad y al mayor alcance que llega en la banda de 2.4 GHz.

[3]IEEE Standard. Op cit.

Cada estándar también difiere en el tipo de tecnología de modulación de radio usada, como se muestra a continuación:

• El estándar 802.11b usa espectro ensanchado por secuencia directa (DSSS) y soporta velocidades de ancho de banda de hasta 11 Mpbs.

• Los estándares 802.11a y 802.11g usan multiplexación por división de frecuencia ortogonal (OFDM) y soportan velocidades de hasta 54 Mpbs[4]. Como OFDM es más adaptable a ambientes externos y a la interferencia, se lo usa más frecuentemente en soluciones de acceso para áreas metropolitanas.

La tecnología OFDM usa optimización de sub-portadoras (sub-carriers) para usuarios basados en condiciones de frecuencia de radio.

Ortogonal significa que las frecuencias en las que la portadora (carrier) se divide son elegidas para que el pico de una frecuencia coincida con los nulos de la frecuencia adyacente. El flujo de dados es convertido de seriado a paralelo, y cada flujo de datos paralelo es mapeado por un bloque de modulación. Los datos modulados pasan a un bloque de transformación rápida de Fourier rápido (IFFT) para procesamiento. El bloque IFFT convierte las frecuencias moduladas discretas en una señal de dominio de tiempo que se usa para impulsar el amplificador de la frecuencia de radio (RF).

Esta eficiencia espectral mejorada es un gran beneficio para las redes OFDM, lo que las hace ideales para conexiones de datos de alta velocidad en soluciones fijas y móviles.

El estándar 802.11 ofrece 64 sub-portadoras. Estas portadoras son enviados desde la estación base (BS) o AP a la estación del abonado (subscriber station - SS) o cliente y reconstituidos en el lado del cliente. En situaciones “non-line-of-sight” - NLOS (sin línea de vista), estas portadoras chocarán contra paredes, edificios, árboles y otros objetos, que reflejarán la señal y crearán una interferencia multi-path.

[4] IEEE Standard. Op cit.

Cuando las señales de la portadora llegan al cliente para su reconstitución, las señales de la portadora individual ya están demoradas. Por ejemplo, una portadora puede haberse reflejado una vez y llegado 1 µ más tarde que otro, y el segundo puede haberse reflejado dos veces y llegar 2 µ más tarde. Cuanto más sub-portadoras sobre la misma banda resulta en sub-portadoras menores, que equivale a mayores períodos de símbolo de OFMD. En consecuencia, el mismo porcentaje de tiempo de guarda o prefijo cíclico (CP) dará valores cíclicos mayores en tiempo para mayores demoras y aumentarán la resistencia a interferencia multi-path. Como los estándares 802.11a y 802.11g usan OFDM, son más elásticos que el estándar 802.11b en ambientes propensos a multi-paths. Estos factores se tomaron en cuenta para elaborar el estándar 802.16-2004.

La topología de red de malla amplía el alcance de LANs y WLANs tradicionales. En una topología de red de malla, se conecta cada nodo y se comparten los protocolos de comunicación en todos los nodos. Una infraestructura Wi-Fi se forma cuando enlaces 802.11 interconectan un grupo de nodos basados en 802.11a, b o g. El estándar 802.11 es el más usado en enlaces AP a AP debido a su desempeño y la superposición con transmisiones 802.11b o 802.11g (Ver tabla 1.1). Las redes de malla aprenden automáticamente y mantienen configuraciones dinámicas de path. Los dispositivos inalámbricos en una topología de red de malla crean un path para datos entre sí sobre un espectro de exención de licencia a 2.4 o 5 GHz con velocidades de hasta 54 Mbps.

Implementaciones dorsales de infraestructuras de malla Wi-Fi se basan en soluciones propias. Estas soluciones propias pueden soportar VoIP y QoS. También pueden aumentar el alcance de cobertura del límite de 100 metros de

Estándares de la especificación de redes WLAN IEEE 802.11	
Estándar	**Alcance del estándar**
802.11a	Red WLAN de 54 Mbps,5Ghz
802.11b	11Mbps, 2.4Ghz
802.11e	Calidad de servicio (QoS)
802.11g	Red WLAN de 54Mbps, 2.4Ghz
802.11h	Administración del espectro(802.11a)
802.11i	Seguridad
802.11k	Medición de recursos
802.11s	Redes en malla

Tabla 1.1 Estándares Wi-Fi (IEEE 802.11)

Wi-Fi a más de 10 km. Además, el desempeño puede aumentarse del límite de 54 Mbps de Wi-Fi a más de 100 Mbps. Sin embargo, estas implementaciones no son interoperables, tienen escalabilidad limitada y en ciertas instalaciones se encuentran limitadas por backhaul por cable (wired backhaul). La ratificación de 802.11s estandarizará la topología de red de malla Wi-Fi. Se calcula que el estándar 802.11s sea ratificado en el año 2007. Las topologías de red de malla Wi-Fi pueden ser utilizadas como solución last mile pero son mejores para áreas extensas con acceso 802.11.

A veces a la red de malla también se la denomina red multi-hop (de saltos múltiples). Las topologías de malla ofrecen una arquitectura que puede mover datos entre nodos de forma eficiente.

Dentro de una red de malla, los pequeños nodos actúan como enrutadores. Los nodos se instalan en una extensa área (como, por ejemplo, un barrio o una escuela). Cada nodo transmite una señal baja capaz de alcanzar los nodos vecinos, cada uno de los cuales transmite la señal al próximo nodo, con el proceso que se repite hasta que los datos llegan a su destino. Una ventaja de esta topología es la capacidad que tiene la instalación para circundar un gran

obstáculo, como ser una montaña que impediría que el abonado llegase a una estación base. En una red de malla, los abonados bloqueados pueden llegar a la estación base indirectamente por medio de otros nodos. Aun una pequeña cantidad de malla puede mejorar mucho la cobertura de la estación base si se colocan pequeños nodos.(ver fig 1.5)

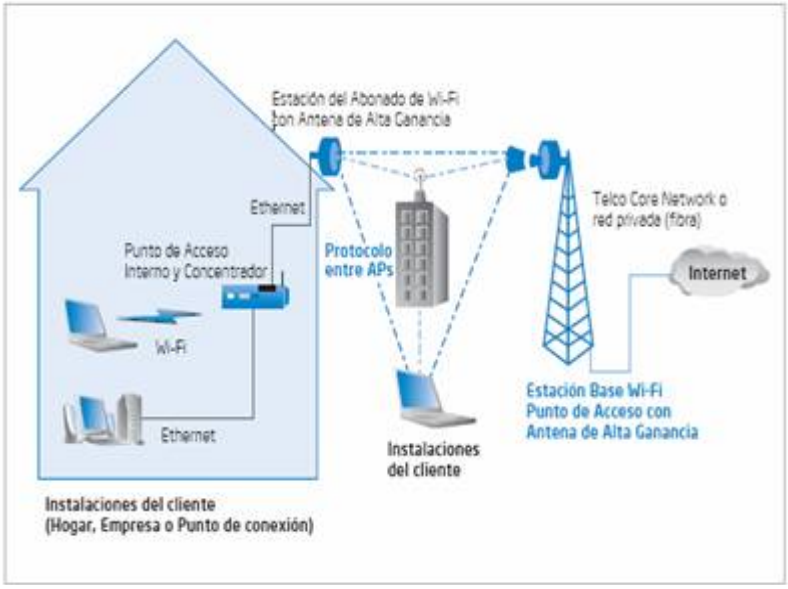


Fig. 1.5 Red de malla 802.11

1.2.2 USO DE WIMAX PARA EL ACCESO DE AREAS METROPOLITANAS

WiMAX es la certificación mundial que trata la interoperabilidad en los productos basados en los estándares IEEE 802.16. El estándar IEEE 802.16 con revisiones específicas trata dos modelos de uso:

• Fijos

• Portátiles

El estándar IEEE 802.16-2004 (que revisa y reemplaza a las versiones IEEE 802.16a y 802.16REVd) está elaborado para los modelos de uso del acceso fijo. También se conoce a este estándar como “inalámbrico de fijos” porque usa

una antena instalada donde se encuentra el abonado. La antena se instala en un techo o mástil, similar al plato de la televisión satelital. La IEEE 802.16-2004 también trata de instalaciones internas, en cuyo caso pueden no ser tan robustas como las instalaciones externas.

El estándar 802.16-2004 es una solución inalámbrica para acceso a Internet de banda ancha que ofrece una solución interoperable de clase de portadora para last mile. La solución WiMAX de Intel para acceso fijo funciona en las bandas con licencia de 2.5 GHz, 3.5 GHz y en la exenta de licencia de 5.8 GHz. Esta tecnología ofrece una alternativa inalámbrica al módem por cable, a la línea de abonado digital de cualquier tipo (xDSL), a circuitos de transmisión/intercambio (Tx/Ex) y a circuitos de nivel de portadora óptica (OC-x).

El estándar 802.16e usa un acceso multiplexado por división de frecuencia ortogonal (OFDMA), que se parece a un OFDM pues divide a las portadoras en múltiples sub-portadoras. Sin embargo, el OFMDA va un paso más allá al agrupar a las sub-portadoras en sub-canales. Un cliente o estación de abonado puede transmitir utilizando todos los sub-canales dentro del espacio de la portadora, o clientes múltiples pueden transmitir cada uno usando una parte del número total de sub-canales simultáneamente.

El estándar IEEE 802.16-2004 mejora la entrega last mile en varios aspectos claves:

• Interferencia multi-path
• Diferencia de demora
• Robustez

Una interferencia multi-path y una diferencia de demora mejoran el desempeño en situaciones en las que no hay path directo line-of-sight (sin línea de vista) entre la estación base y la estación del abonado.

El control de acceso a medios (MAC) es optimizado para enlaces de larga distancia porque está proyectado para tolerar demoras y variaciones de demora más largas. La especificación 802.16 alberga mensajes para permitir

que la estación base consulte a la estación del abonado, aunque exista un cierto tiempo de demora.
Los equipos WiMAX que operan en las bandas de frecuencia exentas de licencia usarán dúplex por división de tiempo (TDD); los equipos que operan en bandas de frecuencia con licencia usarán TDD o dúplex de división de frecuencia (FDD). El estándar IEEE 802.16-2004 usa un OFMD para optimización de servicios inalámbricos de datos. El sistema se basa en los estándares 802.16-2004 emergentes que son las únicas plataformas de redes inalámbricas de áreas metropolitanas (WMAN) basadas en un OFMD.
En el caso de 802.16-2004, la señal se divide en 256 portadoras en vez de 64 como en el estándar 802.11. Cuanto más sub-portadoras sobre la misma banda resulta en sub-portadoras más estrechas, que equivalen a períodos de símbolo. El mismo porcentaje de tiempo de guaria o prefijo cíclico (CP) provee mayores valores absolutos en tiempo para una diferencia de demora e inmunidad multi-path mayores.

El estándar 802.16e es una enmienda a la especificación base 802.16-2004 y su objetivo es el mercado móvil al agregar portabilidad y el recurso para clientes móviles con adaptadores IEEE 802.16a para conectar directamente la red WiMAX al estándar.

Con la atención enfocada en WiMAX, es fácil olvidarse que Wi-Fi también está evolucionando rápidamente. Las radios Wi-Fi están apareciendo no sólo en laptops y asistentes personales digitales (PDAs) sino también en equipos tan diversos como teléfonos móviles, parquímetros, cámaras de seguridad y equipos de entretenimiento del hogar. Como resultado de su creciente adopción, Wi-Fi seguirá haciéndose más rápida, segura, fiable y con más recursos. Estos avances, a su vez impulsarán la adopción continuada.

Actualmente para la conectividad intra-malla, Wi-Fi ofrece ventajas. Los chipsets y radios Wi-Fi aprobados por la industria están disponibles fácilmente y son económicos. Funcionan en regiones del espectro sin licencia. El

resultado es una tecnología intra-malla[5] que ofrece gran desempeño al menor costo (Ver Fig 1.6). Esencialmente, las conexiones intra-malla backhaul pueden reducir los costos relacionados con el cableado de cada nodo. Cuando estén disponibles, los APs Wi-Fi y WiMAX ofrecerán mejor desempeño y una solución mucho más robusta.

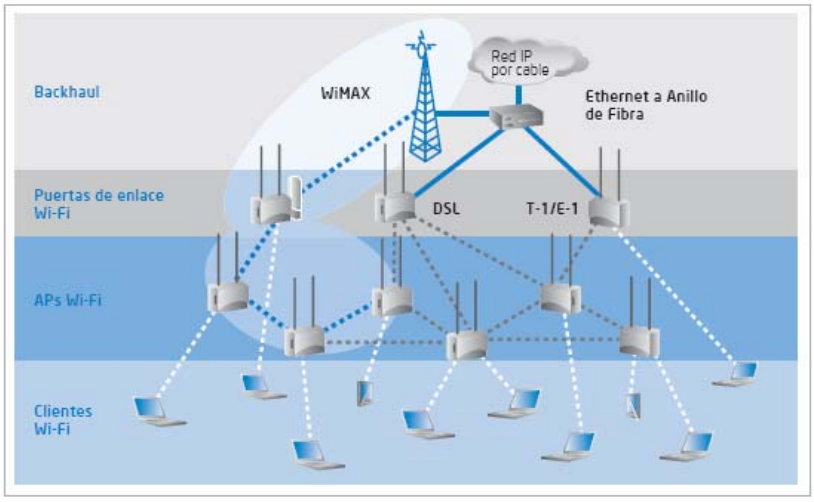


Fig 1.6 Wimax como una opción intra-malla backhaul

[5] http://www.intel.com/espanol/netcomms/wp03_espanhol.pdf

1.3 SISTEMAS ENMALLADOS DE PRIMERA, SEGUNDA Y TERCERA GENERACION

El mercado de las soluciones para redes inalámbricas enmalladas metropolitana esta todavía en su infancia, por esta razón compañías "pequeñas" como tropos networks Belait Networks, PacketHop, skypilot y Reamad son lideres de esta industria en conjunto con nuevas iniciativas de grandes compañías como Cisco sistem , Nortel Networks y Motorota. Estas implementaciones han sido en su mayoría, redes enmalladas metropolitanas para comunidades pequeñas rurales o para sectores limitados de grandes ciudades, sin embargo este año se han lanzado solicitudes de propuestas para grandes coberturas en Chicago nueva Cork y silicon valley , etc.

1.3.1 Sistemas enmallados de primera generación

Los sistemas inalámbricos de acoplamiento "ad hoc" utilizan un solo radio y proporcionan el servicio (conexión a los dispositivos individuales del usuario) y el backhaul (acoplamientos a través del acoplamiento a la conexión atado con alambre o de la fibra), así que la congestión en enlaces inalámbricos y la contención ocurren en cada nodo.

En una red ad hoc mesh hay un canal de radio en el cual todos los nodos se comunican entre si. Para que los datos sean retransmitidos de un nodo mesh a otro, estos deben ser repetidos de una manera store-and-forward. Un nodo primero recibe los datos y en seguida los retransmite.

Estas operaciones no pueden ocurrir simultáneamente porque, con solamente un canal de radio, la transmisión y la recepción simultáneas interferirían uno con otro. Esta inhabilidad de transmitir y de recibir simultáneamente es una desventaja seria de la arquitectura ad hoc mesh.

Simplemente, si un nodo no puede enviar y recibir al mismo tiempo, pierde el ½ de su ancho de banda mientras que procura retransmitir los paquetes arriba y abajo del camino inalámbrico del backhaul. Una pérdida de ½ con cada salto implica que después de 4 saltos, dejarían un usuario con (½ * ½ * ½ * ½) = 1/16 del ancho de banda disponible en el enlace Ethernet. Esto es una relación $1(2^N)$ donde esta ecuación define la fracción de la anchura de banda que está disponible para un usuario después de N saltos.

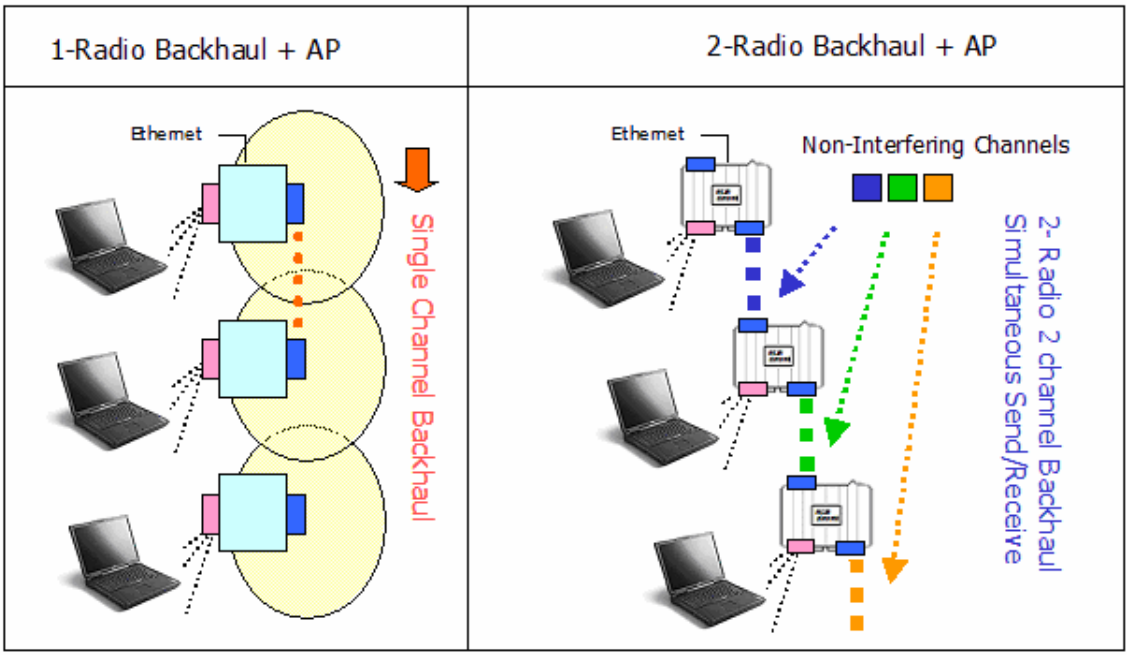


Fig. 1.7 Comparación entre sistemas de uno y dos radios

Entre el grupo de fabricantes de esta generación se destaca Tropos Network. En estos sistemas, los nodos y los clientes comparten el mismo espectro y por lo general sufren interferencias[6]. En el caso de la implementación de doble radio se usa uno para el acceso y otro para el backhaul. Son una solución económica.

[6]Revista EVENCO TECHNOLOGY "redes enmalladas metropolitanas 802.11" junio 2006

1.3.2 Sistemas enmallados de segunda generación

Con el fin de solucionar los problemas de contención y de congestión, el acoplamiento de segunda generación fue desarrollado colocando dos radios en cada nodo, combinando una radio del servicio 802.11b/g con una radio del backhaul 802.11a. Mientras que esto ofreció a excedente de la mejora del funcionamiento el acoplamiento de primera generación, sigue habiendo los problemas. Con demanda pesada del usuario, todavía hay contención y congestión significativas en los acoplamientos del backhaul.

Esta configuración se puede también referir como una red “1+1”, puesto que cada nodo contiene dos radios, uno para proporcionar servicio a los clientes, y otra para crear la red mesh para el backhaul. La denominación “1+1” indica que estos radios están separados uno de otro (Ver Fig.1.7). El radio que proporciona servicio no participa en el backhaul, y el radio que participa en el backhaul no proporciona servicio a los clientes. Estos dos radios pueden funcionar en diversas bandas[7]. Por ejemplo, una radio 2.4 GHz IEEE 802.11 b/g se puede utilizar para el servicio y una radio de IEEE 802.11a (5 GHz) se puede utilizar exclusivamente para el backhaul.
Cisco, Nortel, Belait y Skypilot son fabricantes de este tipo de soluciones. Los radios trabajan entre las bandas de 2.4GHz y 5.8GHz, de este modo se separa el acceso del trafico del backbone, lo cual permite mejor adaptación a cualquier interferencia.

[7] http://www.meshdynamics.com/third_generation.html

1.3.3 Sistemas de tercera generación

En los sistemas de tercera generación cada nodo puede enviar y recibir datos de sus vecinos y adicionalmente a esto se maneja cada acoplamiento por separado, los canales se pueden reutilizar lo cual amplia la disposición del espectro. La inteligencia distribuida en cada nodo permite para que la conmutación de canal ágil evite fuentes de interferencia mientras que todavía permite la disposición y adiciones rápidas a la red sin hilos del acoplamiento (Ver Fig. 1.8)

Los fabricantes que han desarrollado su arquitectura basada en esta generación con productos multi-radio que soportan múltiples configuraciones de red son Belait, Skypilot y Strix Systems.

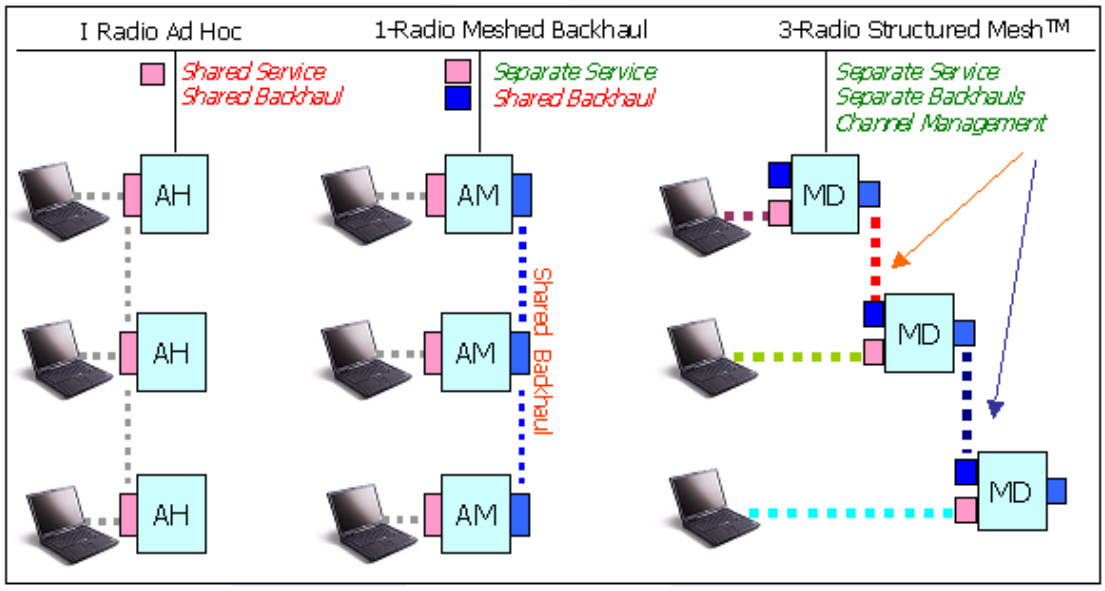


Figura 1.8 sistemas enmallados de acoplamiento

En la tercera generación cada enlace se maneja independientemente, los canales disponibles se pueden reutilizar a través de la red. Esto amplía el espectro disponible, aumentando el funcionamiento de la red 50 veces o más comparado a las soluciones de primeras y segunda generación.

Las soluciones patentadas y patente-pendientes comienzan agregando radios lógicos o físicos adicionales a cada nodo. Una radio se utiliza para crear un enlace a su (más cerca la fuente alambrada o al nodo “raíz”) nodo upstream. Otra radio crea un enlace downstream al nodo vecino siguiente. Diferente a la solución de segunda generación, estos dos radios pueden hacer uso diversos canales.

La inteligencia distribuida en cada nodo permite para que la conmutación de canal evite fuentes de interferencia mientras que todavía permite la disposición y adiciones rápidas a la red mesh.

1.4 FUTURO DE LAS REDES MESH

En los próximos dos años la IEEE hará sus últimos esfuerzos por mejorar la estandarización de las redes mesh. Establecimiento de una red mesh será asumido por los vendedores de los productos que incorporan el estándar 802.11s con el fin de que el público adopte esta tecnología.

Según estudios realizados en el 2006 se predice que la tecnología de redes mesh será acogida los próximos 3 años, lo que garantiza que dichos productos estarán muy pronto en el mercado con el fin de satisfacer todas las necesidades de los clientes.

