MANET´S (MOBILE AD HOC NETWORKS)

REDES MOVILES INALAMBRICAS AD HOC

MIGUEL ÁNGEL CORTÉS GRAJALES

MÁRYORI TATIANA ALVIS LARA

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIA ELECTRONICA

CARTAGENA - COLOMBIA

MANET´S (MOBILE AD HOC NETWORKS)

REDES MOVILES INALAMBRICAS AD HOC

Autores

MIGUEL ÁNGEL CORTÉS GRAJALES

MÁRYORI TATIANA ALVIS LARA

Monografía presentada para optar al titulo de Ingeniero Electrónico

Director

DAVID SENIOR ELLES

Ingeniero Electrónico

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIA ELECTRONICA

CARTAGENA – COLOMBIA

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma de presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Cartagena, Noviembre de 2004

RESUMEN

El objetivo de las redes móviles Ad hoc (MANET), es soportar de manera eficiente y robusta la operación de las redes móviles inalámbricas incorporando la funcionalidad de enrutamiento en nodos móviles. Estas redes están diseñadas para ser dinámicas y aleatorias, con topologías cambiantes que están compuestas normalmente por conexiones inalámbricas de un ancho de banda relativamente restringido.

Una MANET (*Mobile Ad hoc Network*) es una colección de nodos móviles inalámbricos que forman una estructura temporal sin la necesidad de una infraestructura. Debido a la naturaleza dinámica de la topología de este tipo de redes, el establecimiento de rutas en una MANET puede ser suspendido debido a la movilidad de los nodos. Las frecuentes caídas y recuperaciones de los enlaces, dificultan el comportamiento de protocolos de enrutamiento que soporten este tipo de redes.

En este trabajo se realiza una descripción general acerca de las redes Ad hoc, se entrega una visión general de los protocolos MANET existentes en la actualidad clasificados según distintos criterios y su implementación en distintas aplicaciones.

CONTENIDO

Pág

INTRODUCCION

IDENTIFICACIÓN Y DESCRIPCIÓN DEL PROBLEMA

OBJETIVOS

JUSTIFICACION

REVISION DE ANTECEDENTES

METODOLOGÍA DE INVESTIGACION

1. GENERALIDADES 2

1.2 Redes con infraestructura 3

1.3 Redes sin infraestructura (*Ad-hoc*) 3

2. ESTADO DEL ARTE 5

2.1 Historia 5

2.2 ¿Qué es una red Ad hoc? 6

2.2.1 Características de una red Ad hoc 7

2.2.2 Aplicaciones 12

2.3 ¿Cómo podría evolucionar una red Ad hoc? 15

2.4 Investigaciones y estudios de algunas aplicaciones. de redes Ad hoc 16

2.4.1 Aplicaciones con PDAs en una red Ad hoc 16

2.4.1.1 Prototipo de guía turístico 16

2.4.1.2 SUOSAS (*Small Unit Operation Situation Awarness System*) 17

2.4.1.3 Procesamiento de imágenes en un ambiente *MANET* 17

2.4.1.4 Redes Ad hoc como tecnología de soporte para la computación ubicua (*Ubiqmuseum)*. 20

2.4.2 Vehicular Ad hoc Networks 23

2.4.3 Variables de entrada empleadas en simuladores OPNET, GloMoSim y NS2 en redes Ad hoc 25
3. CAPA FÍSICA EN REDES AD HOC 27
3.1 El Estándar IEEE 802.11 27
3.1.1 Espectro ensanchado 28
3.1.1.1 FHSS (*Frequency Hopping Spread Spectrum)* 30
3.1.1.2 DSSS (*Direct Sequence Spread Spectrum*) 32
3.1.1.2.1 BPSK 33
3.1.1.2.2 QPSK 34
3.2 Estándar 802.11b 36
3.3 Tecnología Bluetooth 37
3.3.1 Descripción 39
3.3.2 Especificaciones 40
3.3.3 Arquitectura de Capas 41
3.3.3.1 Radio Frecuencia (RF) 42
3.3.3.2 Banda base 43
3.4 HIPERLAN 2 44
3.4.1 ARQUITECTURA 46
3.4.2 CAPA FÍSICA HIPERLAN 2 46
3.4.2.1 Multicanalización OFDM 47
3.4.3 Técnicas de modulación 48
3.4.3.1 QAM 49
4. PROTOCOLOS DE ENRUTAMIENTO EN REDES AD HOC 50
4.1 Basados en tablas de enrutamiento (Proactivos) 51
4.2 Basados en enrutamiento bajo demanda (Reactivos) 52
4.3 Protocolos híbridos 53
4.4 Protocolo DSR 63
4.4.1 Descubrimiento de rutas 63
4.4.2 Mantenimiento de ruta 66
4.4.3 Ventajas en DSR 67

4.4.4 Desventajas en DSR 67
4.5 Protocolo AODV 68
4.5.1 Descubrimiento de rutas 69
4.5.2 Mantenimiento de rutas 73
4.5.3 AODV en la capa de red 74
4.5.4 Estructuras de datos 75
4.5.4.1 Tabla de Enrutamiento 75
4.5.4.2 Tabla de RREQ's recibidas 75
4.5.5 Formato de paquetes 76
4.5.5.1 Paquete de datos 76
4.5.5.2 Paquete de descubrimiento de ruta (RREQ) 76
4.5.5.3 Paquete de respuesta de ruta (RREP) 77
4.5.5.4 Paquete de error en ruta (RERR) 78
5. CONCLUSIONES 81
BIBLIOGRAFIA 82

LISTA DE FIGURAS

	Pág
Figura 1. Estructura de una red Ad hoc	2
Figura 2. Redes con infraestructura	3
Figura 3. Red Ad hoc	4
Figura 4. Terminal oculto	8
Figura 5. Entorno Simétrico	11
Figura 6. Entorno Asimétrico	11
Figura 7. Red Ad hoc	14
Figura 8. PDA Compaq IPAQ y LCDC	19
Figura 9. Interfaz grafica PDA IPAQ de Compaq	20
Figura 10. Arquitectura de *UbiqMuseum*	21
Figura 11. Prototipo de auto inteligente	24
Figura 12. Arquitectura de capas según el modelo OSI	28
Figura 13. Espectro ensanchado	29
Figura 14. Espectro ensanchado por frecuencia directa	32
Figura 15. Secuencia Barker	33
Figura 16. Modulación BPSK	34
Figura 17. Modulación QPSK	35
Figura 18. Comparación de estándares	36
Figura 19. Rangos de transmisión 802.11b	37
Figura 20. Arquitectura de capas Bluetooth	41
Figura 21. Arquitectura de capas HIPERLAN 2	46
Figura 22. Multicanalización OFDM	48

Figura 23. Protocolos de enrutamiento 51
Figura 24. Comparación de protocolos 62

LISTA DE TABLAS

Pág

Tabla 1. Parámetros de evaluación en redes Ad hoc 25
Tabla 2. Modulación BPSK 33
Tabla 3. Modulación QPSK 34
Tabla 4. Especificaciones del estándar 802.11b 36
Tabla 5. Técnicas de modulación 49
Tabla 6. Protocolos de enrutamiento 50
Tabla 7. Ejemplo de una tabla de enrutamiento 68
Tabla 8. Formato de paquete de datos 76
Tabla 9. Formato del paquete de descubrimiento de ruta (RREQ) 76
Tabla 10. Formato del paquete de respuesta de ruta (RREP) 77
Tabla 11. Formato del paquete de error en ruta (RERR) **78**

INTRODUCCIÓN

El emergente campo de la computación móvil e inalámbrica debería tender a ampliarse y a requerir una tecnología de red móvil y altamente adaptiva. En este contexto, aparecen las Redes Móviles Ad hoc (MANET). Una MANET[1] es una estructura de red autónoma compuesta de varios nodos que pueden moverse libremente, es decir, una plataforma móvil donde todos los nodos actúan como routers y hosts indistintamente. Resulta interesante saber cuales son sus características, cómo este tipo de redes lleva a cabo el enrutamiento de paquetes y que aspectos importantes poseen los protocolos que son utilizados bajo condiciones tan extremas.

En este trabajo, se estudiarán los protocolos proactivos (se mantienen permanentemente actualizando las rutas), reactivos (descubren nuevas rutas según la demanda), y los protocolos híbridos (mezclan las características de los anteriores). Se hará énfasis en dos de los protocolos mas importantes (AODV y DSR), que han sido actualmente objeto de estudios y evaluaciones para lograr optimizaciones y mejoras de su funcionamiento en una red Ad hoc.

Luego se obtendrán las primeras conclusiones, que permitirán conocer los contextos en que un protocolo tiene mejor desempeño que otro. En resumen, primero se analizarán algunas características de las redes MANET, se comentaran acerca de las clasificaciones generales que se pueden hacer de los diferentes protocolos de las redes Ad hoc, luego se analizarán las características de un grupo de ellos, se realizará un estudio de la capa física, el cual es la base sobre el que las redes Ad hoc trabajan, y por ultimo se comentaran las diferentes aplicaciones en las que se están implementando estas redes.

---

[1] *Mobile Ad hoc Network*, www.ietf.org/html.charters/manet-charter.html.

IDENTIFICACIÓN Y DESCRIPCIÓN DEL PROBLEMA

Las redes Ad hoc están formadas por hosts móviles y que pueden estar conectados entre sí arbitrariamente y de manera dinámica, utilizando como medio de transmisión el espacio libre. En este tipo de redes, todos los nodos funcionan como enrutadores (*routers*) y se ven involucrados tanto en el descubrimiento como en el mantenimiento de rutas.

Uno de los mas grandes retos o desafíos que se plantean en este tipo de redes es lograr la transparencia, es decir, que el usuario final no tenga que hacer un tipo de conexión diferente de acuerdo al tipo de red (fija o móvil) para extenderlas a una mayor cantidad de usuarios.

Además por su naturaleza inalámbrica, existen pérdidas de paquetes por errores de transmisión y pérdidas de paquetes debido a la movilidad de la red ad hoc, teniendo en cuenta que la dinámica de esta red es una de sus principales características.

Muchas veces, en redes convencionales, disponer de infraestructura cableada fija o puntos de acceso no siempre es posible o viable, por lo menos en el caso de entornos civiles de carácter temporal y en lugares donde han ocurrido desastres naturales. Es por esto que este tipo de redes puede ser una solución muy acertada y se hace muy interesante para nuestro estudio.

Para esto, nosotros como investigadores debemos estudiar las fortalezas que tienen este tipo de redes, al igual que sus desventajas, para exponerlas de forma clara y precisa y así observar si es factible o no su implementación en futuras aplicaciones a nivel local.

OBJETIVOS

Objetivo General

Analizar y desarrollar el contexto global, infraestructura, evolución tecnológica y componentes de las redes Ad hoc, teniendo como punto de referencia los estándares de las redes inalámbricas.

Objetivos Específicos

- Analizar el estado de arte general de las redes móviles Ad hoc (MANETS).
- Describir los protocolos de enrutamiento en este tipo de redes.
- Estudiar la capa física de este tipo de redes.

JUSTIFICACION

En la actualidad se está presentando un desarrollo tecnológico impresionante, en donde nosotros como estudiantes debemos participar de él. Esto se puede hacer poniendo en práctica los conocimientos adquiridos en nuestra formación como profesional y como personas íntegras.

Escogimos la redes ad hoc debido a que es un tema de última generación que se está desarrollando actualmente, por tal razón es preciso realizar un análisis de lo que está ocurriendo en este campo, conocer sus debilidades y fortalezas, aportar nuestros conocimientos para la búsqueda de alternativas de mejoramiento e intentar llevar a la práctica este tipo de redes para el beneficio común.

REVISION DE ANTECEDENTES

Los antecedentes de las redes Ad hoc puede remontarse al año 1972 en conjunto con la creación de la PRNET (Red de Radio Paquete) por parte del DoD (Departamento de defensa de EE.UU.). La meta fue proporcionar intercambios de paquetes, conectando una red de computadoras a los elementos móviles usados en el campo de batalla, tales como soldados, tanques, aviones, etc.

A principios de los años noventa, la idea de una infraestructura con una colección de hosts móviles se propuso en dos conferencias, y el subcomité IEEE 802.11 adoptó el término "interconexión de redes Ad hoc".

Luego a mediado de los noventa, y estimulados por el creciente interés en las redes Ad hoc, se desarrollaron un número de estándares comerciales y no comerciales, que se encuentran avalados por la IETF (*Internet Engineering Task Force)*, y que se han implementado en algunas aplicaciones para estudiar su desarrollo y futura evolución.

El desarrollo de las redes Ad hoc viene acompañado del rápido proceso evolutivo de las tecnologías de comunicaciones. Hoy en día ya podemos observar aplicaciones de estas redes, en congresos locales, reuniones, aeropuertos y en sistemas vehiculares.

METODOLOGÍA DE INVESTIGACION

La investigación que se realizó fue del tipo descriptiva, utilizando recursos documentales, es decir, nos basamos en artículos de actualidad, papers propuestos en la IEEE, tutoriales y presentaciones expuestas en la pagina oficial de las redes Ad hoc en Estados Unidos (Advanced Network Technologies Division).

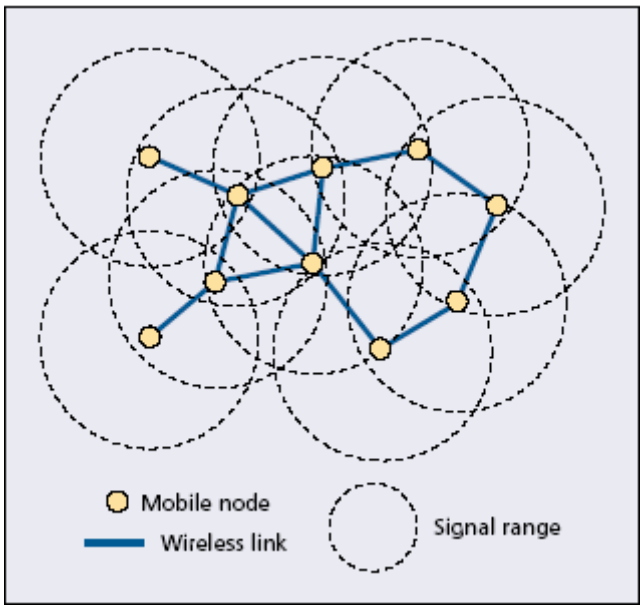
A nivel Iberoamericano investigamos y describimos algunas aplicaciones que están siendo objeto de estudios y simulaciones tales como robots, museos, vehículos, y aeropuertos.

Para la elaboración del trabajo final dedicamos un tiempo aproximado de cuatro meses, en el que investigamos y desarrollamos cada objetivo propuesto, comenzando primero por el estado del arte de las redes Ad hoc, siguieron luego los protocolos de enrutamiento en la que este tipo de redes se basa, y por ultimo desarrollamos la capa física, que es la base fundamental sobre la cual esta y todas las redes trabajan.

1. GENERALIDADES

Con el actual desempeño de los avances en la computación y las comunicaciones inalámbricas, las tecnologías de computación móvil están presentando un gran impacto, y se espera que muy pronto su uso y aplicaciones se extiendan, lo que por supuesto involucra el uso de nuevos protocolos.

Figura 1. Estructura de una red Ad hoc



La historia de redes inalámbricas empezó en los años setenta y el interés ha estado creciendo desde entonces. Durante la última década, y especialmente al final, el interés casi ha explotado probablemente debido al crecimiento rápido de Internet.

Entonces para comenzar a hablar de una red Ad hoc, debemos definir primero las generalidades en las que ella se basa, y en donde se definen dos grande grupos de redes inalámbricas o (*Wireless*):

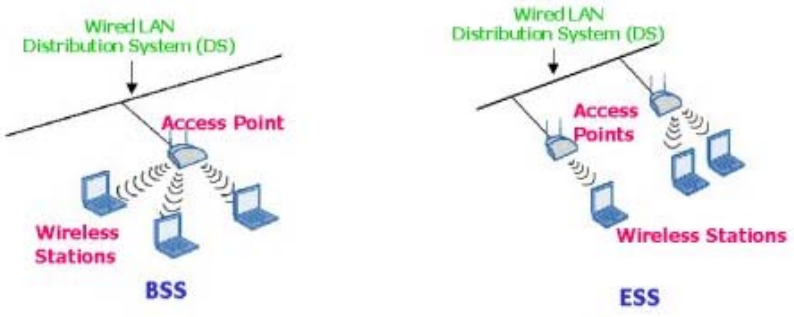
- Redes con infraestructura.
- Redes sin infraestructura (Ad-hoc).

1.2 Redes con infraestructura

En el modo infraestructura, la red *wireless* consiste por lo menos en un punto de acceso conectado a un número fijo de enlaces cableados entre sí, y un set de estaciones *wireless*. Esta configuración se denomina BSS (*Basic Service Set*). Un ESS (*External Service Set*) es un set de dos o más BSS formando una subred.

Cada host móvil debe comunicar con uno de estos enlaces dentro de su radio de acción. El nodo puede moverse libremente pero si sale fuera del rango de su enlace, debe conectar con otro para asegurar que la información llegue a su destino. Un ejemplo de este tipo de redes es la red de telefonía móvil formada por numerosas estaciones y antenas dispersas por todas las ciudades.

Figura 2. Redes con infraestructura

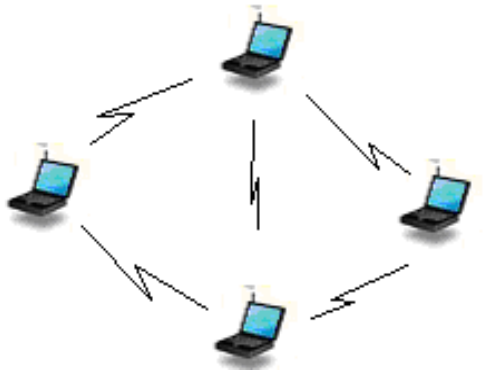


1.3 Redes sin infraestructura (Ad-hoc)

El modo Ad hoc también llamado IBSS (*Independent Basic Service Set*), es simplemente un set de estaciones que puede trabajar bajo la tecnología 802.11, HIPERLAN 2 o Bluetooth (hablando de capa física), que comunican directamente con otra sin necesidad de un punto de acceso y con una conexión de forma arbitraria y de manera dinámica. Es decir, no hay ningún elemento fijo y la topología de la red puede adoptar múltiples formas siendo igual de funcional.

En este tipo de redes, todos los nodos funcionan como enrutadores (routers) y se ven involucrados tanto en el descubrimiento como en el mantenimiento de rutas.

Figura 3. Red Ad hoc



Cuando se habla de una red Ad hoc normalmente se piensa de una red con nodos que son relativamente móviles en comparación con una red cableada. Su topología de red es mucho más dinámica y se presentan cambios imprevisibles, caso contrario a una red cableada. Este hecho crea muchos desafíos para la investigación que permitan la solución a problemas como *bandwidth* (ancho de banda), poder de la batería, latencia y QoS (calidad de servicio) entre otros.

Los protocolos empleados en las redes del tipo cableadas, o los protocolos utilizados en redes con infraestructura del tipo BSS o ESS, son imposibles de utilizar en estas redes Ad hoc debido al alto ambiente dinámico de los nodos. Con el desarrollo de Arpanet ahora conocido como Internet, y con el ejército quien era uno los mayores contribuyentes, se presentó el desarrollo de las redes Ad hoc. El pensamiento inicial era que este tipo de redes era perfecto para el campo de batalla, donde no se puede plantear ninguna infraestructura para comunicación.

