INSTITUTO POLITÉCNICO NACIONAL

CENTRO DE INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍA DIGITAL

MAESTRÍA EN CIENCIAS EN SISTEMAS DIGITALES

"APLICACIÓN DEL ALGORITMO AD-HOC REACTIVO DE VECTOR DISTANCIA EN UNA RED INALÁMBRICA IEEE 802.11X"

TESIS

QUE PARA OBTENER EL GRADO DE

MAESTRÍA EN CIENCIAS

PRESENTA:

DIEGO ARMANDO TRUJILLO TOLEDO

BAJO LA DIRECCIÓN DE:

DR. MOISÉS SÁNCHEZ ADAME Y DR. MIGUEL AGUSTÍN ÁLVAREZ CABANILLAS

DICIEMBRE 2008 TIJUANA, B. C., MÉXICO

SIP-14

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de Tijuana, B.C. siendo las 14:00 horas del día 2 del mes de diciembre del 2008 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de CITEDI para examinar la tesis de grado titulada:

APLICACIÓN DEL ALGORITMO AD-HOC REACTIVO DE VECTOR DISTANCIA EN UNA RED INALAMBRICA IEEE 802.11x

Presentada por el alumno:

TRUJILLO	TOLEDO	DIEGO ARMANDO
Apellido paterno	materno	nombre(s)

Con registro:

B0	6	1	1	8	9

aspirante al grado de:

MAESTRÍA EN CIENCIAS EN SISTEMAS DIGITALES

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACIÓN DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISION REVISORA

Director de tesis

DR. MIGUEL AGUSTIN ALVAREZ CABANILLAS

Director de tesis

DR. MOISES SANCHEZ ADAME

DR. ROBERTO HERRERA CHARLES

M.C. ERNESTO EDUARDO QUIROZ MORONES

S. E. P.
INSTITUTO POLITECNICO NACIONAL
CENTRO DE INVESTIGACION Y DESARROLLO
DE TECNOLOGIA DIGITAL
DIRECCION

M. C. VICTOR MANUEL IZQUIERDO BLANCO

EL PRESIDENTE DEL COLEGIO

DR. LUIS ARTURO GONZALEZ HERNANDEZ

S. E. P.
INSTITUTO POLITECNICO NACIONAL
CENTRO DE INVESTIGACION Y DESARROLLO
DE TECNOLOGIA DIGITAL
DIRECCION

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de Tijuana, Baja California, el día 04 del mes DICIEMBRE del año 2008, el (la) que suscribe DIEGO ARMANDO TRUJILLO TOLEDO alumno (a) del Programa de MAESTRÍA EN CIENCIAS EN SISTEMAS DIGITALES con número de registro B061189, adscrito al CENTRO DE INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍA DIGITAL, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección de DR. MIGUEL A. ÁLVAREZ CABANILLAS Y DR. MOISÉS SÁNCHEZ ADAME y cede los derechos del trabajo intitulado APLICACIÓN DEL ALGORITMO AD-HOC REACTIVO DE VECTOR DISTANCIA EN UNA RED INALÁMBRICA IEEE 802.11X, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

DIEGO ARMANDO TRUJILLO TOLEDO

Nombre y firma

DEDICATORIA

Después de dos años y medio de haber trabajo en esta investigación, es difícil escribir con el corazón, ya que me he acostumbrado a escribir científicamente; que un artículo aquí, que un artículo por allá, que empieza los capítulos de la tesis, en fin. Pero ha llegado el momento más difícil de la escritura de la tesis, realizar la dedicatoria y los agradecimientos.