Por otro lado en un futuro se seguirán teniendo diversos tipos de tráfico en la red, por lo cual deberán realizarse distintas políticas que permitan introducir Calidad de Servicio (QoS) en la red. Los paquetes de voz deben tratarse con

mayor prioridad, debe existir la posibilidad de priorizar siempre algún flujo de tráfico especial para la activación de avisos o alarmas, ya sea mediante una comunicación de voz u otro mecanismo. También pueden introducirse mecanismos de control de congestión, de manera que se evite el envío de tráfico por rutas que se presenten muy saturadas, y se aprovechen otros caminos posibles entre fuente y destino a través de la red mallada. También deben evaluarse los distintos tipos de hardware disponibles para realizar funciones de encapsulado de la información mediante interfaces y protocolos estándar, o bien, la realización de controladores específicos para los dispositivos necesarios.

2. INFRAESTRUCTURA DE LA WMN

2.1 TOPOLOGIAS DE REDES INALAMBRICAS

Es importante identificar las diferencias entre la topología y el modo de funcionamiento de los dispositivos inalámbricos. La topología se refiere a la disposición lógica de los dispositivos, mientras que el modo de funcionamiento hace referencia al modo de actuación de cada dispositivo dentro de la topología escogida. Las redes Mesh WLAN fueron principalmente construidas para casas, comercio, barrios, comunidades, municipios, banda ancha s rurales, seguridad pública, negocios pequeños y grandes, grandes empresas y redes militares.

Cada uno de estos mercados representa uno o una combinación de dos importantes topologías Ad Hoc e infraestructura.

2.1.1 Topología Ad-hoc

Una red ad hoc es una red de área local independiente que no está conectada a una infraestructura cableada y donde todas las estaciones se encuentran conectadas directamente unas con otras, esto quiere decir que Dicha red está formada sin la ayuda de ninguna entidad externa ni servidor central. La configuración de una red de área local inalámbrica en modo ad hoc, se utiliza para establecer una red donde no existe la infraestructura inalámbrica o donde no se requieran servicios avanzados de valor agregado[8], como por ejemplo una exposición comercial o colaboración eventual por parte de colegas en una localización remota.

[8]Evenco technology . “redes enmalladas metropolitanas”, octubre 2006

Cada nodo no sólo opera como un fin de sistema, también como un router para retransmitir los paquetes. Los nodos son libres moverse y se organizan ellos mismos en una red. Las redes móviles ad hoc no requieren una infraestructura fija tales como estaciones base, además, es una opción atractiva para tener una red de dispositivos móviles de forma rápida y espontánea. Las redes ad-hoc móviles tienen varias características sobresalientes, como son, las topologías dinámicas, la capacidad reducida de ancho de banda, capacidad variable en las ligas, debido a estas características, las redes móviles ad hoc son particularmente vulnerables a ataques por negación de servicio lanzado por un nodo intruso.

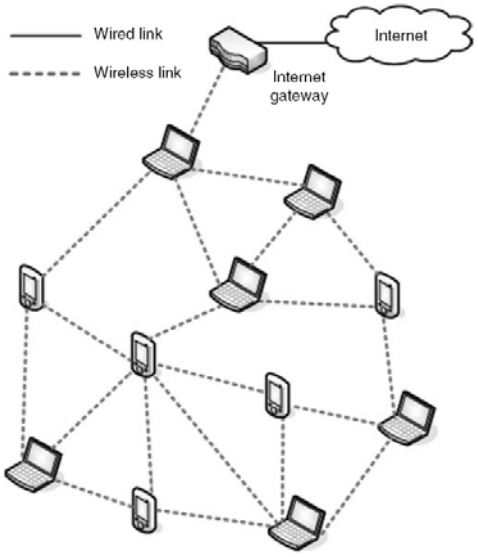


Fig 2.1 topología Ad-hoc (client mesh)

Las redes ad hoc presentan cambios de topología frecuentes e impredecibles debido a la movilidad de sus estaciones. Estas características impiden la utilización de protocolos de encaminamiento desarrollados para redes cableadas y crean nuevos retos de investigación que permitan ofrecer

soluciones de encaminamiento eficientes que superen problemas tales como topología dinámica, recursos de ancho de banda y energéticos limitados.

2.1.2 Topología de infraestructura

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. 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.

Un portátil o dispositivo inteligente, que se caracteriza como una "estación" en términos inalámbricos de una red, primero tiene que identificar los puntos y las redes disponibles de acceso (Ver Fig. 2.2). Esto se hace a través del monitoreo de cuadros periódicos desde puntos de acceso, anunciándose así mismo o probando activamente una red en particular utilizando cuadros de prueba.

La estación elige una red de las que están disponibles y sigue a través de un proceso de autenticación con el punto de acceso. Una vez que se han verificado entre sí el punto de acceso y la estación, se inicia el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y capacidades. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso en la red para dispersar

conocimiento de la ubicación actual de la estación en la red. Sólo después de terminar la asociación la estación puede transmitir o recibir cuadros en la red.

En la modalidad de infraestructura, todo el tráfico en red de las estaciones inalámbricas en la red pasan a través de un punto de acceso para llegar a su destino y una red LAN ya sea cableada o inalámbrica

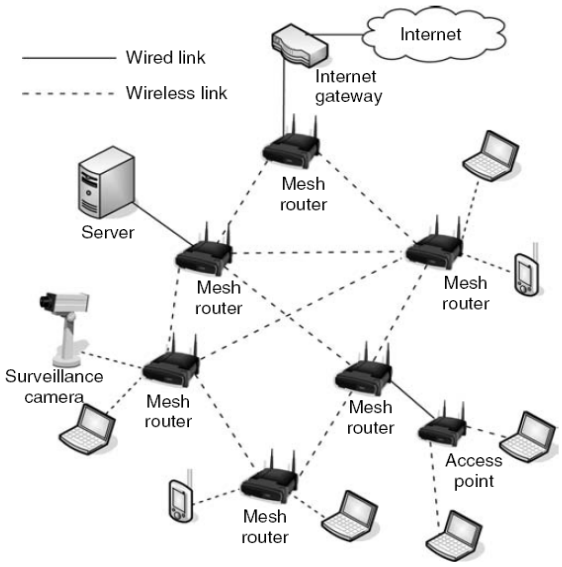


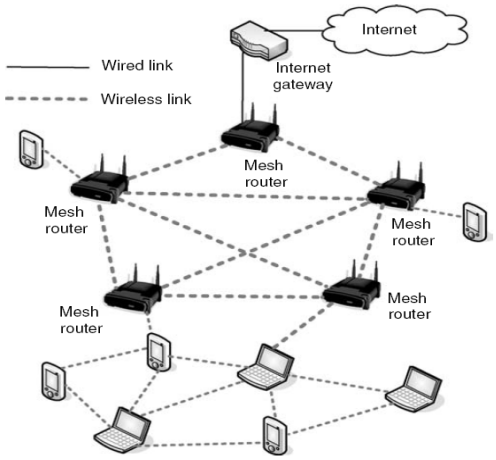
Fig 2.2 Topología de infraestructura

2.1.3 Topología hibrida

Esta topología combina la flexibilidad de Ad Hoc y la robustez de la infraestructura. Un WMN híbrido consiste de routers mesh que conforman la espina dorsal de la red. Además, los clientes móviles pueden participar activamente en la creación del enmallado proporcionando funcionalidades de red, tales como encaminamiento y forwarding de paquetes de los datos[9]. Los clientes que ponen estas funcionalidades en ejecución pueden por lo tanto actuar como extensión automática a la pieza más estática de la infraestructura

[9]Evenco technology . “redes enmalladas metropolitanas”, octubre 2006

del enmallado. Las redes mesh son muy flexibles y permiten combinar las ventajas de las arquitecturas infraestructura y del cliente y En muchas ocasiones, la topología en malla se utiliza junto con otras topologías para formar una topología híbrida.



2.3 Topología Hibrida

2.1.4 Comparación entre redes Mesh y Ad-hoc

La principal diferencia entre estas redes es la movilidad de los nodos y la topología de red. La red AD HOC tiene una alta movilidad donde la topología de red cambia dinámicamente. Por otro lado están las redes mesh las cuales son relativamente estáticas con su nodos fijos retransmitiendo. Por lo tanto, la movilidad de la red de WMNs es muy baja en comparación con redes AD HOC.

Respecto al funcionamiento del encaminamiento, las redes AD HOC son totalmente distribuidas mientras que en las redes MESH pueden ser total o parcialmente distribuido.

Otra diferencia importante entre estas dos categorías de redes es el uso del panorama. Por lo general las redes ad hoc son tenidas en cuenta para usos militares, mientras que las WMNs se utilizan para ambos, usos militares y civiles. Algunos de los usos civiles populares de WMNs incluyen el

aprovisionamiento de los servicios baratos del Internet a alamedas de compras, calles, y ciudades. En esta topología no se requiere movilidad de puntos Backhaul exceptuando el roaming de APs de RF o de otro tipo de puntos que cumplan con estas características. Las casas, comunidades, municipios y los negocios de pequeño y gran tamaño son un ejemplo de redes en infraestructura.

Sin embargo una red IP basada en una subred inalámbrica ad-hoc, también denominada a veces red mesh, está constituida por nodos de funcionalidad idéntica desde el punto de vista de la red, que se comunican entre sí a través de sus radios. No existe una infraestructura jerarquizada, de forma que cada nodo se coordina con los demás como un igual a nivel de enlace y control de acceso al medio. Todos los nodos tienen funcionalidad completa de encaminadores IP y las comunicaciones extremo a extremo suceden por varios saltos (multihop), para lo cual se emplean habitualmente protocolos de encaminamiento dinámico especialmente diseñados para este tipo de redes[10].

[10]http://www.ehas.org:9673/Portales/EHAS/trabajo/C_tecnologia/mesh/RouterWiFi

2.2 ESTANDARIZACIÓN DE LAS REDES MESH 802.11S

Algunas aplicaciones comerciales son interesantes para redes de alta velocidad basadas en redes Mesh de área local se han desarrollado recientemente. Esta tecnología viable económicamente hablando ya que ha sido construida para redes de banda ancha, municipales, de seguridad publica y a gran escala en las llamadas zonas calientes. La arquitectura de las redes Mesh surgió de las redes móviles MANETs usadas para redes militares. El grupo de trabajo IEFT MANET ha estado desarrollando varios protocolos por casi una década. Debido a la popularidad de las redes Mesh y a la cantidad de vendedores que comenzaron a construir dispositivos para redes Mesh se vio la necesidad de crear un estándar que se evidencio en el 2003. El trabajo del grupo de la IEEE que creo el estándar 802.15.5, fue seguido por otro grupo que creo el estándar 802.11s en el 2004. El estándar IEEE 802.11 especifica las operaciones de acceso a las redes entre clientes y Access points (APs). El estándar 802.11 fue creado para Mesh, Backhaul (infraestructura WLAN) y gateway (infraestructura WLAN a redes LAN cableadas) ver figura 2.4.

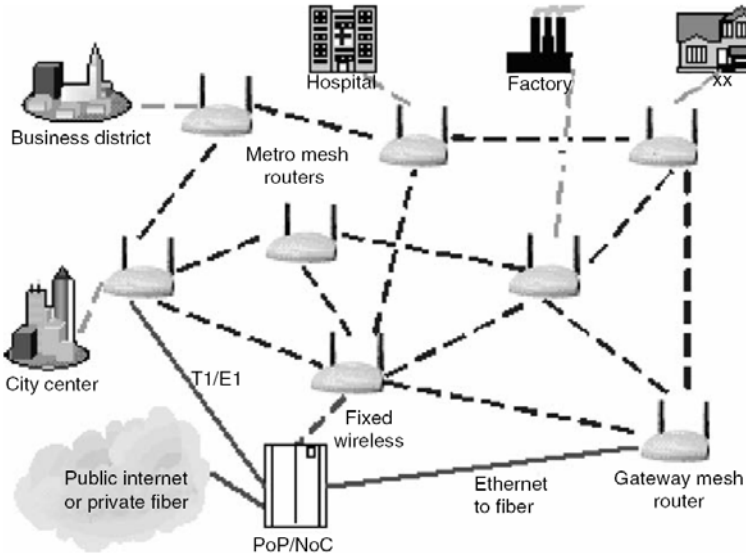


Fig 2.4 Wireless LAN Mesh Networks.

El estándar ofrece flexibilidad, requerida para satisfacer los requerimientos de ambientes residenciales, de oficina, champús, seguridad pública y aplicaciones

militares. La propuesta se enfoca sobre múltiples dimensiones: La subcapa MAC, enrutamiento, seguridad y la de interconexión. Además, define sólo sistemas para ambientes en interiores, pero los principales fabricantes de equipos inalámbricos le están apostando también a sistemas en ambientes exteriores.

El estándar IEEE 802.11 esta soportada por dos modos adicionales de operación, el Ad Hoc que puede comunicarse directamente sin necesidad de usar AP y por el modo de distribución inalámbrica que utiliza AP punto a punto, donde cada AP actúa no solo como estación base sino que son nodos despachadores. Sin embargo el estándar 802.11 puede ser usado para formar redes Mesh Efectivas, algunos funcionamientos, seguridad y manejo de problemas que necesitan ser ubicados.

2.2.1 Propósito general

802.11s es el estándar en desarrollo del IEEE para redes Wi-Fi malladas, también conocidas como redes Mesh. La malla es una topología de red en la que cada nodo está conectado a uno o más nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. En los últimos años han surgido numerosos proyectos de implantación de redes Wi-Fi malladas. El nicho en el que esta tecnología parece haberse desarrollado de forma más espectacular es el de la redes Wi-Fi municipales, promovidas y financiadas por ayuntamientos. También denominadas *Metro Wi-Fi*, es un fenómeno que surgió inicialmente en Estados Unidos y que ha conocido en 2006 su año de mayor desarrollo.

Inicialmente estos sistemas se concibieron como una forma económica de satisfacer las necesidades de comunicaciones de los ayuntamientos y de los servicios de emergencia, pero últimamente la utilización de Wi-Fi se está planteando como una alternativa gratuita o de bajo coste para proporcionar servicios de banda ancha.

2.2.2 Redes Wlan tradicionales y Redes Mesh

Una red WLAN tradicional consta de uno o más puntos de acceso (PA) inalámbrico (Access Point) que se conectan mediante un cable UTP categoría 5 directamente a un switch/hub Ethernet hacia la red cableada. De esta misma manera se podrían conectar más puntos de acceso para incrementar el área de cobertura de la red.

Con las redes Wi-Fi en malla es posible que estos puntos de acceso se puedan conectar y comunicar entre ellos de forma inalámbrica, utilizando las mismas frecuencias del espectro disperso, ya sea en 2.4 GHz o en la banda de 5.8 GHz. Las redes Wi-Fi en malla son menos ambiciosas pero más reales. Para operar sólo necesitan de clientes ordinarios IEEE 802.11

Las redes Wi-Fi en malla son simples, todos los puntos de acceso comparten los mismos canales de frecuencia. Esto hace a los AP relativamente baratos. El único problema es que el canal es compartido, es decir el ancho de banda de la red. Los APs actúan como hubs, así la malla funciona de manera similar a una red plana construida completamente de hubs; es decir todos los clientes contienden para acceder al mismo ancho de banda.
Los sistemas multiradio utilizan un canal para enlaces hacia los clientes Wi-Fi y el resto para enlaces en malla hacia otros APs. En la mayoría de las arquitecturas los enlaces a los clientes están basados en 802.11b/g, debido a que la banda de frecuencia de 2.4 GHz es la más utilizada por el hardware de los equipos Wi-Fi. En cambio la red de malla está basada en el estándar 802.11a debido a que la banda de 5 GHz está menos congestionada, habiendo menos riesgo de interferencia entre los enlaces de la malla y los clientes. Sin embargo, el estándar 802.11 no soporta nativamente las mallas, así que cada fabricante necesita implementar su propia tecnología propietaria por encima del 802.11a. El estándar 802.11s, tiene la finalidad de reemplazar estas tecnologías propietarias, tanto para sistemas de un solo canal o de varios canales de radio.

Las redes Wi-Fi en malla son útiles en lugares donde no existe cableado UTP, por ejemplo, oficinas temporales o edificios tales como bodegas o fábricas. Pero muchos de los fabricantes se están concentrando más bien en ambientes exteriores. En muchos lugares se ha incrementado el Internet público sobre redes Wi-Fi, tales como aeropuertos o comercios. Quizá Wi-Fi en malla sea un modesto competidor de otra tecnología más madura conocida como WiMax.

Un aspecto fundamental del funcionamiento de las redes en malla es que la comunicación entre un nodo y cualquier otro puede ir más allá del rango de cobertura de cualquier nodo individual. Esto se logra haciendo un enrutamiento multisaltos, donde cualquier par de nodos que desean comunicarse podrán utilizar para ello otros nodos inalámbricos intermedios que se encuentren en el camino. Esto es importante si se compara con las redes tradicionales WiFi, donde los nodos deben de estar dentro del rango de cobertura de un AP y solamente se pueden comunicar con otros nodos mediante los AP; estos AP a su vez necesitan de una red cableada para comunicarse entre sí. Con las redes en malla, no es necesario tener AP, pues todos los nodos pueden comunicarse directamente con los vecinos dentro de su rango de cobertura inalámbrica y con otros nodos distantes mediante el enrutamiento multisalto ya mencionado.

2.2.3 Mejoras y funcionalidades específicas

Según la normativa 802.11 actual, una infraestructura Wi-Fi compleja se interconecta usando LANs fijas de tipo Ethernet. 802.11s pretende responder a la fuerte demanda de infraestructuras WLAN móviles con un protocolo para la autoconfiguración de rutas entre puntos de acceso mediante topologías multisalto. Dicha topología constituirá un WDS (*Wireless Distribution System*) que deberá soportar tráfico *unicast*, *multicast* y de *broadcast*. Para ello se realizarán modificaciones en las capas PHY y MAC de 802.11 y se sustituirá la

especificación BSS (*Basic Service Set*) actual por una más compleja conocida como ESS (*Extended Service Set*)[11].

Aún no se conoce mucho de los detalles técnicos del estándar, pero parece que la redacción del mismo se está orientando de forma preferente a dotar a la multitud de puntos de acceso aislados existentes en viviendas y oficinas de la capacidad de conectarse con nodos exteriores pertenecientes a una red Mesh metropolitana existente. De esta forma el grupo de trabajo evitará que sus desarrollos se solapen con las avanzadas tecnologías desarrolladas desde hace años por los fabricantes comerciales de redes Mesh metropolitanas, pero podrá hacer uso de las mismas para ofrecer al usuario final una plataforma estable desde la que acceder a nuevas aplicaciones y servicios. Otra ventaja añadida consiste en que se mejorará la ocupación del espectro radioeléctrico urbano al conectarse el cliente a su propio AP, y no directamente al nodo exterior. Por último, se pondrá especial énfasis en que 802.11s recoja las mejoras en cuanto a tasa binaria, calidad de servicio y seguridad que se incorporen en 802.11n, 802.11e y 802.11i, respectivamente.

Primeras redes mesh

Los estándares 802.11a y 802.11g han incrementado sustancialmente la rata de datos de las WLAN usando esquemas de modulación eficientes (a 54Mbps). EL estándar 802.11 AP (Conocido como punto Mesh [MP] cuando es usado en redes Mesh WLAN). Los puntos MP-a-MP forman una troncal inalámbrica conocida como Mesh Backhaul, la cual proporciona a los usuarios bajo costo, alto ancho de banda y servicios de interconexión multihop con un número de puntos de Internet y con otros usuarios sin la red.

---

[11]IEEE wireless communications “emerging standard for wireless mesh technology” abril 2006

Estos dispositivos son llamados Mesh Access Point (MAPs). La figura 2.4 muestra una red mesh WLAN típica con sus componentes. Una WLAN Mesh esta definida como: Una red Mesh WLAN esta basada en el sistema de

distribución inalámbrico del estándar 802.11 (WDS),en la cual una parte DS que consiste en una distribución de dos o mas MPs interconectadas por los puntos 802.11 y la comunicación a través de los servicios Mesh WLAN.

Selección del canal Backhaul

La topología de una red Mesh WLAN pueden incluir MPs con uno o más interfaces de radios y puede utilizar uno o más canales para la comunicación entre MPs. Cuando cada canal esta siendo usado cada interfase de radio opera en una MPs sobre un canal al tiempo. Pero el canal debe cambiar durante el tiempo de vida de la red Mesh de acuerdo a los requerimientos de selección de frecuencias dinámicas (DFS). La selección de un canal específico usado en una red Mesh debe variar de acuerdo a los requerimientos de la aplicación y a las diferentes topologías. Una variedad de interfaces de radio MP que están interconectadas a otras por medio de un canal común, son llamados canales gráficos unificados (UCP). El mismo dispositivo puede tener diversos UCGs. La interfase de radio establece puntos de conexión con los vecinos que activa la identificación de la red y el perfil, y selecciona su canal basado un valor procedente del canal más alto.

Protocolo de unificación de canal simple

Una interfaz lógica de radio que es configurado en modo unificado de canal simple que funciona con técnicas de escaneo pasivo y activo para descubrir los vecinos MPs. Si una MP no puede detectar un vecino MPs, adopta una identificación de acoplamiento a partir de uno de sus perfiles, y selecciona un canal para la operación, así como un valor inicial de la procedencia del canal.
El valor inicial procedente del canal se puede ser iniciado al número de microsegundos más un valor al azar.

2.3 DESCRIPCION DE OPERACION UNA WMN

2.3.1 Características de una red Mesh

Una red enmallada esta compuesta por una colección de nodos que se comunican entre si, de manera directa, transmitiendo la información de otros nodos hasta su destino final por medio de múltiples saltos no hay necesidad de una unidad centralizada que los controle el modo de operación de conoce como distribuido. En caso de existir una unidad que administre las condiciones de operación de la red se conoce como centralizado.

Una red enmallada es compuesta por una colección de nodos que se comunican entre sí, de manera directa. Si no hay necesidad de una entidad centralizada que los controle el modo de operación se conoce como distribuido, pero puede existir una entidad central que administre las condiciones de operación de la red, en cuyo caso se conoce como centralizado. En cualquier caso, la comunicación se realiza entre los nodos directamente y cada nodo puede ser al mismo tiempo fuente o destino de los datos o un enrutador de la información de otro nodo. En la Figura 2.5 se muestra un diagrama de una red de múltiples saltos, donde la información es llevada desde un extremo a otro por diferentes nodos.

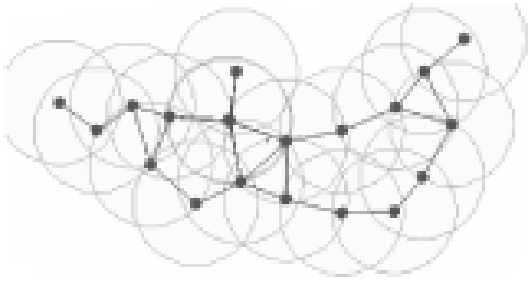


Figura 2.5 Diagrama de Red enmallada.

Si los nodos de la red se conectan de manera autónoma, sin configuración previa, se dice que la red opera en modo *ad hoc.* Si los nodos tienen movilidad, entonces se conocen como redes móviles *ad hoc* o MANET (Mobile ad-hoc

Network). Su característica principal es que existe un continuo cambio en la topología de la red, con enlaces que aparecen y desaparecen de modo permanente.

Las características más relevantes de las redes enmalladas inalámbricas son las siguientes:

• **Robustez:** La presencia de enlaces redundantes entre los usuarios permite que la red se reconfigure automáticamente ante fallas.

• **Topología dinámica:** Se supone que las redes enmalladas tienen la capacidad de reaccionar ante cambios de la topología de la red. Por lo tanto la topología cambiante es una condición de diseño necesaria.

• **Ancho de banda limitado:** Como el proceso de comunicación exige transportar datos de otros usuarios y la cercanía de unos con otros precisa una coordinación en los tiempos de transmisión, las redes enmalladas cuentan con enlaces que usualmente permanecen en condiciones de congestión.
Existen esfuerzos importantes en el estándar 802.16-2004 para mejorar el acceso al medio y lograr mejores desempeños en la red. Las primeras versiones de redes enmalladas basadas en el estándar 802.11 son bastante ineficientes en el aprovechamiento del espectro.

• **Seguridad:** La información transmitida se encuentra expuesta a la amenaza de viajar a través de un medio compartido. El estándar define una subcapa de seguridad para proteger la información de los usuarios y evitar el acceso de usuarios no autorizados.