Las redes Ad hoc son un campo muy amplio de investigación en el mundo actual de las telecomunicaciones, y ahondar en su conocimiento e investigar sobre este tipo de redes es algo que puede resultar muy contributivo al desarrollo de estas.

2. ESTADO DEL ARTE

2.1 Historia

La historia de las redes Ad hoc puede remontarse al año 1972 en conjunto con la creación de la PRNET (Red de Radio Paquete) por parte del DoD (Departamento de defensa de EE.UU.), y que se desarrollo en el programa *Survivable Adaptive Radio Networks* (SURAN) a principios de los años ochenta. La meta de estos programas fue proporcionar intercambios de paquetes, conectando una red de computadoras a los elementos del campo de batalla tales como soldados, tanques, avión, etc. en una infraestructura móvil. La PRNET usó una combinación entre ALOHA y CSMA para el acceso al medio, y un tipo de enrutamiento basado en el vector distancia. SURAN mejoró significativamente en los diseños de los dispositivos de radio, haciéndolos más pequeños, más baratos, y con más poder, y en el desarrollo de nuevos algoritmos. Los protocolos de enrutamiento estaban basados en el estado de enlaces jerárquico y con la ventaja de ser escalables.

A principios de los años noventa la abundancia de nuevos desarrollos tecnológicos, marcaron una nueva etapa en la interconexión de redes Ad hoc. La idea de una infraestructura con una colección de hosts móviles se propuso en dos conferencias, y el subcomité IEEE 802.11 adoptó el término "interconexión de redes Ad hoc". El concepto comercial (no militar) de redes Ad hoc había llegado, así que se sugirieron otras nuevas posibilidades no militares, y el interés creció.

Aproximadamente en el mismo tiempo, el DoD continuó de donde partió, consolidando programas tales como *Global Mobile Information Systems* (GloMo), y *Near-term Digital Radio* (NTDR). La meta de GloMo era proporcionar ambientes de oficina y conectividad *Ethernet* de tipo multimedia en cualquier momento y en cualquier parte.

Los métodos de acceso al medio estaban ahora en los modelos de CSMA/CA y TDMA, y fueron desarrollados nuevas topologías y protocolos de enrutamiento. NTDR ahora utilizado por el ejército de los EE.UU., es el único real (no prototipo) en el uso de redes Ad hoc hoy en día.

Estimulado por el creciente interés en las redes Ad hoc, se desarrollaron un número de estándares comerciales y no comerciales a mediados de los 90. Dentro del IETF, las redes Ad hoc (MANET) se crearon, para estandarizar los protocolos de enrutamiento. El desarrollo de los protocolos de enrutamiento dentro del grupo de trabajo de MANET llevó la clasificación de estos, en dos grupos: protocolos de enrutamiento reactivos y proactivos. El subcomité 802.11 estandarizó un protocolo de acceso al medio que estaba basado en la anulación de la colisión y la solución del problema de los terminales ocultos, siendo utilizable, para la construcción de nuevos prototipos en redes Ad hoc, para ser implementados en las tarjetas PCMCIA de los *notebooks*. HIPERLAN y Bluetooth fueron algunos estándares que beneficiaron el desarrollo de las redes Ad hoc.

2.2 ¿Qué es una red Ad hoc?

Una red móvil Ad hoc (MANET) es un conjunto de estaciones o conjunto de nodos móviles que se comunican entre sí, sin necesidad de un punto de acceso (AP), en donde todos los nodos enrutan, producen y consumen, y que utilizan como medio transmisor el espacio libre, es decir, es una red que no posee infraestructura alguna. El termino Ad hoc, aunque podría ser interpretado con connotaciones negativas tales como “improvisado” o “desorganizado[2]”, en el contexto de las redes inalámbricas hace referencia a redes flexibles, en las cuales todas las

[2] CANO Juan-Carlos, CALAFATE Carlos, MALUMBRE Manuel, MANZONI Pietro. Redes Inalámbricas Ad hoc como Tecnología de Soporte para la Computación Ubicua. http://www.smart-its.org/main_novitica.pdf.

estaciones ofrecen servicios de enrutamiento para permitir la comunicación de estaciones que no tienen conexión inalámbrica directa.

El objetivo de las redes móviles Ad hoc (MANET), es soportar de manera eficiente y robusta la operación de las redes móviles inalámbricas incorporando la funcionalidad de enrutamiento en nodos móviles, y tratando de lograr la transparencia, es decir que el usuario final no tenga que hacer un tipo de conexión diferente de acuerdo al tipo de red (fija o móvil) para extenderlas a una mayor cantidad de usuarios. Estas redes están diseñadas para ser dinámicas y aleatorias, con topologías cambiantes que están compuestas normalmente por conexiones inalámbricas de un ancho de banda relativamente restringido. Como toda red, este tipo de redes puede estar aislada del resto de redes o estar conectada a Internet.

2.2.1 Características de una red Ad hoc

- Terminales autónomos.
  - ✓ Cada terminal móvil es un nodo autónomo.
  - ✓ Cada nodo autónomo puede cumplir ambas funciones, como host o como router.
- Operación distribuida.
  - ✓ El control y el manejo de la red es distribuido entre los terminales.
  - ✓ Los nodos involucrados en una red Ad hoc se colaboran entre ellos mismos.

- Enrutamiento de múltiples saltos (*multihop routing*).

  ✓ Existen algoritmos de enrutamiento, que pueden ser de un solo salto (*single hop*) o de múltiples saltos, basados en diferentes atributos de enlace y de protocolos de enrutamiento.

  ✓ Los protocolos *single hop* son más simples que los *multihop*, en términos de estructura e implementación.

  ✓ Cuando se quiere enviar paquetes de datos desde el origen hasta en destino, y este se encuentra fuera del rango directo de transmisión, los paquetes deberían ser enviados a través de nodos intermedios hasta llegar a su destino.

  ✓ Se puede presentar el problema del terminal oculto.

Figura 4. Terminal oculto

El nodo B se puede comunicar tanto con C como con A, y los nodos A y C no pueden escucharse entre si.

Cuando el nodo A le transmite a B, el nodo C no puede detectar la transmisión usando el mecanismo de *carrier sense*, por lo tanto si C quiere transmitir a B ocurrirá una colisión en el nodo B. Por esto se dice que el nodo A es un terminal oculto para el nodo C.

- ✓ Se puede presentar el problema del terminal expuesto. El nodo B se quiere comunicar con el nodo A, y el nodo C quiere comunicarse con otro terminal diferente del nodo A y B. El nodo C utiliza el *carrier sense* “escucha el medio”, encuentra el medio en uso y tiene que esperar. El nodo A no puede escucharse con el nodo C, por tanto la espera no es necesaria, por esto se dice que el nodo C es un terminal expuesto al nodo B.

- Topología de red dinámica.

  - ✓ Los cambios en la topología de red son imprevisible.

  - ✓ La conectividad entre terminales puede cambiar con el tiempo.

  - ✓ Tanto toda la red como los nodos deberían adaptarse al tráfico y a las condiciones de propagación.

  - ✓ Los nodos móviles en la red, establecen enrutamientos dinámicos entre ellos mismos.

- Capacidad de enlace fluctuante.

  - ✓ La taza de error de bits puede ser mas alta que en una red inalámbrica convencional.

  - ✓ El canal sobre el cual los terminales se comunican esta sujeto a factores como ruido, interferencia y desvanecimiento.

  - ✓ Posee menos ancho de banda que una red cableada.

- Terminales limitados.

  - ✓ Los nodos en redes Ad hoc son dispositivos móviles con menos capacidad de procesamiento, pequeñas memorias y reducido poder de almacenamiento (Batería).

  - ✓ Se necesitan algoritmos optimizados en cada uno de los nodos para que presenten mayor eficiencia en relación a la característica anterior.

- Limitaciones debidas al medio inalámbrico.

  - ✓ Radio de transmisión limitado: Debido a la naturaleza inalámbrica, la distancia y la potencia están limitadas. Conforme la distancia aumenta la velocidad de transmisión disminuye.

  - ✓ Ancho de banda reducido: En un ambiente inalámbrico el ancho de banda es usualmente restringido, y por consiguiente tanto el trafico que es necesitado para el mantenimiento de la red como para el trafico causado por las aplicaciones debe ser mínimo.

  - ✓ Errores de transmisión/perdidas de paquetes: Se pueden presentar pérdidas de paquetes trasmitidos a través de la red, debido a varios intentos de retransmisión predeterminadas. La pérdida de estos paquetes se debe a factores como calidad de enlace, desactualizada información de rutas, y desbordamiento de buffer.

  - ✓ Seguridad restringida: Los requisitos de seguridad en una red móvil Ad hoc son los mismos que los existentes en redes tradicionales, y se enumeran a continuación: confidencialidad, integridad, autenticación, encriptación y disponibilidad.

- Limitaciones debidas al carácter móvil de las estaciones.

  - ✓ Topologías dinámicas (rutas dinámicas).
  - ✓ Energía reducida (dependen de baterías).

- Pueden trabajar en entornos completamente simétricos.

  - ✓ Todos los nodos tienen capacidades y responsabilidades idénticas.

Figura 5. Entorno Simétrico

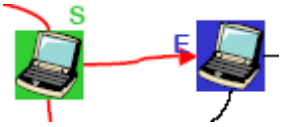


Figura 6. Entorno Asimétrico

- Pueden trabajar en entornos asimétricos.

  - ✓ Pueden tener diferentes radios de transmisión.
  - ✓ La duración de la batería difiere de acuerdo al equipo utilizado.
  - ✓ Capacidad de procesamiento diferente en cada equipo.
  - ✓ Se pueden utilizar diferentes tecnologías.

Al tener el espacio libre como canal de comunicación estas redes están expuestas a los problemas típicos de las redes inalámbricas, de igual forma las redes Ad hoc plantean grandes retos tales como:

- ✓ Garantía de detección de colisiones.
- ✓ Garantía de QoS (Calidad de servicio).
- ✓ Direccionamiento diferente.
- ✓ Debido a que los recursos son escasos, el consumo de ancho de banda y el acceso al medio debe ser lo mas mínimo.

Además por su naturaleza inalámbrica, existen pérdidas de paquetes por errores de transmisión y pérdidas de paquetes debido a la movilidad de la red Ad hoc, teniendo en cuenta que la dinámica de esta red es una de sus principales características.

Entre las ventajas podemos destacar:

- ✓ Son redes que se pueden utilizar de forma temporal y rápida.
- ✓ Fácil y rápido despliegue
- ✓ Bajo costo
- ✓ Robustez, ya que no posee una infraestructura como tal.
- ✓ Sirve de base para la computación ubicua

2.2.2 Aplicaciones

PAN´S (REDES DE AREA PERSONAL)

- ✓ Telefonía móvil.
- ✓ Agenda electrónica.

OPERACIONES DE EMERGENCIA

- ✓ Búsqueda y rescate.
- ✓ Policía.
- ✓ Bomberos.

ENTORNOS MILITARES

- ✓ Vehículos, soldados.
- ✓ Redes tácticas

ENTORNOS CIVILES

- ✓ Reuniones y congresos.
- ✓ Servicios de información contextual (Museos).
- ✓ Aeropuertos.
- ✓ Sincronización transparente entre dispositivos (entornos domésticos, entornos de oficina): esto debido que se pueden utilizar de forma temporal y rápida, sin necesidad de tendido de cable alguno, y además son entornos donde pueden actuar los dispositivos de un limitado rango de alcance.

La aplicabilidad más especifica e importante se refiere a aquellas que dan soporte a las comunicaciones militares y de auxilio durante un operativo o una emergencia.

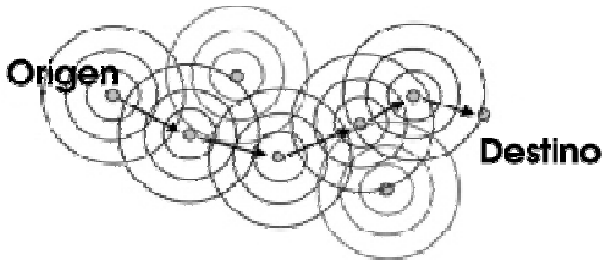
Para que pueda existir una comunicación entre los nodos, y se presente el intercambio de datos, debe existir una serie de protocolos que permitan el enlace

entre nodo y nodo. Para facilitar esta comunicación dentro de la red, un protocolo de enrutamiento es usado para descubrir las rutas entre los nodos, de la selección de la mejor ruta, o la más efectiva, ahí radica el hecho del estudio de cada uno de ellos. La construcción de la ruta en forma ideal, sea cual sea, debería ser hecha con un mínimo de consumo overhead (cabecera) y ancho de banda.

Dada la alta dinámica que poseen las redes MANET, la infraestructura de enrutamiento y los métodos de direccionamiento pueden variar de acuerdo a la topología de la red en un tiempo determinado. Esto implica que en la simulación de un nuevo protocolo de enrutamiento para una red Ad hoc sea necesario usar un modelo que represente de la forma más precisa posible el movimiento de los nodos. Se deben estudiar sus métodos y encontrar sus cualidades, ventajas y desventajas y la influencia de sus resultados en el estudio de los modelos de enrutamiento.

Los modelos de enrutamiento en las redes Ad hoc, tiene como objetivo primario establecer la ruta más eficiente entre dos nodos; pero en las redes Ad hoc se hace mucho mas énfasis en que el consumo de recursos de red y sobrecarga debe ser lo mínimo posible, sin comprometer la confiabilidad de la MANET. Es por ello que se han creado una serie de protocolos que intentan solucionar de la forma más adecuada este problema y de aquí la necesidad de evaluarlos bajo una serie de parámetros que permitan luego emitir una conclusión sobre el desempeño de la red.

Figura 7. Red Ad hoc



Esta figura muestra una sencilla red Ad hoc. El nodo origen quiere enviar un paquete al nodo destino, pero éste está fuera del alcance de su sistema de transmisión (representado por círculos en la

figura). Es necesario que los nodos intermedios formen parte del juego y retransmitan el paquete desde origen hasta destino. En el ejemplo, el camino por el que viaja el paquete de datos está representado por flechas.

2.3 ¿Cómo podría evolucionar una red Ad hoc?

Para apreciar el papel que desempeñan las redes Ad hoc es probable ponerlas en uso pensando en el futuro, teniendo en cuenta que hay que considerar el ancho de banda para las diferentes aplicaciones. Esto es porque, más capacidad implica la necesidad de un ancho de banda más alto y mejor uso del espectro de frecuencias. El ancho de banda más alto se encuentra a frecuencias más altas, donde el nivel de propagación es bajo.

La evolución continua de las redes Ad hoc es inminente, ya podemos observar ejemplos como los siguientes: una red Ad hoc de automóviles para el estudio del tráfico en el momento; los sensores en robots que forman parte de una red multimedia que permite visualización remota y de mando; múltiples routers aerotransportados automáticamente proporcionando conectividad donde sea necesario, una red Ad hoc alrededor de una nave espacial, entre otras. Esto puede parecer como ciencia ficción, pero en realidad son ideas que se están desarrollando por la comunidad de investigación de redes Ad hoc. Es por esto que los postulados anteriores son una visión del potencial tecnológico y notable evolución del estado del arte.

El desarrollo de las redes Ad hoc viene acompañado del rápido proceso evolutivo de las tecnologías de comunicaciones. Los dispositivos de comunicación inalámbrica están siendo más pequeños, más baratos y más sofisticados.

La explotación de estas tecnologías para el mejoramiento de una red Ad hoc dan lugar a nuevos problemas que requieren de nuevas investigaciones, por ejemplo,

el uso de antenas inteligentes, nuevos protocolos de descubrimiento de rutas, habilidad de alterar los códigos del espectro, técnicas de modulación y la forma de onda.

Las soluciones de redes basadas en la tecnología Ad hoc en última milla aumentarán su popularidad e incluso puede ser una solución dominante. La red Ad hoc militar tendrá capacidades más altas y aplicaciones multimedia de apoyo, será más adaptables, y evolucionará hacia un sistema donde los elementos de campo de batalla, móviles o estacionarios son conectados por multimedia.

2.4 Investigaciones y estudios de algunas aplicaciones de redes Ad hoc

2.4.1 Aplicaciones con PDAs en una red Ad hoc

Estas son algunas de las aplicaciones que sean estado evaluando y desarrollando con dispositivos PDA en redes Ad hoc.

2.4.1.1 Prototipo de guía turístico

En junio del 2001 la Universidad central de Taiwán ha realizado un prototipo para un sistema de guía turístico[3] en su propio campus, basado en el conocimiento del contexto. El sistema esta compuesto por un receptor GPS (sistema global de posicionamiento) el cual es conectado a un puerto de un portátil, el software del sistema de guía turístico es implementado en java, y esta compuesto de tres partes:

- ✓ Mapa 2D: aquí se muestra el posicionamiento de los turistas en el campo.
- ✓ Mundo virtual 3D: en este punto se realiza un tour virtual en el campus y se tiene la posibilidad de acceder a una red virtual, la cual posee toda la

[3] Yu-Chee Tseng, Shih-Lin Wu. Location Awareness in Ad hoc Wireless Mobile Networks. IEEE *Computer*

información almacenada del campus. En este mundo virtual los visitantes pueden interactuar con otros usuarios.

2.4.1.2 SUOSAS (*Small Unit Operation Situation Awarness System*)

En abril del 2000 *ITT industries* con la cooperación de DARPA se trabajó en una unidad pequeña de sistema de reconocimiento (SUOSAS)[4], este es un sistema desarrollado para el intercambio de información militar. El programa SUOSAS analiza cuatro grupos principales:

- ✓ La obtención de una amplia capacidad de comunicación en áreas geográficamente extensas.
- ✓ La realización de técnicas para inspeccionar la posición, independiente del sistema GPS.
- ✓ Definición de mecanismo de manejo de información para satisfacer la necesidad de los soldados.
- ✓ Determinar una solución que permita balancear los desempeños del sistema con el problema de peso, dimensión y consumo de energía.

2.4.1.3 Procesamiento de imágenes en un ambiente *MANET*

En agosto del 2000 se realizó un proyecto de investigación de procesamiento de imágenes[5] entre *STMicroelectronics* (STM) y la Universidad de Messina que abarca los casos de: transferencia de archivos, video *stream*, aplicaciones de mensajes orientados, entre otros.

---

[4] L. J. J. P. Tate, A. and J. Dalton, "Using a planning technology for army small unit operations," in *Poster Paper in Proceedings of the Fifth International Conference on Planning and Scheduling Systems (AIPS)*, (Breckenridge, Colorado, USA).

[5] R. Gonzalez and R. W. Digital, "Digital image processing,". *Digital Image Processing, Addison-Wesley Publishing Company*.

- ✓ Transferencia de archivo: si existe un dispositivo de video conectado a la *MANET* como el caso de una LCDC (*Low cost digital camara*), podría ser útil tener la posibilidad de descargar las imágenes capturadas o las vistas previas de estas. Puede ser posible descargar las imágenes capturadas en una variedad de dispositivos también conectados a la *MANET*. Para hacer esto, es necesario una fase preliminar en la cual se establezca la conexión con la información a intercambiar (características de la imagen), como por ejemplo que tipo de imagen se descarga, cuales son las resoluciones que soportan los dispositivos, el numero de colores que se puede visualizar, el tipo de encoders, etc.