Primeramente quiero dedicar este trabajo, a mis padres **José Luis y Teresa,** *por darme la mejor educación, por estar siempre a mi lado aunque no físicamente por la distancia que nos separa pero si con el corazón y el pensamiento y por apoyarme incansablemente en cualquier decisión que yo tomara para lograr mi objetivo.*

A mis hermanos **José Luis y Teresita**, *que siempre estuvieron al pendiente de lo que me hiciera falta, y me visitaran alguna ocasión, haciendo mi estancia fuera de mi hogar más agradable.*

A mi abuelita **Tere** † *y mi* **tío Angel** † *que de alguna manera los tuve presentes y me cuidaron.*

A toda mi **familia**, *que siempre me recibieron con los brazos abiertos en temporadas de vacaciones y siempre creyeron en mí.*

AGRADECIMIENTOS

Le doy gracias a Dios que me permite vivir cada día y me bendijo con una familia maravillosa, además que me cuidó estos dos años y medio de una ciudad tan peligrosa como lo es Tijuana.

Gracias a mis padres pues les debo la vida.

Le agradezco a mis hermanos, que de alguna manera me motivaron por salir adelante.

Gracias a mi familia por preocuparse por mí.

Le agradezco a mis amigos, que mejor dicho yo los vi como hermanos porque vivimos juntos estos años: Yazmin, Ismael, Gabriel, José Ángel, Jesús mejor conocido como Camacho y Topacio.

A los miembros del grupo "Los Chuchis": Lupita, Ismael, Gabriel y por supuesto yo estoy dentro del grupo selecto, que muchos quisieron imitar.

A todos mis nuevos compañeros y amigos del centro de investigación: Carmen, Martha, Roy, Christian, Oriol, Jorge, Sonia, Cesar, Ricardo, Raúl, Iván, Konstantin, Paul, Colores, Adriana, Marcel, Narce, David, Miguel, Sergio, Rogelio, Noé, Coria y Perla.

A mis maestros, de la maestría y de la ingeniería que me brindaron parte de su conocimiento.

Gracias a mis amigos de Mazatlán, Culiacán, Ensenada, Chihuahua, Guadalajara y Tijuana, que por medio de internet nos mantuvimos comunicados y llegábamos a pasar horas platicando. En especial a Diana, Dacíl, Alicia, Carmen, Alejandra, Sheila, Jesse, Gil, Iván, Aarón y muchos más.

A mis directores de tesis: DR. Moisés Sánchez Adame y DR. Miguel Agustín Álvarez Cabanillas. Que gracias a sus conocimientos me dirigieron hasta llegar al final del trabajo a través de arduas e intensas revisiones.

Gracias a todos los miembros del comité tutorial: M.C. Víctor M. Izquierdo Blanco, M.C. Ernesto E. Quiroz Morones y al DR. Roberto Herrera Charles, por el tiempo, conocimiento y esfuerzo invertido en las revisiones de la tesis, con el fin de obtener mejores resultados.

Al Programa de Becas del Instituto Politécnico Nacional y al Consejo Nacional de Ciencia y Tecnología por brindarme el apoyo económico para poder realizar mis estudios.

Al Centro de Investigación y Desarrollo de Tecnología Digital CITEDI-IPN Tijuana, por haberme permitido realizar los estudios de posgrado.

Gracias al personal docente y administrativo, que labora en el centro, que realizaron todos los tramites desde la inscripción en el primer semestre hasta mi titulación. En especial a Lulu, Blanquita, Hilda, Yara, Paty, Oscar, entre otros.

Gracias también a mi novia Verónica, por el amor, apoyo y comprensión en momentos difíciles que como arte de magia me los convertía en momentos felices.

Gracias, muchas gracias a todos y a cada uno de ellos y los que me faltaron, que por falta de espacio no los menciono, pero en mi corazón estarán, todos forman parte de este trabajo y por tal motivo guardan un espacio en mi corazón.

RESUMEN

"APLICACIÓN DEL ALGORITMO AD-HOC REACTIVO DE VECTOR DISTANCIA EN UNA RED INALÁMBRICA IEEE 802.11X"

En este trabajo se investigaron los diferentes tipos de algoritmos que se pueden emplear bajo el estándar IEEE 802.11 para redes móviles Ad-Hoc.

Se realizó el análisis de ruta implementando dos algoritmos de ruteo; el algoritmo proactivo de estado de enlace optimizado (OLSR) y el algoritmo reactivo de vector distancia (AODV).