• **Canales de comunicación aleatorios:** A diferencia de las redes fijas, las redes inalámbricas cuentan con la incertidumbre propia de los canales de comunicación de radio. La característica cambiante de los mismos hace bastante inciertas las condiciones de comunicación. El estándar define

aspectos como la modulación y codificación adaptativas para hacer frente a este problema.

• **Carencia de modelos de dimensionamiento apropiados:** El modelo de capacidad de redes de datos está orientado a determinar la capacidad del enlace ante procesos de multiplexación de la información de los usuarios. El modelo de capacidad de las redes enmalladas de múltiples saltos es un problema abierto, Las redes enmalladas proveen, sin embargo, condiciones que permiten el acceso a usuarios en regiones apartadas.

	Estática	**Baja Movilidad**	**Alta Movilidad**
Descubrimiento de la red	Pasivo/Activo	Pasivo/Activo	Activo
Enrutamiento	Actualizaciones poco frecuentes. Rendimiento altamente estable	Actualizaciones poco frecuentes. Rendimiento altamente estable	Actualizaciones frecuentes. Bajo overhead.
Seguridad	Infrecuentes re-autenticaciones	Infrecuentes re-autenticaciones	frecuentes autenticaciones
QoS	Mecanismos estáticos/lentos.	Mecanismos lentos.	Mecanismos dinámicos/Rápidos
Consumo de energía	Principalmente dispositivos conectados a la red eléctrica.	Una mezcla pero dominan los dispositivos conectados a la red eléctrica.	Principalmente dispositivos basados en el uso de baterías.

Tabla 2.1 Características de las redes inalámbricas enmalladas según la movilidad de los nodos

2.3. 2 Operación de una red Mesh

La operatividad del sistema no solo depende del buen diseño, sino también de la elección correcta del equipamiento y la robustez de los mismos. Por ello, es necesario diseñar un conjunto de estaciones tanto Gateway como Relay a fin de crear alternativas de diseño según sean los requerimientos. Aparte de estos prediseños, se tienen que tener en cuenta las ganancias de las antenas, direccionalidad de antenas, potencia de amplificadores, etc.

Para crear una red mesh se debe conectar un punto de acceso mesh a algún

Tipo de acceso a Internet. Este acceso a Internet puede ser una línea dedicada, una ADSL (Línea de Suscriptor Digital Asimétrica), una SDSL (Línea de Suscriptor Digital Simétrica) o en áreas remotas, por medio del satélite. Todo es compatible siempre que use IP (Protocolo de Internet) El tamaño y el tipo de acceso a Internet se decidirá según una variedad de factores:

- Lo que se tenga disponible
- La cantidad de usuarios que se deba atender
- Los requerimientos de ancho de banda de los usuarios
- El costo

Se configura el primer Mesh-AP con un canal inalámbrico, usualmente un canal 802.11b, un SSID. Al Punto de Acceso a la red Mesh se lo refiere como gateway.
También se utilizan nodos que tienen exactamente la misma programación del nodo gateway. La única cosa que decide si los Mesh-AP se muestran como gateway es si han obtenido una dirección IP de un DHCP o son configurados con una dirección IP fija.

El primer nodo repetidor se desplegará dentro del alcance del primer nodo Mesh-AP, simplemente dándole energía, el mismo canal y el mismo SSID del gateway. Cuando se inicie el Mesh-AP se sabrá que no es un nodo repetidor por el hecho de no haber obtenido una dirección IP. Este tratará de descubrir el nodo gateway. Una vez que haya sido establecido un enlace con un nodo gateway, el tráfico de Internet es encaminado desde el cliente, por medio del nodo repetidor y a Internet por medio del gateway.

De esta manera pueden agregarse más nodos al mesh, y, siempre que el nodo mesh agregado esté dentro del radio de alcance de un nodo que sea o bien un gateway o bien otro nodo que pueda alcanzarlo, entonces el tráfico de Internet

será encaminado a través del mesh, por medio de la ruta a Internet más eficiente.

2.3. 3 Alcance de una red Mesh

Para definir el alcance de una red Mesh hay que tener en cuenta una Variedad de factores que afectan su radio de acción. Algunos de estos Factores son:

- La potencia de la tarjeta inalámbrica
- El tipo y ganancia de la antena
- La ubicación de la antena
- El terreno en que se encuentra, la existencia de intrusiones u obstrucciones en la ruta de la señal inalámbrica.
- La existencia de interferencia inalámbrica de otros dispositivos que provoquen un incremento en el nivel ruido general.
- La sensibilidad inalámbrica de los dispositivos de recepción
- El tipo de antena, ganancia y ubicación de los dispositivos de recepción.

La apropiada revisión de los sitios, la correcta instalación, la experiencia y una selección cuidadosa del equipamiento de recepción, todo esto optimizará la capacidad de cobertura del mesh. Existen cálculos, tablas y fórmulas que aparecen más adelante en este mismo documento que pueden ser de gran utilidad para analizar y tomar decisiones acerca del alcance potencial de la red enmallada.

El sistema Mesh tiene la capacidad de llevar a cabo un gran número de Funciones. Estas se describirán con mayor detalle más adelante. A Continuación aparece una muestra de algunas de las características de Mesh:

• Servicios DHCP
• Servidor VPN2

• Calidad de servicio o prioridad para protocolos de voz SIP, IAX – y H323
• Soporte a Bluetooth
• Cámaras Web USB de circuito cerrado de televisión accesibles desde Internet público
• Administración remota basada en web.
• Informes estadísticos remotos
• Encriptación de 2048 bits
• Mapeo de servidor y puertos hacia dispositivos
• Autenticación
• Servicios DNS en cada AP
• Firewall - Cortafuegos
• Agrupación para permitir otras interfaces inalámbricas

3. ARQUITECTURA WMN

3.1 PROBLEMAS FUNCIONALES EN REDES MESH Y SUS CAUSAS

Capacidad limitada

A pesar de los grandes avances tecnológicos de la capa física, la capacidad sigue siendo limitada en los sistemas inalámbricos de un solo salto.

Por otro lado esta el problema de ancho de banda para las redes Mesh inalámbricas ya que al momento de establecerse la conexión todos los nodos operan sobre el mismo canal de radio. Esto resulta de una substancial interferencia entre las transmisiones de nodos adyacentes de la misma ruta como de la ruta de los nodos vecinos, reduciendo la capacidad de la red.

La capacidad para los nodos mesh es limitada para un sistema de un solo canal comparado con un sistema multicanal. En la tabla 3.1 se puede observar el rendimiento de una topología string. Se puede observar fácilmente que a medida que aumentan las longitudes de las rutas el rendimiento cae. En general son muchos los problemas que contribuyen al mal rendimiento como son las características del protocolo MAC, el problema de los nodos expuestos, los impredecibles y altos errores en un canal inalámbrico. Todos estos son los problemas que agravan los sistemas de un solo canal. Por ejemplo en la figura 3.1 se muestra que cuando el nodo 1transmite al nodo 2, especialmente cuando el protocolo MAC se basa en CSMA/CA, los nodos 2 y 3 no pueden iniciar otra transmisión. El nodo 2 es prevenido de transmisiones simultaneas, como interfaces inalámbricas. En la mayoría de las WMNS las comunicaciones son half duplex. De esta manera el nodo 2 se abstrae de establecer comunicación con el nodo 3 porque esta estableciendo comunicación con el nodo 1.

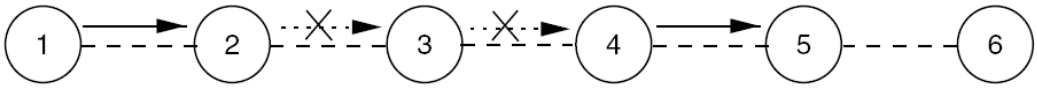


Fig 3.1 un ejemplo de la topología string y problema de nodo expuesto en las WMN.

	1 Hop	*2 Hops*	*3 Hops*	*4 Hops*	*5 Hops*	*>5 Hops*
Normalized throughput	1	0.47	0.32	0.23	0.15	0.14
$\frac{1}{\text{Hoplength}}$	1	0.5	0.33	0.25	0.2	0.16

Tabla 3.1 Degradación del throughput en las WMN con topología string

La métrica más simple para redes Mesh es la métrica contadora de saltos. Sin embargo el uso de conduce a la selección de trayectoria optima.

Un gran problema es que cuando los saltos son cortos y se vuelven extensos

Se presenta un error y se desbalancean las cargas del trafico a través de la red, lo cual reduce la capacidad de la red.

El problema de limitación de capacidad es tocado mas a fondo por el protocolo TCP que no puede utilizar con eficacia la anchura de banda disponible. El protocolo TCP el ACK que es una señal que pide retransmisión de la ruta del paquete que se usa en el caso de que el paquete se pierda en un salto intermedio. Esto conduce al despilfarro de la anchura de banda en todos los saltos precedentes donde las transmisiones necesiten del ACK, pudiéndose utilizar mejor en trasmisiones en las cuales el paquete es transmitido en forma acertada[12].

Otro problema que limita la capacidad es el control ineficiente de la congestión. El control de la congestión de TCP tiene en cuenta pequeños segmentos de la información del paquete para detectar la congestión de la red. Sin embargo en redes inalámbricas los paquetes también se caen debido a los errores presentes en los pequeños segmentos que calculan la congestión de la red.

[12]http://www.it46.se/downloads/courses/wireless/es/13_Redes-Mesh

El TCP no puede distinguir entre estos pequeños segmentos y la congestión verdadera. Los errores del canal pueden conducir a la falta de aprovechamiento substancial de la red.

Confiabilidad y robustez: Otra motivación importante para usar WMNs es que debe mejorar la confiabilidad y la robustez de la comunicación. La topología parcial del acoplamiento en una WMN proporciona alta confiabilidad y diversidad de la trayectoria contra faltas del nodo y del acoplamiento. Las WMNs proporcionan el ingrediente más importante para la robustez en la comunicación diversidad. Por ejemplo en los sistemas inalámbricos, el error en los canales son altos en comparación con los sistemas cableados. Sin embargo la alta degradación de la comunicación por los errores en los canales es necesaria. Esto es muy importante cuando las WMNS emplean frecuencias que están por fuera del espectro. De esta manera las WMNS emplean diferentes frecuencias al usar diferentes interfaces multiradio, cuando es difícil alcanzar una sola interfaz de radio.

Manejo de recursos: El manejo de Recurso se refiere al manejo eficiente de los recursos de la red tales como almacenamiento de energía, anchura de banda e interfaces. Por ejemplo, los recursos de energía se pueden utilizar eficientemente en las WMNs con la reserva limitada de la energía si cada nodo en el sistema tiene una nueva interfaz de baja potencia además de una interfaz regular. El consumo de energía total, incluso en modo ocioso, depende mucho del tipo de interfaz. Por lo tanto, la IEEE 802.11 baso las WMNs con la reserva limitada de la energía, un interfaz de baja potencia y de datos bajos de tarifas adicionales se pueden utilizar para llevar la información que está fuera de banda para controlar la alta potencia y los altos datos en la interfaz de los datos. Los recursos de la anchura de banda se pueden también manejar mejor en un ambiente del multiradio. Por ejemplo, si la carga es balanceada a través de interfaces múltiples se podría contribuir a prevenir cualquier canal particular que provoca congestionado pesado y embotellamiento en la red.

PROBLEMAS EN EL DISEÑO DE UNA WMN

Hay muchos problemas que necesitan ser considerados cuando se diseña una WMN para una aplicación en particular. Estos problemas de diseño se pueden clasificar ampliamente en problemas de arquitectura y de protocolos. Una red WMN puede estar diseñada de acuerdo a tres diferentes arquitecturas de red basadas en topologías de red: WMNs planas, WMNs jerárquicas y WMNs hibridas.

WMNs Planas: En una WMN plana, la red esta formada por los dispositivos del cliente que actúan como rebajadoras. Aquí, cada nodo está en el mismo nivel que el de sus pares. Los nodos inalámbricos del cliente coordinan entre sí mismos para proporcionar el encaminamiento, la configuración de red, el aprovisionamiento del servicio, y otros aprovisionamientos de uso. Esta arquitectura es la más cercana a una red inalámbrica ad hoc y es el caso más simple entre las tres arquitecturas de WMN. La ventaja primaria de esta arquitectura es su simplicidad, y sus desventajas incluyen la carencia del escalabilidad de la red y de los altos costos de recursos. Los problemas primarios a la hora de diseñar una WMN plana son el esquema de dirección, el encaminamiento, y el descubrimiento de esquemas de servicio. En una red plana, la dirección es una de los problemas que pueden convertirse en un embotellamiento contra escalabilidad.

WMNs Jerárquicas: En un WMN jerárquico, la red tiene grados múltiples o niveles jerárquicos en los cuales los nodos del cliente de WMN forman están en la parte mas baja de la jerarquía. Estos nodos clientes pueden comunicarse con la red troncal formada por routers de WMN. En la mayoría de los casos, los nodos de WMN son los nodos dedicados que forman una red troncal de WMN. Esto significa que los nodos de la troncal no originar o terminar datos en un tráfico determinado como los nodos del cliente de WMN. Su responsabilidad

es mismo-de organizar y de mantener la red de espina dorsal se proporcionar paquetes a los routers de WMN algunos de las cuales en la red troncal pueden tener interfaces externas al Internet.

WMNs hibridas: Éste es un caso especial de WMNs jerárquico donde el WMN utiliza otras redes inalámbricas para la comunicación. Por ejemplo, el uso de otras WMNs basadas en infraestructura tal como redes celulares, redes de WiMAX, o redes basadas en los satélites. Ejemplos de tales WMNs híbridas incluyen las redes celulares multihop, rendimiento de procesamiento radio realzada en las redes locales del lazo y redes ad hoc de celulares unificadas. Una solución práctica para tal híbrido WMN para los usos de la respuesta de la emergencia es la plataforma de CalMesh. Este es el híbrido WMN que puede utilizar las tecnologías múltiples para WMN y el establecimiento de una red inalámbrica con acoplamiento de transporte del backbone y de la parte posterior. Puesto que el crecimiento de WMNs depende grandemente de la manera como trabaja con otras soluciones inalámbricas existentes de una red, esta arquitectura llega a ser muy importante en el desarrollo de WMNs.

3.2. CLASIFICACION DE LOS PROTOCOLOS DE RUTEO DE REDES ENMALLADAS

La tarea principal de los protocolos de ruteo es la selección de el camino entre el nodo fuente y el nodo destino. Esto tiene que ser hecha de una manera confiable, rápida, y con gastos indirectos mínimos. En general, los protocolos de ruteo pueden ser clasificados en los basados en topología y en los basados en posición. Los protocolos de ruteo basados en topología seleccionan trayectorias basadas en información topológica, como por ejemplo los enlaces de nodos. Los protocolos de ruteo basados en posición seleccionan trayectorias basadas en la información geográficas con algoritmos geométricos. También hay protocolos que combinan esos dos conceptos.

Los protocolos de ruteo híbridos tratan de combinar las ventajas de las 2 filosofías anteriores proactivo es usado para nodos cercanos o para caminos cercanos mientras que el ruteo reactivo es usado para nodos lejanos y por lo general caminos o rutas menos usadas.

Otras posibilidades para la clasificación de protocolos de ruteo son :Flan vs hierarchical, distance vector vs. link state, source routing vs. hopby- hop routing, single-path vs. multipath.

En principio las redes mesh pueden manejar cualquier clase de protocolo de ruteo descrita anteriormente. Sin embargo no cada protocolo trabajará bien. La selección de un protocolo de encaminamiento conveniente depende del panorama, uso, y requisitos de funcionamiento.

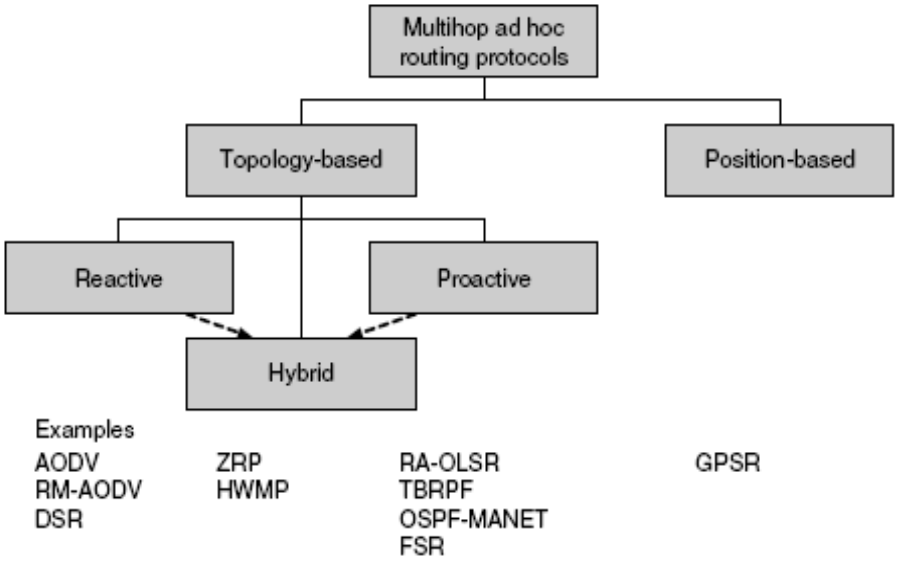


Fig 3.2 Clasificación de Protocolos de ruteo en WMN

3.2.1 Protocolos basados topología (Topology based)

Los protocolos de ruteo basados en topología son separados en 2 categorías que son llamados reactivos, proactivos y los protocolos de ruteo híbrido. los protocolos reactivos tales como AODV y DSR inician la determinación de las rutas solo si existe una petición Esto quiere decir que la información de la ruta solo esta disponible cuando se recibe una petición, utilizando este tipo de implementaciones pueden existir retardos significativos antes de que la ruta al destino pueda ser determinada[13]. También será necesario hacer cierto control de tráfico mientras se busca la ruta. En los protocolos proactivos como OLSR y DSDV, intentan establecer todas las rutas con la red. Esto significa que cuando se necesita una ruta, esta ya es conocida y puede usarse de forma inmediata.

[13]Wireless mesh networking" Architectures, Protocols and Standards" Julio 2006

AODV (Ad Hoc On-Demand Vector Routing)

AODV es un protocolo de ruteo muy popular para MANETs el cual es un protocolo de ruteo reactivo. Este protocolo permite el enrutamiento dinámico, autoarranque y multihop entre todos los nodos móviles que participan en la red. AODV permite a todos los nodos obtener las rutas rápidamente para las nuevas destinaciones y no requiere que los nodos mantengan las rutas hacia los destinos que no están activos en la comunicación.

El protocolo de enrutamiento está diseñado para redes móviles ad hoc con gran cantidad de nodos y con distintos grados de movilidad. Este protocolo se basa en que todos los nodos tienen que confiar en los otros para transportar sus datos, aunque sea por el uso de una clave preconfigurada, o activando mecanismos para evitar la participación de nodos intrusos.

En este apartado lo que se intenta es dar una breve introducción de sus características y sus modos de funcionamiento básicos, así como sus tablas y Mensajes más característicos sin entrar en el formato de estos.
Una característica distintiva de este protocolo es el uso del número de secuencia para cada ruta. Este número de secuencia es creado por el destino para ser incluido con la información necesaria para los nodos que requieren la información. El uso de estos números implica que no se crean *bucles* y la facilidad de programación.

Este protocolo define tres tipos de mensajes: Route Requests (RREQs), Route Replies (RREPs) y Route Errors (RERRs). Estos mensajes se reciben vía UDP. Mientras todos los nodos tengan las rutas correctas de cada nodo el protocolo no intercambia mensajes ni tiene ninguna función. Cuando una ruta hacia un nuevo destino es necesaria, el nodo que la necesita envía una mensaje broadcast RREQ que llega al destino, o a un nodo intermedio que tiene una

ruta suficientemente “fresca” hacia el destino. Una ruta es “fresca” cuando el número de secuencia hacia el destino es como mínimo tan grande como el número que contiene el RREQ. La ruta se considera disponible por el envió de un mensaje RREP hacia el nodo que originó el RREQ.

Los nodos monitorizan el estado de las conexiones de los nodos, a un salto, participantes en las rutas activas. Cuando una conexión se rompe en una ruta activa, se envía un mensaje RERR para notificar a los otros nodos la pérdida de la conexión.
Este protocolo tiene una tabla de rutas. La información de la tabla de rutas debe guardarse incluso para las rutas de corta vida. Los campos que tiene cada entrada de la ruta son los siguientes:

- IP de destino.
- Número de secuencia de destino.
- *Flag* número de secuencia de destino válido.
- Otros estados y *flags* de enrutamiento (válido, invalido, reparable...).
- Interfaz de red.
- Contador de saltos.
- Salto siguiente.
- Listado de precursores.
- Tiempo de vida.

Terminología

En este apartado se definen algunos nombres y sus significados que se utilizan en este protocolo:

- Ruta activa: una ruta que tiene una entrada en una tabla y esta marcada como válida. Sólo estas rutas se pueden usar para la retransmisión.
- Broadcast: estos paquetes no deben ser transmitidos por la red en exceso, pero son útiles para la transmisión de los mensajes del AODV por la red.

• Nodo retransmisión: nodo que permite la retransmisión de paquetes hacia otros nodos, por medio de enviar los paquetes hacia el siguiente salto.
• Ruta de retrasmisión: una ruta configurada para enviar paquetes de datos desde el nodo que origina el descubrimiento de la ruta hacia el destino deseado.
• Ruta inválida: una ruta que ha expirado, tiene el estado inválido. Estas rutas se utilizan para guardar una ruta válida anterior y de este modo tener la información durante más tiempo. Una ruta inválida no puede ser utilizada para la retransmisión de paquetes.
• Nodo originario: un nodo que inicia el mensaje de descubrimiento de ruta para ser procesado y poder ser retransmitido por otros nodos.
• Ruta contraria: una ruta configurada para retransmitir el paquete (RREP) desde el destinatario hacia el que ha originado el mensaje.
• Número de secuencia: un número incremental que mantiene cada nodo originario. En los mensajes del protocolo AODV se usa por los otros nodos para determinar la “frescura” de la información que tiene el nodo Originador.

Mantenimiento de números de secuencia

Cada entrada de la tabla de cada nodo debe incluir la última información sobre el número de secuencia para la dirección IP del nodo destino. Este número de secuencia se llama “número de secuencia de destino”. Se actualiza cada vez que un nodo recibe nueva información del número de secuencia por los mensajes RREQ, RREP o RERR. Este protocolo depende de que cada nodo de la red mantenga su propio número de secuencia de destino para garantizar que no haya bucles. Un nodo destinatario incrementa su propio número de secuencia en dos circunstancias:
• Inmediatamente antes que un nodo origine el descubrimiento de una ruta, debe incrementar su propio número de secuencia.
• Inmediatamente antes que el nodo destino origine un mensaje RREP como respuesta a un RREQ, este nodo debe actualizar su número de secuencia,

eligiendo el valor máximo entre su actual número de secuencia o el número del paquete RREQ que le ha llegado.

Entradas de la tabla de enrutamiento

Cuando un nodo recibe un paquete de control desde un vecino, crea o actualiza una ruta hacia un destino particular o una subred, el nodo comprueba su tabla de enrutamiento por una entrada para el destino. La ruta se actualiza en los siguientes casos:

• El número de secuencia es mayor que el que hay en al tabla de enrutamiento.

• El número de secuencia es igual, pero el nuevo valor del contador de saltos más uno, es menor que el valor que tenia la ruta de la tabla de enrutamiento.

• El número de secuencia es desconocido.

Las entradas de la tabla tiene un campo de tiempo de vida, este tiempo se determina por el paquete de control que llega, o se toma un valor determinado.

Generación de peticiones de rutas

Un nodo envía un mensaje RREQ cuando determina que necesita saber la ruta hacia un destino y no lo tiene en su tabla de enrutamiento o es una entrada no válida. En ese momento se envía un mensaje RREQ con el valor del número de secuencia de destino igual al último número conocido para este destino. El valor del número de secuencia de origen en el mensaje RREQ es el número de secuencia del nodo que es incrementado antes del envío del mensaje.

Al tener en cuenta que las comunicaciones son bidireccionales, además de la ruta para llegar al destino también es necesario saber una ruta de vuelta. Para este cometido cualquier nodo intermedio que genere un mensaje de respuesta (RREP) debe también realizar una acción que notifique al nodo destino una ruta de vuelta hacia el nodo origen.