- ✓ Video *stream*: En este caso ha sido creada una aplicación para videoconferencias en un ambiente local. Los problemas en este caso hacen referencia a la capacidad de visualización de imagen en algunos dispositivos capturadores.

  La configuración de red debe permitir a los nuevos usuarios unirse a este servicio, en el cual tengan la capacidad de conectarse o desconectarse en cualquier momento. Los mecanismos de seguridad deben implementarse a nivel de aplicación para prevenir las intromisiones de usuarios indeseados cuando se realicen las videoconferencias.

- ✓ Aplicación de mensajes orientados: En las aplicaciones de mensajes orientados, si uno a mas termínales que son miembros de una MANET y también están conectados a internen, es posible defina una aplicación con el cual otro dispositivo genérico que se encuentre en la red Ad hoc pueda crear un mensaje multimedia: audio, video y texto sincronizado y formateado según los criterios MMS (*Multimedia Messaging service*). Cuando el mensaje esta preparado, es enrutado entre los nodos de la red, hasta que este llegue al nodo que esta conectado a Internet, y luego es

transmitido a un centro de servicio colocado para la entrega o reparto del mensaje.

Se usaron algunos PDAs como dispositivos móviles inalámbricos y un LCDC como un dispositivo de captura; este LCDC es un prototipo de que aporto la empresa STM. El PDA (IPAQ Compaq con sistema operativo WinCE 3.0) y el LCDC están conectados entre si, emulan una hipotética cámara digital inalámbrica, donde la conexión es hecha utilizando la interfaz RS232 (115 Kbps). El ambiente de aplicación se divide en dos clases: Una se desarrolla en los PDAs y la otra en el emulador DSC. En este emulador se puede determinar cuantos dispositivos compatibles (que han cargado el software de manejo apropiadamente), están presentes en la red. En cualquier momento el DSC puede decidir a quien se le envía la vista previa de las imágenes capturadas. Cabe resaltar que en todos los PDAs fueron utilizados en un campo universitario, con un rango máximo de alcance de 50 metros.

Figura 8. PDA Compaq IPAQ y LCDC

A través del software grafico que se ejecuta en los PDAs, es posible saber en cualquier momento y en cualquier lugar, cuantos dispositivos capturadores de video están conectados a la red.

Según las aplicaciones de mensajes orientados, es posible enviar un mensaje multimedia, a una dilección de e-mail o a una pagina Web privada. La transmisión se completa solamente si uno de los dispositivos presentes en la red Ad hoc está conectado también a Internet. En la siguiente figura se muestra la interfaz grafica que se ejecuta sobre el IPAQ.

Figura 9. Interfaz grafica PDA IPAQ de Compaq

2.4.1.4 Redes Ad hoc como tecnología de soporte para la computación ubicua (*Ubiqmuseum)*.

El principal objetivo de la computación ubicua es el establecimiento de entornos donde los dispositivos con capacidades de procesamiento y comunicaciones (teléfonos móviles, PDA, dispositivos sensores, electrodomésticos, libros electrónicos, etc.) puedan cooperar y comunicarse de forma inteligente y consciente del entorno que les rodea de forma transparente al usuario. Es por esto que las redes Ad hoc se presentan como una tecnología de comunicación ideal en este tipo de entornos y aplicaciones.

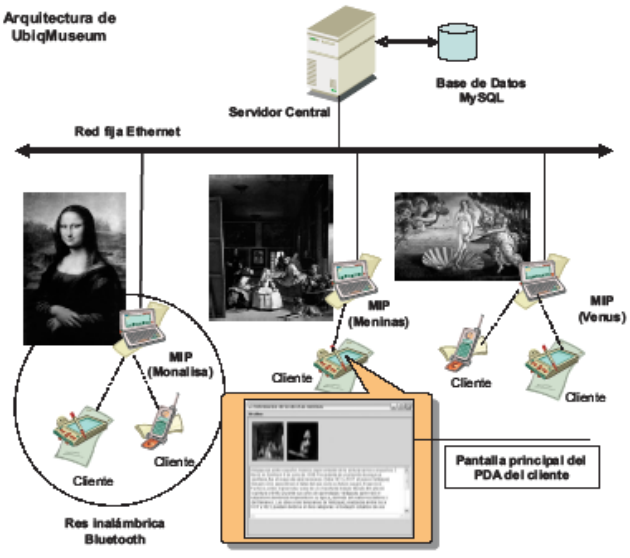
La aplicación *UbiqMuseum*[6] se realizó en el año de 1999 en un museo del estado de la Florida en USA, este utiliza una arquitectura de red que combina la

[6] CANO Juan-Carlos, CALAFATE Carlos, MALUMBRE Manuel, MANZONI Pietro. Redes Inalámbricas Ad hoc como Tecnología de Soporte para la Computación Ubicua. http://www.smart-its.org/main_novitica.pdf.

utilización de una red dorsal con una red aplicación. La red de aplicación utiliza únicamente tecnología Bluetooth, mientras que la red dorsal puede estar basada en tecnología de red local Ethernet o en tecnología de red local inalámbrica 802.11 en modo infraestructura. Como protocolo de encaminamiento global, se utiliza la versión modificada del protocolo AODV.

El sistema utiliza tres tipos diferentes de estaciones: clientes del museo (MICs), puntos de información del museo (MIPs), y un servidor central. Un visitante del museo provisto de un dispositivo PDA con interfaz Bluetooth es un ejemplo de un cliente. Además, debe existir un punto de información asociado con una o más piezas de arte del museo. Finalmente, los diferentes MIPs del museo se conectaran con el servidor central utilizando la tecnología, Ethernet, 802.11 o Bluetooth, dependiendo de las instalaciones del museo donde se despliegue la aplicación.

Figura 10. Arquitectura de *UbiqMuseum*



A medida que un cliente visita las diferentes obras del museo, la aplicación intenta localizar continuamente nuevos puntos de información utilizando la primitiva *inquiry* (procedimiento en el que las estaciones cercanas entre sı pueden localizar

estaciones vecinas) de Bluetooth. Cada vez que se localiza un nuevo punto de información, la aplicación comprobara los servicios que este le puede ofrecer utilizando el protocolo *Service Discovery Protocol* (SDP).

Si el cliente desea recibir la información que el nuevo punto de información le puede ofrecer, este debe enviarle su perfil, el cual fue introducido al iniciarse la aplicación en el dispositivo cliente. A partir del perfil del usuario, el punto de información procesa la petición combinando dicho perfil con el identificador del objeto que el cliente esta visitando y finalmente envía la petición al servidor central. El servidor central almacena la petición y la procesa, enviando la información solicitada al punto de información, el cual la enviará finalmente al cliente. La búsqueda de nuevos puntos de información se puede realizar por defecto de forma automática o bajo petición del usuario. Además, en todo momento el usuario puede modificar su perfil, por ejemplo en el caso de considerar que la información recibida es demasiado avanzada o muy básica para sus conocimientos. Así, la información recibida en sucesivos accesos se adaptará más a sus necesidades y requerimientos.

UbiqMuseum presenta las siguientes características:

Implementación basada en Java: se ha utilizado programación de Java para la tecnología inalámbrica Bluetooth propuesta por el *JavaExpert Group (JSR-82)*. Alrededor de 20 compañías líderes del sector de las comunicaciones han adoptado dicho estándar en sus dispositivos. JSR-82 ofrece un entorno de desarrollo de aplicaciones Bluetooth abierto y no propietario.

Base de datos con soporte SQL: toda la información relativa a los objetos de arte en el museo se almacena en una base de datos relacional. Esta solución ofrece flexibilidad, facilidad de uso, almacenamiento eficiente, procedimientos de mantenimiento y un alto nivel de seguridad.

Flexibilidad: la información que *UbiqMuseum* envía al usuario es completamente dinámica. Así, el formato y la cantidad de objetos gráficos y textuales que se envían al usuario no siguen un patrón predefinido sino que se puede adaptar de forma dinámica en función de la información almacenada en la base de datos.

Soporte de *Scatternet*: en un museo concurrido, es de esperar que más de siete visitantes (Ej. una piconet) puedan estar observando una misma pieza de arte. Para estos casos, se propone un algoritmo capaz de interconectar varias piconets para crear una *scatternet.*

2.4.2 Vehicular Ad hoc Networks

En el año 2002 se realizaron los estudios y evaluaciones de un nuevo proyecto de implementación de Redes Ad hoc en los vehículos[7], en el cual se utilizan vehículos como routers móviles en una MANET, además de esto, dichos vehículos deberían seguir la teoría del trafico, en la cual el trafico libre es descrito por tres parámetros elementales tales como: densidad de tráfico ρ_{veh} (veh/km), flujo de trafico **q** (veh/seg), tiempo neto promedio τ (Seg).

$$d_m = \frac{1000}{\rho_{veh}} - l_m ;$$

$$\tau_m = \frac{d_m}{v_m} = \frac{1}{v_m}\left(\frac{1000}{\rho_{veh}} - l_m\right)$$

$$q_m = \frac{1}{\tau_m} = v_m\left(\frac{1}{\frac{1000}{\rho_{veh}} - l_m}\right)$$

Los vehículos periódicamente envían mensajes *broadcast* que contienen sus localizaciones y el tiempo de la información. Cada vehiculo maneja una tabla de enrutamiento utilizada para almacenar en una base de datos, la información de los

[7] FRANZ Walter, SARMA Amardeo. FleetNet Project. http://www.fleetnet.de.

vehículos, que se encuentran a sus alrededores, se utilizan protocolos de enrutamiento basados en la información de la ubicación del vehículo (GPS), el cual posee características como:

- ✓ Proporciona coordenadas de localización (X, Y), en el tiempo (t).
- ✓ Capacidad para localizar (X, Y) sobre mapas estáticos almacenados en la memoria de los dispositivos.
- ✓ Capacidad para trazar un camino sobre el mapa, basándose en la tabla (x, y, t), y capacidad para trazar múltiples caminos de forma similar.

En la base de datos, cada nodo tiene información local con respecto a los vehículos vecino. Recopilando la información de cada nodo para así crear una vista global de todo el sistema. También se encuentra la ubicación actual de todos los vehículos con sus respectivos tiempos. Cada vehículo tiene su propia visión acerca de la ubicación del resto de los vehículos.

Figura 11. Prototipo de auto inteligente

Este sistema vehicular ofrece:

- ✓ Notificación en casos de emergencia entre los usuarios.
- ✓ Asistencia, en caso de accidentes y percances mecánicos.
- ✓ Información de obstáculos peligrosos en las carreteras.
- ✓ Monitoreo de tráfico.
- ✓ Reporte de estado climático.
- ✓ Chat íntervehicular.
- ✓ Juegos de entretenimiento.

2.4.3 Variables de entrada empleadas en simuladores OPNET, GloMoSim y NS2 en redes Ad hoc.

Tabla 1. Parámetros de evaluación en redes Ad hoc

Parameters	Value
Terrain size	1km x 1km
Number of nodes	50
Node placement	uniform
Nb. of broadcasting nodes	10
Nb. of broadcasts per node	100
MAC protocol	802.11 without RTS/CTS
Bit rate	2 Mbps
Wireless propagation model	FreeSpace
Antenna Type	Omnidirectional
Mobility model	Random Waypoint

- ✓ 10 a 50 nodos que permanecen en forma estacionaria en tiempos de pausa dados en segundos (0-100s) y luego se mueven en forma aleatoria en un espacio de 1000m * 1000m con una velocidad uniforme de 0 -20m/s.

- ✓ Tráfico: (4 - 20 paquetes/s, 64 -1024 bytes/paquete).

- ✓ Rango de poder (1m -300m).

- ✓ Intenta estimar latencia de descubrimiento de ruta, *overhead* de enrutamiento.

Estas son las diferentes variables de entrada que se aplican sobre los simuladores anteriormente mencionados, los cuales nos permiten tener una idea previa del funcionamiento y comportamiento de la MANET antes de implementarla en el campo.

3. CAPA FÍSICA EN REDES AD HOC

Para hablar acerca de la capa física en las redes Ad hoc, comenzaremos a describir las técnicas de modulación y codificación con las cuales trabajan los dispositivos de estas redes y que se encuentran inmersas en los estándares 802.11 y 802.11b, tecnología Bluetooth e HIPERLAN 2.

3.1 El Estándar IEEE 802.11

La arquitectura básica y servicios del 802.11b son definidos por el estándar original 802.11. Las especificaciones del estándar 802.11b afectan únicamente a la capa física, añadiendo velocidades mayores y una conectividad más robusta.

La tecnología basada en el estándar permite a los administradores crear nuevas redes que pueden combinar distintas tecnologías para conseguir lo que más se aproxime a sus necesidades. El estándar 802.11 (modo infraestructura), define dos componentes, una estación *wireless*, que normalmente es un PC equipado con una tarjeta de red (NIC) y un punto de acceso (AP), que actúa como un puente entre las redes wireless y las cableadas.

Un punto de acceso normalmente consiste en una radio, una interfaz de red y un *software briding* que cumple el estándar 802.1d. El punto de acceso actúa como la estación base para la red *wireless*, agregando acceso para múltiples estaciones *wireless* a la red cableada.

Las estaciones wireless pueden ser PC con tarjetas 802.11, tanto ISA, PCI, o PCMCIA. El estándar 802.11 define dos modos de operación: el modo Infraestructura y el modo Ad hoc ó IBSS, los cuales ya se definieron anteriormente en la introducción.

3.1.1 Espectro ensanchado

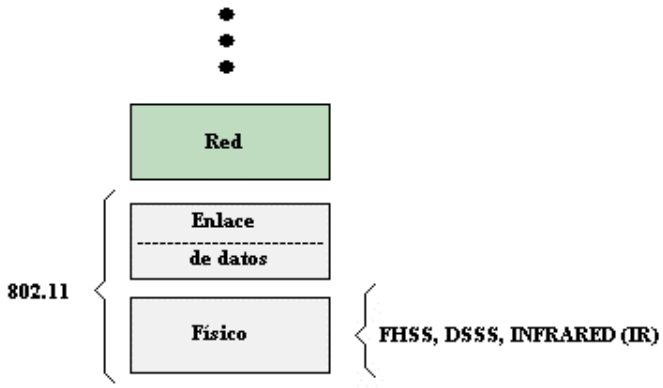
Los estándares basados en radiofrecuencia (RF) operan dentro de la banda 2.4 GHz ISM, teniendo en cuenta que las bandas ISM son:

- ✓ 902 - 928 MHz
- ✓ **2.4 - 2.4853 GHz**
- ✓ 5.725 - 5.850 GHz

Estas bandas de frecuencia son reconocidas por los reguladores internacionales, como FCC (USA), ESTI (Europa), y la MKK (Japón), como operaciones de radio sin licencia, para usos científicos, militares e industriales.

Las tres subcapas físicas originalmente definidas en el estándar 802.11 incluyen dos espectros de radio (FHSS, DSSS) y una especificación de infrarrojos (IR).

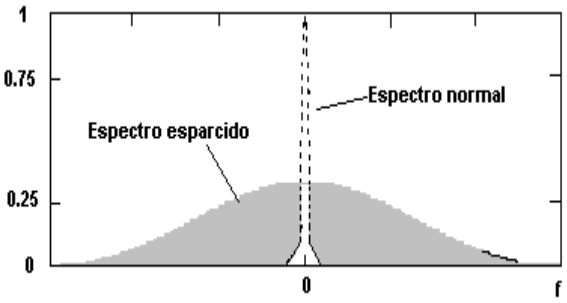
Figura 12. Arquitectura de capas según el modelo OSI



Inicialmente, las técnicas de espectro ensanchado fueron desarrolladas con el propósito de combatir las interferencias en las comunicaciones militares, lo cual se

logra esparciendo el espectro de la señal transmitida sobre determinadas bandas de frecuencias.

Figura 13. Espectro ensanchado



El espectro ensanchado consiste en diseminar o esparcir la potencia de la señal en una banda ancha de frecuencias, consiguiendo ganar rendimiento en la relación señal/ruido, a costa de sacrificar ancho de banda. Con esta técnica se consigue señales menos susceptibles al ruido eléctrico que con las modulaciones tradicionales de radio. Dado que las señales de radio comunes tienen un espectro estrecho solo interferirán en una pequeña porción de la señal "ensanchada en el espectro", obteniendo como resultado una menor interferencia y menores errores en la transmisión. Con tal ensanchamiento del espectro se logran propiedades como son: la capacidad de direccionamiento selectivo, CDMA (acceso múltiple por división de código*)* y rechazo a interferencia.

El espectro ensanchado, toma una señal en banda base, por ejemplo un canal de voz con un ancho de banda de sólo unos KHz y la distribuye sobre un ancho de banda que puede ser de varios MHz. Esto se realiza por modular la señal de información con una señal codificada de banda ancha. Una forma de lograr una señal en espectro ensanchado es la modulación de una portadora por una secuencia digital codificada cuya tasa de bit es mucho más alta que el ancho de banda de la señal de información.

Las técnicas de espectro ensanchado, además de satisfacer los requerimientos mínimos, aumentan la seguridad, elevan el *throughput* (rendimiento), y permiten que varios productos inconexos compartan el espectro sin cooperación explícita y con interferencia mínima.

Existen dos técnicas de espectro ensanchado empleadas en las transmisiones en banda ancha los cuales son mecanismos de señalización fundamentalmente diferentes y que no pueden interoperar entre ellos.

1. FHSS (*Frequency Hopping Spread Spectrum*)
2. DSSS (*Direct Sequence Spread Spectrum*).

El estándar original 802.11[8] define velocidades de 1 y 2 Mbps vía radio frecuencia usando estas técnicas.

3.1.1.1 FHSS (*Frequency Hopping Spread Spectrum)*

Usando la técnica FHSS o técnica de espectro ensanchado por salto en frecuencia, la banda de 2.4 GHz es dividida en 75 subcanales de 1MHz. El emisor y receptor deciden un patrón de salto (*hopping code*) que determina las frecuencias por las que se transmitirá y el orden de uso de estas. Para recibir correctamente la señal, el receptor debe disponer del mismo patrón de salto que el emisor, y escuchar la señal en la frecuencia y momento correcto.

Cada transmisión dentro de la red ocurren sobre un patrón de salto distinto, y los patrones son diseñados para minimizar la probabilidad de que dos emisores usen el mismo subcanal simultáneamente, es decir, cambia la frecuencia de la onda portadora muy rápidamente y en sincronía, utilizando diferentes canales para evitar interferencias.
La regulación impone a los fabricantes el uso de al menos 75 frecuencias distintas para la transmisión de un canal con un tiempo máximo de 400ms de uso por frecuencia.

[8] IEEE Std 802.11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification*, 1999 edition.

Es posible por tanto, disponer de varios equipos empleando la misma banda de frecuencia sin que se interfieran, asumiendo que cada uno de ellos emplea un patrón de salto diferente. Dos patrones de saltos que nunca emplean la misma frecuencia se dice que son ortogonales. La imposición de al menos 75 frecuencias distintas en una banda, permite tener varios canales que no se interfieran.

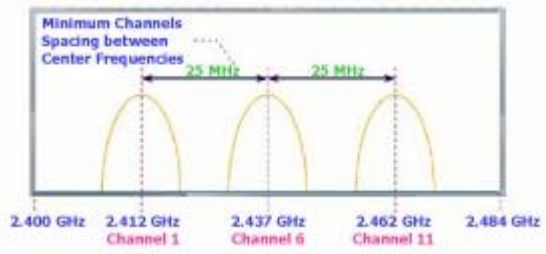
Después de lo descrito se pueden destacar algunas características de ésta técnica de modulación:

- ✓ Coste Superior.
- ✓ Consumo superior.
- ✓ Mayor velocidad de transmisión.
- ✓ Mayor cobertura.
- ✓ Menor numero de canales.