Del algoritmo OLSR se analizó el procedimiento para la obtención de las tablas de ruteo, descubrimiento de vecinos, selección de nodos retransmisores y cálculo de ruta. Se diseñó una topología de red que permitió aplicar los parámetros de control característicos del algoritmo de ruteo proactivo OLSR.

Del algoritmo Reactivo de Vector Distancia (AODV) se analizó su funcionamiento, en especial, el procedimiento de transmisión de la información que se envía a través de los nodos pertenecientes a la red Ad-Hoc. Se diseñó una topología de red específica que permite conocer el potencial de AODV al momento de establecer una ruta.

Se utilizó el simulador de redes NCTUns, para realizar las comparaciones de AODV y de OLSR. Se diseñaron 5 escenarios para comparar el funcionamiento de la topología ad-hoc. De los resultados obtenidos, el algoritmo AODV entrega la mayor cantidad de paquetes comparado con OLSR.

Una vez seleccionado el algoritmo, se realizó una implementación experimental de AODV en una red inalámbrica Ad-Hoc utilizando WinAODV. Usando esta implementación se logró establecer la comunicación en una red Ad-Hoc inalámbrica IEEE 802.11 entre computadoras que se encontraban fuera del área de cobertura, utilizando un nodo intermedio.

Palabras Claves: 802.11, Redes Ad-Hoc, Control de Acceso al Medio (MAC), Algoritmo Proactivo, Estado de Enlace, AODV, OLSR , Vector Distancia, Algoritmo Reactivo, MANET, Windows.

ABSTRACT

"APPLICATION OF THE REACTIVE AD-HOC DISTANCE VECTOR ALGORITHM IN IEEE 802.11X WIRELESS NETWORK"

In this work, different types of algorithms for mobile ad-hoc networks that use the IEEE 802.11 standard were investigated.

The route analysis was done by the implementation of two different types of routing algorithms named the proactive optimized link state routing (OLSR) and the reactive ad-hoc on-demand distance vector (AODV).

In the case of OLSR, the procedures for building routing tables, discovering neighbors, selecting nodes relays and route calculation were discussed. A specific network topology was designed in which it was possible to test typical control parameters for OLSR algorithm.

Regarding the AODV, the focus was on how it works, specially on how the information transmission is carried on through all the nodes belonging to the Ad-Hoc network. A specific network topology was designed to know the AODV's potential at the moment it discovers and builds the route.

The NCTUns network simulator was used to perform comparisons between the two algorithms. Five experiments were designed to compare the ad-hoc network performance. From the results analysis, it is inferred that AODV has a better performance than OLSR.

The AODV algorithm was selected, and an experimental wireless Ad-Hoc network was built using WinAODV. Communication between two long distance nodes was established using intermediate nodes.

Keywords: 802.11, Ad-Hoc Network, Medium Access Control (MAC), Proactive Algorithm, Reactive Algorithm, Link State, Distance Vector, OLSR, AODV, MANET, Windows.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE SÍMBOLOS Y ACRÓNIMOS

AD-HOC	Adecuado, Apropiado, Dispuesto para un fin en específico.
AODV	Ad-Hoc On-demand Distance Vector – Algoritmo Ad-Hoc Vector Distancia Sobre Demanda.
DSDV	Destination Sequenced Distance Vector – Algoritmo Vector Distancia de Secuencia Destino.
DSR	Dynamic Source Routing – Ruteo de Fuente Dinámica.
WRP	Wireless Routing Protocol – Protocolo de Ruteo Inalámbrico.
OLSR	Optimized Link State Routing Protocol – Protocolo de Ruteo de Estado de Enlace Optimizado
ZRP	Zone Routing Protocol – Protocolo de Ruteo de Zona.
TORA	Temporally Ordered Routing Algorithm – Algoritmo de Ruteo Temporalmente Ordenado.
IEEE	Institute of Electrical and Electronics Engineers – Instituto de Ingenieros Electrónicos y Electricistas.
IETF	Internet Engineering Task Force – Fuerza de Trabajo de Ingeniería de Internet
FCC	Federal Communications Commission – Comisión Federal de Comunicaciones
SCT	Secretaría de Comunicaciones y Transportes
TCP	Transport Control Protocol – Protocolo de Control de Transporte
IP	Internet Protocol – Protocolo de Internet
UDP	User Datagram Protocol – Protocolo de Datagrama de Usuario
MAC	Media Access Control – Control de Acceso al Medio
MANET	Mobile Ad-Hoc Networks – Redes Móviles Ad-Hoc
LAN	Local Area Network – Red de Área Local
OSI	Open System Interconnection – Interconexión de Sistemas Abiertos
NCTU	National Chiao Tung University – Universidad Nacional de Chiao Tung, Taiwan
NCTUNS	Network Simulator and Emulator of NCTU – Simulador y Emulador de Redes de NCTU