Para no crear congestión en la red ni hacer que los mensajes circulen indefinidamente por ella, el nodo que origina peticiones debe indicar un TTL

máximo a los mensajes y además seleccionar un *timeout* para esperar una respuesta. Tanto el *timeout* como el TTL son calculados de manera periódica y tiene en cuenta el tamaño de la red y el tiempo que tarda un paquete en cruzarla.

Procesamiento y retransmisión de peticiones de ruta

Cuando un nodo recibe un RREQ, crea o actualiza una ruta hacia el salto anterior. Posteriormente comprueba que no haya recibido una mensaje con el mismo ID y origen y si lo ha recibido descarta este nuevo mensaje. En este apartado se explicará las acciones que se realizan cuando este mensaje no se descarta.

Lo primero que se hace es aumentar el valor del contador de saltos en uno. Después, el nodo busca una ruta hacia la IP origen del mensaje. Si no existe se debe crear esta nueva ruta de vuelta. Una vez se ha creado esta ruta de vuelta se siguen las siguientes acciones:

• El número de secuencia origen se compara con el número de secuencia hacia el destino que se tiene en la tabla, y si es mayor se copia en ella.

• Se valida el campo de número de secuencia.

• El siguiente salto en la tabla de enrutamiento se convierte el nodo desde donde nos ha llegado el mensaje.

• Se copia el número de saltos en la tabla de enrutamiento.

Generación de respuesta de ruta

Un nodo genera un mensaje RREP si él mismo es el destino, o tiene una ruta activa hacia el destino y el número de secuencia de la entrada de la tabla es mayor que el del mensaje RREQ. Una vez se genera el RREP el nodo descarta el mensaje RREQ.

Si un nodo no genera un RREP y el valor del TTL es mayor de uno entonces actualiza y envía el mensaje RREQ a una dirección *broadcast*.

Si el nodo que genera el mensaje RREP no es el nodo destino sino que es un nodo intermedio, copia su propio número de secuencia para el destino en el campo de número de secuencia destino del mensaje RREP. Entonces este nodo intermedio actualiza la ruta de retransmisión poniéndose a él como último nodo en la lista de precursores.

Recepción y retransmisión de respuesta de ruta

Cuando un nodo recibe un mensaje RREP busca una ruta hacia el salto anterior, si es necesario se crea esta ruta. Posteriormente el nodo incrementa el contador de saltos en el mensaje. Entonces se crea una ruta para llegar al destino si no existe. De otra manera, el nodo compara el número de secuencia de destino del mensaje con el que tiene guardado. Después de la comparación la ruta existente se actualiza en los siguientes casos:

• El número de secuencia en la tabla de enrutamiento está marcado como inválido.

• El número de secuencia de destino en el mensaje es mayor que el que el nodo tiene guardado y el valor es válido.

• Los números de secuencia son iguales pero la ruta está marcado como inactiva.

• Los números de secuencia son los mismos, y el nuevo valor del contador de saltos es menor.

Cuando se actualiza una entrada en la tabla la ruta se marca como activa, el número de secuencia de destino también se marca como válido y en el siguiente salto en la entrada de la tabla se asigna el nodo del que ha llegado el mensaje RREP. También se debe actualizar el nuevo valor del contador de saltos, el tiempo de expiración de la ruta y el número de secuencia de destino, se debe actualizar por el número de secuencia del mensaje RREP[14].

[14]Wireless mesh network “introducción to wireless mesh networking” mayo 2005 Gilbert held ,cap 4 pág 60-75

Mensajes de error (RERR)

Normalmente una ruta errónea o el corte de un enlace necesitan un procedimiento similar. Primero invalidar las rutas existentes, listar los destinos afectados, determinar los vecinos afectados y enviar un mensaje apropiado RERR a estos vecinos.

Un nodo inicia el procesamiento de un mensaje RERR en tres situaciones:

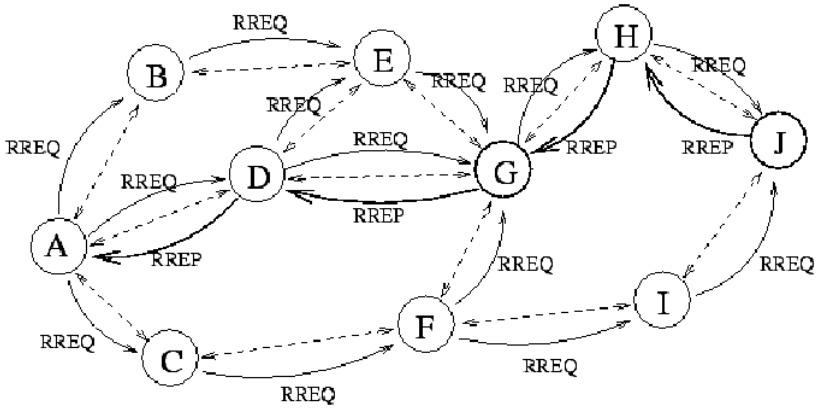
• Si detecta la caída de un enlace para el siguiente salto de una ruta activa en su tabla de enrutamiento mientras envía datos.

• Si recibe un paquete de datos hacia un nodo del que no tiene ninguna ruta activa.

• Si recibe un mensaje RERR desde un vecino por una o más rutas activas.

Ejemplo 1

En la figura 3.3 se puede ver como un nodo (A) busca la ruta hacia otro nodo (J) del que no conoce el camino. Lo primero que hace el nodo A es enviar un mensaje broadcast RREQ hacia todos los nodos, preguntando por el nodo J, con el que se quiere comunicar. Cuando el mensaje RREQ llega al nodo J este genera un mensaje RREP de respuesta. Este mensaje se envía como unicast de vuelta hacia el nodo A utilizando las entradas en memoria de los nodos H, G y D.



3.3 Ejemplo de búsqueda de un nuevo nodo

EJEMPLO 2

Cuando el nodo fuente S quiere enviar paquetes de datos a un nodo destino D pero no tiene una ruta a D en su tabla de ruteo, una ruta de descubrimiento tiene que ser hecha por S. los paquetes de datos son protegidos durante el descubrimiento de la ruta. al ver la figura para una ilustración de el proceso de una ruta de descubrimiento. el nodo fuente S difunde una petición de ruta ,llamada (RREQ) , a través de la red.
Además de varias FLAGS, un paquete de RREQ contiene el hopcount, un identificador de RREQ, la dirección destino y el número de serie de la numeración, y el de la dirección originaria y de serie originaria.

El campo hopcount contiene la distancia a el autor de el RREQ, el nodo de fuente S. ese va a ser el numero de saltos que el RREQ ha realizado hasta ahora. El RREQ ID combinado con la dirección originaria identifica una solamente una petición de ruta.
Esto se utiliza para asegurarse de que los rebroadcasts de un nodo manden una petición de la ruta solamente una vez para evitar confusiones o coaliciones en los datos, aunque un nodo recibe el RREQ varias veces de sus vecinos.

Cuando un nodo recibe un paquete RREQ es procesado como sigue a continuación:

- La ruta de el salto anterior de el cual se ha recibido el paquete de RREQ es creado o es actualizado.
- El RREQ ID y la direccion de donde es originada son verificadas para ver si este RREQ ha sido recibido anteriormente. Si es asi, el paquete es desechado.
- El hopcount es aumentado en 1.

La ruta inversa a el nodo fuente, nodo S, es creada o actualizada.

- Si el nodo es el destino solicitado, este nodo genera una respuesta de la ruta (RREP) y envía el paquete RREP de nuevo al nodo origen a lo largo de la ruta inversa creada al nodo S. de la fuente.
- Si el nodo no es el destino pero tiene un camino valido a D, este publica un RREP a la fuente dependiendo solamente de la bandera (flags) del destino.

Si los nodos intermedios contestan a RREQs, puede ser que sea el caso que el destino no detecte cualquier RREQ es decir no llegara, de modo que no tenga una ruta trasera a la fuente. Si las flags gratuita de RREP se fija en el RREQ, el nodo intermedio que contesta enviará un RREP gratuito a el destino. Esto fija la ruta al autor del RREQ destino. Si el nodod no genera una RREP, el RREP es actualizado y regenerado si el TTL es > 1.
En recibo al mensaje de RREP, un nodo creará o pondrá al día su ruta a el destino D. El hopcount es incrementado por uno, y el RREP actualizado será remitido al nodo origen del RREQ correspondiente. Eventualmente, el nodo S de la fuente recibirá un RREP si existe una ruta al nodo destino. Los paquetes protegidos de los datos se pueden ahora enviar al nodo D en la trayectoria nuevamente descubierta.

La información de la conectividad es proporcionada y mantenida periódicamente difundiendo mensajes de gestión de protocolo ruteo. Si un nodo no ha enviado un mensaje de difusión, un mensaje de RREQ, con el ultimo intervalo HELLO, el nodo puede difundir un HELLO MESSAGE. Un HELLO es realmente un RREP con el TTL= 1 y el mismo nodo como destino. Si un nodo no recibe ninguna clase de paquetes de un nodo vecino por un tiempo definido, el nodo considera que el enlace con ese nodo vecino se encuentra roto. Cuando ha sucedido una caída en el enlace, el nodo antes de que el enlace haya caído comprueba primero si cualquier ruta activa había utilizado este enlace antes. Si éste no es el caso, nada se puede hacer. Por otra parte, si ha habido trayectorias activas, el nodo puede procurar una

reparación local. El nodo envía un RREQ para establecer una nueva segunda mitad de la ruta al destino.

El nodo que realiza la reparación del local protege los paquetes de los datos mientras que espera cualquier contestación de la ruta.
Si la reparación local falla o no se ha procurado, el nodo genera un mensaje del error de la ruta (RERR) que Contiene las direcciones y los números de serie correspondientes a el destino de todas los destinatarios activas que lleguen a ser inalcanzable debido a la falta del enlace[15]. El mensaje de RERR se envía a todos los vecinos que sean precursores de las destinaciones inalcanzables en este nodo. Un nodo que recibe un RERR invalida las entradas correspondientes en su tabla de encaminamiento. Quita todas las destinaciones de las cuales no tener el transmisor del RERR como salto siguiente de la lista

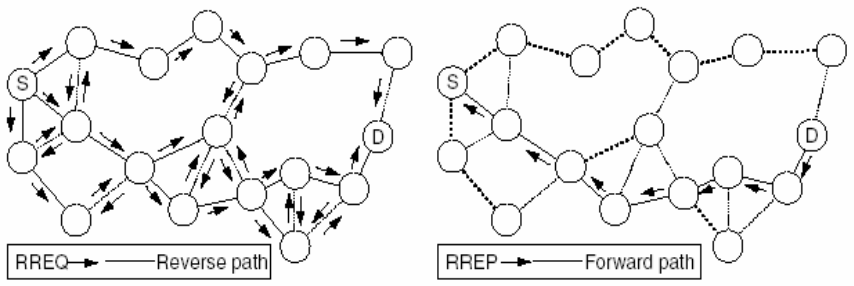


Figura 3.4 descubrimientos de la ruta AODV: a) ruta de petición (izq) y b) ruta de contestación (der).

DSR (Dynamic Source Routing)

El protocolo DSR se fundamenta en el encaminamiento desde el origen, es decir, los paquetes de datos incluyen una cabecera de información acerca de los nodos exactos que deben atravesar. No requiere ningún tipo de mensajes periódicos (reactivo), disminuyendo así la sobrecarga con mensajes de control. Además ofrece la posibilidad de obtener, con la solicitud de una ruta, múltiples

[15]Wireless mesh networking “Architectures, Protocols and Standards” 2006
Yan Zhang • Jijun Luo • Honglin Hu pag 113-135.

caminos posibles hacia el destino. Tampoco son un problema, a diferencia de la mayoría de protocolos de encaminamiento en este tipo de redes, los enlaces unidireccionales. Para poder realizar el encaminamiento en el origen, a cada paquete de datos se le inserta una cabecera DSR de opciones que se colocará entre la cabecera de transporte y la IP. Entre dichas opciones se incluirá la ruta que debe seguir el paquete nodo a nodo. Cada nodo mantiene una memoria caché de rutas en la que se van almacenando las rutas obtenidas a través de procesos de descubrimiento de rutas ya sean propios o obtenidos a través de escuchas en la red. En los procesos de descubrimiento de rutas se generan mensajes de solicitud, respuesta y error siendo estos mensajes ROUTE REQUEST, REPLY y ERROR respectivamente.

OLSR (Optimized Link State Routing Protocol)

OLSR es un protocolo de ruteo proactive para wireless ad hoc netwoks. Este protocolo desarrollado para redes móviles ad hoc, opera en modo proactivo. Cada nodo selecciona un grupo de nodos vecinos como “multipoint relay” (MPR), en este caso sólo los nodos seleccionados como tales son responsables de la retransmisión de tráfico de control[16]. Estos nodos también tienen la responsabilidad de declarar el estado del enlace a los nodos que los tienen seleccionados como MPR.

Es muy útil para redes móviles densas y grandes, porque la optimización que se consigue con la selección de los MPR trabaja bien en estos casos. Cuanto más grande y densa sea una red mejor es la optimización que se consigue con este protocolo. OLSR utiliza un enrutamiento salto-a-salto, es decir, cada nodo utiliza su información local para enlutar los paquetes.

La selección de los nodos MPR reduce el número de retransmisiones necesarias para enviar un mensaje a todos los nodos de la red. OLSR optimiza

[16]http://www.montevideolibre.org/manuales:libros:wndw:capitulo_3:redes_mesh

la reacción a cambios en la topología reduciendo el intervalo de transmisión de los mensajes periódicos de control. Como este protocolo mantiene rutas hacia todos los destinos de la red trabaja muy bien en redes donde el tráfico es aleatorio y esporádico entre un gran número de nodos.

OLSR trabaja de manera distribuida sin ninguna entidad central. Este protocolo no requiere transmisiones seguras de mensajes de control porque los mensajes son periódicos, y se pueden permitir algunas pérdidas. Tampoco necesita una recepción de mensajes secuencial, se utiliza números de secuencia incrementales para que el receptor sepa que información es más reciente.

Terminología

Palabras claves para entender el funcionamiento de este protocolo:

• Nodo: Router que implementa el protocolo OLSR.

• Interfaz OLSR: interfaz de un equipo que participa en el protocolo OLSR. También se debe tener en cuenta que hay otras interfaces en estos equipos que no trabajan en el protocolo.

• Dirección principal: la dirección principal de un nodo, se utilizará como la dirección de origen del tráfico de control en OLSR emitida por este nodo.

• Nodo vecino: un nodo X es vecino de otro nodo Y, si el nodo Y puede escuchar nodo X. Existe un enlace entre los dos nodos. Dos nodos son vecinos si ambos se encuentran dentro del área de cobertura del otro.

• Vecino a 2 saltos: un nodo “escuchado” por un vecino. Nodo, no vecino, que está dentro del área de cobertura de un nodo vecino.

• Vecino a 2 saltos estricto: un nodo que es vecino de un vecino del nodo que se esta mirando.

• MPR (Multiponit relay): un nodo que es seleccionado por su vecino, nodo X, para retransmitir todos los mensajes *broadcast* que recibe del nodo X.

• MPR selector (MS): un nodo que ha seleccionado su vecino como su MPR. MPS de un nodo x es todo aquel que tiene a x como MPR.

• Enlace: pareja de interfaces OLSR sensibles a “escuchar” el otro. Los enlaces pueden ser simétricos (enlace bidireccional), asimétricos (sólo verificados en un sentido).
• Vecindario simétrico de 1 salto: de un nodo X es el grupo de nodos que tiene un enlace simétrico hacia X.

OLSR está modulado para tener un núcleo de funcionalidades, que siempre es requerido, y un grupo de funcionalidades auxiliares.

Funcionamiento núcleo

El núcleo especifica el comportamiento de un nodo que tiene interfaces OLSR. Se basa en las siguientes funcionalidades:

• Formato de paquete y retransmisión: OLSR se comunica mediante un formato de paquete unificado para todos los datos del protocolo. El propósito de esto es facilitar la extensión del protocolo. Estos paquetes se envían como datagramas UDP. Cuando recibimos un paquete básico, un nodo examina el mensaje, y basándose en un campo donde se indica el tipo de mensaje determinará el procesamiento del mensaje que seguirá los siguientes pasos:

- Si el paquete no contiene mensaje (el tamaño es demasiado pequeño) se descarta.
- Si el valor del TTL es menor o igual que 0 también se descarta.
- Condiciones de proceso: Si es un mensaje es duplicado (la dirección de origen y la número de secuencia ya se han tratado) no se procesa. En caso contrario el paquete es tratado de acuerdo al tipo de mensaje que haya llegado.
- Condiciones de retransmisión: Si es un mensaje duplicado no se retransmite, si no es duplicado se retransmite el mensaje siguiendo el algoritmo del tipo de mensaje.
- Percepción de enlace: Se consigue saber el estado del enlace mediante el envío de mensajes “HELLO”. El propósito de esta funcionalidad es que cada nodo tenga asociado un estado en el enlace a cada uno de sus vecinos. El

estado puede ser simétrico (enlace verificado es bidireccional) y asimétrico indica que los mensajes “HELLO” se han escuchado pero no podemos asegurar que este nodo escuche las respuestas.

- Detección de vecino: Dada una red de nodos con sólo una interfaz, un nodo debe deducir los vecinos que tiene mediante la información intercambiada durante la percepción de enlace. Cada nodo debe tener guardados su grupo de vecinos. Cada vecino debe tener asociado el estado del enlace. Cuando se detecta la aparición de un nuevo enlace, se debe crear una entrada con un vecino que tiene un enlace asociado, en esta entrada también se debe guardar el estado de este enlace. Se debe tener en cuenta que cada vez que varía el estado del enlace se debe comprobar en la tabla que el cambio se lleva a cabo. Si no se recibe información de un enlace durante un tiempo establecido se debe borrar el enlace en cuestión y el vecino asociado.
- Selección de MPR y señalización MPR: La selección de los MPR sirve para seleccionar los nodos vecinos que se quiere que hagan *broadcast* de los mensajes de control. La señalización viene dada mediante mensajes “HELLO”. Cada nodo elige uno o más MPRs de manera que se asegura que a través de los MPRs seleccionados, cada nodo llega a todos los vecinos a dos saltos.
- Difusión de mensajes de control de topología. Estos mensajes se difunden con el objetivo de dar a cada nodo de la red la información necesaria para permitir el cálculo de rutas, son llamados mensajes TC (Topology Control). Estos mensajes que retransmite un nodo hacia sus vecinos seleccionados como MPR, tienen la información de todos sus enlaces para que los otros nodos conozcan los vecinos a los que puede llegar.
- Cálculo de rutas: Dada la información del estado del enlace que se adquiere mediante el intercambio de mensajes periódicos. Cada nodo mantiene una tabla de enrutamiento que permite encaminar los paquetes de datos destinados a otros nodos. Esta tabla esta basada en la información contenida en las bases de información de enlace y de la topología. Esta tabla se actualiza cuando se detecta algún cambio en estos campos:

- El enlace
- El vecino
- El vecino de dos saltos
- La topología

Funciones auxiliares : Hay situaciones donde funcionalidades auxiliares son necesarias, como por ejemplo un nodo con múltiples interfaces, donde algunas de ellas participan en el otro dominio de enrutamiento.

Interfaces no OLSR: Hay nodos que pueden tener interfaces que no son OLSR, estas interfaces pueden ser conexiones punto a punto o conectar con otras redes. Para poder tener conectividad entre las interfaces OLSR y estas otras el router debe ser capaz de introducir información externa de encaminamiento a la red. Para esto las interfaces no OLSR crean un mensaje Host and Network Association (HNA) que contiene información suficiente para poder crear nuevas rutas con esta información.

Notificación capa enlace: OLSR no trabaja con información de capa enlace. Sin embargo, si la información de esta capa está disponible, esta información se utiliza además de la información de los mensajes “HELLO”, para mantener información de los vecinos y los MPR. Por ejemplo: la pérdida de conectividad de la capa de enlace se puede deber a la ausencia de reconocimientos de capa de enlace.

Información redundante de topología: Para poder proveer redundancia a la información de topología, la información de anuncio que emite el nodo ha de tener información de enlaces hacia nodos vecinos que no necesariamente tengan a este nodo como MPR. El mensaje de anuncio publica información de todos los enlaces de los nodos vecinos. Hay tres posibles niveles de redundancia:

- Sin redundancia: sólo se emite información del grupo que ha elegido a este nodo como MPR.

- Redundancia media: se emite información del grupo que ha elegido el nodo como MPR y también información de los nodos que este ha elegido como MPR.
- Redundancia alta: se emite información de todos los enlaces hacia los vecinos.

MPR redundante: Esta funcionalidad especifica la habilidad del nodo de seleccionar MPR redundantes. Aunque la redundancia crea mucho más tráfico y pierde eficiencia el mecanismo de MPR, se tiene una gran ganancia al asegurar la llegada de los paquetes a sus destinos. Esta funcionalidad es útil para situaciones en que la red tiene mucha movilidad y mantener una buena cobertura con los MPR.

Ejemplo de utilización

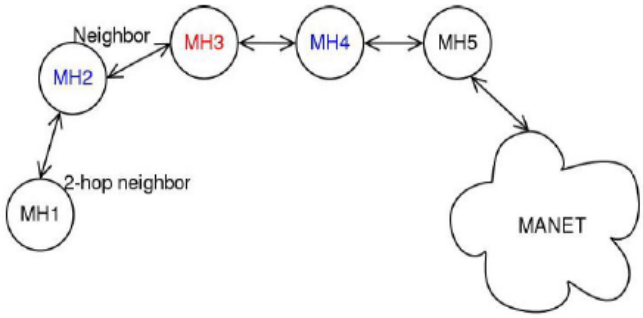


Fig 3.5 Topología de red.

En este dibujo podemos ver una red con 5 nodos colocados de manera estratégica para que todos ellos tengan un vecino a cada lado. En la siguiente tabla podemos ver un ejemplo de la tabla de enrutamiento del nodo MH3[17].

[17] http://www.mitre.org/tech_transfer/mobilemesh.html

		1	2	3
MH 2	Asim.Link	MH1	MH3	
	Sim.Link		MH1	MH1,MH3
	2-hop neibours			MH4
MH 3	Asim.Link		MH2,MH4	
	Sim.Link			MH2,MH4
	2-hop neibours			MH1,MH5
MH 4	Asim.Link		MH3	MH3,MH5
	Sim.Link	MH5	MH5	MH2,MH4
	2-hop neibours			

Tabla 3.2 tabla de enrutamiento del nodo MHP

En la tabla 3.2 podemos ver que los vecinos pueden estar en dos estados como enlace asimétrico o simétrico según la calidad de los enlaces en el momento en

el que llegan los paquetes. Cada una de las columnas de la tabla indican un momento del proceso de recepción de paquetes de señalización. En la tercera columna se puede observar que ya ha llegado a converger la red. En cambio en las dos primeras columnas había nodos que no se habían detectado o incluso algunos que se habían detectado pero no se había comprobado la comunicación en ambos sentidos. También se puede ver en esta tabla como los vecinos a dos saltos son aquellos que son vecinos de algún nodo que tenemos en el estado de enlace simétrico.

3.2.2 Protocolos de ruteo basados en position-based

Esta clase de algoritmos de ruteo son paquetes enviados basados en la posición geográfica del nodo a llegar, sus nodos vecinos, y el destino. Estos protocolos requieren que cada nodo conozca su posición geográfica. La posición del destino ha ser dada por un *location service*.

Es un algoritmo simple de búsqueda, tal como el greedy forwarding puede ser usado con esta información de la posición. El paquete se envía al vecino mas cercano del nodo destino. Sin embargo el algoritmo simple de búsqueda puede

acercarse pero no alcanzar el nodo destino aunque exista un enlace con el destino según lo ilustrado en el figura 3.6

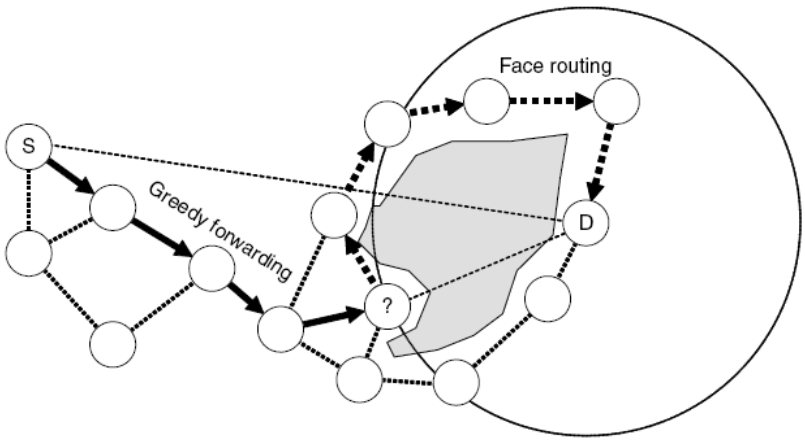


Fig. 3.6 Expedición basada en posición

FACE ROUTING

Se utiliza generalmente como estrategia del retraso del grafico de la red es lógicamente segmentado en donde los enlaces considerados no se cruzan con otros. Esta plantación de la red de tráfico se puede hacer localmente con algoritmos distribuidos.