La ventaja de la técnica FHSS es que permite un diseño de radio simple, pero como desventaja la velocidad esta limitada a un máximo de 2Mbps. Esta limitación viene impuesta principalmente por regulaciones de la FCC, que restringe los canales a un ancho de banda máximo de 1 MHz. Estas regulaciones obligan al sistema FHSS a usar la banda 2.4GHz por completo, con lo que deben saltar a menudo, lo que conlleva una gran carga de overhead para los saltos.

3.1.1.2 DSSS (*Direct Sequence Spread Spectrum*)

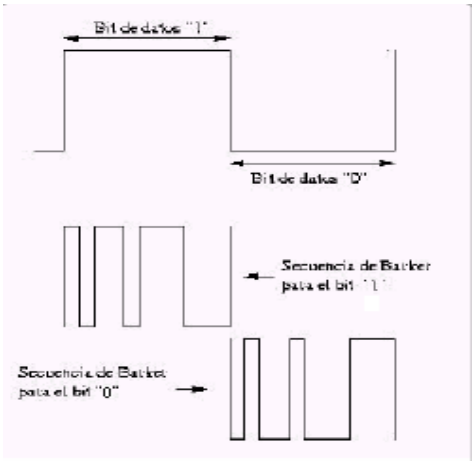
Figura 14. Espectro ensanchado por frecuencia directa



La técnica DSSS o técnica de espectro ensanchado por frecuencia directa, divide la banda de 2.4 GHz en 14 subcanales. En USA, solo están disponibles 11 canales. Para que múltiples canales coexistan en la misma zona, deben estar separados 25 MHz para evitar interferencias. Esto significa que al menos 3 canales pueden coexistir en una misma zona. La información es enviada sobre uno de estos canales sin necesidad de que salte a otro canal. Para evitar el ruido de un canal, se usa una técnica llamada *chipping*. Cada bit de datos es convertido en una serie de patrones redundantes de bit llamados *chips*. La redundancia inherente de cada *chip* combinado con el envío de la señal a través del canal da como resultado una forma de detección y corrección de errores; incluso si parte de la señal está mal, se puede recuperar en muchos casos, minimizando la necesidad de retransmisión. DSSS especifica una secuencia de 11 bits para el chipping llamada secuencia *Barker* para codificar todos los datos enviados a través del aire. Cada secuencia de 11 bits representa un solo bit de datos (1 o 0), y se convierte en una forma de onda, llamada símbolo, que puede ser enviada a través del aire. Estos símbolos son transmitidos con una tasa de símbolos de 1MSps (1 millón de símbolos por segundo) usando la técnica BPSK (*Binary Phase Shift Keying*). En el caso de 2 Mbps, se usa una implementación más sofisticada llamada QPSK (*Quadrature Phase Shift Keying*), que dobla la tasa de datos que soporta BPSK mejorando la eficiencia en el uso del ancho de banda. La secuencia de Barker tiene la siguiente forma:

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

Figura 15. Secuencia Barker



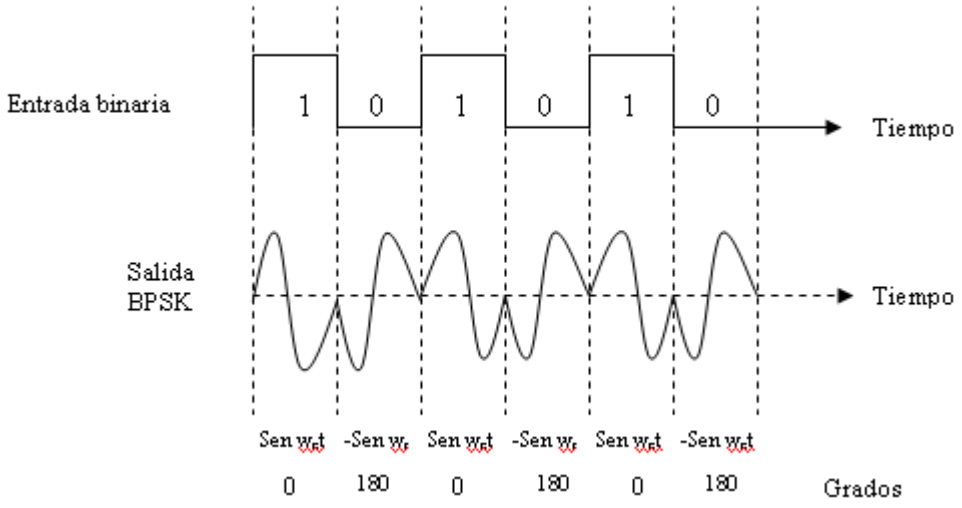
3.1.1.2.1 BPSK

Modulación por desplazamiento binario de fase. Es un sistema de modulación digital angular de amplitud constante. Con esta técnica son posibles dos fases de salida para una sola frecuencia portadora. Una fase de salida presenta un 1 lógico y la otra un 0 lógico. Cuando la señal de entrada digital cambia de estado, la fase de la portadora de salida varia entre dos ángulos que están desfasados 180°, es decir, un ángulo a 0° (+Sen $W_c t$) para un 1 lógico, y el otro ángulo a 180° (-Sen $W_c t$) para un 0 lógico.

Tabla 2. Modulación BPSK

Entrada binaria	Fase de salida
0 lógico	180°
1 lógico	0°

Figura 16. Modulación BPSK



3.1.1.2.2 QPSK

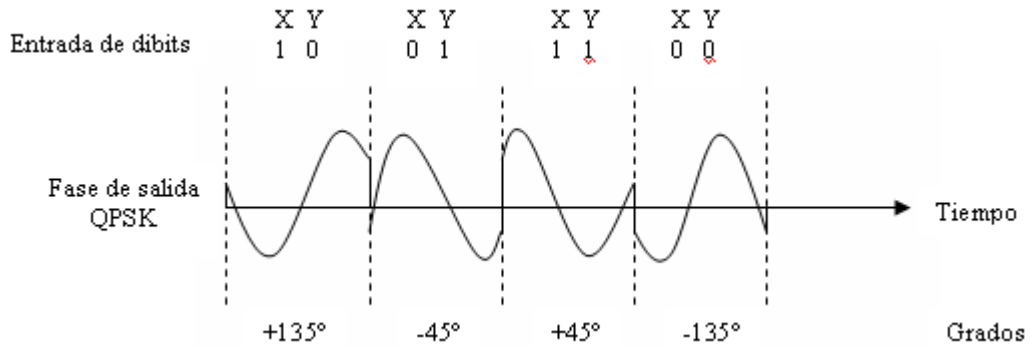
Modulación por desplazamiento cuaternario de fase. Es otra forma de modulación digital angular de amplitud constante. Con esta técnica son posibles cuatro fases de salida para una sola frecuencia portadora. Como hay cuatro fases distintas de salida, debe haber cuatro condiciones distintas de entrada. Ya que la entrada digital a un modulador QPSK es una señal binaria, para producir cuatro condiciones distintas de entrada se necesita más de un solo bit de entrada. Con dos bits hay cuatro condiciones posibles: 00, 01, 10, 11.

Tabla 3. Modulación QPSK

Entrada binaria		Fase de salida QPSK
X	Y	
0	0	-135°
0	1	-45°
1	0	+135°
1	1	+45°

En consecuencia en QPSK los datos binarios de entrada se combinan en grupos de dos bits llamados dibits. Cada dibit de código genera una de las cuatro fases posibles de salida. Así, para cada dibit de dos bits sincronizado en el modulador, se obtiene un solo cambio en la salida.

Figura 17. Modulación QPSK



DSSS en vez de modificar la frecuencia de la portadora, utiliza ese patrón para codificar cada uno de los bits de datos, de manera que la pérdida de uno de ellos causada por interferencias, no implica la retransmisión del paquete entero, ya que es posible reconstruir por técnicas estadísticas el patrón casi completamente.

Algunas de las características de ésta técnica de modulación mas destacadas son:

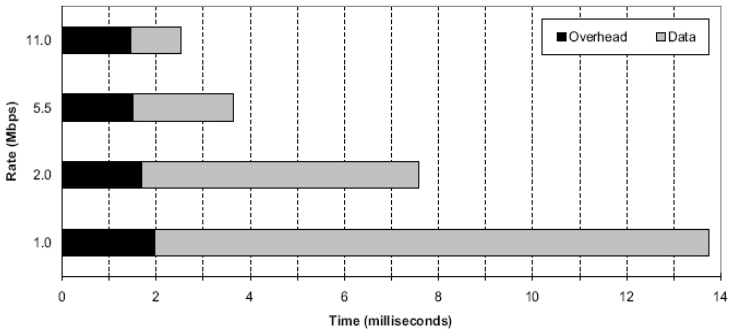
- ✓ Menor coste.
- ✓ Consumo menor.
- ✓ Menor cobertura.
- ✓ Tolerante a interferencias de señales.

Para finalizar podemos decir que si se requiere un óptimo desempeño y la interferencia no es un problema, es recomendable utilizar radios de secuencia directa. Pero si lo que se desean son unidades móviles pequeñas y baratas la técnica de salto de frecuencia es la más adecuada. Es importante resaltar que con cualquiera de los dos métodos el resultado es un sistema que es extremadamente

difícil de violar, que no interfiere con otros sistemas y que transporta grandes cantidades de información.

3.2 Estándar 802.11b

Figura 18. Comparación de estándares



La principal contribución del 802.11b[9] al estándar de WLANs era estandarizar el soporte de la capa física para dos nuevas velocidades, 5.5 Mbps y 11 Mbps. Para conseguir esto, se debía usar la técnica DSSS, porque, el FHSS no permite velocidades mayores de 2 Mbps debido a las restricciones de la FCC. Los sistemas 802.11b podrán ínter-operar con sistemas de 1 y 2 Mbps que usen DSSS, pero no con los que usen FHSS.

Tabla 4. Especificaciones del estándar 802.11b

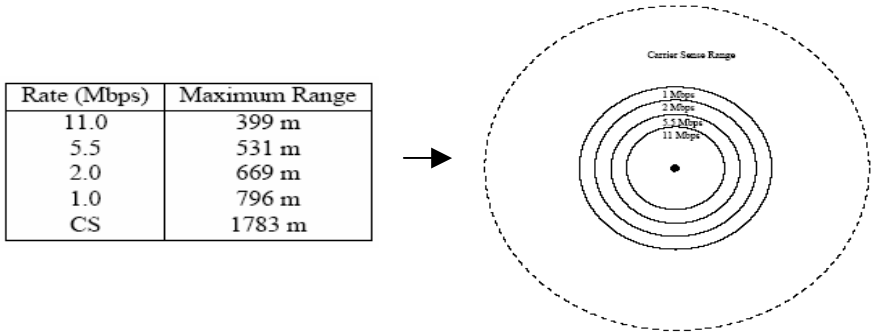
IEEE 802.11b Data Rate Specifications				
Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Para incrementar la tasa de datos en el estándar 802.11b, se desarrollaron técnicas de codificación avanzadas. Mejor que las dos secuencias Barker de 11 bits, el 802.11b especifica la codificación *Complementary Code Keying* (CCK), que consiste en un conjunto de 64 palabras código de 8 bits. Como conjunto, estas palabras código tienen propiedades matemáticas únicas que les permiten distinguirse correctamente uno de otra por un receptor incluso en presencia de un ruido importante e interferencia multicamino. La tasa de 5.5 Mbps usa el CCK para

[9] IEEE Std 802.11b. http://standards.ieee.org.

codificar 4 bits por portadora, mientras que la tasa de 11 Mbps codifica 8 bits por portadora. Ambas velocidades usan la técnica de modulación QPSK y señal a 1.375 MSps. Así es como se obtiene altas tasas de datos.

Figura 19. Rangos de transmisión 802.11b



Rate (Mbps)	Maximum Range
11.0	399 m
5.5	531 m
2.0	669 m
1.0	796 m
CS	1783 m

3.3 Tecnología Bluetooth

La tecnología bluetooth[10] es el resultado de la unión de esfuerzos y logros de nueve compañías líderes en la industria de telecomunicaciones e informática (*3com, Ericsson, Intel, IBM, lucent, Microsoft, Motorota, Nokia y Toshiba*). Más de 1300 fabricantes, procedentes de todo el mundo y de diferentes áreas de negocio, se han unido actualmente a la familia bluetooth. Esto ha posibilitado que dicha tecnología sea el prototipo industrial que mayor y más rápido crecimiento haya experimentado jamás.

Bluetooth es una tecnología utilizada para la conectividad inalámbrica de corto alcance entre dispositivos como PDA´s (*Personal Digital Assistance*), teléfonos celulares, teclados, máquinas de fax, computadoras de escritorio y portátiles, módems, proyectores, impresoras, etc. El principal mercado es la transferencia de datos y voz entre dispositivos y computadoras personales.

[10] LEDESMA Karen, CASTELLAR Israel. Diseño de una PAN Basada en Tecnología Bluetooth. Universidad Tecnológica de Bolívar. Monografía Minor de Comunicaciones y Redes. Facultad de Ingeniería de Sistemas.

El enfoque de Bluetooth es similar a la tecnología de infrarrojo conocida como IrDAs (*Infrared Data Association*). Sin embargo, Bluetooth, es una tecnología de radiofrecuencia (RF) que utiliza la banda de espectro disperso de 2.4 GHz. Muchas veces también se le confunde con el estándar IEEE 802.11, otra tecnología de RF de corto alcance. IEEE 802.11 ofrece más caudal eficaz pero necesita más potencia de transmisión y ofrece menos opciones de conectividad que Bluetooth para el caso de aplicaciones de voz.

Bluetooth intenta proveer significantes ventajas sobre otras tecnologías inalámbricas similares tales como IrDA, IEEE 802.11 Y *HomeRF*, claros competidores en conexiones PC a periféricos. IrDA es una tecnología muy popular para conectar periféricos, pero es limitada severamente a conexiones de cortas distancias en rangos de un metro por la línea de vista requerida para la comunicación. Debido a que Bluetooth funciona con RF no está sujeto a tales limitaciones. Las distancias de conexión en Bluetooth puede ser de hasta 10 metros o más dependiendo del incremento de la potencia del transmisor, pero los dispositivos no necesitan estar en línea de vista ya que las señales de RF pueden atravesar paredes y otros objetos no metálicos sin ningún problema.

Bluetooth puede ser usado para aplicaciones en redes residenciales o en pequeñas oficinas, ambientes que son conocidos como WPANs (*Wíreless Personal Área Network*). Una de las ventajas de las tecnologías inalámbricas es que evitan el problema de alambrar las paredes de las casas u Oficinas.

En el año 2002 la IEEE aprobó el estándar IEEE 802.15.1 compatible totalmente con la tecnología Bluetooth v1.1. En este estándar se definen las especificaciones de la capa física y MAC (*medium access control*) para las redes WPANs.
El nuevo estándar permitirá una mayor validez y soporte en el mercado de las especificaciones de Bluetooth, además es un recurso adicional para aquellos que implementen dispositivos basados en esta tecnología. Anteriormente a la

estandarización, dispositivos Bluetooth no podían coexistir con los dispositivos basados en IEEE 802.11b debido a que ambos se interferían entre sí. Otro esfuerzo importante para buscar la compatibilidad entre tos dos sistemas lo están haciendo la compañía *Intersil Corp*., fabricante de chips para el protocolo IEEE 802.11 b (Wi-Fi) y la compañía *Sílicon Wave Inc*. fabricante de sistemas de radio de Bluetooth. Este esfuerzo entre Wi-Fi y Bluetooth es conocido como "blue802" y permitirá la operación simultánea de estos dos protocolos inalámbricos.

3.3.1 Descripción

Bluetooth define dos rangos de cobertura. El rango corto abarca distancias de hasta 10m, mientras que el rango medio cubre distancias de unos 100 metros. Este enlace radio es capaz de proveer transmisión de voz y datos a velocidades de hasta 720 Kbps por cada canal que esté operando en la piconet, la cual se define como la agrupación de 2 a 8 dispositivos Bluetooth en topología de estrella.
El radioenlace opera sobre una banda que no requiere licencia, la cual se denomina banda ISM (*Industrial, scientific and medical*). El ancho de banda del enlace se encuentra entre 2.4GHz y 2.48GHz utilizando un sistema de ensanchamiento del espectro (*spread spectrurn*) con saltos de frecuencia del orden de 1600 saltos por segundo (FHSS), y una serial fullduplex. Una misma señal fluctúa entre 79 frecuencias con intervalos de 1 MHz entre ellas, lo que hace que el rechazo a las interferencias sea alto. Para la versión de cobertura corta (10m), se tiene que la potencia de la señal de radiofrecuencia de salida es de 0dBm, es decir, de 1 mW. En cambio, para la especificación que ofrece coberturas de 100m se tiene que la potencia de salida deberá ser mayor, especificándose en una potencia de hasta 20dBm (100mW), aunque es capaz de operar con potencias de salida de hasta 20dBm. La especificación del enlace radio, integra toda la parte referente a radiofrecuencia sobre un circuito integrado basado en tecnología CMOS, la cual posee una serie de ventajas como reducción de costos, bajo consumo y tamaño del chip reducido, características ideales para

dispositivos móviles, los cuales tienen características críticas para las ventajas ofrecidas por la tecnología propuesta.

Para el tipo de transmisión que se puede llevar a cabo con esta tecnología, diferenciando entre transmisión de voz y transmisión de datos, se tiene en cuenta las siguientes características para cada tipo de transmisión:

- ✓ **Voz**: La tecnología ofrece la posibilidad de usar tres canales simultáneos sincronos de voz, o bien optar por la posibilidad de compartir un solo canal para el transporte simultáneo de datos asíncronos y voz síncrona. Cada canal de voz soporta un canal sincrono de voz a 64 Kbps tanto para el enlace de subida como para el de bajada.

- ✓ **Datos:** El canal de transporte de datos asíncronos es capaz de soportar tasas de hasta 723.2Kbps en modo asimétrico (manteniendo una tasa de 57.6Kbps en la dirección de retorno), mientras que en transmisión simétrica otorga tasas de transmisión de hasta 433.9 Kbps.