1
INTRODUCCIÓN

Comunicación inalámbrica es aquella que se lleva a cabo sin el uso de cables de interconexión entre los usuarios que participan en ella; por ejemplo, una comunicación con teléfono celular es inalámbrica, mientras que una comunicación con teléfono fijo tradicional no lo es.

El primer servicio que se liberó del cable fue la transmisión de telégrafo. La revolución de las computadoras personales y el gran desarrollo de internet están haciendo que el uso de la tecnología sea tan común en la vida diaria como lo es el teléfono celular. Existen computadoras de escritorio, portátiles, PDA (*Personal Digital Assistant, Asistente Digital Personal*), además también de la tecnología en el coche hasta el aire acondicionado o los juguetes de los niños en el hogar. Todos estos dispositivos pueden interconectarse entre sí, aunque se puede hacer con cables, pero su mayor potencial se llega mediante el uso de comunicación inalámbrica.

Las redes inalámbricas se utilizan para dos propósitos principales, para transmisión de voz y la transmisión de datos. En el primer caso, la telefonía móvil es un ejemplo muy claro, mientras que las redes inalámbricas de datos no es más que un conjunto de computadoras, o de cualquier otro dispositivo informático, comunicados entre sí de manera inalámbrica.

Las redes inalámbricas de datos se clasifican por su alcance [1], se puede observar en la figura 1.1. Alcance se refiere a la distancia máxima a la que pueden situarse dos dispositivos para establecer una comunicación inalámbrica. De acuerdo con lo anterior la clasificación es la siguiente:

- Redes Inalámbricas de Área Personal (*Wireless Personal Area Network; "WPAN"*).
- Redes Inalámbricas de Área Local (*Wireless Local Area Network; "WLAN"*).
- Redes Inalámbricas de Área Metropolitana (*Wireless Metropolitan Area Network; "WMAN"*).
- Redes Inalámbricas de Área Regional (*Wireless Regional Area Network, "WRAN"*)
- Redes Inalámbricas de Área Extensa (*Wireless Wide Area Network, "WWAN"*).