Como hemos visto hasta ahora, los algoritmos basados en distancia se comportan cada vez mejor conforme aumenta la densidad, tendiendo al camino mas corto; no requieren memoria en los nodos ni en el mensaje, están libres de bucles, son de camino simple y trivialmente robustos a nodos que desaparecen o se mueven. Su gran defecto es, pues, el problema de los mínimos locales en que existe un hueco en la red que no pueden sortear. Si bien esto es solventable mediante inundaciones locales, entonces se pierde la propiedad de camino simple.

Para solventar este problema se han propuesto una serie de soluciones que se ha dado en llamar encaminamiento en facetas, teselas, perímetro, o regla de la

mano derecha (face routing, perimeter routing, right-hand rule). La idea que subyace al encaminamiento en facetas es la siguiente: tómese un grafo plano (esto es, cuyas aristas no se cortan) arbitrario. Llamamos faceta o tesela a cada polígono delimitado por las aristas del grafo (Ver Fig.3.7). Tenemos f facetas, de las cuales f − 1 son finitas y una de ellas es infinita; esta ultima es la faceta exterior que envuelve a todas las demás. Si tenemos dos nodos origen y destino y los unimos con una recta imaginaria, esta recta interfecta con un subconjunto de facetas. La regla de la mano derecha nos dice que si seguimos una figura poligonal manteniéndonos siempre en contacto con la mano derecha en la “pare”, la rodearemos en sentido horario si estamos en el exterior, o en sentido antihorario si estamos en el interior. En cualquier caso, el dato relevante es que antes o después regresaremos al punto de origen.

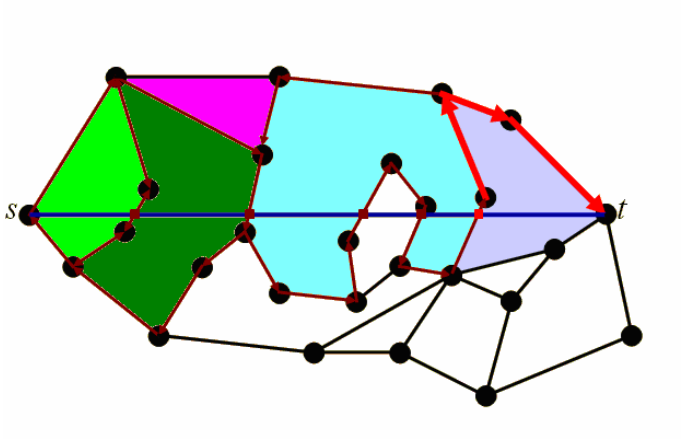


Fig. 3.7 Encaminamiento en grafos planos mediante facetas.

Sabiendo esto, el paquete parte del nodo origen y se envía a recorrer la faceta que contiene dicho nodo y que está más próxima al destino, intersecando la recta Origen-Destino. De algún modo se determina otro nodo en esta faceta que también pertenece a la siguiente faceta más próxima al destino, y allí se efectúa un cambio de faceta hacia el destino. Si el grafo es conexo, se puede probar que se alcanzaría el destino en un número finito de pasos. No hay que olvidar que estamos considerando también la faceta infinita.

A la vista de estos primeros resultados queda claro que los algoritmos en la familia FACE son costosos en comparación con los voraces. Su ventaja radica en la garantía de entrega.

GPSR

Uno de los primeros protocolos de ruteo position-based prácticos para las redes inalámbricas es el Greedy Perimeter Stateless Routing mas conocido por sus siglas como (GPSR). El GPRS combina el greedy forwarding con el fase routing fallback.

GPSR, es un protocolo que reacciona rápidamente, además de un eficiente protocolo de ruteo para redes móviles inalámbricas. Este algoritmo es distinto a los algoritmos de ruteo antes mencionados , que utilizan nociones gráfico-teóricas de las trayectorias más cortas y de la capacidad transitiva para encontrar las rutas, GPSR explota la relación entre la posición y la conectividad geográficas en una red inalámbrica, usando las posiciones de nodos para tomar decisiones con respecto a el forwarding de los paquete. GPSR utiliza *greedy forwarding* para remitir los paquetes a los nodos que están siempre progresivamente más cercano a el destino. En las regiones de la red donde no existe una camino greedy (es decir, la única trayectoria requiere que un movimiento temporalmente se encuentre mas lejos del destino), GPSR se recupera por la busqueda en perimeter mode, en el cual un paquete atraviesa caras sucesivas más cercanas de un subgraph planar del gráfico de radio completo en la conectividad de la red, hasta alcanzar un nodo más cercano a necesitada (nodo destino), donde el greedy forwarding termina.

GPSR permitirá la construcción de las redes que no pueden escalar con los algoritmos anteriores del encaminamiento para las wire networks y wireless network. Tales clases de redes incluyen:

Rooftop networks:(Redes del tejado) despliegue fijo, denso de números extensos de nodos.

Redes ad hoc: densidad móvil, que varía, ninguna infraestructura fija

Redes del sensor: densidad móvil, potencialmente grande, números extensos de los nodos, recursos empobrecidos del por-nodo

Redes de vehículos: densidad móvil, no-energía-obligada, movilidad.

Esta nueva tecnología permite desdoblar la transmisión de voz y datos en diferentes canales que transmiten de forma paralela, permitiendo mantener conversaciones sin cortar la transmisión de datos. En GPRS se puede elegir entre varios canales, de forma similar a como se realiza en Internet. El aumento de la velocidad se produce porque los datos se comprimen y se envían a intervalos regulares, llamado conmutación por paquetes, lo que aprovecha mejor la banda de frecuencia.
La mayor ventaja de GPRS no es la tecnología en si misma sino los servicios que facilita. Los terminales de este nuevo sistema permiten personalizar funciones, desarrollar juegos interactivos, e incorporan aplicaciones para el intercambio de mensajes y correos electrónicos, a los cuales se podrá acceder directamente sin la necesidad de conectarse a Internet. Incorporan además una ranura para introducir la tarjeta de crédito con chip que facilitará las transacciones electrónicas más seguras. Con la tecnología GPRS se da un paso hacia la localización geográfica, en función de donde se encuentre el usuario, la operadora le puede ofrecer mayor información de la zona.

3.2.3 Hybrid wireless mesh protocol (HWMP)

HWMP es el protocolo de encaminamiento por defecto para el establecimiento de una red enmallada WLAN. Cada dispositivo que es regido por IEEE 802.11s será capaz de usar este protocolo de encaminamiento. La naturaleza híbrida y la flexibilidad de configuración de HWMP proporcionan un buen funcionamiento en todos los panoramas anticipando su uso.

La realización de HWMP es una adaptación de ruteo reactivo al protocolo AODV, a la capa 2 y a la métrica radio-aware llamada la radio métrica AODV (RM-AODV). Un nodo mesh, generalmente un portal mesh, puede ser configurado periódicamente anunciando una difusión, que es fijado en la cima que la cual permite el ruteo proactive hacia este portal en mallado.
La parte reactiva de HWMP sigue los conceptos generales de AODV según lo descrito antes. El protocolo HWMP Utiliza el método de vector distancia y el proceso de descubrimiento de la ruta con la petición de la ruta y su respuesta respectiva. Los números de serie de la destinación se utilizan a reconocer la vieja información de ruteo. Sin embargo, hay significativas diferencias en los detalles. La Fig. 3.8 muestra la estructura de la Petición de la ruta de HWMP para ilustrar las nuevas características.

HWMP utiliza direcciones MAC como protocolo de ruteo para la capa 2 en vez de direcciones IP. Además, HWMP puede hacer uso de una métrica de ruteo más sofisticada que el hopcount tal como métricas radio-aware. Un campo métrico de la nueva trayectoria es incluida en los mensajes de RREQ/RREP que contiene el valor acumulativo de los enlaces métricos de la trayectoria hasta ahora. El ruteo por default métrico de HWMP es el airtime métrico donde las métricas separadas del enlace se agregan hasta conseguir la trayectoria métrica.

Puesto que los cambios métricos radio-aware son utilizados mas a menudo que el hopcount métrico, es preferible tener solamente el destino a contestar a RREQ de modo que la trayectoria métrica sea actualizada. Por esta razón, la flag de la destinación solamente es fijada (DO=1) por default en HWMP.

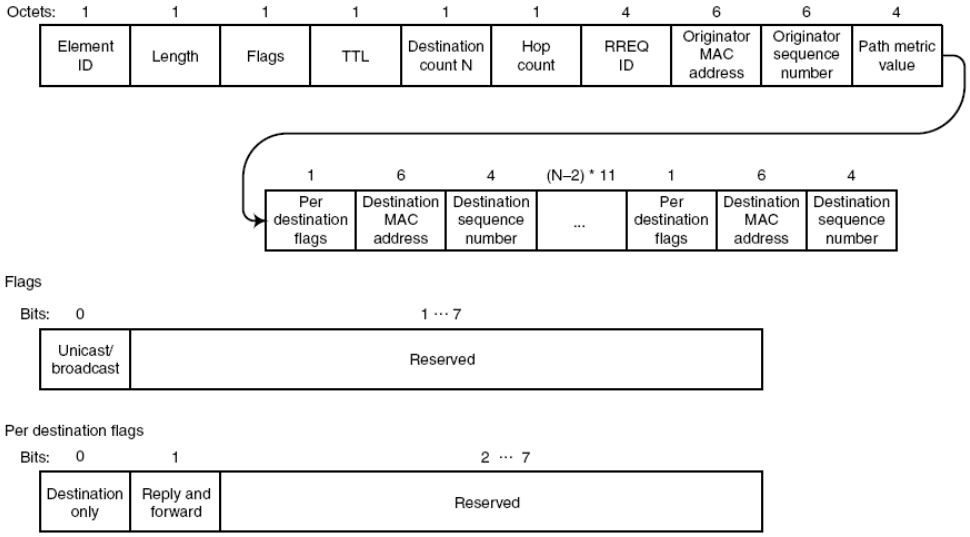


Fig 3.8 ruta de petición de HWMP

Explícitamente fijando la bandera de el destino solamente DO=0, es posible dejar nodos intermediarios para la respuesta. Esto da un estado latente más corto para descubrimiento de la ruta. Pero el camino métrico no está actualizado. Por lo tanto, el nodo intermedio que contestó con un RREP remitirá el RREQ a el destino. Esto es controlado por una respuesta y una forward flags. También es fijada por el defecto (RF=1), pero puede ser un set (variable) para conseguir el comportamiento tradicional de AODV. La bandera de el destino serà fijada en el RREQ remitido.(DO=1). Esto evita que otros nodos intermedios generen las contestaciones de la ruta y que pudieran ser muchas.

Cualquier información de encaminamiento recibida (RREQ/RREP) se comprueba para saber si hay validez con una comparación número de serie (sequence number). La información de encaminamiento es válida si el número de serie no es más pequeño que el número de serie en la información anterior.

Si los números de serie son iguales y la información de ruteo, que es la trayectoria métrica, es mejor, entonces la nueva información será utilizada y el nuevo mensaje será procesado.

HWMP puede utilizar el mantenimiento RREQs periódico para mantener una mejor trayectoria métrica entre la fuente y el destino de trayectorias activas. Esto es una característica opcional. HWMP permite destinos múltiples en los mensajes de RREQ, que reduce los gastos indirectos del ruteo cuando un nodo mesh tiene que encontrar las rutas a varios nodos simultáneamente. Éste es el caso para reparar enlaces rotos y para el mantenimiento RREQs.
Algunas flags pueden tener valores diferentes para cada destino. Por esta razón, flags destinadas son asociadas con cada destino y secuencia numérica. Esas son las flags específicamente relacionadas a la generación de los mensajes RREP.
Un campo explícito del Time to Live (TTL) es necesario, puesto que no hay nada en la cabecera como en AODV tradicional.

El uso de la extensión preactiva a RM-AODV es configurable. La extensión proactive utiliza la misma metodología vector distancia como RM-AODV y hace uso mensajes de ruteo de RM-AODV.

Utilizar la extensión proactive, por lo menos un portal mesh tiene que estar configurado para difundir periódicamente broadcast del portal mesh. Esto acciona una selección de la raíz y un proceso del mediador, fuera de los cuales un solo portal de la raíz se desarrolla. El portal fija el tipo de aviso de la bandera a 1 (raíz) en sus avisos periódicos del portal del acoplamiento. En recibo de el aviso del porta de la raíz, un nodo mesh instalará una camino al portal de la raíz, un nodo mesh que recibió el aviso portal de la raíz con la mejor trayectoria métrica. Una camino al portal mesh es anunciado, se puede también instalar en el recibo de avisos portal con el tipo flag del aviso fijada a 0

(portal). La disposición de la trayectoria conducirá a un árbol fundamentado en el portal de la raíz (acoplamiento).

Si la bandera de registro no se fija en el mensaje del aviso (non-register mode), el proceso de los avisos de raíz son paradas aquí. Cuando un nodo mesh desea enviar tramas de los datos portadle la raiz, puede enviar un RREP gratuito al portal de la raíz inmediatamente antes del primer paquete de datos. Esto instalará el camino el portal de la raíz al nodo de la fuente.

Si la bandera del registro se fija en el mensaje del aviso (registration mode), el nodo mesh espera cierto rato para la raíz adicional los mensajes llegados pudieron también publicar un RREQ[18] con TTL=1 explícitamente para pedir a sus nodos vecinos rutas a la raíz portal. El nodo mesh elige la trayectoria con la mejor trayectoria métrica a el portal de la raíz. Se coloca con el portal de la raíz enviando un gratuito RREP al portal de la raíz. El registro tiene que ser cada vez que el nodo cambia su nodo original.

Una descripción de las diversas opciones de la configuración de HWMP es demostrado en la Fig. 3.9.

[18]Wireless mesh networking “Architectures, Protocols and Standards” 2006 Yan Zhang • Jijun Luo • Honglin Hu pag 125-147

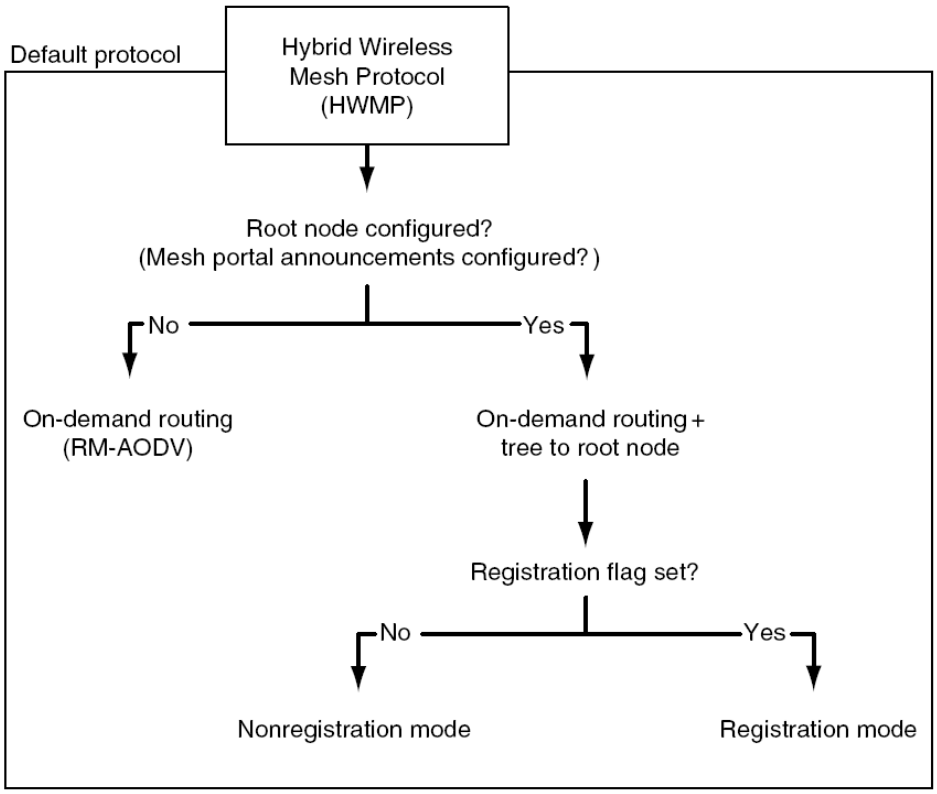


Fig 3.9 Configurabilidad de HWMP

4. SEGURIDAD Y FABRICANTES EN WMN

4.1 USO DE LAS CAPAS DEL MODELO OSI EN REDES MESH

4.1.1 Capa física

A través del tiempo se han hecho comprobaciones, acerca de las técnicas avanzadas que se usan en esta capa y que están disponibles para las redes inalámbricas enmalladas. Y se ha llegado a la conclusión que debido a la gran densidad de nodos que poseen estas redes y al espectro limitado, es indispensable optimizar el uso de los canales minimizando las interferencias. Estos mecanismos son la selección dinámica de frecuencia (DFS) y el control de potencia (TPC).

Con el fin de aumentar la capacidad, mitigar la atenuación, delay e interferencia entre canales, se han creado sistemas multi-antenas como es el caso de las antenas pequeñas y los sistemas MIMO que hace uso de esta tecnología con fin de conseguir capacidades superiores a los 108 Mbps en el enlace inalámbrico.

Por otro lado existen otras tecnologías de radio que usan las técnicas como son el acceso múltiple de la frecuencia ortogonal (OFDM) y Banda ultra-ancha (UWB).

4.1.2 Capa Mac

Existen grandes diferencias entre la capa de acceso al medio en una WMNs y las contrapartes clásicas de las redes inalámbricas. Las redes clásicas poseen serias limitaciones en los multisaltos debido a los problemas del nodo oculto y el nodo expuesto.

Existen mecanismos de acceso al medio que son muy útiles para las redes Mesh como es el caso de TDMA (Time Division Multiple Access) y CDMA (Code Division Multiple Access) los cuales pueden disminuir los efectos de las

interferencias, ya que dos nodos pueden ocupar simultáneamente el mismo empleando códigos diferentes.

Protocolos convencionales

La principal responsabilidad de los protocolos de la capa MAC es asegurar el compartimiento de recursos. Hay dos grandes categorías de los esquemas MAC como son los protocolos basados en contención y los protocolos basados en libres colisiones de los canales.

Los protocolos basados en contención asumen que no hay entidad central que asigne los canales en la red. Para transmitir cada nodo debe contener su propio medio. Las colisiones resultan cuando más de un nodo trata de transmitir al mismo tiempo. Como es bien sabido los protocolos basados en contención incluyen Aloha, CSMA y CSMA/CA. En contraste, los protocolos de de libre colisión asigna canales dedicados a cada nodo que desea comunicarse. Los protocolos de libre colisión pueden eliminar colisiones con eficacia, liberando asi los canales de alto trafico. Ejemplos de estos protocolos son el TDMA, CDMA y FDMA.

ALOHA y SLOTTED ALOHA

La importancia de ALOHA se basa en que usaba un medio compartido para la transmisión. Esto reveló la necesidad de sistemas de gestión de acceso como CSMA/CD, usado por Ethernet. A diferencia de ARPANET donde cada nodo sólo podía comunicarse con otro nodo, en ALOHA todos usaban la misma frecuencia. Esto implicaba la necesidad de algún tipo de sistema para controlar quién podían emitir y en qué momento. La situación de ALOHA era similar a las emisiones orientadas de la moderna Ethernet y las redes Wi-Fi.

En Aloha, cada estación transmite los mensajes conforme le van llegando, de modo que si más de una estación tiene mensajes para transmitir, los paquetes

colisionan en el canal destruyéndose. Cada estación interpreta que se ha producido colisión si al vencer un determinado temporizador de time out, no se ha recibido reconocimiento del mensaje enviado. De este modo, tras la colisión, cada estación retransmitirá el mensaje transcurrida una cantidad de tiempo aleatoria. Hay que señalar que aunque solamente una parte del paquete transmitido haya sido destruido (colisión parcial), la estación retransmitirá el paquete completo. El inconveniente es que, si la red está saturada, el número de colisiones puede crecer drásticamente hasta el punto de que todos los paquetes colisionen. Para ALOHAnet el uso máximo del canal estaba en torno al 18%, y cualquier intento de aumentar la capacidad de la red simplemente incrementaría el número de colisiones, y el rendimiento total de envío de datos se reduciría, fenómeno conocido como colapso por congestión.

En aloha rasurado los mensajes se transmiten sólo en determinados intervalos de tiempo llamados slots, lo cual tiene el efecto de doblar el rendimiento efectivo del sistema puesto que en este caso los paquetes, ó no sufrirán colisión, ó la colisión afectara al paquete completo (dos o más estaciones transmitiendo sobre el mismo slot).

Los mecanismos de detección de colisiones son mucho más difíciles de implementar en sistemas inalámbricos en comparación con los sistemas cableados, y ALOHA no intentó siquiera comprobar las colisiones. En un sistema cableado, es posible detener la transmisión de paquetes que colisionen, detectando primero la colisión y notificándolo a continuación al remitente. En general, esta no es una opción viable en sistemas inalámbricos, por lo que ni siquiera se intentó en el protocolo ALOHA[19].

---

[19]Diseño de protocolos MAC para redes ad-hoc utilizando antenas direccionales inteligentes. Septiembre del 2005

VENTAJAS DE ALOHA RANURADO SOBRE ALOHA PURO

- La eficiencia de este protocolo es el doble que la del protocolo aloha puro
- Se adapta a un número variable de estaciones

DESVENTAJAS DE ALOHA RANURADO

- Se requiere de sincronización entre estaciones para determinar
- Requiere almacenar la trama transmitida debido posibles retransmisiones

CSMA/CD

El protocolo CSMA/CD (Acceso Múltiple con Escucha de Portadora y Detección de Colisiones) es una técnica usada en redes Ethernet para mejorar sus prestaciones. Anteriormente a esta técnica se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones. Por eso apareció primeramente la técnica CSMA, que fue posteriormente mejorada con la aparición de CSMA/CD. Significa que se utiliza un medio de acceso múltiple y que la estación que desea emitir previamente escucha el canal antes de emitir.

CSMA/CD supone una mejora sobre CSMA, pues la estación está a la escucha a la vez que emite, de forma que si detecta que se produce una colisión, para inmediatamente la transmisión. La ganancia producida es el tiempo que no se continúa utilizando el medio para realizar una transmisión que resultará inútil, y que se podrá utilizar por otra estación para transmitir.

Protocolos IEEE 802.11 CDF

DCF esta basado en CSMA/CA y opera de manera similar. Un nodo que desea trasmitir primero sensa el canal. Si se encuentra el medio ocupado, se sensa hasta encontrarlo libre.

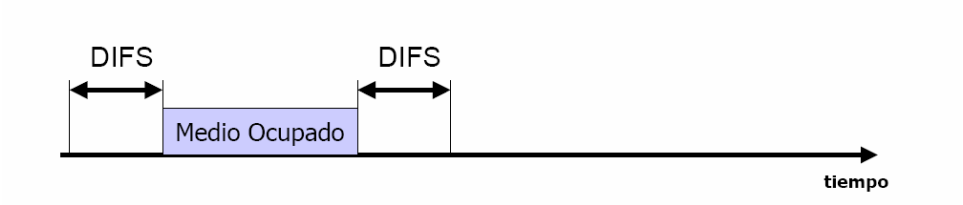


Fig 4.1 Censado del canal de CFS[20]

Si el medio esta libre para un determinado periodo de tiempo llamado DIFS (distributed inter frame space) el nodo puede transmitir.

SI el receptor recibió correctamente el paquete este envía un mensaje ACK después de fijar un periodo de tiempo llamado SIFS (short Inter frame space).