3.3.2 Especificaciones

La especificación de Bluetooth cubre desde el transceptor de radio hasta varias interfaces de protocolos basados tanto en hardware como en software. Bluetooth opera en una banda de uso libre conocida como ISM (*Industrial, Scientific, and Medical*), donde otros dispositivos de uso común la utilizan como es el caso de puertas de garajes, teléfonos inalámbricos, hornos microondas, entre otros. Para que los dispositivos Bluetooth puedan coexistir y operar confiablemente con los otros dispositivos, cada piconet es sincronizada a una frecuencia específica del patrón de salto por frecuencia. Este patrón, que salta a 1.600 frecuencias diferentes por segundo, es único para una piconet en particular. Cada "salto" de frecuencia es una ranura de tiempo durante la cual los paquetes de datos son

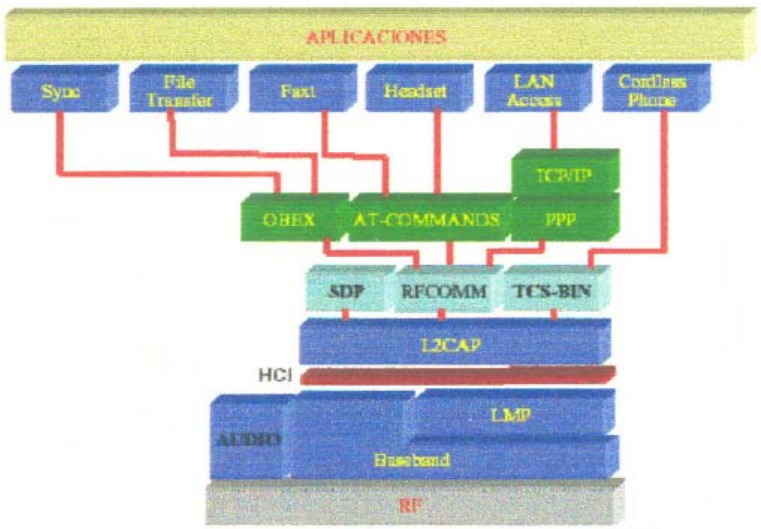
transferidos. Un paquete puede abarcar hasta 5 ranuras de tiempo, en la cual la frecuencia permanece constante durante la duración de esa transferencia.

Si los dispositivos van a saltar a las nuevas frecuencias después de cada paquete, ellos deben ponerse de acuerdo en la secuencia de las frecuencias que utilizarán. Los dispositivos Bluetooth operan en 2 modos, como maestro y esclavo. En una piconet uno de los dispositivos participantes trabaja como maestro y el resto como esclavos, entonces el dispositivo maestro asigna la secuencia de salto de frecuencia, y los esclavos sincronizan al dispositivo maestro en tiempo y frecuencia seguido de la secuencia de salto del dispositivo maestro.

3.3.3 Arquitectura de Capas

La siguiente figura muestra un esquema de los protocolos utilizados para la tecnología Bluetooth los cuales son empleados en la comunicación de voz y datos.

Figura 20. Arquitectura de capas Bluetooth



3.3.3.1 Radio Frecuencia (RF)

Define los requerimientos del dispositivo Bluetooth que opera en la banda ISM a 2,4GHz. Esta capa se basa en el método de división de espectro conocido como espectro ensanchado, utilizando 75 saltos de frecuencia en cada MHz, comenzando en 2,402GHz y acabando en 2,480GHz. En algunos países como por ejemplo Francia, el ancho de banda de esta frecuencia se reduce temporalmente, utilizando en este caso un sistema de 23 saltos de frecuencia.

En ambos sistemas se utiliza una banda de guarda entre cada salto, con el fin de respetar las regulaciones de cada país en cuanto al tema de evitar las transmisiones fuera de banda.
Se tienen tres clases de dispositivos utilizados en Bluetooth que se agrupan según la potencia:

Potencia Clase 1. Dispositivos de largo alcance (aprox. 100m), con una potencia máxima de salida de 20dBm.

Potencia Clase 2. Dispositivos de medio alcance (aprox. 10m), con una potencia máxima de salida de 4dBm.

Potencia Clase 3. Dispositivos de corto alcance (aprox. 10cm), con una potencia máxima de salida de 0 dBm.

La interfaz radio Bluetooth se basa en una antena de potencia nominal de 0dBm. Cada dispositivo puede variar su potencia de manera opcional. El equipamiento con control de potencia optimiza la potencia de salida con comandos procedentes del protocolo de enlace.

Esto se hace midiendo el RSSI (*Receiver Signal Strength Indicator*), retornando un mensaje indicando si la potencia debe ser incrementada o decrementada. Este sistema es similar al de GSM, donde las colas de tos paquetes de información

GSM tienen al final un bit de control de potencia. Si es 0 se disminuye la potencia 1 dB, mientras que si es 1 se aumenta la potencia en 1dB.

La modulación utilizada en Bluetooth es GFSK (*Gaussian FreQuency Shift Keying*), donde un 1 binario se representa con una desviación positiva de frecuencia, mientras que un cero se expresa como una desviación negativa de la frecuencia. Las emisiones que se degeneran tanto dentro de la banda como fuera de ella, se miden con un transmisor de saltos de frecuencia saltando solo en una frecuencia. La precisión de la frecuencia central debe estar entre más o menos 75KHz de la frecuencia central.

3.3.3.2 Banda base

La banda base de Bluetooth provee canales de transmisión para voz y datos, y es capaz de soportar un enlace asíncrono de datos y hasta tres enlaces de voz síncronos (o un enlace soportando ambos). Los enlaces orientados a conexión síncronos (SCO) son típicamente empleados para transmisiones de voz. Esos enlaces son conexiones simétricas punto a punto que reservan ranuras de tiempo para garantizar la transmisión a tiempo. Al dispositivo esclavo siempre se le permitirá responder durante la ranura de tiempo inmediatamente seguido de una transmisión tipo SCO del maestro. Un dispositivo maestro puede soportar hasta tres enlaces SCO a uno o varios esclavos, pero un solo esclavo puede soportar sólo enlaces SCO para diferentes dispositivos maestros. Los paquetes SCO nunca son retransmitidos.

Los enlaces orientados a no conexión (ACL, *Asynchronous Connectionless*) son típicamente empleados para transmisión de datos. Las transmisiones sobre estos enlaces son establecidas en base por ranura (en ranuras no reservadas para enlaces SCO). Los enlaces ACL soportan transferencias punto-multipunto de datos asíncronos como sincronos. Después de una transmisión ACL del maestro,

sólo el dispositivo esclavo diseccionado puede responder durante la siguiente ranura de tiempo o si el dispositivo no está direccionado, los paquetes son considerados como mensajes difundidos (*broadcast*). La mayoría de los enlaces ACL incluyen retransmisión de paquetes. La máquina de estado de bandabase es controlada por el administrador de enlaces. Este microcódigo provee el control del enlace basado en hardware para configuración, seguridad y control de enlaces. Sus capacidades incluyen autentificación y servicios de seguridad, monitoreo de calidad de servicio y control del estado de bandabase.

3.4 HIPERLAN 2

HIPERLAN 2[11] es un estándar Radio LAN flexible diseñado para suministrar acceso de alta velocidad (hasta 54 Mbps en la capa física) a una variedad de redes incluyendo redes móviles 3G, redes ATM Y redes basadas en IP; y también para uso privado como un sistema de LAN inalámbrica. Las aplicaciones básicas incluyen datos, voz y video, con parámetros específicos de calidad de servicio (QoS).

Los sistemas HIPERLAN 2 pueden ser desarrollados en oficinas, salones de clases, casas, fábricas, áreas de exhibición y generalmente donde la transmisión por radio es una eficiente alternativa o una tecnología complementaria a la cableada. Por lo que respecta a las conexiones que se pueden establecer bajo esta especificación, en una red de HIPERLAN 2 los datos se transmiten en conexiones entre el MT (Terminal Móvil) y el AP (Punto de Acceso).

Hay dos tipos de conexiones, bidireccional punto a punto, y unidireccional punto a multipunto y siempre en sentido hacia el MT.

[11] MENDOZA Reynaldo, OSORIO Jessica. Tecnología Inalámbrica Radio LAN de Alto Rendimiento. Universidad Tecnológica de Bolívar. Monografía Minor de Comunicaciones y Redes. Facultad de Ingeniería Electrónica

Esta tecnología posee características como:

- ✓ Orientado a conexión.
- ✓ Soporte de QoS (*Quality of Service*): es necesaria para soportar tráfico desde aplicaciones como navegación Web hasta teleconferencia.
- ✓ Selección automática de frecuencia que evita problemas de ecos e interferencias.
- ✓ Soporte para terminales en movimiento mediante protocolos de paso de testigo (*handover*) entre distintos puntos de acceso.
- ✓ Bajo consumo energético.

Las especificaciones de HIPERLAN 2 son desarrolladas por ETSI BRAN, responsable de la estandarización con ETSI para redes de acceso por radio de banda ancha.

ETSI Proyecto BRAN también pone su atención en el funcionamiento de las especificaciones de prueba para el estándar central de HIPERLAN 2, hasta asegurar la interoperabilidad de los dispositivos y productos producidos por diferentes vendedores. Las especificaciones de prueba incluyen tanto radio y protocolos de prueba. En desarrollo de estas especificaciones de prueba, ETSI es soportado por el Foro Global HIPERLAN 2 (H2GF), un consorcio mundial de líderes en comunicaciones y de información tecnológica, que se han unido para asegurar la realización del están dar HIPERLAN 2 y promoverlo a nivel mundial.

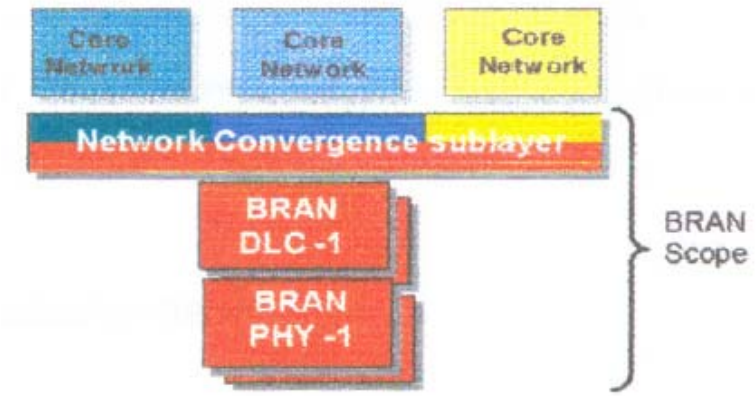
EP BRAN estuvo trabajando con IEEE-SA (Grupo de trabajo 802.11) Y con MMAC en Japón (Grupo de trabajo en Acceso de Alta Velocidad en Redes inalámbricas) para convenir los sistemas desarrollados por tres asociaciones en 5 GHz. Después de completar los reportes técnicos (TRs) que contienen los

Requerimientos (TRs 101 031) y los sistemas de visión general (TRs 101 683), la primera versión del estándar HIPERLAN 2 fue publicada en Abril del 2000. HIPERLAN 2 usa conexiones de multiplexación por división de tiempo, es orientado a conexión, ya sea bidireccional punto a punto o unidireccional punto – multipunto. Hay también un canal *broadcast* dedicado a través del cual el tráfico de AP alcanza todas las terminales.

3.4.1 ARQUITECTURA

HIPERLAN 2 puede ser usado con una variedad de redes. Esto es posible debido a la flexibilidad de la arquitectura aplicada por todos los estándares BRAN, en el cual define una capa física (PHY) y una capa de control de enlace de datos (DLC y un conjunto de especificaciones de las capas de convergencia (CL) en la parte superior de la capa DLC.

Figura 21. Arquitectura de capas HIPERLAN 2



3.4.2 CAPA FÍSICA HIPERLAN 2

La capa física traza un mapa de las MAC PDUs hasta PHY PDUs y adiciona señalización física como parámetros de sistema y el encabezamiento para la señal

de sincronización RF. La modulación de la señal esta basada en la Multicanalización por División Ortogonal De Frecuencia (OFDM) con varias sub-portadoras moduladas y envío de corrección de error que permiten poner varias configuraciones en el canal. Los principales parámetros tienen los siguientes valores:

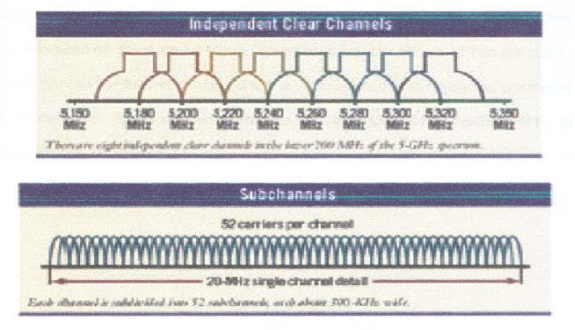
- ✓ Número de sub-portadoras usadas: 52, donde 48 sub-portadoras son usadas para datos y el resto para corrección de errores.
- ✓ Espacio de canal: 20 MHz.
- ✓ Rata de muestreo: 20 Muestras/s.
- ✓ Modulación de la sub-potadora: BPSK, QPSK, 16QAM y 64QAM.
- ✓ Taza de transmisión de datos: 6, 9, 12, 18, 27, 36, 54 Mbps.
- ✓ Interpolación: Bloque de interpelación con el tamaño de un símbolo OFDM (4 microsegundos).

3.4.2.1 Multicanalización OFDM

Es un esquema de canalización que ofrece ventajas sobre el espectro ensanchado en cuanto a disponibilidad del canal y tasa de datos. La disponibilidad del canal es significativa porque hay más canales independientes disponibles, así la red se vuelve más escalable.

La alta tasa de datos se logra combinando muchas sub-portadoras de baja velocidad para crear un canal de alta velocidad. Con OFDM se define un total de canales sin traslapamiento de 20 MHz; cada uno de estos canales se divide en 52 sub-portadoras, de aproximadamente 300 KHz de ancho.

Figura 22. Multicanalización OFDM



Las sub-portadoras se transmiten en paralelo, significando que se envían y se reciben simultáneamente. El dispositivo receptor procesa estas señales individuales, cada una representa una fracción de los datos totales que, juntos, crean la señal real. Con estas múltiples sub-portadoras abarcando cada canal, una enorme cantidad de información puede ser enviada de una vez.

3.4.3 Técnicas de modulación

Las técnicas usadas en HIPERLAN 2 son: BPSK, QPSK, 16 QAM. 64 QAM. BPSK, QPSK las cuales ya fueron explicadas anteriormente, pero cabe destacar que BPSK en HIPERLAN 2 es usado para codificar 125 Kbps de datos por canal, es decir, una velocidad de datos de 6 Mbps; y con QPSK se dobla la cantidad de datos codificados produciendo una velocidad de datos de 12 Mbps. Usando 16QAM se logra una tasa de datos de 24 Mbps (codificando 4 bits por hertz) y con 64QAM se obtiene una velocidad de datos de 54 Mbps, (produce 8 bits por ciclo o 10 bits por ciclo). OFDM provee flexibilidad considerando la realización de las diferentes alternativas de modulación.

Tabla 5. Técnicas de modulación

Mode	Modulation	PHY bit rate	Bytes/OFDM
1	BPSK	6 Mbps	3.0
2	BPSK	9 Mbps	4.5
3	QPSK	12 Mbps	6.0
4	QPSK	18 Mbps	9.0
5	16QAM	27 Mbps	13.5
6	16QAM	36 Mbps	18.0
7	64QAM	54 Mbps	27.0

3.4.3.1 QAM

En la modulación de amplitud en cuadratura (QAM) la información digital esta contenida, tanto en la amplitud como en la fase de la portadora transmitida; para alcanzar 54 Mbps, HIPERLAN 2 utiliza la modulación 64QAM para colocar la máxima cantidad de información posible (permisible por el estándar) en cada sub-portadora. A diferencia de PSK, la señal de salida de un modulador de QAM no es una señal de amplitud constante. En 16QAM los datos de entrada binaria se dividen en cuatro canales; y hay un cambio en la señal de salida (en fase, amplitud o ambos), para cada 4 bits de datos de entrada, en consecuencia se obtiene una razón de baudio cuatro veces menor que la razón de bits de entrada.

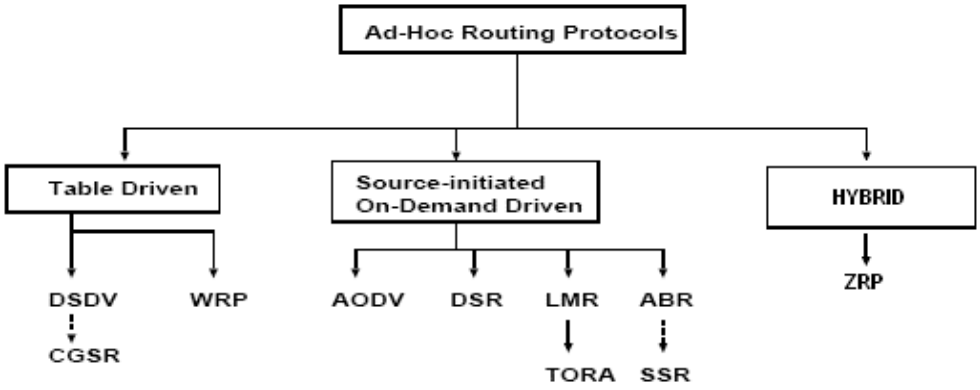
4. PROTOCOLOS DE ENRUTAMIENTO EN REDES AD HOC

Las técnicas utilizadas para enrutar paquetes de datos en las redes clásicas cableadas no pueden ser utilizadas en redes Ad-hoc. Los protocolos clásicos presuponen que la topología de la red es poco cambiante y, en consecuencia, están basados en complicados protocolos que tratan de conocer la mejor ruta hacia cualquier destino. En las redes Ad-hoc, debido a la movilidad de los nodos, es inviable esta alternativa. Además, el ancho de banda y la memoria son reducidas y se saturaría muy pronto la red debido al denso tráfico de control desplegado en este tipo de protocolos y al rápido crecimiento de las tablas de enrutamiento. Para solucionar este problema se han diseñado distintas técnicas para conseguir enrutar de manera efectiva. Los protocolos de enrutamiento usados en las redes Ad-hoc se pueden clasificar en tres grupos los cuales están presentados en la siguiente tabla, además de los descritos, existen otros protocolos que se estén implementando en base a simulaciones.

Tabla 6. Protocolos de enrutamiento

Basados en tablas de enrutamiento (Proactivo)	Basados en enrutamiento bajo demanda (Reactivo)	Híbrido
Destination Sequenced Distance Vector (DSDV) *Wireless Routing Protocol (WRP)* *Cluster Switch Gateway Routing (CSGR)*	*Signal Stability Routing (SSR)* ***Dynamic Source Routing (DSR)*** *Temporary Ordered Routing Algorithm (TORA)* ***Ad Hoc on Demand Distance Vector Routing (AODV)*** *Associativity Based Routing Protocol (ABR)*	*Zone Routing Protocol (ZRP)*

Figura 23. Protocolos de enrutamiento



4.1 Basados en tablas de enrutamiento (Proactivos):

Poseen las siguientes características:

- ✓ Tratan de mantener la información necesaria para el enrutamiento continuamente actualizada.
- ✓ Mantienen rutas entre cada par de host todo el tiempo, por el cual se consume mayor ancho de banda.
- ✓ Puede o no existir pequeños retardos en la determinación de ruta.
- ✓ Mantiene rutas que pueden no ser utilizadas.
- ✓ Cada nodo mantiene una o más tablas con los datos para enrutar hacia cualquier otro nodo de la red.
- ✓ Los cambios en la topología de la red propician el envío masivo de paquetes para mantener las tablas actualizadas.

Los siguientes protocolos se encuadran dentro de esta categoría:

- ✓ DSDV (*The Destination-Sequenced Distance-Vector Routing Protocol*).
- ✓ CGSR (*Clusterhead Gateway Switch Routing*).
- ✓ WRP (*The Wireless Routing Protocol*).

Los protocolos anteriores difieren en el número de tablas utilizadas y en la política de envío de paquetes para mantener las tablas actualizadas.