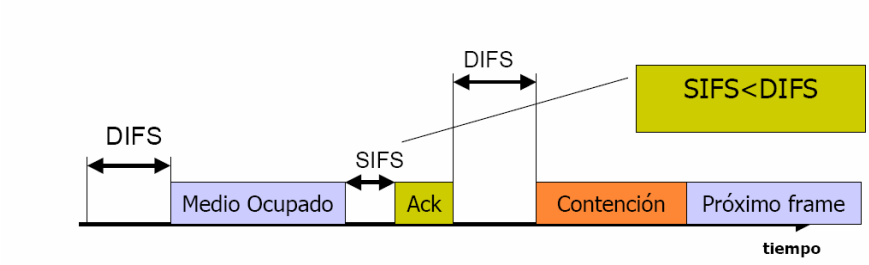


Fig 4.2 Mecanismo de transferencia Datos y ACK

Si el ACK no es recibido el transmisor asume que ha ocurrido una colisión y doblega el tamaño del paquete de su ventana de contención. Luego el transmisor escoge un número de random Back-off entre cero y su ventana de contención.

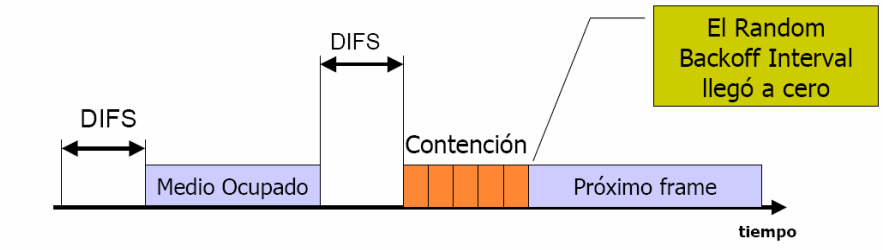


Fig. 4.3 Ventana de contención en CFS

[20]www.ewh.ieee.org/reg/9/etrans/vol3issue4Oct.2005/3TLA4_1Britos.pdf

El transmisor permitirá la transmisión del paquete cuando el canal es libre para un DIFS aumentado por el tiempo random back-off. El paquete se cae después de un número dado de retransmisiones fallidas.

Para reducir las coliciones, el estándar define un mecanismo de sensado de portadora. Un nodo que desea transmitir, primero transmite un paquete pequeño de control llamado RTS, el cual incluye fuente, destino y duración de transmisión del paquete. Si el medio esta libre el receptor responde con un mensaje CTS que incluye la duración del paquete de datos y su ACK. Cualquier nodo esta recibiendo el RTS y/o CTS se asigna un vector (NAV) el da la duración. Una vez pasa esto el NAV cuenta en forma decreciente hasta llegar a cero. Un nodo no puede transmitir hasta que el NAV no llegue a cero.
La información de la duración llevada por el RTS protege el transmisor de colisiones cuando recibe el ACK.

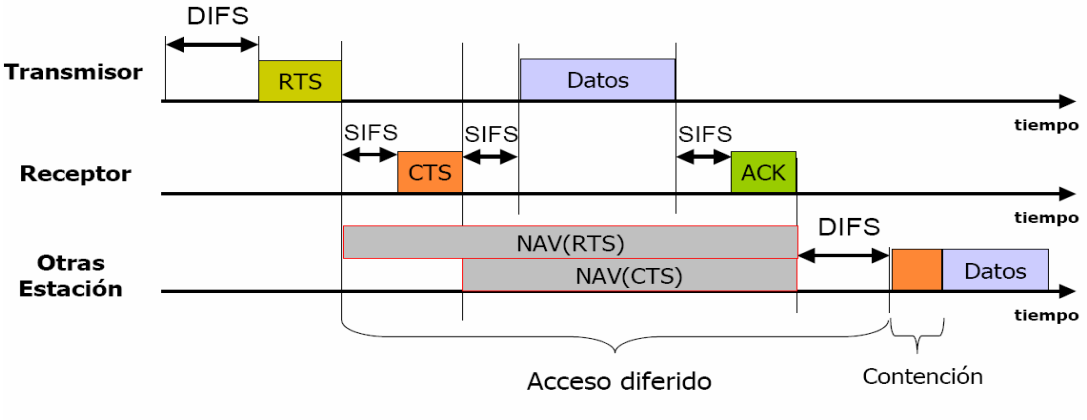


Fig 4.4 Network Allocation Vector (NAV)

Protocolos IEEE 802.11e

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo

IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

(EDCA) Enhanced Distributed Channel Access y (HCCA) Controlled Access.

El denominado EDCA es el acceso con contención que representa una evolución del acceso DCF del estándar IEEE 802.11. Por el otro lado el HCCA corresponde al acceso sin contención basado en polling. Obviamente, el nuevo modo de operación HCCA, en tanto que considera un control acceso centralizado, supone la mejor alternativa para soportar la QoS. Sin embargo los sistemas centralizados suponen más complejidad, no son eficientes para transmisiones de datos y necesitan sincronización. Es por ello que el modo centralizado PCF del IEEE 802.11, predecesor del HCCA, apenas ha sido implementado, lo que sin duda cuestiona la futura implementación del modo HCCA. A pesar de los posibles inconvenientes en términos de QoS, el acceso con contención es más sencillo, fácil de instalar y no supone gran coste en cuanto a mantenimiento y gestión. Además su uso, tipo “plug and play” es más cómodo para el usuario, por lo que es previsible que, al menos inicialmente, el estándar IEEE802.11e centre su desarrollo en el modo EDCA. Por consiguiente el desarrollo de técnicas de gestión de recursos que garanticen la QoS cuando se opera en contención con el mecanismo EDCA resulta imprescindible. Al mismo tiempo, y debido a su naturaleza, la gestión de recursos radio en EDCA supone también un desafió relevante. Como la operación de HCCA y PCF requieren una central de control y sincronización entre nodos y esto es complicado para las redes Mesh, por este motivo hay que fijar la atención en EDCA.

Protocolos Mac avanzados para WMNs

Los protocolos diseñados para WMNs asumen antenas omnidirecionales que transmiten señales de radio y reciben señales de todas las direcciones. Cuando dos nodos se están comunicando, todos los otros nodos de entre los

vecinos tienen que seguir siendo silenciosos, mientras tenga un impacto negativo en la capacidad[21]. De otro modo la capacidad disminuye con el aumento del número de nodos. Con las antenas direccionales (antenas elegantes incluyendo), dos pares de nodos situados en de cada uno de los radios vecinos puede comunicarse potencialmente y simultáneamente, dependiendo en las direcciones de la transmisión.

Para nodos equipados con antenas direccionales, ocurre el problema del nodo oculto que ocurre cuando dos transmisores están cerca y sus antenas apuntan en diferentes direcciones, entonces estos son invisibles entre ellos mientras se causan colisiones en el receptor.

Existen cinco problemas que se plantean al usar antenas direccionales como son el Nodo expuesto direccional, Desconocimiento del estado del canal, Nodos ocultos debido a asimetría en ganancia, Formas de las regiones "silenciosas" y "Deafness".

Nodo expuesto direccional

A quiere enviar un paquete a B, y E quiere enviar un paquete a C. El nodo A envía el RTS direccionalmente al nodo B, pero esta transmisión la oye el nodo de manera que no puede enviar el paquete aun no interfiriendo en la comunicación A-B. El nodo E está direccionalmente expuesto.

Desconocimiento del estado del canal

A está transmitiendo un paquete a D después del envío RTS-CTS. El nodo E que no escucha esta transmisión decide enviar un RTS al nodo B. Cuando A acaba de transmitir, decide enviar al nodo F ya que no sabe que hay una Comunicación entre E y B. A interfiere en esta comunicación. Éste sería un caso de desconocimiento del estado del canal del nodo A.

---

[21]http://www.ceditec.etsit.upm.es/InfTecnologia

Nodos ocultos debido a asimetría en ganancia

El nodo B envía un RTS direccional (DRTS) al nodo F. El nodo F responde con un CTS direccional (DCTS) de ganancia Go. El nodo A tiene un paquete a Transmitir al nodo E. Y determina el canal libre ya que no le llega la potencia de la antena F. El nodo A por lo tanto envía un DRTS con ganancia Gd al nodo E que sí oye la transmisión del nodo F. De esta manera hay interferencia y por lo tanto colisión de paquetes y los datos no llegan correctamente al receptor.

Formas de las regiones "silenciosas"

Debido al aumento de la ganancia en antenas direccionales las formas de las zonas "silenciosas" o sin cobertura son diferentes en antenas omnidireccionales y antenas direccionales. Esto afecta indirectamente en características topológicas como patrones de tráfico y ancho del lóbulo de la transmisión direccional.

"Deafness"

Para explicar este problema debido al uso de antenas direccionales, utilizaremos el escenario de la Fig. 4.5. Los nodos C y D quieren transmitir al nodo B a través del nodo E. Si E responde el paquete de D, C no lo sabría con DMAC y transmitiría un RTS a E. E al tener el lóbulo dirigido a D no recibe el RTS de C. De manera que E vuelve a retransmitir. E está "sordo" ya que no

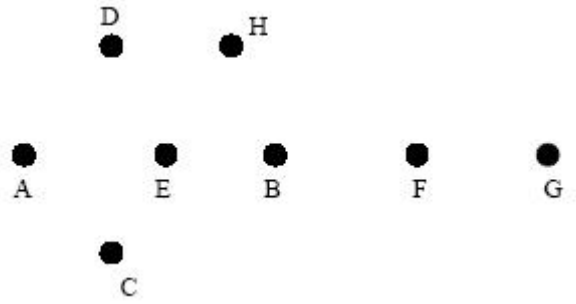


Fig. 4.5. Escenario ejemplo de nodos ocultos debidos a asimetría en Ganancia.

oye las transmisiones del nodo C en otra dirección. Esto provoca un desperdicio de la capacidad de la red en envíos de paquetes de control innecesarios.

A diferencia de estos nodos están los que están equipados con antenas omnidireccionales, en los cuales el problema del nodo oculto no ocurre. El problema deafness ocurre cuando falla la comunicación entre el transmisor y el receptor porque el receptor esta escuchando en otra dirección.

La interferencia direccional[22] alta es causada por la alta ganancia en las antenas. Para estos problemas están algunos protocolos MACs basados en la 802.11 DCF el cual comprende RTS, CTS, DATA y ACK. El DCF transmite los mensajes de control y datos omnidireccionalmente con antenas direccionales. Se pueden manejar antenas direccionales usando diferentes combinaciones de mensajes direccionales y omnidireccionales.

Los protocolos MAC donde se utilizan las antenas direccionales se denominan Direccional-MAC (DMAC).

Antenas usadas en la capa Mac

Existen dos esquemas importantes que son utilizados en esta capa como son: las antenas MACs direccionales y las antenas MACs con energía controlada.

Por otro lado el IEEE esta trabajando en el estándar 802.11s y propone el MMAC (Multichannel MAC) y HMCP (Hybrid Multichannel Protocol). En MMAC se emplean varios canales con una sola interfaz de radio, por lo que se requiere señalización y coordinación con el fin de que todos los nodos escuchen el cana adecuado en cada momento. Por otra parte en HMCP los nodos tienen varias interfaces, unas trabajan en canales fijos y otros variables, empleando los canales fijos para control y señalización.

---

[22]http://www.wifinetnews.com/

Antenas MACs direccionales: El primer sistema elimina todos los nodos expuestos si la viga de la antena se asume como perfecta. Sin embargo, debido a la transmisión direccional, se producen nodos ocultos. Estos esquemas también hacen frente a otras dificultades tales como costo, complejidad del sistema, y sentido práctico de antenas direccionales orientables rápidas.

Antenas MACs con energía controlada: Este sistema reduce nodos expuestos, usando energía baja de la transmisión, y mejora así el factor espacial de la reutilización del espectro en WMNs. Sin embargo, la aplicación de los nodos ocultos puede llegar a ser peor porque una transmisión baja más el nivel de la energía y reduce la posibilidad de detectar un nodo potencial que interfiere. Proponer protocolos innovadores en la capa MAC, no es una buena solución sabiendo que se tiene una pobre escalabilidad en una red multi-hop, en este caso es imprescindible el uso de los protocolos TDMA y CDMA.

Diseño de un protocolo MAC 802.11 con antenas Direccionales

Rehúso espacial: En anteriores estudios se confirma que el uso de antenas direccionales aumenta el rehúso espacial con el uso de un protocolo MAC Específico para antenas direccionales.

Mayor alcance: Además, el uso de antenas direccionales permite tener un mayor alcance a los nodos de la red. Todas las transmisiones son direccionales ya que de esta manera se utiliza todo el rango de cobertura posible con antenas direccionales y no se ocupa el canal innecesariamente con Transmisiones omnidireccionales.

NAV direccional: Adaptando el mecanismo de NAV a antenas direccionales se diseña un mecanismo para que los nodos vecinos puedan conocer si hay una transmisión que puedan dañar y así retrasar su intento de transmisión.

Tabla de localización: La localización de los nodos no se asume a priori a diferencia de los antiguos protocolos ya que existe un mecanismo que informa a los nodos de la localización de los nodos vecinos.

Solución a los nodos ocultos: Este protocolo aporta una solución para reducir el problema de nodos ocultos que aparece al utilizar antenas direccionales. De esta manera, el número de colisiones será menor y aumentará el *throughput*.

RTS circular

Este protocolo está basado en el envío de RTS circular como en [6]. La transmisión del RTS es direccional y se envía consecutivamente y circularmente a todos los nodos vecinos. Se asume que todos los nodos tienen un máximo de antenas que cubre el área del transmisor. Primero se envía un RTS en una dirección predefinida como es la primera antena direccional, la antena 0. Seguidamente se envía un RTS en la dirección de la segunda antena, 1. Se envía un RTS en las direcciones de las antenas hasta llegar al máximo de antenas.
Cuando el nodo transmisor acaba de enviar todos los RTS por todas las antenas del nodo y, por lo tanto el nodo receptor habrá recibido el RTS, se envía el CTS direccional. En este protocolo el envío del CTS también es circular a diferencia de [6] que explicamos en la siguiente sección.

El uso de RTS y CTS circular va a resolver el problema de nodos ocultos. Además permite mantener actualizada una tabla de localización con lo que no es necesario un sistema extra de localización, como podría ser Global Positioning System (GPS). En contrapartida, el uso del RTS y el CTS circular va a alargar el tiempo de una transmisión ya que se necesitan más slots times para hacer el recorrido circular.

Si al añadir los mecanismos de RTS y CTS circular el tiempo necesario para efectuar una transmisión se alarga, significa que el *throughput* va a ser menor. Sin embargo, la principal ventaja del uso de antenas direccionales, como se ha comentado anteriormente, es que permiten que más de dos parejas de nodos se comuniquen al mismo tiempo aún así estando próximos. Este efecto se ha denominado "rehúso espacial". Esta ventaja va a significar un aumento del *throughput* total del sistema y aunque ahora con este nuevo esquema el tiempo para realizar una transmisión sea mayor, el *throughput* que se consigue gracias Al rehúso espacial va a ser mayor. Ante este nuevo esquema se espera que cuantos más nodos y cuanto mayor sea el número de antenas direccionales, el Rehúso espacial hará que el *throughput*[23] aumente cada vez más exponencialmente. En definitiva, cuanto mayor es el número de nodos y cuanto Mayor es el número de antenas direccionales en cada nodo, mayor es el número de posibles combinaciones de parejas de nodos que pueden comunicarse a la vez. Continuando con la explicación del RTS circular, cuando los nodos vecinos reciben el RTS sabrán si deben retrasar su intento de transmisión con un mecanismo que se detalla más adelante.

Una vez se envía el último RTS el transmisor escucha el medio omnidireccionalmente a la espera de la recepción del CTS del nodo receptor. Si éste llega antes de un tiempo predefinido (CTS timeout), el receptor envía los datos y el receptor envía el ACK. El paquete de datos y el de ACK son enviados de la misma manera que en el tradicional protocolo MAC 802.11, pero con la diferencia que todas estas transmisiones se realizan con antenas direccionales.

---

[23]http://nodos.typepad.com/nodos_prime/2007/01/toma_de_decisio.html

Es decir, la segunda gran ventaja del uso de antenas direccionales es que su alcance es mayor. Las antenas direccionales concentran toda la energía en una sola dirección, obteniendo un diagrama de radiación en el que el lóbulo principal está enfocado en la dirección de interés y el resto de los lóbulos quedan minimizados. Como conclusión, una antena direccional puede llegar a transmitir a nodos más lejanos que una antena omnidireccional con la misma Cantidad de energía disponible para la transmisión. Y, por lo tanto, también una antena direccional necesita menos energía para transmitir a un nodo que esté a una distancia alcanzable por una antena omnidireccional. Para conseguir esto último sería necesario un esquema de control de la potencia de transmisión de la antena.

La Fig.4.6 muestra el mecanismo del RTS circular. Este mecanismo se describe en la siguiente sección, junto al mecanismo del CTS circular.

CTS circular

El esquema del CTS circular es el mismo que el del RTS circular. Cuando el nodo receptor recibe el RTS, y después del envío del RTS por la última antena del nodo transmisor, el nodo receptor envía el CTS en la dirección del nodo transmisor. Seguidamente se envía un CTS por todas las antenas e informa de esta manera a los nodos vecinos que hay una transmisión.
En la Fig.4.6 el nodo 2 tiene un paquete para el nodo 4. De manera que envía un RTS al nodo 4 por la antena 0 y posteriormente envía un RTS por la antena 1 a los nodos vecinos para informar de la transmisión. De manera que los nodos 0, 1 y 3 serán informados de dicha transmisión, Cuando se envía el RTS por la última antena, si el nodo receptor, 4, lo recibe correctamente, se envía un CTS en la dirección del nodo transmisor con la antena 1.
Seguidamente el nodo receptor envía el CTS por la antena 0 y los nodos 5 y 6 serán informados de la transmisión. Si el envío del CTS no fuera circular los nodos 5 y 6 no estarían informados de la transmisión y podrían intentar enviar

un paquete por la antena 1 y destruir la comunicación. Con el envío del CTS circular hay más nodos informados de la comunicación de manera que se reducen los nodos ocultos y de esta manera las colisiones.

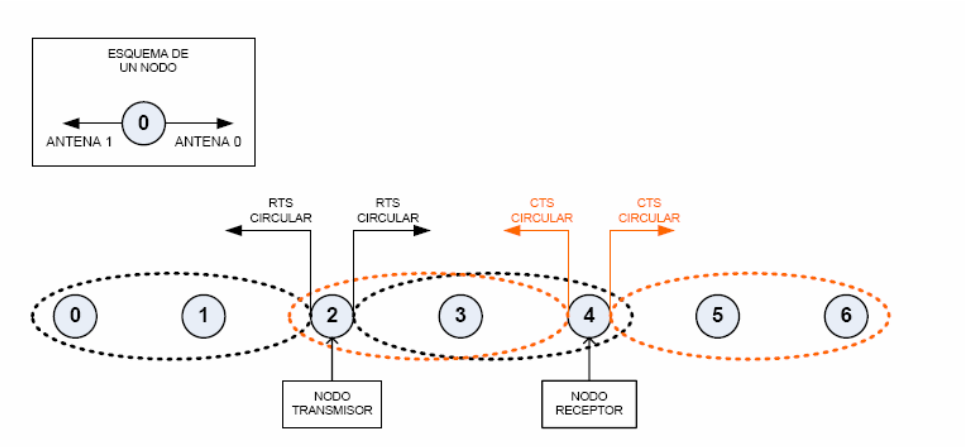


Fig.4.6 Mecanismos de RTS Circular y CTS Circular

Tabla de localización

Al utilizar RTS circular, este protocolo asegura que el RTS llega al nodo receptor. El RTS al llegar al nodo receptor podrá saber por diversidad selectiva la dirección por la cual ha recibido el RTS y así poder localizar dónde está el nodo transmisor. De la misma manera el nodo transmisor con la recepción del CTS puede saber la localización del nodo receptor.

Cada nodo tiene una tabla de localización como es explicada anteriormente. La tabla informa de qué nodo se trata, el nodo por el que se ha escuchado el paquete, la antena por el cual el transmisor escuchó el paquete y la antena por el cual el receptor escuchó el paquete[24].

En la Tabla 4.1 podemos ver la tabla de localización del nodo 0 correspondiente a la Fig. 4.7 El nodo 0 puede ver al nodo 1 por la antena 0 y

---

[24]Diseño de protocolos MAC para redes ad-hoc utilizando antenas direccionales inteligentes. Septiembre del 2005

el nodo 1 con la antena 4. El nodo 0 puede ver al nodo 2 por la antena 5 y el nodo 2 con la antena 1. Y finalmente, puede ver al nodo 3 por la antena 6 y el nodo 3 con la antena 2.

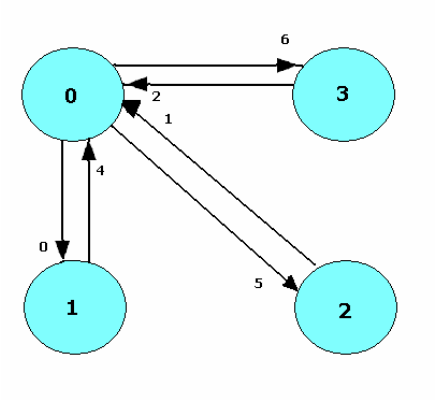


Fig.4.7 Envío de RTS y CTS

Nodo	Vecino	Antena	Antena del vecino
0	1	0	4
0	2	5	1
0	3	6	2

Tabla 4.1. Tabla localización Nodo 0 de la Fig 4.7

Al principio esta tabla está vacía. La tabla de localización se actualiza en cada recepción por la movilidad de los nodos. Esta información es importante para la Decisión de los nodos vecinos en enviar un paquete o atrasar esta transmisión.

4.1.3 Capa de red

A pesar de la disponibilidad de muchos protocolos del encaminamiento para las redes ad hoc, el diseño de los protocolos del encaminamiento para WMNs sigue siendo un área activa de la investigación. En realidad el protocolo óptimo de encaminamiento para WMNs debe tener diferentes características:

- Métrica de funcionamiento múltiple: Consiste en escoger la trayectoria adecuada para el envío de paquetes.
- Escalabilidad: Se requiere el uso de un protocolo que perdure mucho tiempo en funcionamiento y que sea útil para las nuevas tecnologías, puesto que las WMNs aun no se han explorado por completo.
- Robustez: Consiste en Evitar la interrupción del servicio, WMNs debe ser robusto para ligar faltas o la congestión. Los protocolos del encaminamiento también necesitan hacer balanceo de la carga.
- Infraestructura Mesh con ruteo eficiente: Los protocolos de encaminamiento se espera que sean más simples que los protocolos de una red Ad Hoc. Con la infraestructura Mesh proporcionada por los routers, el protocolo de ruteo para clientes Mesh pueden ser más simple.

De acuerdo a estas características se recomienda el uso de MANET (Mobile Ad-Hoc Networks) del IETF, que tiene dos tipos de protocolos: activos como es el caso de AODV (Ad-Hoc ondemand Distance Vector) y preactivos como es el OLSR (Optimizad Link State Routing).
Por otra parte, si los routers Mesh no tienen movilidad y sus rutas no varían tan dinámicamente, se pueden emplear otro tipo de protocolos, como el OSPF (Open Shortest Path First) con la extensión de movilidad que permita la autoconfiguracion de la red en el caso de que se caiga algún enlace.

Tipo de métricas funcionales: El impacto de la métrica del funcionamiento en un protocolo, es importante a la hora de Seleccionar una trayectoria según la métrica de la calidad del acoplamiento. Para esto se tienen en cuenta los siguientes tipos de ruteo:

- Encaminamiento de Multi-Radio: un multi-radio LQSR es una nueva métrica que asume que todas las radios en cada nodo están templadas a los canales que no interfieren con la asignación que cambia infrecuentemente.

- Encaminamiento multidireccional: Los objetivos principales con este tipo de encaminamiento es hacer una carga se balancee mejor y proporcionar alta tolerancia de avería. Las trayectorias múltiples se seleccionan entre la fuente y el destino. Cuando un acoplamiento está quebrado en una trayectoria debido a una mala calidad o movilidad del canal, otra trayectoria en el sistema de trayectorias existentes puede ser elegida. Así, sin esperar al sistema para arriba una trayectoria nueva del encaminamiento. Sin embargo, dado un funcionamiento métrico, la mejora depende de la disponibilidad de las rutas entre la fuente y la destinación. Otra desventaja del encaminamiento multidireccional está su complejidad.
- Encaminamiento Jerárquico: Este tipo de encaminamiento se emplea para agrupar nodos de red en racimos. Cada racimo tiene una o más cabezas del racimo. Los nodos en un racimo pueden tener uno o más saltos a una distancia lejana de la cabeza del racimo. Puesto que la conectividad entre los racimos es necesaria, algunos nodos pueden comunicarse con más de un racimo y trabajar como entrada. Cuando la densidad del nodo es alta, los protocolos del encaminamiento hierarchical tienden para alcanzar un funcionamiento mucho mejor debido hay menos trayectoria y procedimiento es más rápido debido la disposición de encaminar la trayectoria. Sin embargo, la complejidad de mantener la jerarquía puede comprometer el funcionamiento del protocolo del encaminamiento. Por otra parte, en WMNs, un cliente de acoplamiento debe evitar de ser una cabeza del racimo porque puede convertirse en un embotellamiento debido a su capacidad limitada.

- Encaminamiento Geográfico: consiste en proyectar los paquetes delanteros solamente usando la información de la posición de nodos en la vecindad y el nodo de destino[25]. Así, el cambio de la topología tiene menos impacto en el encaminamiento geográfico que los otros protocolos del encaminamiento. Los

---

[25]http://personales.ciudad.com.ar/technical_support/mastutoriales/nivel.rtf

algoritmos geográficos son un tipo de esquemas codiciosos del encaminamiento de una sola trayectoria en los cuales la decisión de la expedición de paquete se hace basándose en la información de la localización del nodo de la expedición, sus vecinos, y el nodo de destino. Sin embargo, todos los algoritmos codiciosos del encaminamiento tienen un problema común, es decir, la entrega no está garantizada aunque exista una trayectoria entre la fuente y el destino.

4.1.4 Capa de transporte

Hasta el momento, no se ha propuesto ningún protocolo del transporte específicamente para WMNs. Sin embargo, una gran cantidad de protocolos del transporte están disponibles para las redes ad hoc. Estudiar estos protocolos ayuda en el diseño de los protocolos del transporte para WMNs. Diversos protocolos del transporte son necesarios para ser usados en tiempo real como es el caso del tráfico tráfico.

Transporte confiable de los datos: Los protocolos confiables del transporte se pueden clasificar más a fondo en dos tipos: Variantes del TCP y nuevos protocolos del transporte. Las variantes del TCP mejoran el funcionamiento del clásico TCPs abordando los problemas siguientes:

- Pérdidas del paquete de la No-Congestión: El TCPs clásico no puede distinguir las pérdidas de la congestión y la no congestión. Como resultado, cuando ocurren las pérdidas de la no-congestión, el rendimiento de la red cae rápidamente debido a la evitación innecesaria de la congestión. Además, cuando los canales inalámbricos vuelven a la operación normal, el TCP clásico no se puede recuperar rápidamente. Se puede utilizar un mecanismo de la regeneración para distinguir diversas pérdidas del paquete.

- Falta desconocida del acoplamiento: La falta del acoplamiento ocurre con frecuencia en las redes ad hoc móviles, puesto que todos los nodos son

móviles. Por lo que en las WMNs, la falta del acoplamiento no es tan crítica como en redes ad hoc móviles. Debido a los canales y a la movilidad Inalámbrica en clientes de acoplamiento, la falta de acoplamiento inmóvil puede suceder.

- Asimetría de la red: La asimetría de la red se define como situación en la cual la dirección delantera de una red es perceptiblemente diferente de la dirección contraria en términos de anchura de banda, tarifa de la pérdida, y estado latente. Así, afecta la transmisión de ACKs. Puesto que el TCP es críticamente dependiente del ACK, su funcionamiento se puede degradar seriamente por asimetría de la red.

- Entrega en tiempo real: Para apoyar entrega end-to-end del tráfico en tiempo real, un protocolo del control de la tarifa (RCP) es necesario trabajar con el UDP. Aunque las RCPs se proponen para las redes atadas con alambre, no hay esquemas disponibles para WMNs.

4.1.5 Capa de aplicación

Los usos apoyados por WMNs son numerosos y pueden ser categorizados en varias clases.

Acceso a Internet: Los usos variados del Internet proporcionan información oportuna, para hacer la vida más confortable, y para aumentar eficacia y productividad del trabajo. En un hogar o un ambiente de negocio pequeño o mediano, la solución del acceso de la red más popular es un módem inmóvil de DSL o de cable junto con IEEE 802.11 puntos de acceso. Sin embargo, comparado con este acercamiento, WMNs tiene muchas ventajas potenciales: un costo más bajo, una velocidad más alta, y una instalación más fácil.

Almacenaje y compartimiento de información distribuida: tener acceso a Backhaul en Internet no es necesario en este tipo de uso, y los usuarios se comunican solamente dentro de WMNs. Un usuario puede desear almacenar datos en grandes cantidades en los discos poseídos por otros usuarios, archivos de la transferencia directa discos de otros usuarios los cuales están basados en mecanismos del establecimiento de una red del par-a-par. Los usuarios dentro de WMNs pueden también desear charlar, hablar en los teléfonos de video, y los jugar en línea con varias personas.

Intercambio de información a través de múltiples redes inalámbricas: Por ejemplo, un teléfono portátil puede desear hablar con otro usuario Wi-Fi con WMNs, o un usuario en una red Wi-Fi puede esperar supervisar el estado en varios sensores en redes de un sensor de la radio. Por lo tanto, hay principalmente tres direcciones de la investigación en la capa de uso.

Mejorar los protocolos de cada capa existentes que están en uso: En una red inalámbrica, los protocolos en las capas más bajas no pueden proporcionar la ayuda perfecta para la capa que este en uso. Por ejemplo, según lo percibido por la capa de uso, la pérdida del paquete puede siempre no ser cero, el retraso del paquete puede ser variable[26]. Estos problemas llegan a ser más severos en WMNs debido a su comunicaciones ad hoc y multi-hop. Tales problemas pueden ocasionar fallas en muchos usos del Internet que trabajen suavemente en una red atada con alambre. Actualmente, muchos
Protocolos del par-a-par están disponibles para la información que comparte en el Internet. Sin embargo, estos protocolos no pueden alcanzar funcionamiento

---

[26]Seminario de redes de computadores “Mobile Ad hoc Networks”2002 Cristian Bravo

Satisfactorio en WMNs puesto que WMNs tiene características mucho diversas que el Internet. Desarrollar los usos innovadores para WMNs. Tales usos deben traer enormes ventajas a los usuarios, y también no pueden alcanzar el mejor funcionamiento sin WMNs. Tales usos permitirán a WMNs ser una solución única del establecimiento de una red.

4.2. SEGURIDAD EN WIRELESS MESH NETWORKS

4.2.1 Descripción de la tecnología en seguridad

Esta sección da una descripción de la tecnología utilizada para la seguridad básica que es necesaria para WMNs. Aquí se hará un resumen general sobre la seguridad en las wireless mesh networks. Las WMN se exponen a las mismas amenazas básicas comunes de las redes alambradas e inalámbricas: los mensajes pueden ser interceptados, modificados, retrasados, reenviado, o los nuevos mensajes pueden ser insertados. Una red que posee recursos importantes, se podría acceder sin autorización.

Los servicios de seguridad que por lo general tratan de combatir estas amenazas son:

- Confidencialidad: Los datos se revelan solamente en las entidades o personas interesadas.
- Autentificación: Una entidad tiene de hecho la identidad que demanda tener, es decir, reconocimiento de los usuarios dueños del servicio.
- Control de acceso: Se asegura de que solamente las acciones autorizadas puedan ser realizadas.
- No negación: Protege las entidades que participan en un intercambio de la comunicación puede negar más adelante algo falso que ocurrió el intercambio.
- Disponibilidad: Se asegura de que las acciones autorizadas puedan tomar lugar.

Los Servicios de seguridad en el futuro serán mucho más restringidos buscando para el usuario privacidad (anonimato, seudonimidad, usuario perfilado, y tracing) y la confidencialidad del tráfico.

La protección del tráfico de comunicación implica: la confidencialidad (cifrado), la autentificación de los socios de la comunicación, así como la protección de la integridad y de la autenticidad de mensajes intercambiados.

La protección de la integridad se refiere no sólo a la integridad del mensaje, sino también al orden correcto de los mensajes relacionados (reenvío, el reordenamiento, o cancelación de mensajes). Esta sección describe la tecnología de protección para el tráfico de la comunicación. Estas tecnologías pueden también ser utilizadas dentro de una red mesh para autenticar los nodos Mesh (MNs) y para establecer las llaves de la sesión que protegen la confidencialidad y la integridad del tráfico intercambiado entre MNs.

El tráfico de la comunicación puede ser protegidas por diversas capas (capa de enlace, capa de red, capa de transporte y capa de aplicación): especialmente en sistemas inalámbricos, (GSM, UMTS, DECT, IEEE 802.11 WLAN, Bluetooth, 802.16 WiMax), que incluye medios de proteger el enlace inalámbrico. Éstos utilizan diversos esquemas de encapsulación de tramas, diversos protocolos de autentificación, y diversos algoritmos criptográficos[27].

Redes de área local inalámbricas (WLAN) basada en IEEE 802.11i (acceso de Wi-Fi Protected: WPA, WPA2) apoya dos modos de seguridad: también una shared key (llaveo compartida) es configurada en los dispositivos de WLAN (preshared llaveo [PSK]), que es de uso frecuente en las redes caseras, los usuarios pueden ser autenticados con un servidor autentificador (servidor AAA). Para este propósito, se utiliza el protocolo extensible de autentificación (extensible authentication protocol) (EAP).
La autentificación real ocurre entre la estación móvil (MS) y el servidor AAA

[27]Wireless mesh networking “Architectures, Protocols and Standards” 2006
Yan Zhang • Jijun Luo • Honglin Hu pag 183-225

Usando EAP (véase Fig.4.8). El EAP es transportado entre el MS y el punto de acceso (AP) que usan EAPOL, y entre el AP y el servidor AAA por el protocolo RADIUS. Si es habilitado el nodo, una sesión maestra de llaveo (MSK) es utilizada, el cual se envía desde el servidor de la autentificación (AS) al WLAN AP. Se utiliza como entrada al WLAN

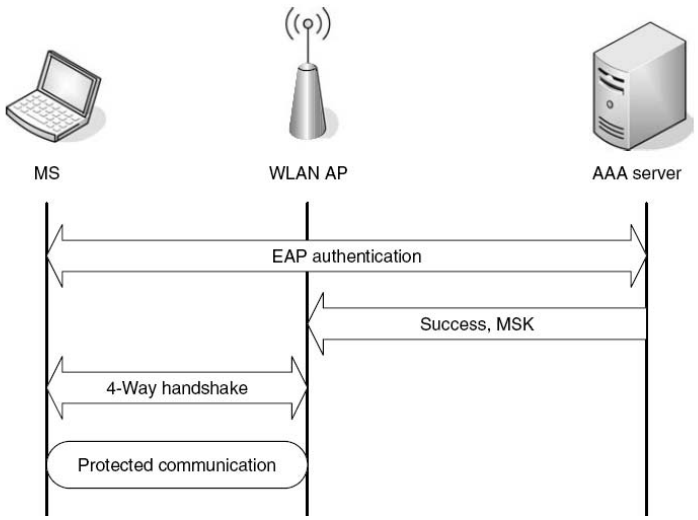


Fig. 4.8 Acceso a WLAN basada en EAP

Hay 4 maneras que establece una sesión de llaveo temporal para proteger el enlace inalámbrico. Esta llave se utiliza realmente para proteger el tráfico del usuario, usando cualquier protocolo dominante temporal de la integridad ([TKIP], la parte de WPA) o AES-basado en CCMP (CTR con el protocolo de CBC-MAC, parte de WPA2). Los varios métodos de EAP existen para una autentificación basada en los certificados digitales, las contraseñas, o los protocolos móviles reusing de la autentificación de la red (EAP-SIM, EAP-AKA). El acceso EAP-basado en WLAN se utiliza particularmente para las redes de la empresa y los hot-spots públicos donde está disponible una base de datos del usuario. El tráfico de la comunicación se puede también proteger en la capa enlace. IPsec protege tráfico IP en la capa de la red (IP). La arquitectura de IPsec especifica dos protocolos de seguridad: ENCAPSULATION SECURITY

PAYLOAD (ESP) y AUTHENTICATION HEADER (AH). En el caso de ESP, ella encapsula solamente la carga útil (payload) del paquete del IP (modo del transporte) o del paquete entero del IP (modo del túnel). Una IPsec security association (SA) define las llaves (keys) y los algoritmos criptográficos para utilizar. Un SA es identificado por 3 cosas consistentes en: un IP address de la destinación, un identificador del protocolo (AH o ESP), y un índice del parámetro de la seguridad.

Este SA unidireccional se puede configurar explícitamente, o puede ser establecido dinámicamente, por ejemplo, por el protocolo del Internet key Exchange (IKEv2). Un uso común de IPsec son las redes privadas virtuales (VPN) para tener acceso con seguridad a un Intranet de la compañía. El tráfico de la comunicación se puede proteger en la capa de transporte usando el protocolo de la seguridad de la capa de transporte (TLS), que se basa en el encendido y es muy similar al secure socket layer (SSL). Su uso principal está para proteger El HTTP sobre TLS/SSL (https), pro esta puede también ser utilizada como protocolo independiente. Los protocolos TLS/SSL[28] incluyen la autentificación y el establecimiento del llaveo basado en certificados digitales. Recientemente, la ayuda para preshared o compartir las llaves (PSK-TLS) también fue introducida. Es también posible a proteger el tráfico en capas más altas. Esto permite para realizar operaciones y aplicaciones específicas de la seguridad. Por ejemplo, los E-mails pueden ser encriptados (protección a la confidencialidad) y/o ser señalados como (autentificación, la integridad, y no compartido del origen) que usa S/MIME o el PGP.

[28]http//searchsecurity.techtarget.com/sDefinition

4.2.2 Ediciones de seguridad Mesh

Uno de los objetivos de las WMNs son diversificar las capacidades de redes ad hoc. Las redes ad hoc se pueden considerar realmente como subconjunto

De WMNs. Ambas Comparten características comunes, tales como el multihop, wireless, topología dinámica, y membresía dinámica. Por otra parte, las mesh pueden tener infraestructura/backbone wireless y tener menos movilidad. Los esquemas existentes de la seguridad propuestos para las redes ad hoc pueden ser adoptadas para WMNs. Sin embargo, la mayor parte de las soluciones de la seguridad para las redes ad hoc todavía no son bastante maduras para ser puestas en ejecución. Por otra parte, las diversas arquitecturas de red entre WMNs y las redes ad hoc pueden dar una solución para las redes ad hoc ineficaces en WMNs.

Desafíos para la seguridad

Los desafíos para la seguridad de las WMNs se basan en sus características topológicas. Analizando las características de WMNs y comparándolas con otras tecnologías de red, los autores demuestran que los nuevos desafíos de la seguridad son debido a las comunicaciones inalámbricas multihop y por el hecho de que los nodos no están protegidos físicamente.
El Multihopping es imprescindible para que WMNs amplíe la cobertura de redes inalámbricas actuales y proporcionar una non-line-of-sight (NLOS) en la conectividad entre los usuarios. El Multihopping retrasa la detección y el tratamiento de los ataques, hace encaminar un servicio de red crítico, los nodos confían en otros nodos para comunicarse, y la cooperación del nodo es así imprescindible. Mientras que el uso de enlaces inalámbricos hace una red mesh susceptible a los ataques, la exposición física de los nodos permite que un adversario tome, clone, o trate de forzar a estos dispositivos.

Otros desafíos específicos para WMNs son:

- Las WMN puede ser dinámicas debido a cambios en su topología y su membresía (es decir, los nodos entran y salen con frecuencia de la red). Ninguna seguridad con configuración estática sería suficiente.

- En WMNs, los routers mesh y clientes mesh llevan a cabo características muy diversas tales como la movilidad y la energía. Consecuentemente, la misma solución de la seguridad puede no trabajar para ambas al mismo tiempo para mesh router y mesh client.

Descripción de los ataques potenciales a WMNs

Hay dos fuentes de amenazas en las WMNs. Primer, los atacantes externos que no pertenecen a la red mesh pueden atorar la comunicación o inyectar una información errónea. En segundo lugar, amenazas más severas vienen de nodos internos comprometidos, puesto que los ataques internos no son tan fáciles de prevenir como los externos.
El ataque puede ser racional, es decir, el adversario no deseado (misbehaves) es bueno para la red solamente si el misbehaving es beneficioso en términos de precio, calidad obtenida del servicio o ahorro del recurso; si no es indeseado.

Los ataques pueden ser distinguidos pasivos y activos. Los ataques pasivos se preponen robar la información y espiar en la comunicación dentro de la red. En ataques activos, el atacante modifica e inyecta paquetes en la red. Además, los ataques podrían apuntar varias capas de protocolos. En la capa física, un atacante puede embotellar las transmisiones de antenas inalámbricas o simplemente destruir el hardware de cierto nodo. Tales ataques se pueden detectar y localizar fácilmente.

En la capa del MAC, un atacante puede abusar de la imparcialidad del acceso medio enviando los paquetes totales del control y de los datos del MAC o personificar un nodo legal. Un atacante podía también explotar los protocolos de la capa de red.
Un tipo de ataques es insinuar el conocimiento de los mecanismos de ruteo. Otro tipo es el de packet forwarding, es decir, el atacante puede no cambiar las tablas de ruteo, pero los paquetes en la la trayectoria de encaminamiento puede ser conducida a diferentes destinos que no sea consistente con el protocolo de la encaminamiento. Por otra parte, el atacante puede esconderse en la red, y personificar un nodo legítimo y no sigue las especificaciones requeridas de un protocolo de encaminamiento. En la capa de aplicacion, un atacante podía inyectar una información falsa o imitada, así dañando la integridad de su uso.
Los tipos del ataque se resumen para las redes ad hoc, que están también son aplicables a WMs:

Imitación: La imitación es un ataque en el cual un adversario procura asumir la identidad de un nodo legítimo en la red del acoplamiento. Si los spoofs del adversario legítiman un Nodo, el adversario pueden tener el acceso a la red para rechazar o recibir los mensajes previstos para nodo spoofed[26]. Si el adversario spoofs una mesh networks, entonces el Nodo legítima o MNs pueden ser atacados y controlados por el adversario. Considerar el panorama siguiente en el cual un AP comprometido en una red mesh 802.11 finge comportarse normalmente y según los requisitos de 802.11i obtiene las llaves en parejas principales (PMKs) de las estaciones inalámbricas conectadas (WSs).

[26]http://es.wikipedia.org/wiki/Spoofing

Normalmente un WS y un AP tienen la opción para depositar el PMK por un período del tiempo. Con esta información, el AP puede engañar fácilmente las WSs y conseguir el *authenticated* usando el PMK almacenado. El AP comprometido puede así aumentar el control sobre este los WS conectándolo con una red del adversario.

Ataque de Sinkhole: Se lanza un ataque del sinkhole cuando una MN malevolo (haber comprometido o adversario que personifica un nodo legítimo) convence nodos vecinos de que sea "lógico" y que tenga salto siguiente para los paquetes de forwarding. El nodo malévolo entonces cae arbitrariamente los paquetes forwarded por nodos vecinos. Este ataque también tiene el potencial de trenzar áreas grandes de la red mesh que son geográficamente distante del nodo malévolo tirando mensajes de sus previstas trayectorias.

Ataque del Wormhole: Un ataque del wormhole procura convencer a nodos que utilicen una trayectoria malévola con medios legítimos. Un adversario con capacidades rápidas de búsqueda puede remitir rápidamente un mensaje con un acoplamiento bajo del estado latente.

Ataque egoísta y codicioso del comportamiento: Un nodo aumenta su poseer la parte del recurso común de la transmisión no pudiendo adherir a los protocolos de red o tratando de forzar con su interfaz inalámbrica.

Ataque de Sybil: En un ataque de Sybil, un nodo malévolo finge identidad de varios nodos, haciendo tan indetectable la eficacia de los esquemas de la fault-tolerace, tales como la redundancia de muchos protocolos de encaminamiento. Los ataques de Sybil también plantean una amenaza significativa a los protocolos geográficos de ruteo. La ruteo enterado de localización requiere a menudo nodos para intercambiar la información coordinada por sus vecinos para encaminar eficientemente los paquetes

geográficamente tratados. Usando el ataque de Sybil, un adversario puede actuar adentro más de un lugar al mismo tiempo.

Privación del sueño: Los ataques de privación del sueño son solicitar servicios de cierto nodo, repetidamente, haciendo que el nodo no pueda ir en marcha lenta ni preservando la energía, así privándolo de su sueño y futuro agotando su batería.

DOS y el inundar (Flooding): Los ataques del DOS pueden ser causados por Flooding, es decir, nodos que sobrecargan. Ataques más avanzados del DOS se basan en mensajes de gestión de protocolo inteligente que tratan de forzar. Por ejemplo, los sinkholes son una de las maneras principales de iniciar la expedición selectiva o el nonforwarding de mensajes.

4.3 FABRICANTES DE EQUIPOS PARA REDES ENMALLADAS INALAMBRICAS

La Alianza Wi-Mesh es un grupo de compañías cuyo objetivo consiste en establecer con rapidez un estándar para WLANs en malla que permita una comunicación fluida entre los usuarios de dispositivos inalámbricos, no obstante el proveedor del equipo. La propuesta de la Alianza Wi-Mesh se desarrolló de acuerdo con los lineamientos de la Asociación de Estándares IEEE. Asimismo, se basa en los protocolos 802.11 pendientes para permitir la reutilización y la compatibilidad de tecnología (Ver Tabla 4.2).

	Enlace del cliente	Frecuencia	Radios por Router	Tipo de red
Belait Network	802.11b/g	5Ghz	1,2 o 4	MAN
Cisco Systems	802.11b/g	5Ghz	2	MAN
Firetire	Ethernet	2.4Ghz, 5Ghz	1	MAN/LAN
Nortel Networks	802.11a/b/g, Bluetooth	5Ghz	2	MAN
Strix Systems	802.11b/g	2.4Ghz, 5Ghz	2 a 6	MAN/LAN
Tropos Netwoks	802.11a/b/g/n	2.4Ghz, 5Ghz	1 o mas	LAN

Tabla 4.2 principales fabricantes de tecnología 802.11s[29]

4.3.1 Firetide

Firetide es una empresa de tecnología inalámbrica especializada en redes malladas que desarrolla equipamiento con altas prestaciones, escalabilidad y fácil de instalar. La solución es idónea para construir infraestructura backbone

[29] http://www.meshdynamics.com/future_proof.html

Para redes WiFi, HotZones de acceso a Internet, video-vigilancia y redes temporales en una variedad de entornos como puedan ser aeropuertos, hoteles, campus y otras áreas donde es muy difícil o muy cara la instalación por cable.

Firetide, líder en conexiones de redes mesh inalámbricas, ha creado el software de administración de mesh HotView Pro(TM) para proveedores de servicio y grandes empresas, ofreciendo una escalabilidad mesh de hasta 1.000 nodos y la capacidad de desplegar y administrar numerosos entornos mesh. La empresa también creo The Cloud, la principal red WiFi de Europa, y la ciudad de Río Rancho, Nuevo México son clientes beta.

Los equipos que ha fabricado Firetide son:

- HotPort 3203 Outdoor Wireless Mesh Nodes
- HotPort 3101 Indoor Wireless Mesh Nodes
- HotPort 3103 Indoor Wireless Mesh Nodes
- HotPort 6201 Outdoor Single Radio
- HotPort 6202 Oudoor Dual Radio
- HotPort 6101 Indoor Single Radio
- HotPort 6102 Indoor Dual Radio
- HotView Mesh Management Software
- HotView Pro™ Mesh Management Software

Los equipos HotPort de exteriores trabajan en las bandas de 2.4 GHz y 5 GHz, tienen capacidad de hasta 25 Mbps, con 100 mW de potencia de salida, poseen encriptación avanzada (WEP / AES), tienen 2 puertos Ethernet 10/100, compatibles con IEEE802.3af (PoE) y 2 antenas omnidireccionales de 4 dBi, con posibilidad de utilizar antenas de mayor ganancia.