4.2 Basados en enrutamiento bajo demanda (Reactivos):

- ✓ En contraste con los protocolos basados en tablas, las rutas son creadas solo cuando se requieren (bajo demanda).
- ✓ El origen inicia el descubrimiento de ruta.
- ✓ Bajo *overhead* desde que las rutas sean determinadas bajo demanda.
- ✓ Existe un significante atraso en el momento de determinar la ruta.
- ✓ Emplea el método de *flooding* (búsqueda global)

Cuando un nodo requiere una ruta hacia un destino concreto se inicia un proceso de descubrimiento de ruta. Este proceso termina cuando se encuentra un camino hacia el destino o cuando se examinan todas las alternativas y ninguna lleva al destino final. Cuando la ruta es descubierta, es necesario mantenerla (mantenimiento de ruta) hasta que el destino se vuelva inalcanzable o la ruta deje de ser necesaria. Algunos ejemplos de estos protocolos son:

- ✓ AODV (*Ad hoc On-Demand Distance Vector Routing*)
- ✓ DSR (*Dynamic Source Routing*)
- ✓ TORA (*Temporary Ordered Routing Algorithm*)
- ✓ ABR (*Associative-Based Routing*)
- ✓ SSR (*Signal Stability Routing*)

4.3 Protocolos híbridos

Estos protocolos son los que resultan de la combinación de los protocolos proactivos y reactivos. Entre sus características están:

- ✓ El origen inicia el descubrimiento de ruta.
- ✓ Establece rutas bajo demanda.
- ✓ Mantenimiento de ruta restringido.
- ✓ Actualizan el estado de la red y mantiene rutas sin tener en cuenta si existe o no trafico de datos.
- ✓ Solo determina rutas hacia un destino, si hay algún dato que va a ser enviado hacia el.

Uno de estos protocolos es el ZRP, que se describirá mas adelante.

- DSDV (*Destination Sequence Distance Vector*): Este protocolo basado en tablas de enrutamiento fue diseñado por Charles E. Perkins y Pravin Bhagwat. Cada nodo de la red mantiene una tabla de enrutamiento que contiene todos los posibles destinos y el número de saltos que daría un paquete que viajará hacia el destino especificado. Cada entrada posee un número de secuencia

asignado por el nodo destino. Los números de secuencia permiten distinguir rutas antiguas de rutas modernas. Continuamente se deben enviar mensajes de actualización a través de la red para mantener la consistencia de las tablas. Para ayudar a minimizar la gran cantidad de tráfico que ocasionan estas actualizaciones, se utilizan dos tipos de paquetes. El primero recibe el nombre de *full dump*. Este paquete transporta toda la información disponible sobre el enrutamiento y puede requerir que su envío se divida en varias unidades más pequeñas. Cuando los cambios en la red son pequeños, es raro que se use este tipo de paquete. En cambio, hay un segundo tipo que solo contiene la información que ha variado desde el último *full dump*. Este paquete se llama *incremental*. Los nodos disponen de una tabla adicional donde guardan los datos recibidos por los paquetes *incremental*. Las nuevas rutas contienen la dirección de destino, el número de saltos requeridos para alcanzar al destino, el número de secuencia asociado al destino y un nuevo número que identifica todo el mensaje. En el caso de que haya dos rutas distintas hacia un destino, se usará la que contenga el número de secuencia más moderno. Además, si ambos números coincidieran, la ruta con menor número de saltos sería la que se usaría. En general, DSDV es un protocolo aceptable en escenarios en los que todos los nodos intervienen en las comunicaciones y en los lo que la movilidad es media.

- CGSR *(Clusterhead Gateway Switch Routing)*: Este protocolo difiere de otros protocolos en el tipo de direccionamiento y en el esquema empleado de organización de red. Bajo este protocolo, se agrupan nodos móviles en los *clusters* y cada uno de estos tiene una cabecera del *cluster*. Una cabecera del *cluster* puede controlar un grupo de hosts y realizando *clustering* proporciona *framework* para la separación de la red (entre *clusters*), canal de acceso, enrutamiento y también la asignación del ancho de banda. Usa DSDV como el algoritmo de la asignación de ruta subyacente y cada nodo mantiene una tabla de *cluster* y una de enrutamiento.

La desventaja de tener un esquema de cabecera de *cluster* es que los frecuentes los cambios de la cabecera pueden afectar el desempeño de los protocolos de enrutamiento desde que los nodos estén ocupados en la selección de cabecera de *cluster*, en lugar del paquete transmitido.

- WRP (*The Wireless Routing Protocol*): Creado por S. Murthy y J.J. García-Luna-Aceves. Protocolo basado en tablas cuyo objetivo principal es mantener información actualizada de todos los nodos de la red. Cada nodo es responsable de mantener cuatro tablas:

  - ✓ Tabla de distancias.
  - ✓ Tabla de enrutamiento.
  - ✓ Tabla de coste de ruta.
  - ✓ Tabla con la lista de mensajes retransmitidos (MRL).

  La MRL se utiliza para gestionar el envío de los paquetes de actualización de rutas. Cada entrada de la MRL contiene el número de secuencia que identifica el paquete de actualización de rutas, un contador de retransmisiones, un vector de asentimientos con una entrada por vecino y una lista de las unidades enviadas en el paquete de actualización (como se mencionó anteriormente, en ocasiones el paquete se dividía en unidades más pequeñas). La MRL almacena que unidades deben ser retransmitidas y qué vecinos deben asentir todavía los envíos. Los nodos se informan entre ellos de los cambios en las rutas a través de los paquetes de actualización. Estos paquetes son enviados solo entre vecinos y contienen los elementos a actualizar en las rutas. Los nodos envían estos paquetes cuando procesan las actualizaciones recibidas de otros vecinos o cuando ellos mismos detectan un cambio en el enlace con algún vecino. Los nodos mantienen el enlace con los vecinos activo, siempre y cuando reciban asentimientos u otros mensajes de ellos. Si un nodo no está

enviando mensajes, debería enviar un paquete *HELLO* cada cierto tiempo a sus vecinos, para que éstos no creyeran que el nodo se había vuelto inalcanzable. Por consiguiente, la omisión de mensajes por parte de un nodo ocasionará la ruptura de ese enlace. Cuando un nodo recibe un mensaje *HELLO* de un nuevo nodo, éste nodo será añadido a la tabla de enrutamiento y una copia de esta tabla será enviada al nuevo nodo.

- ZRP (*Zone Routing Protocol*): Creado por Zygmunt J. Haas y Marc R. Pearlman. Es un protocolo híbrido a medio camino entre los protocolos basados en tablas y los basados en enrutamiento bajo demanda. Es utilizado en una clase particular de redes Ad-Hoc llamadas RWNs (*Reconfigurable Wireless Networks*). Estas redes se caracterizan por tener gran cantidad de nodos, mucha movilidad y alto tráfico. Los protocolos anteriores no satisfacían las necesidades específicas de estas redes y los autores se decidieron a crear un nuevo protocolo. ZRP usa zonas similares a *clusters*, en las que los nodos que actúan de bordes se van seleccionando dinámicamente. Además, el radio de estas zonas se reajusta sobre la marcha según las condiciones de la red. Se pueden usar protocolos distintos para comunicarse dentro de las zonas y entre zonas distintas.

- AODV (*Ad hoc On-Demand Distance Vector*): Creado por Charles E. Perkins como evolución de su anterior protocolo (DSDV). Sostuvo la idea de mantener números de secuencia y tablas de enrutamiento pero añadió el concepto de enrutamiento bajo demanda, es decir, solo se guarda información de los nodos que intervengan en la transmisión de datos. La optimización primordial que se consiguió en relación a su anterior diseño fue el decremento del tiempo de proceso, disminución del gasto de memoria y reducción del tráfico de control por la red. Además AODV es muy cuidadoso con las rutas, manteniéndolas en caché mientras son necesarias e inhabilitándolas cuando su información no es útil.

- DSR (*The Dynamic Source Routing*): Creado por David B. Johnson y Josh Broch. Protocolo basado en el concepto de enrutamiento en origen. Los nodos mantienen cachés, cuyas entradas incluyen el destino y la lista de nodos para llegar a él. Las entradas de esta tabla son actualizadas según se aprendan rutas nuevas. El protocolo consta de dos mecanismos principales: descubrimiento de ruta y mantenimiento de ruta.

- TORA (Temporally Ordered Routing Algorithm): Creado por M. Scott Corson y Vincent Park. Es un protocolo de tipo *Link Reversal Routing*, que se basa en mantener un grafo dirigido y sin ciclos para llegar al destino. El objetivo es minimizar la carga sobre la red. La diferencia con otros protocolos es la imposibilidad de estimar constantemente la distancia hacia el destino o de mantener siempre la ruta más corta. Sin embargo, tiene la ventaja de que es un protocolo muy eficiente pues no satura en exceso de tráfico la red.

- ABR (*Associativity-Based Routing*): Este protocolo es libre de lazos, bloqueo, y duplicación de paquete, y define una nuevo enrutamiento métrico para las redes móviles Ad hoc. Este enrutamiento métrico es conocido como estabilidad de asociación. En ABR, una ruta se selecciona basándose en el grado de estabilidad de la asociación de nodos móviles. Periódicamente cada nodo genera una señal para dar a conocer su existencia. Cuando esta señal es recibida por nodos vecinos, permite que las tablas de asociación sean actualizadas. Para cada señal recibida, los *tick* de asociabilidad del nodo actual con respecto a la señal de nodo, se incrementa. La estabilidad de la asociación es definida por estabilidad de conexión de un nodo con respecto a otro nodo sobre tiempo y espacio. Un grado alto de estabilidad de asociación puede indicar un estado bajo de movilidad del nodo, mientras que un grado bajo puede indicar un estado alto de movilidad del nodo. Se restablece el *tick* de asociabilidad cuando los vecinos de un nodo o el propio nodo se mueven fuera de su proximidad. Un objetivo fundamental de ABR es deducir largas rutas

para las redes móviles *Ad hoc*. Este protocolo posee tres fases que son: el descubrimiento de ruta, la re-construcción de ruta (RRC), y la supresión de ruta.

- SSR (*Signal Stability Routing*): Este es otro protocolo bajo demanda y es descendiente de ABR. SSR selecciona rutas basado en la señal más fuerte entre los nodos y en la estabilidad de la localización de un nodo. Este criterio de selección de ruta tiene el efecto de escoger rutas que tengan una comunicación más fuerte. SSR puede ser dividido en dos protocolos cooperativos: el protocolo de asignación de ruta dinámico (DRP) y el protocolo de asignación de ruta estático (SRP).

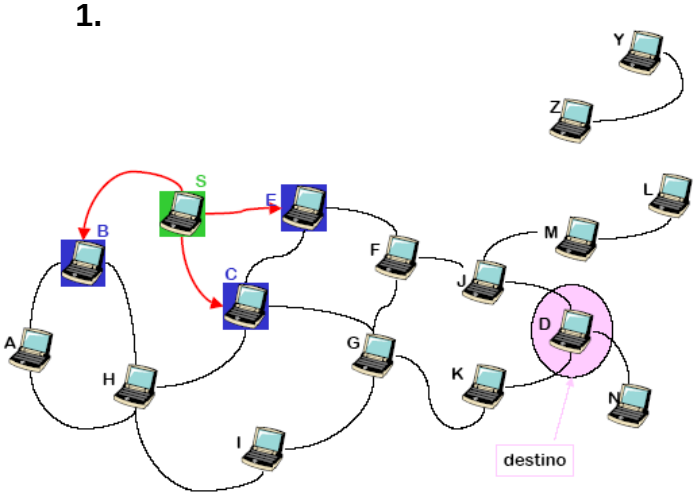
  El DRP es responsable del mantenimiento de la tabla de señal estable (SST) y la tabla de enrutamiento (RT). El SST registra la señal más fuerte de nodos vecinos, que son obtenidos por señales periódicas de la capa de enlace de cada nodo vecino. La señal más fuerte puede registrarse como un canal fuerte o débil. Todas las transmisiones se reciben por el DRP. Después de actualizar todas las entradas de las tablas adecuadas, el DRP le pasa el paquete recibido al SRP.

  El SRP procesa los paquetes de la siguiente forma: pasa el paquete a la pila si es el receptor indicado o busca el destino en la tabla de enrutamiento, y por último envía el paquete si lo es. Si ninguna entrada se encuentra para el destino en la tabla de enrutamiento, se comienza un proceso de descubrimiento de ruta.

Los protocolos AODV y DSR que se describirán a continuación se basan en el *FLOODING*. El *flooding* para entrega de datos es una forma de transmisión que consta de las siguientes características.

- ✓ Los paquetes de control se utilizan para descubrir las rutas.
- ✓ Las rutas establecidas se utilizan posteriormente para enviar los paquetes de datos.
- ✓ La sobrecarga que se debe al flooding de los paquetes de control se amortiza gracias a los paquetes de los datos transmitidos entre los floodings consecutivos de paquetes del control.

1.

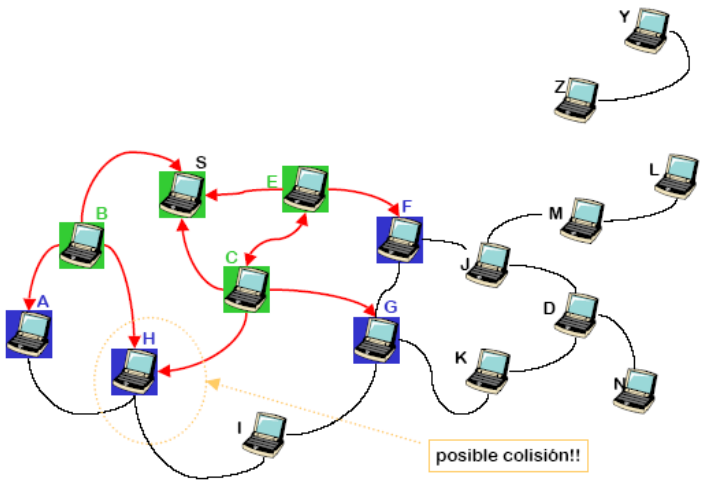


 Nodo que acaba de enviar una trama.

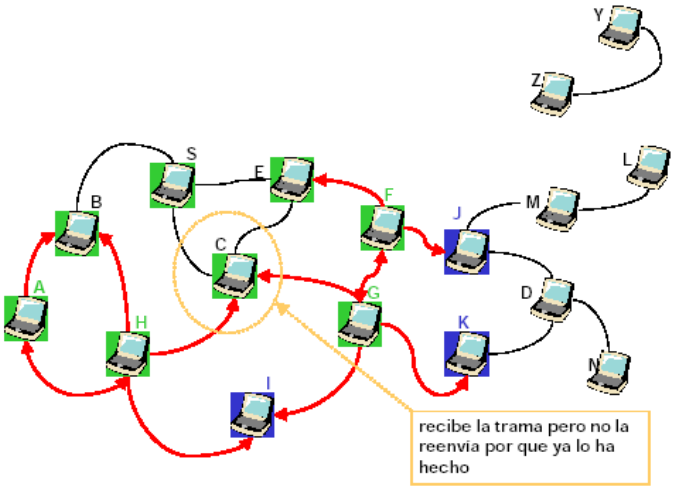
 Nodo que acaba de recibir una trama.

 Envio *broadcast* de una trama

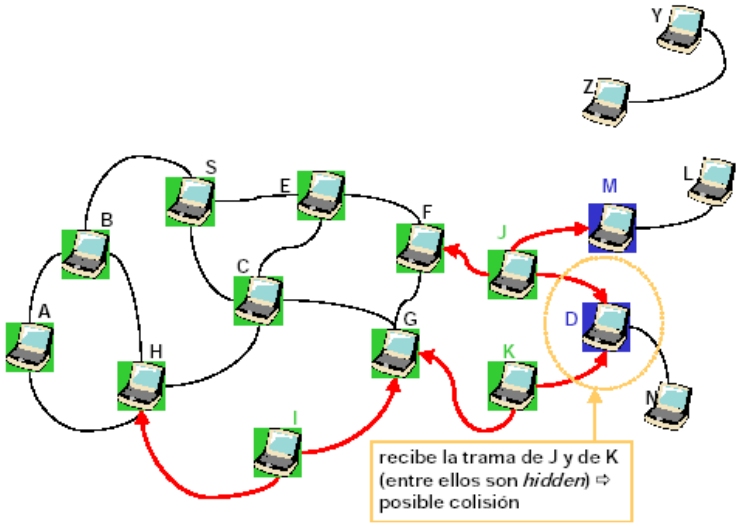
2



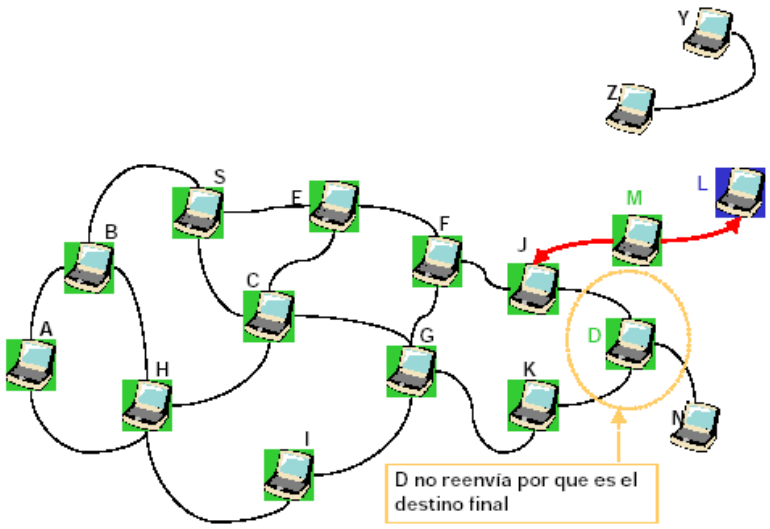
3.


Y
Z
S
E
F
L
M
B
J
C
D
A
G
K
H
N
I
recibe la trama pero no la reenvia por que ya lo ha hecho

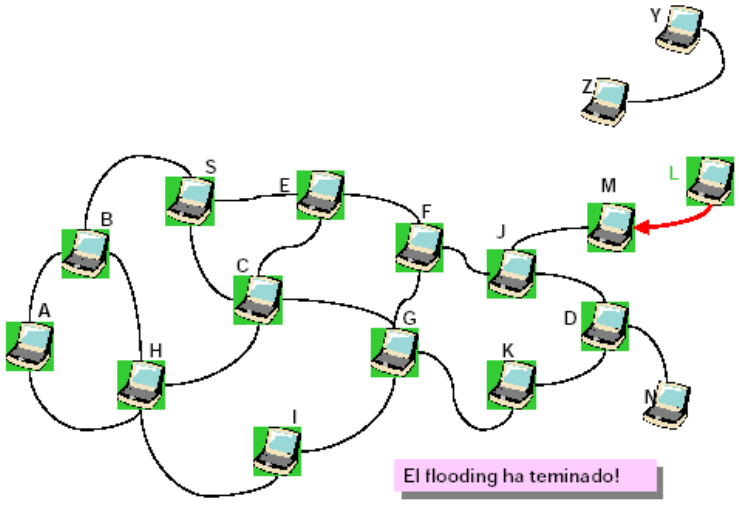
4.


Y
Z
S
E
M
L
F
B
J
C
A
G
D
K
H
N
I
recibe la trama de J y de K (entre ellos son *hidden*) ⇨ posible colisión

5.


Y
Z
S
E
F
L
M
B
J
C
A
G
D
H
K
N
I
D no reenvía por que es el destino final

6.


Y
Z
S
E
L
M
B
F
J
C
A
G
D
H
K
N
I
El flooding ha teminado!