Los equipos Mesh de interiores trabajan en las bandas de 2.4 GHz y 5 GHz, tiene capacidad de hasta 25 Mbps, con 100 mW de potencia de salida, poseen encriptación avanzada (WEP / AES), tienen 4 puertos Ethernet 10/100 y 2 antenas omnidireccionales de 5 dBi.

4.3.2 Tropos Networks

Combinando la cobertura ubicua del celular con la facilidad y la velocidad del Wi-Fi, las redes de Tropos produjeron la primera arquitectura de MetroMesh que es capaz de proporcionar rentabilidad y seguridad, entregando datos de banda ancha a los clientes estándares Wi-Fi en las áreas de la cobertura que atraviesan hot-spots o hot-zones, en metro-áreas enteras.

La arquitectura de Tropos MetroMesh proporciona la flexibilidad máxima en la instalación y la capacidad de reaccionar y de responder a las fallas sin interrupción del backhaul inalámbrico debido a los factores tales como interferencia o pérdida de un acoplamiento atado con alambre del backhaul con un mínimo de intervención del operador. Tropos Networks está desarrollando su propio protocolo de enrutamiento, llamado PWRP (Predictive Wireless Routing Protocol), el cual es una variante del protocolo tradicional de las redes cableadas OSPF (Open Shortest Path First).

Las herramientas del análisis y del control de Tropos MetroMesh reducen al mínimo el planeamiento de red, el despliegue y costos de la gerencia. Estas herramientas incluyen:

- Control de Tropos, un sistema de gerencia, el cual es un elemento clave para las redes de MetroMesh
- Penetración de Tropos, un analizador y optimizador avanzado de MetroMesh

- Impulsión de Tropos, una aplicación que se encarga de probar el servicio suministrado a los clientes para determinar cobertura y rendimiento de procesamiento en las redes de MetroMesh
- SignalMX, una herramienta de gran alcance del planeamiento de la cobertura de MetroMesh de la radio de EDX

Las herramientas del análisis y del control de Tropos MetroMesh[30], fueron diseñadas para dar a operadores de red centralización y visibilidad en todos los aspectos del funcionamiento de la red. Además permite el análisis, la optimización y el control de los sistemas altamente dispersados del acoplamiento. Cabe destacar que Tropos Network es el fabricante con mayores ventas en el mundo. En el siguiente grafico se puede observar todos los países que disfrutan de sus servicios.

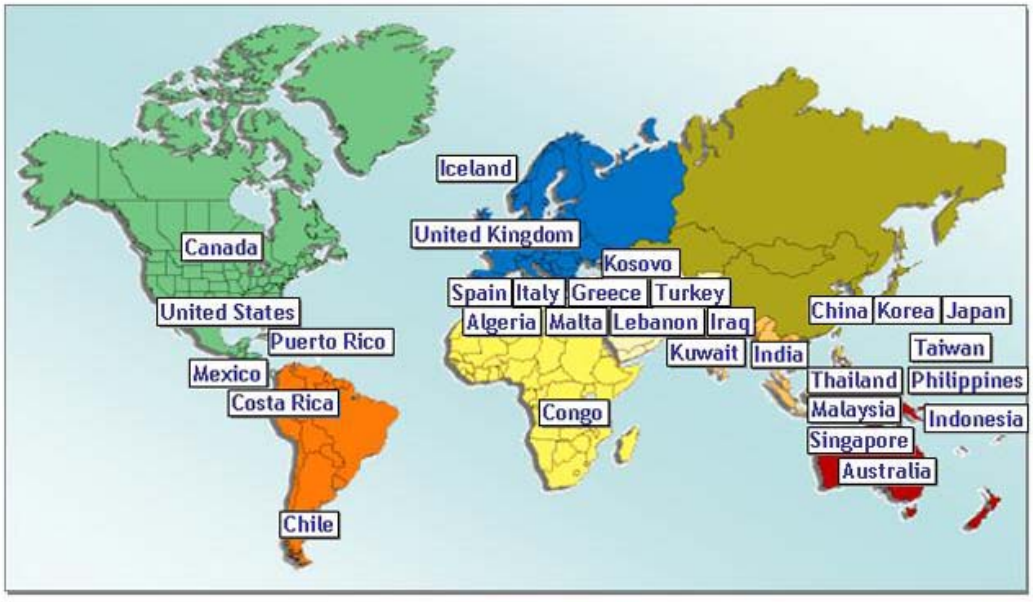


Fig. 4.9 Expansión de Tropos Network en el mundo

[30] http://www.tropos.com/products/metromesh_os.html

4.3.3 Skypilot

Skypilot con sede en Silicon Valley (California), es proveedor de banda ancha inalámbrica carrier-class. Sus diferentes productos permiten desplegar de manera rápida y eficiente una red por la que el usuario podrá utilizar servicios de VoIP, videovigilancia y servicio WiFi público. Sus soluciones ofrecen un alto ROI y técnicamente permiten hacer enlaces de larga distancia.

Skypilot utiliza el protocolo TDD (Time Division Duplex) el cual es el encargado de sincronizar todas las transmisiones para maximizar el rendimiento. Usando el sistema de localización global (GPS), la tecnología SyncMesh coordina las transmisiones simultáneas a través de la red Mesh.

Su estrategia está enfocada a dotar de cobertura WiFi a grandes áreas como pueden ser un municipio. Skypilot se caracteriza por la utilización en sus diferentes nodos de un arreglo de 8 antenas para conseguir mejores zonas de cobertura y capacidades superiores a sus competidores. Su tecnología está patentada y es miembro del foro WiMAX. El despliegue de SkyPilot requiere una huella mínima, sacando ventaja de la estructura municipal existente, como azoteas de edificios o postes de alumbrado público para lograr un costo efectivo del despliegue. Ninguna otra solución Mesh inalámbrica puede soportar el rango de aplicaciones en demanda de los municipios y de proveedores de servicio con esta combinación de facilidad de proporción y flexibilidad.

Los equipos que proporciona Skypilot son los siguientes:

- **SkyGateway:** Conecta la infraestructura Mesh con Internet. Posee una modulación OFDM, funciona en la banda de 5GHz y su distancia máxima es de 16 Km.

- **SkyGateway DualBand:** Conecta la infraestructura wireless Mesh con Internet., pero además da cobertura Wi-Fi. El backhaul funciona en la banda de 5GHz y Wi-Fi en la banda de 2.4GHz.
- **SkyExtender :** Permite aumentar la cobertura que proporciona el SkyGateway (Backhaul). Es un repetidor. Funciona en la banda de 5GHz y trabaja con OFDM.
- **SkyExtender DualBand:** Es un repetidor (Backhaul), al igual que el Extender, pero además da cobertura Wi-Fi. El backhaul funciona en la banda de 5GHz y Wi-Fi en la banda de 2.4GHz.
- **SkyAccess DualBand:** Se pueden conectar tanto a un Skyextender como a un SkyGateway. Son los puntos finales de la Mesh a donde podemos acceder a través de un puerto ethernet. El backhaul funciona en la banda de 5GHz y Wi-Fi en la banda de 2.4GHz. La distancia máxima del backhaul es de 12Km
- **SkyConnector :** Hay un modelo para interior y otro para exterior. Se pueden conectar tanto a un Skyextender como a un SkyGateway. Son los puntos finales de la Mesh a donde podemos acceder a través de un puerto ethernet. Funciona en la banda de 5 GHz[31].

4.3.4 Locustworld

Mesh LocustWorld está diseñado para proveer acceso inalámbrico a áreas geográficas muy amplias, fundamentalmente por medio del uso de 802.11b, ya que se adapta mejor para instalaciones a la intemperie y también por que los dispositivos que usan 802.11b pueden conseguirse en cualquier parte y son de muy bajo costo, aunque se le hayan agregado más interfaces, incluyendo a 802.11a.

---

[31] http://www.sistelec.es/es/Productos/FAB_Skypilot.asp

LocustWorld proporciona dos versiones de su sistema del establecimiento de una red del acoplamiento. El MeshAP y el MeshAP-Favorable. Ambos sistemas utilizan el mismo encaminamiento de AODV para construir redes inalámbricas del acoplamiento de la escala grande. MeshAP es utilizado por los operadores no comerciales, y el MeshAP-Favorable contiene características adicionales para apoyar ISPs sin hilos que proporciona servicios comerciales.

El acoplamiento de LocustWorld proporciona un uso comprensivo del centro de las operaciones de la red. Esto permite a operador maneja sus nodos del acoplamiento, mantiene controles de acceso del usuario, supervisa operaciones, visualiza la topología de la red y localiza averías ediciones del establecimiento de una red.

Los usuarios se pueden conectar con el acoplamiento usando conexiones de red atadas con alambre o sin hilos. El acoplamiento aparece a ellos como rebajadora del TCP/IP que da una conexión a Internet una vez que los autentiquen. El acceso de usuario a los servicios del Internet es controlado con la conexión de la tela, el MAC address o la conexión del PPTP VPN.

4.3.5 Nortel

La solución Wireless Mesh Network de Nortel se ha implementado en empresas, universidades y agencias gubernamentales, tales como las ciudades de Taipei y Kaohsiung en Taiwán, la Universidad de Arkansas, la Universidad Edith Cowan en Australia, y la Universidad Seo Won y el Black Stone Golf & Resort en Corea. La propuesta de diseño de la Alianza Wi-Mesh pretende ser compatible con las modificaciones futuras al rendimiento 802.11n. Este enfoque brindará soporte para la actual base instalada de redes Wi-Fi a nivel mundial, al tiempo que extenderá la implementación de redes Wi-Fi dentro

de la frecuencia de radio designada. Nortel tiene negocios en más de 150 países**.**

Nortel Proporciona una entrada de valor añadido en el negocio sin hilos de alta velocidad del paquete y de los datos, Ofrece el acceso inalámbrico de alta velocidad de los datos del paquete a través de un área más amplia de la cobertura, es muy económico ya que Los algoritmos de la auto configuración en punto de acceso sin hilos eliminan los costes asociados a la ingeniería y a la organización de la red sin hilos del backhaul[32].

Esta solución puede utilizarse tanto en interiores como en exteriores y resulta ideal para ambientes extensos y de amplia cobertura, como empresas, universidades, fábricas, centros comerciales, aeropuertos, lugares de diversión y eventos especiales, operaciones militares, instalaciones temporales, seguridad pública y municipalidades, incluyendo centros de ciudades, áreas residenciales, parques y servicios de transporte en áreas públicas o comunidades residenciales.

---

[32] http://www.nortel.com/corporate/corptime/index.html

Anexo 1. ACRONIMOS

AAA Authetication , Authorization and Accounting: Autenticación, Autorización y Administración.

AH Authentication Header: Autentificación De Cabecera.

AODV Ad hoc On Demand Distance Vector: Vector distancia en demanda Ad Hoc

AP Access Point: Punto de Acceso

ACK Acknowledgement : Acuse de recibido.

CSMA/CD Carrier Sense Multiple Access with Collision Detection: Acceso Múltiple con Escucha de Portadora y Detección de Colisiones

CTS Clear To Send: Libre para envío.

DFS Distributed File System: Sistema de archivos distribuidos

DHCP Dinamic host configuration protocol**:** Protocolo de configuración de servidor dinámico

DNS Domain Name System : sistema de nombres de dominio

DSL digital subscriber line: Línea de suscripción digital

EAP Extensible Authentication Protocol: protocolo extensible de autentificación.

ESP Encapsulation Security Payload : cabecera de seguridad encapsulada.

FIFO First In, First Out: primero en llegar, primero en ser servido.

GPSR Greedy Perimeter Stateless Routing: protocolo apátrida del encaminamiento del perímetro codicioso.

IKEv2 Internet key Exchange.

IPsec Internet Protocol Security : seguridad para protoloco Internet.

MN Mesh nodes : nodos mesh.

MPR Multiple protocol router: Enrutador de protocolo múltiple

MS Movil Station : estacion movil

MSK master sesion key : sesión maestra de llaveo.

OFDMA Orthogonal Frequency Division Multiple Access: Acceso multiple de frecuencia ortogonal

OLSR Optimized Link State Routing protocol: Protocolo de encaminamiento de estado de acoplamiento

QoS Quality of Service: Calidad de servicio

RTS Request To Send: Solicitud de envío

UDP Protocol datagram users: Protocolo de datagramas para usuarios

VPN Virtual Private Network: Red privada virtual

WDS Wireless Distribution System: Sistema de distribución inalámbrica

WMN Wireless mesh network: Redes enmalladas inalambricas

WLAN Wireless local area network : Redes inalambricas de area local.

WPA Wi-Fi Protected Access : Acceso de Proteccion Inalambrica.

PSK preshared key : clave precompartida.

SSL Secure Socket Layer: capa de seguridad de zocalo.

TLS Transport Layer Security : Seguridad de la capa de transporte.

CONCLUSIONES

LAS WMN resultan muy atractivas para la industria y para la sociedad debido a sus bajos costos y a las facilidades de despliegue que poseen, muchos fabricantes, (Tropos, Nortel, Motorola, etc.), los cuales ofrecen hoy en día soluciones muy viables para este tipo de redes. Los grupos de estandarización también se encuentran definiendo nuevas extensiones a las redes inalámbricas para ofrecer funcionamiento enmallado tal como en el caso del 802.11s. Este estándar ofrece flexibilidad requerida para satisfacer los requerimientos de ambientes residenciales, de oficina, campus, seguridad pública y aplicaciones militares. La propuesta se enfoca sobre múltiples dimensiones: La subcapa MAC, enrutamiento, seguridad y la de interconexión.

La IEEE 802.16 (WIMAX) define la posibilidad de funcionar en modo mallado aunque la no compatibilidad con los otros modos puede limitar su utilización en el mundo real debido a los altos precios que esta implementación acarrea, pues el costo de una tarjeta de red Wi-Fi puede aumentar unos diez dólares el precio de una computadora, mientras que las terminales IEEE 802.16 (WiMax) son más aparatosas y cuestan diez veces más.

A nivel técnico, los nuevos retos que suponen estas redes se basan en una estrecha relación entre las distintas capas de pila de protocolos, ya que es necesario optimizar la eficiencia a todos los niveles, siendo difícil si no se tiene información sobre la calidad del enlace para la selección de rutas óptimas. Se podría decir que el diseño de protocolos cross layer es un tópico importante en la investigación actual. Los protocolos usados por las redes Mesh pueden estar basados en topología o en posición, los primeros se encargan de establecer los enlaces entre los nodos dependiendo de la información que se tenga de estos o de la información que aporten los nodos vecinos, en su tabla de enrutamiento; mientras que los segundos establecen el enlace dependiendo de la trayectoria y posición geográfica entre los nodos.

El encaminamiento geográfico presenta interesantes características para redes Mesh con un tamaño de moderado a grande. Sin embargo debido a su alto costo, en la actualidad se han empleado protocolos híbridos que combinan los protocolos basados en posición y los basados en topología.

Tal y como se a presentado en este documento, se puede comprobar una estrecha relación entre las capas física, Mac y los protocolos de encaminamiento; relación que se acentúa mas al emplear varios canales de radio que requieren de mayor coordinación entre las capas y nuevos mecanismos que se encargan de optimizar el uso del ancho de banda (antenas adaptivas, inteligente, etc.) y minimizar las interferencias.

Las redes Mesh presentan varios problemas debido a que han sido diseñadas para uso público. En este momento son muchas las personas que utilizan sus servicios (voz, video y datos) y debido a esto se han hecho gran des cambios en las capas del modelo OSI que contribuyen al mejoramiento de la capacidad, robustez, rendimiento y confiabilidad.

Las redes Mesh están apoyadas en las capas física y Mac, sin embargo se están haciendo investigaciones para implementar protocolos en las otras capas. A nivel de la capa física se han creado sistemas Multiantenas y se plantea la incorporación de antenas Mimo (IEEE 802.11n) y las tecnologías de radio OFDM y UWB. En la capa Mac se han dejado atrás los protocolos convencionales como son el aloha y el CSMA, y se incorporan protocolos avanzados como son el RTS y CTS circular, estos protocolos son los encargados de mandarle información a los nodos vecinos para evitar problemas de nodos ocultos, nodos expuestos e interferencias. A nivel de seguridad en la actualidad se están utilizando los protocolos WEP y WPA, los cuales no son muy confiables, y debido a las propiedades de auto-descubrimiento de nuevos nodos y auto-reparación de rutas proporcionada por los protocolos de encaminamiento que utilizan las WMNs, es complejo establecer mecanismos totalmente seguros que permitan autenticar la

información recibida, pues si no hay una validación de la información de encaminamiento de los nodos, un atacante malicioso puede comprometer un nodo o introducir un nuevo elemento que puede inyectar a la red información errónea sobre las rutas poniendo en peligro el destino del paquete, empleando diferentes ataque como son la imitación, sybil, wormhole entre otros. Sin embargo se están haciendo investigaciones para decidir si en posible la incorporación del protocolo HTTPS.

BIBLIOGRAFIA

8 Yang Zhang . Jijun Luo. Honglin Hu Wireless mesh networking ”Architectures,Protocolsand Standards” Auerbach Publications Taylor and Francis Group Julio 2006

P. Gupta, P.R. Kumar. ‘‘The Capacity of Wireless Networks,’’ IEEE Transactions on Information Theory, Vol. 46, No. 2, 2000, pp. 388–404.

J. Jun, M.L. Sichitiu. ‘‘The Nominal Capacity of Wireless Mesh Networks,’’ Wireless Communications, IEEE, Vol. 10, No. 5, 2003, pp. 8–14.

Saad Biaz, Nitin H. Vaidya. ‘‘Discriminating Congestion Losses from Wireless Losses Using Inter-Arrival Times at the Receiver,’’ IEEE Symposium ASSET, 1999.

S. Douglas, J. De Couto, Daniel Aguayo, Benjamin A. Chambers, Robert Morris. ‘‘Performance of Multihop Wireless Networks: Shortest Path Is Not Enough’’, Proceedings of HotNets, 2002.

S. Xu, Saadawi T. ‘‘Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?’’ Communications Magazine, IEEE, Vol. 39, No. 6, 2001, pp. 130–137.

S. Douglas, J. De Couto, Daniel Aguayo, John Bicket, Robert Morris. ‘‘A high-Throughput Path Metric for Multi-Hop Wireless Routing,’’ Proceedings of ACM Mobicom, 2003.

Douglas S.J. Couto, Daniel Aguayo, John Bicket, and Robert Morris, ‘‘A High-Throughput Path Metric for Multi-Hop Wireless Routing,’’ Proceedings of ACM MobiCom 2003, San Diego, CA, September 2003.

R. Draves, J. Padhye, and B. Zill, ‘‘Routing in Multi-Radio Multi-Hop Wireless Mesh Networks,’’ Proceedings of ACM MobiCom 2004, Philadelphia, PA, September 2004.

IEEE P802.11sTM/D0.01, draft amendment to standard IEEE 802.11TM: ESS Mesh Networking, March 2006.

Uppsala University Ad hoc Implementation Portal. Available at: http://core. it.uu.se/AdHoc/ImplementationPortal.

P.R. Choudhury and N.H. Vaidya, ‘‘Deafness: A MAC problem in ad hoc networks when using directional antennas’’, University of Illinois at Urban

SITIOS WEB

[5] http://www.intel.com/espanol/netcomms/wp03_espanhol.pdf

[7] http://www.meshdynamics.com/third_generation.html

[10] http://www.ehas.org:9673/Portales/EHAS/trabajo/C_tecnologia/mesh/RouterWiFi

[12] http://www.it46.se/downloads/courses/wireless/es/13_Redes-Mesh

[16] http://www.montevideolibre.org/manuales:libros:wndw:capitulo_3:redes_mesh

[17] http://www.mitre.org/tech_transfer/mobilemesh.html

[21] http://www.ceditec.etsit.upm.es/InfTecnologia

[22] http://www.wifinetnews.com/

[26] http://es.wikipedia.org/wiki/Spoofing

[29] http://www.meshdynamics.com/future_proof.html

[30] http://www.tropos.com/products/metromesh_os.html

[32] http://www.nortel.com/corporate/corptime/index.html

REDES INALAMBRICAS ENMALLADAS METROPOLITANAS

INTEGRANTES

DIANA ACUÑA MARTINEZ 0204072

RAFAEL RONCALLO KELSEY 0104504

DIRECTOR

Margarita Upegui Ferrer

Magíster en Ciencias Computacionales

PROPUESTA PRESENTADA COMO REQUISITO PARA OPTAR AL TITULO DE INGENIERO ELECTRONICO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍAS

Programa de Ingenierías Eléctrica y Electrónica

CARTAGENA DE INDIAS D. T. Y C.

03-06-07

1. TITULO

Redes Inalámbricas Enmalladas Metropolitanas

2.ÁREA DE ESTUDIO

Gestión de Redes

3. COBERTURA DE INVESTIGACIÓN

Local

4. CAMPO DE INVESTIGACION

Universidad Tecnológica de Bolívar

5. FORMULACION DEL PROBLEMA

Las redes inalámbricas mesh son un tipo de redes de comunicación especiales orientadas a proveer acceso remoto a usuarios en lugares donde una red común (celdas) no es óptima. La característica de estos lugares es que son sitios remotos con baja densidad de usuarios y de difícil acceso con una simple estación base. Ejemplos de estos escenarios son las comunicaciones rurales e Internet banda ancha de acceso residencial. Adicionalmente a esto tipo de redes se pueden realizar las operaciones de dos maneras diferentes: distribuida o centralizada, dependiendo de los requerimientos.

6. JUSTIFICACION

Antiguamente no se usaba la estructura de redes Mesh porque el cableado necesario para establecer la conexión entre todos los nodos era imposible de instalar y de mantener. Hoy en día con la aparición de las redes wireless este problema desaparece y nos permite disfrutar de sus grandes posibilidades y beneficios. Las redes Mesh son la evolución de WI-FI que consisten en una variante del WiFi tradicional, en la que las clásicas celdas basadas en cableado Ethernet hasta el switch se sustituyen por una red mallada, donde los nodos se comunican entre sí sin cables, estableciendo cobertura que puede cubrir hasta una ciudad. La tecnología utiliza puntos de acceso inalámbricos WiFi a los que se conectan los usuarios. Estos puntos se ubican de tal manera que otorgan una cobertura continua, ya que conmutan las conexiones de los usuarios de un punto a otro sin interrumpir el servicio, como una especie de roaming. Además tiene como principal característica que es tolerante a fallos, puesto que la caída de un solo nodo no implica la caída del resto de la red. Las redes Mesh tienen como fin el establecimiento de ciudades inteligentes.

7. Objetivos

7.1 Objetivo General

Estudiar las redes inalámbricas enmalladas (Wireless Mesh Networks) como solución tecnológica de punta

7.2 Objetivos Específicos

- Presentar estructuradamente los protocolos que se utilizan las redes enmalladas inalámbricas.
- Analizar y describir las características del estándar 802.11s.

- Identificar los principales problemas que enfrentan las redes Mesh para la prestación de servicios.

8. RECURSOS

Para la realización de la monografía se utilizaron varios recursos que favorecieron la búsqueda de información como son los recursos humanos, y bibliográficos se utilizaron equipos que contribuyeron a dicha busqueda.

8.1 RECURSOS HUMANOS

Ing. Mario Hernandez

PhD Andrés Felipe Millan

8.2 BIBLIOGRÁFICOS

[1] Lee M.,"Emerging Standards for Wireless Mesh Technology", IEEE Wireless Communications, April 2006.

[2] Millan A.,"Redes Enmalladas 802.11, Infraestructura de las ciudades inalámbricas "USC, Mayo 2006.

[3] Hiertz G., "IEEE Standardization, 802.11s Mesh Progress, IEEE 802.11s, Marzo 2006.

[4] Caballero M.," La Banda de 2.1 GHz Abierta Para WiFi Mesh a Cambio de Publicidad" www.redesenmalladas.com, Mayo 19 del 2006.

[5] Bustamante R. Hincapié R., "Análisis, Modelamiento y Simulación de Redes Enmalladas Basadas en el Estándar 802.16", Sistemas y Telemática, Universidad ICESI, 2004, 45-59.

[6] Marshall Phil., "Myth and Realities of WiFi Mesh Networking", Yankee Group Report, Febrero 2006.

8.3 EQUIPOS UTILIZADOS

- Computador
- Impresora
- Reproductor de DVD
- Textos

9. AUTORES Y ASESOR

9.1 AUTORES

Diana Margarita Acuña Martínez

Rafael Julio Roncallo Kelsey

a. ASESOR

Margarita Upegui Ferrer-Magíster en Ciencias Computacionales