Ventajas:

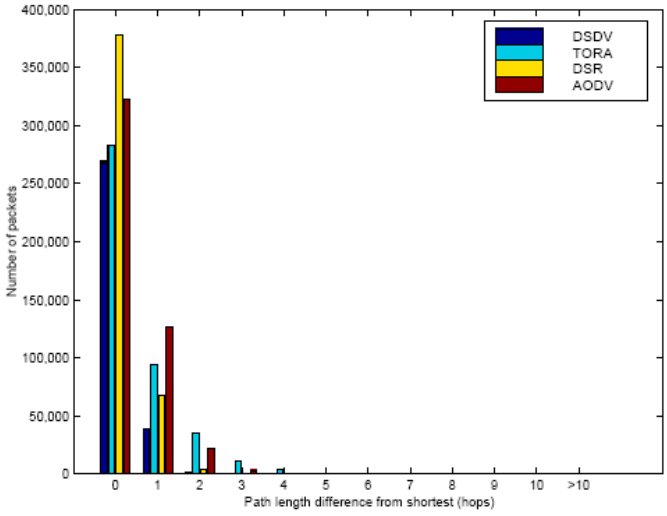
- ✓ Sencillo.
- ✓ Es más eficiente si la tasa de envío es baja, entonces el *overhead* de los procesos de búsqueda y mantenimiento de rutas explicitas resulta ser más alto.
- ✓ Potencialmente la entrega de los datos es más fiable, por que se pueden utilizar múltiples rutas.

Desventajas:

- ✓ *Overhead* potencialmente muy alto.
- ✓ Potencialmente la entrega de los datos es menos fiable a causa del uso de difusiones.

A continuación se describen las características de los principales protocolos de enrutamiento para redes Ad hoc mencionados anteriormente, teniendo en cuenta que en nuestra investigación, vamos a profundizar en los dos protocolos mas importantes y los mas eficientes (AODV y DSR), que actualmente están siendo utilizados, y que además son objeto de estudios para optimizar su funcionamiento en este tipo de redes.

Figura 24. Comparación de protocolos



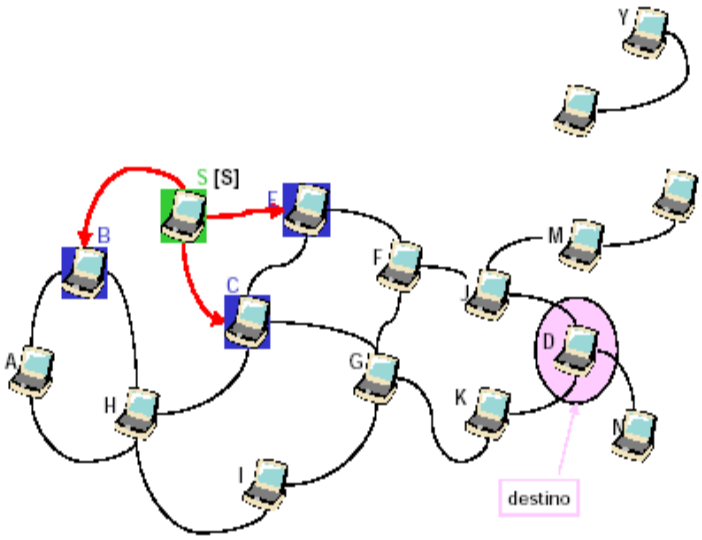
4.4 Protocolo DSR

4.4.1 Descubrimiento de rutas

Cuando un nodo quiere enviar un paquete a un destino, primero consulta su caché para determinar si dispone de una ruta hacia el destino. Si tiene una ruta válida, la usará para enviar el paquete. Sin embargo, si el nodo no dispone de dicha ruta iniciará un descubrimiento de ruta enviando un paquete RREQ (*Route Request*). Este paquete contiene la dirección de destino buscada, la dirección del nodo que origina el envío y un identificador único. Cada nodo que reciba el paquete verificará si posee una ruta hacia el destino. Si no la tiene, añadirá su propia dirección en el registro de rutas del paquete y después reenviará el paquete a través de todos sus enlaces para limitar la propagación excesiva de descubrimientos de ruta, un nodo solo reenviará este mensaje si la misma petición no fue recibida con anterioridad. Cuando un RREQ alcanza su destino final, este nodo genera una respuesta de ruta (RREP). También podría contestar con un RREP un nodo intermedio que tuviera en su caché una ruta válida hacia el destino del RREQ. Si el nodo que genera la respuesta es el destino, colocará el registro de rutas contenido en el RREQ dentro del RREP. Si es un nodo intermedio el que responde, extraerá de su caché la ruta para llegar al destino, que unida al registro de rutas contenido en el RREQ compondrá la ruta a introducir en el RREP.

Un nodo S desea enviar un paquete al nodo D, pero no conoce una ruta hacia D y por lo tanto inicia un descubrimiento de la ruta (*route discovery*). El nodo fuente S hace un flooding de Route Request (RREQ). Cada nodo añade su propio identificador cuando reenvía un RREQ.

1.

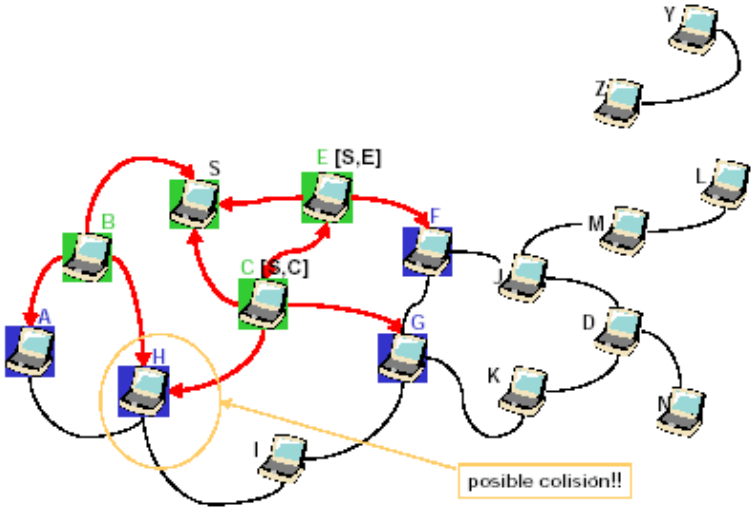


Nodo que acaba de enviar un RREQ.

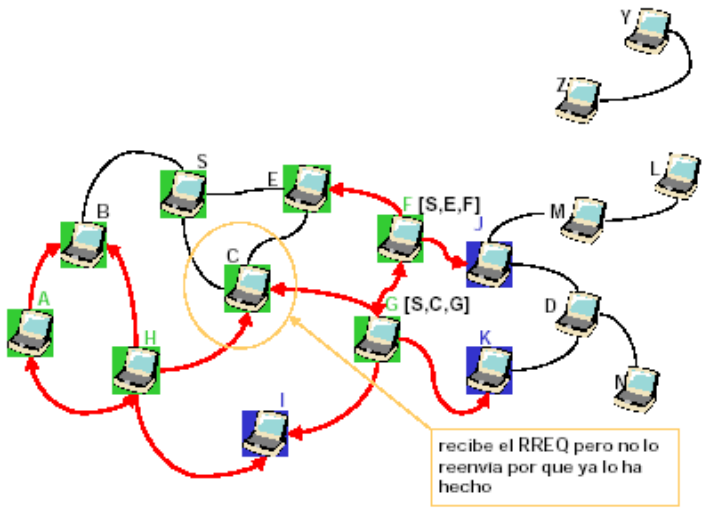
Nodo que acaban de recibir un RREQ.

[X,Y]: Lista de IDs añadidos al RREQ

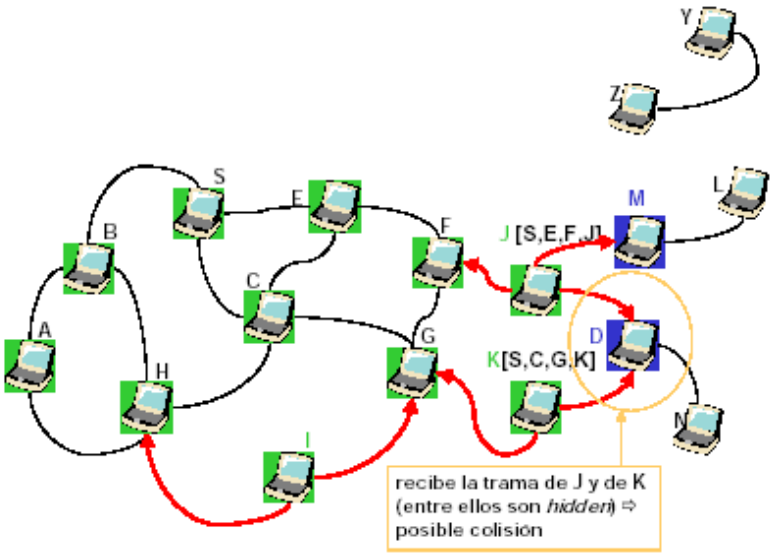
2.



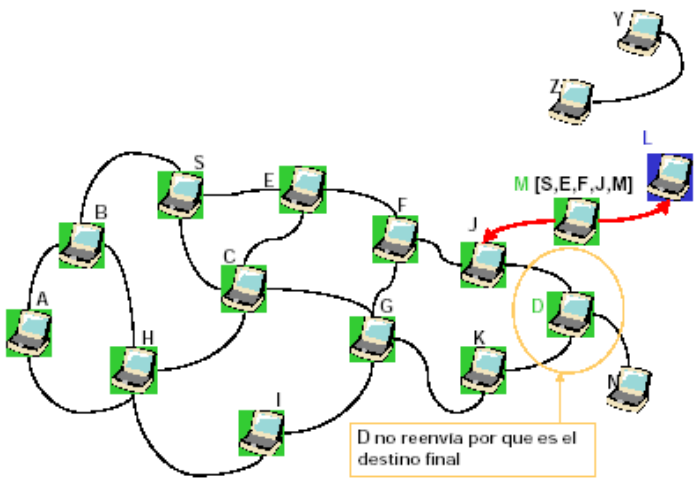
3.


Y
Z
S
E
F [S,E,F]
L
M
B
J
C
A
G [S,C,G]
D
H
K
N
I
recibe el RREQ pero no lo reenvia por que ya lo ha hecho

4.


Y
Z
S
E
M
L
B
F
J [S,E,F,J]
C
A
G
D
K[S,C,G,K]
H
I
recibe la trama de J y de K (entre ellos son *hidden*) ⇨ posible colisión

5.



4.4.2 Mantenimiento de ruta

El mantenimiento de rutas se completa con el uso de paquetes de error en ruta (RERR) y asentimientos. Los paquetes de error en ruta son iniciados por un nodo cuando encuentra un problema en la transmisión con algún enlace. Cuando un RERR es recibido, el nodo que provocó el error es eliminado del caché de rutas. También serán borradas todas las rutas en las que intervenga el enlace roto. Además de los mensajes de error, se usan asentimientos para verificar que las operaciones con los enlaces son correctas.

- ✓ Si un nodo detecta una falla en un enlace, a lo largo de la ruta, un paquete de error de ruta es enviado al nodo S.
- ✓ Los nodos intermedios que reciben el RERR, eliminan esas rutas inválidas hacia D.
- ✓ El nodo S debe iniciar un nuevo descubrimiento de ruta si desea comunicarse con D.

4.4.3 Ventajas en DSR

- ✓ Se gestionan solo las rutas entre nodos que quieren comunicarse, por lo tanto se reduce la carga para mantener varias rutas.
- ✓ El uso de la caché puede reducir la carga de futuros procesos de descubrimiento de ruta.
- ✓ Un solo proceso de RR puede producir variar rutas hacia el destino gracias a las respuestas de las caches de los nodos intermedios.

4.4.4 Desventajas en DSR

- ✓ El tamaño de la cabecera crece al crecer de la ruta debido al uso del *source routing* (enrutamiento en origen).
- ✓ El *flooding* de las peticiones de ruta puede potencialmente alcanzar todos los nodos en la red.
- ✓ Hay que evitar las colisiones producidas por la retransmisión de los RREQ.
- ✓ Se insertan retardos aleatorios antes de enviar el RREQ.
- ✓ Problema de tormenta de *Route Reply.*
- ✓ Se puede evitar forzando un nodo a no enviar un RREP si escucha otro RREP con una ruta más corta.

4.5 Protocolo AODV

Una de las características que define a AODV es el uso de tablas de enrutamiento en cada nodo para evitar transportar rutas en los paquetes.

Cada destino de la tabla de enrutamiento lleva asociado un número de secuencia y un temporizador o *lifetime*. Este número permite distinguir entre información nueva e información antigua, de tal manera, que se evita la formación de ciclos y la transmisión de rutas antiguas o caducadas por la red. La función del temporizador es evitar usar enlaces de los que no se conoce su estado desde hace mucho tiempo.

Tabla 7. Ejemplo de una tabla de enrutamiento.

Destino	Siguiente salto	Nº Secuencia	Nº Saltos	Tiempo de vida	Última modificación

AODV no mantiene rutas para cada nodo de la red. Estas rutas son descubiertas según se vayan necesitando. AODV es capaz de proveer de transmisión *unicast*, *multicast* y *broadcast*. La transmisión *unicast* consiste en enviar datos de un nodo a otro, la transmisión *multicast* consiste en enviar información de un nodo a un grupo de nodos y la transmisión *broadcast* consiste en enviar datos de un nodo al resto de nodos de la red. Los descubrimientos de rutas son siempre bajo demanda y siguen un ciclo de petición - respuesta de ruta. Las peticiones son enviadas usando un paquete especial denominado RREQ (*Route Request*). A su vez, las

respuestas son enviadas en un paquete denominado RREP (*Route Reply*). A continuación se resume la secuencia de pasos para descubrir una ruta:

- ✓ Cuando un nodo desea conocer una ruta hacia un nodo destino, envía por *broadcast* un RREQ.
- ✓ Cualquier nodo que conozca una ruta hacia el destino solicitado (incluido el propio destino) puede contestar enviando un RREP.
- ✓ Esta información viaja de vuelta hasta el nodo que originó el RREQ y sirve para actualizar las rutas de los nodos que lo necesiten.
- ✓ La información recibida por el nodo destino del RREP se almacena en su tabla de enrutamiento.

Ahora, el nodo ya podría enrutar su paquete de datos, pues ya conoce un camino hacia su destino.

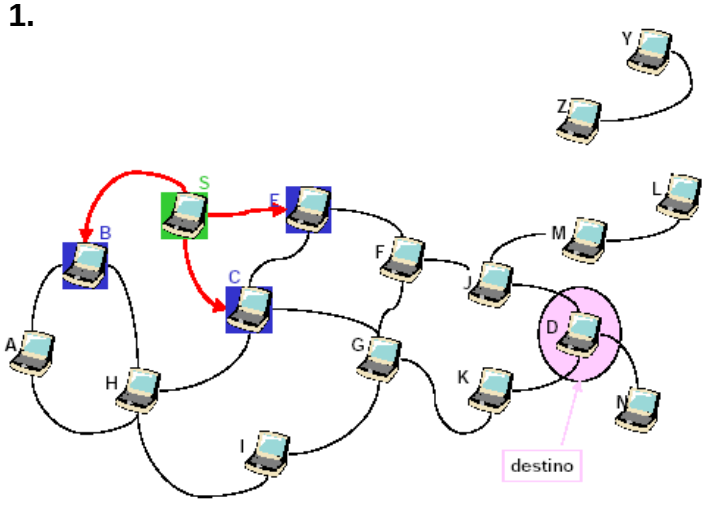
4.5.1 Descubrimiento de rutas

Cuando un nodo desea enviar datos a otro, primero chequea si tiene alguna entrada en su caché de rutas para dicho destino. Si tiene alguna entrada activa, encamina los datos por el vecino que le indica la tabla. Sin embargo, si el origen no dispone de una entrada activa, bien porque es la primera vez que se va a comunicar con él, o bien porque el plazo para esa destino ha expirado (al comprobar el campo *lifetime* y la fecha de última modificación), se inicia un descubrimiento de ruta. Para ello se debe crear un paquete RREQ que contiene información relativa al nodo destino e información propia. Cada paquete RREQ es identificado unívocamente con un identificador propio, unido al originador del mensaje. Este identificador se incrementa cada vez que se genere un nuevo RREQ y lo utilizan los nodos intermedios, para saber si deben retransmitir el paquete o, por el contrario, descartarlo porque ya lo retransmitieron con

anterioridad. Dichos nodos, aún no siendo los destinatarios del RREQ, si mantienen una entrada para ese destino en su tabla de enrutamiento, contestarían al origen para evitar la propagación innecesaria de RREQ a través de la red. Incluso teniendo alguna entrada activa, es necesario que se cumpla que dicha ruta es más moderna que la última ruta recibida por el originador del RREQ. Aquí es donde entran en juego los números de secuencia. Cuando un nodo reenvía un RREQ, añade una ruta inversa en su tabla, que apunta al origen del RREQ (supone enlaces simétricos). Si este paquete llega al destinatario, éste devolverá un RREP al origen, a través del camino inverso por el que le llegó la petición. Por ejemplo, supongamos que el nodo A quiere descubrir una ruta hacia el nodo D:

Para iniciar un descubrimiento de ruta el nodo S transmite un RREQ enviando un único paquete en modo *broadcast*, el cuál es recibido por todos los nodos que están en el rango de transmisión de S.

1.



Nodo que acaba de enviar una trama.

Nodo que acaba de recibir una trama.

Envio *broadcast* de una trama.

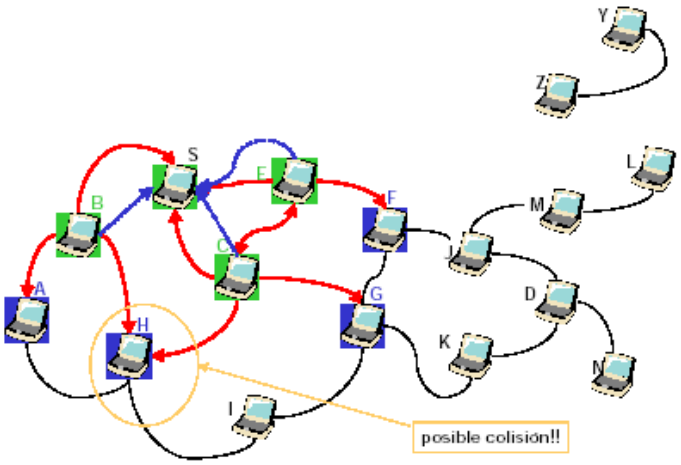
Cada *Route Request* incluye el origen y el destino del descubrimiento de ruta, además del identificador único (ID) otorgado por el iniciador de la petición. Cada *Route Request* contiene, además, datos del origen para que los nodos

Saltos: 0
Origen: S
ID: 1
Destino: D

intermedios puedan actualizar sus tablas con esta información. Por último también se añade un campo con información del número de saltos que da el paquete.

Cuando otro nodo reciba esta petición, si él fuera el destinatario del descubrimiento de ruta, devolvería al origen un RREP. Cuando el origen recibiera esta *Route Reply*, almacenaría en su caché este camino para los futuros envíos al mismo destino. Los nodos que reciben el *Route Request*, comprueban que no le han llegado con anterioridad otra petición con mismo origen y mismo identificador. Después de esto, verifican que no son los destinatarios del RREQ, y reenvía por *broadcast* la petición incrementando en una unidad el número de saltos.

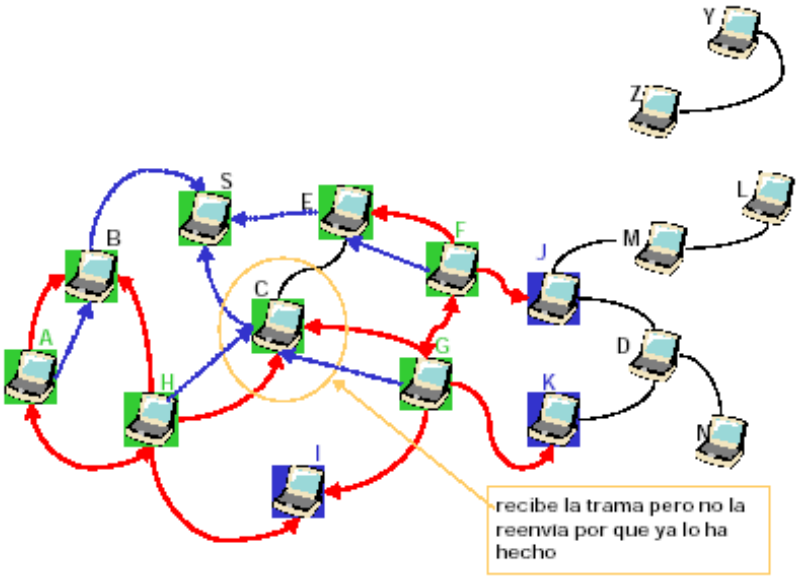
2.



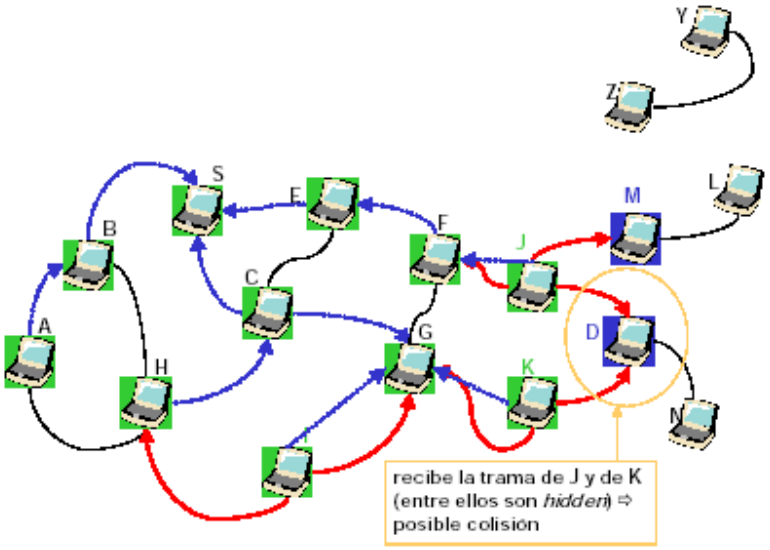
Cuando un nodo retransmite un *Route Request*, activa también una ruta inversa que apunta a la fuente, puesto que, AODV supone canales bidireccionales.

Este envío de broadcast lo realizan cada uno de los nodos hasta que el paquete llegue a su destino.

3.

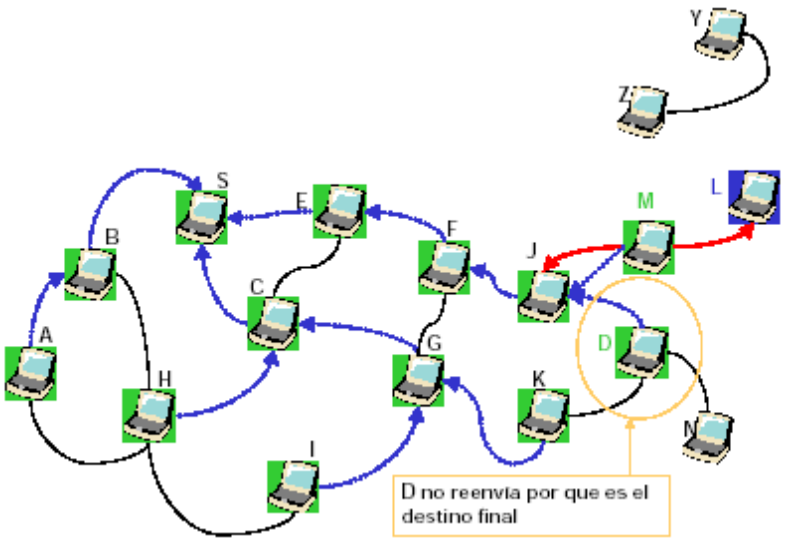


4.



Por último, la petición llega al nodo D que es el destino. Este último, mandará el *Route Reply* correspondiente al nodo S con la ruta obtenida por *Route Request*. Para enviar este paquete al nodo A, mirará en su caché para obtener algún camino o iniciará otro *Route Discovery* si fuera necesario.

5.



4.5.2 Mantenimiento de rutas

Cuando se establece una ruta entre dos nodos, la ruta se considera válida durante un periodo de tiempo. Esto es debido a que los nodos son móviles y un camino que antes era óptimo, pasado un tiempo puede que ni siquiera sea válido. Para defenderse de estas situaciones, AODV utiliza el mantenimiento de rutas. Si el nodo origen de un envío se mueve (y altera la topología de la red), él debe reiniciar un nuevo descubrimiento de ruta hacia el destino. Sin embargo, si ha sido el nodo destino de los datos el que se ha movido o algún nodo intermedio, y hay algún mensaje dirigido hacia él, un mensaje especial de error en ruta (*RERR*) será enviado al nodo que originó el envío, por el nodo que advierta el cambio en la topología de la red.

Es importante resaltar que no todos los cambios de los nodos ocasionan operaciones en el protocolo, recordemos que AODV encamina bajo demanda. Todos los nodos por los que atraviese este paquete (RERR), cancelarán las rutas que pasaran por el nodo que se ha vuelto inaccesible. En el momento que el

RERR llegue a su destino, éste puede decidir dar por terminado el envío o iniciar un nuevo RREQ si aún necesitase establecer la comunicación. Es preciso mantener información actualizada de quiénes son los vecinos de cada nodo cada cierto tiempo. Cada vez que un nodo recibe un paquete de algún vecino, la entrada para ese vecino en la tabla de rutas se refresca, pues se sabe con seguridad que sigue en su lugar.

Si no hubiera entrada todavía para el vecino, se crearía una nueva en la tabla de enrutamiento. Además, cada cierto intervalo de tiempo, se mandan paquetes *HELLO* a los vecinos para informarles que el propio nodo sigue activo. Esta información es usada por los vecinos para actualizar los temporizadores asociados a dicho nodo o en su defecto, para deshabilitar las entradas que se encaminen por el nodo que no responde.

4.5.3 AODV en la capa de red

La funcionalidad más importante que debe ofrecer el nivel de red es garantizar que se puedan enviar datos a cualquier nodo de la red, aún en el caso de que origen y destino estén a una distancia mucho mayor que la del alcance de sus radios. Esto se consigue haciendo que todos los *hosts* de la red funcionen como enrutadores o routers, es decir, sean capaces de reenviar los datos que reciben al nodo correcto para que el paquete llegue a su destino. Esto es en definitiva de lo que se encarga AODV, de ejecutar los protocolos apropiados y mantener las estructuras de datos necesarias para que todo esto sea posible.

Es necesario un despliegue de protocolos y de paquetes para conseguir un funcionamiento adecuado. Cada uno de estos paquetes tiene su función (iniciar petición de ruta, paquete con respuesta a una ruta, etc.).

4.5.4 Estructuras de datos

En este nivel es necesario disponer de las siguientes estructuras de datos:

4.5.4.1 Tabla de Enrutamiento

Tabla donde se almacenan las rutas conocidas. Cada entrada incluye el destino, número de secuencia asociado a la ruta, nodo por el que se encaminan los paquetes hacia ese *host*, número de saltos hasta llegar al destino, el instante de la última modificación y el campo *lifetime*. Estos dos últimos campos son los que se utilizarán para distinguir las rutas válidas de las inválidas.

4.5.4.2 Tabla de RREQ's recibidas

Tabla que dispone de dos campos: Dirección de un nodo e identificador de RREQ. Cada vez que se reciba un RREQ, se incluirá una nueva entrada en la tabla con la dirección del nodo que originó el RREQ y el identificador de dicho RREQ. Esta entrada se consultará cada vez que se reciban RREQ's. En el caso de que coincidieran los campos correspondientes de la petición con los almacenados en la tabla, se descartaría la petición de descubrimiento de ruta, pues ya se trató con anterioridad.

Cuando un nodo origina un RREQ, si al cabo de un tiempo no recibe RREP, podría retransmitir el envío por si se hubiera perdido el paquete anterior. El problema es que podría ocurrir que determinados nodos que si recibieron el paquete antes, lo descartaran y nunca llegara al destino final. Para solucionar este problema podría haber dos soluciones:

- ✓ Añadir temporizadores a las rutas de la tabla que almacena los paquetes RREQ recibidos. De esta manera y ajustando correctamente los tiempos de caducidad, se podrían volver a aceptar antiguos RREQ's con el objetivo de reenviarlos ante posibles pérdidas.

- ✓ Que cada vez que el origen retransmitiera un RREQ incrementara su identificador de RREQ.

4.5.5 Formato de paquetes

4.5.5.1 Paquete de datos

Tabla 8. Formato de paquete de datos

Type	*Hop Sourc.*	*Hop Destin.*	*Destin. Addr.*	*Origin. Addr.*	*Size*	*Data*
0	1	2	3	4	5	...

0 ***Type*****:** Identificador de paquete (0).

1 ***Hop Source****:* Nodo origen del siguiente salto.

2 ***Hop Destination****:* Nodo destino del siguiente salto.

3 ***Destination Address****:* Destino final del paquete de datos.

4 ***Originator Address***: Origen inicial del paquete de datos.

5 ***Size***: Tamaño en bytes de los datos.

6 ***Data***: Datos.

4.5.5.2 Paquete de descubrimiento de ruta (RREQ)

Tabla 9. Formato del paquete de descubrimiento de ruta (RREQ)

Type	*Hop Src.*	*Hop Dst.*	*Hop Count*	*RREQ ID*	*Dst.Addr.*	*Dst.Seq.Num.*	*Org.Addr.*	*Org.Seq.Num.*
0	1	2	3	4	5	6	7	8

0 ***Type***: Identificador de paquete (1).

1 ***Hop Source:*** Nodo origen del siguiente salto.

2 ***Hop Destination:*** Nodo destino del siguiente salto.

3 ***Hop Count***: Número de nodos que hay desde el origen del paquete hasta el nodo que recibe la petición de ruta.

4 ***RREQ ID:*** Número de secuencia único que identifica unívocamente una petición de ruta cuando se combina con el campo *Originator Address*.

5 ***Destination Address***: La dirección de destino del nodo hacia el que buscamos una ruta.

6 ***Destination Sequence Number***: El último número de secuencia recibido por el origen, contenido en una ruta hacia el destino.

7 ***Originator Address***: Dirección del nodo que originó la petición de ruta.

8 ***Originator Sequence Number***: El número de secuencia actual que mantiene el origen del RREQ para rutas hacia él.

4.5.5.3 Paquete de respuesta de ruta (RREP)

Tabla 10. Formato del paquete de respuesta de ruta (RREP)

Type	*Hop Source*	*Hop Destin.*	*Hop Count*	*Destin. Addr.*	*Destin.Seq.Num.*	*Originat. Addr.*	*Lifetime*
0	1	2	3	4	5	6	7

0 ***Type****:* Identificador de paquete (2).

1 ***Hop Source***: Nodo origen del siguiente salto.

2 ***Hop Destination***: Nodo destino del siguiente salto.

3 ***Hop Count***: Número de nodos que hay desde el origen del paquete hasta el nodo que recibe la petición de ruta.

4 ***Destination Address****:* La dirección del nodo del que se quería conocer una ruta, es decir, la dirección del nodo destino del RREQ.

5 ***Destination Sequence Number***: El número de secuencia asociado con esta ruta.

6 ***Originator Address***: La dirección del nodo que originó el descubrimiento de ruta y hacia el cuál se dirige este paquete.

7 ***Lifetime***: Tiempo de vida del paquete. En cada salto se decrementa y si llega a 0 no se retransmitirá.

4.5.5.4 Paquete de error en ruta (RERR)

Tabla 11. Formato del paquete de error en ruta (RERR)

Type	*Hop Source*	*Hop Destin.*	*Unreachable Destin. Addr.*	*Unreachable Destin.Seq.Num.*	*Destin. Addr.*
0	1	2	3	4	5

0 ***Type:*** Identificador de paquete (3).

1 ***Hop Source***: Nodo origen del siguiente salto.

2 ***Hop Destination***: Nodo destino del siguiente salto.

3 ***Unreachable Destination Address:*** Dirección del nodo inalcanzable.

4 ***Unreachable Destination Sequence Number:*** Último número de secuencia asociado al nodo inalcanzable.

5 ***Destination Address***: Dirección del nodo destino del paquete RERR.

Se han descartado dos campos de la especificación original: El primero destinado a contar el número de nodos inalcanzables y el segundo para futuras ampliaciones. En nuestro caso, el paquete solo advierte del error en ruta de un solo nodo.

Por último se debe destacar que en todos los paquetes se han añadido dos campos extras: *Hop Source* y *Hop Destination*. El primer campo se usa para que los nodos que reciban cualquier paquete sepan qué vecino se lo mandó. El segundo campo es para dirigir el paquete a un nodo concreto, de tal manera que

los nodos que lo reciban pero no sean los destinatarios del paquete lo puedan descartar.

A manera de conclusión podemos decir que una de las partes indispensables para que AODV funcione correctamente es la necesidad de descubrir rutas o caminos hacia otros nodos. Un nodo conoce un camino hacia un determinado destino si dispone de una entrada válida hacia dicho nodo en su tabla de enrutamiento. Cuando no existe tal entrada se desencadena todo un proceso que terminará con la inclusión de un nuevo camino hacia el destino buscado. Este proceso es el descubrimiento de ruta o *Route Request (*RREQ*)*.

Además como ya sabemos las redes *Ad-hoc* son un tipo de redes en las que los *hosts* son móviles. Esto conlleva que las rutas que hace un tiempo eran utilizables, en otro momento no lo sean. El agotamiento de las baterías es otra razón para el cambio de topologías. Por esto es necesario disponer de algún mecanismo para asegurar que las rutas conocidas sigan siendo válidas. De esto es lo que se encarga el mantenimiento de rutas o *Route Maintenance*.

Cada entrada de la tabla de rutas tiene una fecha de última modificación, que junto con el campo *lifetime* definen el intervalo de vida de ese camino. Cada vez que se consulta una entrada, si el instante actual ha sobrepasado el instante de su última modificación, más el número de segundos que indique su *lifetime*, dicha entrada se marcará como inválida y se dejará de usar.

Por el contrario, hay ocasiones en las que se puede refrescar la fecha de última modificación porque podemos deducir que el nodo correspondiente sigue en su lugar. Estas situaciones son cuando recibimos algún paquete *broadcast* de dicho nodo, cuando le enviamos datos o cuando recibimos un paquete *HELLO*.

Un paquete *HELLO* es un paquete especial del protocolo que sirve para recordar a los vecinos que el nodo emisor del *HELLO* sigue en su sitio. Es decir, se utilizará

para que los vecinos refresquen sus entradas para el *host* que inicia el envío. Cada cierto intervalo fijo definido por una constante, todo nodo debe enviar un paquete de este tipo a sus vecinos. Este paquete no es más que un paquete RREP destinado a todos (*broadcast*) con el campo *lifetime* a 1. Esto es con la finalidad de que dicho RREP no sea retransmitido.

Hay determinadas situaciones insalvables desde el punto de vista de la comunicación. Cuando se pretende enviar datos a un nodo que es inalcanzable, el protocolo retransmite al nodo origen un mensaje de error en ruta para que éste se de cuenta de que dicho nodo es inaccesible.

5. CONCLUSIONES

El auge de las redes móviles Ad hoc y sus especiales características han provocado la aparición de gran cantidad de grupos de investigación para afrontar el desarrollo de los tradicionales servicios que podemos usar en Internet. En esta monografía se han analizado tres aspectos principales de redes móviles Ad hoc, tales como: definición y características, protocolos de enrutamiento y la evolución que han tenido estas redes, reflejándola en algunas aplicaciones.

En base a esta investigación podemos decir que las redes ad hoc son redes que ofrecen muchas ventajas con respecto a las redes cableadas tradicionales. Son redes que se forman de manera temporal y cuando se necesitan. Los protocolos empleados en las redes del tipo cableadas, o los protocolos utilizados en redes con infraestructura, son imposibles de utilizar en estas redes Ad hoc debido al alto ambiente dinámico de los nodos.

El objetivo de estas redes en principio, era para usos exclusivamente militares, en donde el terreno de batalla impedía la implementación de redes con infraestructura alguna. Ha sido tan impactante su evolución que ahora se han implementado en ambientes civiles, de acceso público, de servicios, y en todos aquellos en la que su implementación resulte útil.

En base a lo anterior, se han identificado algunas aplicaciones en las cuales se implementan los protocolos anteriormente mencionados, permitiéndonos verificar cual de todos ellos ofrece mejores resultados, llegando a la conclusión, de que cada protocolo presenta ventajas y desventajas de acuerdo a la aplicación en el que se este empleando, es decir, uno puede ser más eficiente que otro, dependiendo del campo en el que se desarrollen.

BIBLIOGRAFIA

LEDESMA, Karen y CASTELLAR, Israel. Diseño de una PAN (Personal Area Network) para el Laboratorio de Redes y Sala 407 de la Tecnológica de Bolívar. Universidad Tecnológica de Bolívar. Monografía. Minor de Comunicaciones y Redes. Facultad de Ingeniería Electrónica, 2003.

MENDOZA, Reynaldo y OSORIO, Jessica. Tecnología Inalámbrica Radio LAN de Alto Rendimiento como una Solución Alternativa a las Redes Cableadas. Universidad Tecnológica de Bolívar. Monografía. Minor de Comunicaciones y Redes. Facultad de Ingeniería Electrónica, 2003.

WYNE, Tomasi. Sistemas de Comunicaciones Electrónicas. 4ta Edición. México: Prentice Hall, 2003.

IEEE standard for Wireless LAN, Medium Access Control and Physical Layer Specification, 1999. [Online].
http:// standards.ieee.org.

Specification of the Bluetooth System. [Online].
http://www.bluetooth.com

JOHNSON David. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. Internet Draft, draft-ietf-manet-dsr-05.txt, March 2001.

CHIANG, C y GERLA, Meredith. Adaptive Shared Tree Multicast in Mobile Wireless Networks. Proceedings of GLOBECOM '98, Publications Number: 18171822, 1998.

PERKINS, C y ROYER, Maurice. Ad Hoc On Demand Distance Vector (AODV) Routing. Internet Draft, draft-ietf-manet-aodv-02.txt, November 1998.

PARK, Víctor y CORSON, Marsha. A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks. Proceedings of INFOCOM '97, April 1997.

Advanced Network Technologies Division. [Online].
http://w3.antd.nist.gov/wctg/manet/draft-baker-manet-review-01.txt

VAIDYA, Nitin. Routing, MAC and Transport Issues in Mobile Ad Hoc Networks. Tutorial, 2001. [Online]
http://www.crhc.uiuc.edu/~nhv