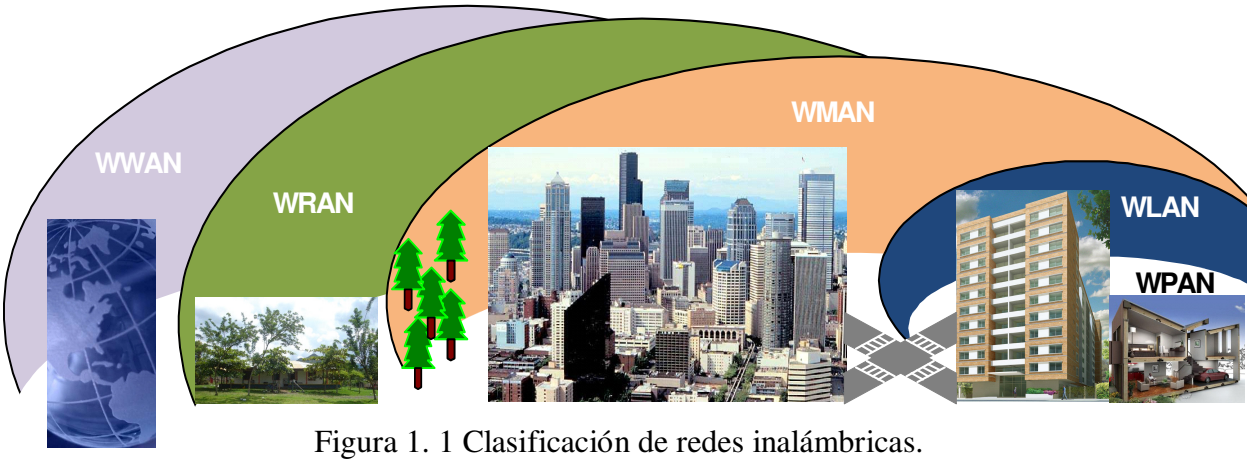


Figura 1. 1 Clasificación de redes inalámbricas.

Otra clasificación que se les da a las redes inalámbricas es redes de infraestructura y redes ad-hoc. Las redes de infraestructura se caracterizan por contar con un dispositivo central que coordina toda conexión entre dispositivos, como por ejemplo una estación base o un punto de acceso.

La palabra ad-hoc es una expresión compuesta del latín que juntas tiene un significado y no por el significado de cada palabra, de acuerdo con la Real Academia Española (RAE) literalmente significa "para esto" [2] y como adjetivo significa "adecuado", "apropiado" o "dispuesto especialmente para un fin" [2]. Por lo anterior se dice que una red ad-hoc está formada para un fin especifico, esto quiere decir que se permite la formación dinámica y espontánea de la misma, eliminando la necesidad de un dispositivo central que controle el flujo de tráfico en esta red.

Actualmente el desarrollo de las redes de comunicaciones y las necesidades de los usuarios demandan movilidad y es precisamente este requerimiento el que resulta ser uno de los mayores

retos para la interconectividad entre los usuarios de las redes de datos. Comúnmente el protocolo utilizado para movilidad global es el IP Móvil (MIP, *Mobile IP*) [3], también IPv6 incorpora una extensión de movilidad, sin embargo, solamente es funcional para redes inalámbricas de infraestructura.

Por otro lado, surge la red móvil ad-hoc conocida como MANET (*Mobile Ad-hoc NETworks*), esta se define como "una colección de dispositivos móviles que se comunican usando un medio inalámbrico, formando una red autónoma donde no existe un punto centralizado" [4]. Cabe mencionar que este tipo de redes presentan topologías dinámicas y aleatorias, presentándose espontáneamente.

El problema se presenta cuando un dispositivo requiere comunicarse con otro dispositivo dentro de la red, éste usa ya sea comunicación directa mediante un enlace directo o comunicación indirecta mediante una ruta multisaltos que propaga los paquetes a través de los dispositivos intermedios hasta llegar al dispositivo destino. Lo que significa que todos los miembros de la red deberán incorporar técnicas de enrutamiento.

Como se mencionó, el ambiente donde se desarrollan estas comunicaciones es móvil formando una topología de red dinámica y espontánea, dependiendo del área de cobertura de cada dispositivo y la disponibilidad de éstos, por lo que hacen susceptible a que la comunicación entre los dispositivos de la red se interrumpa por diferentes motivos como salir del área de cobertura de transmisión, apagar el dispositivo, velocidad de movimiento, entre otras más. También se tiene que considerar si un dispositivo nuevo entra a la red por lo tanto se tendrá que incorporar rápidamente al proceso de comunicación.

El diseño de protocolos de enrutamiento rápidos y eficientes es la parte medular en el desempeño de las MANET's, no sin olvidar el área encargada del consumo de energía, que también juega un papel muy importante ya que los dispositivos utilizan baterías para su funcionamiento.

Este tipo de redes tienen una aplicación potencial en áreas como la militar, civil, social y muy especial en casos de desastres ya que al sufrir una baja en la corriente eléctrica, todos los

dispositivos de comunicación que utilizan puntos de acceso o estaciones base dejarán de transmitir y perder comunicación alguna.

Por lo anterior resulta de interés realizar un análisis de los protocolos de enrutamiento para redes móviles ad-hoc así como realizar una implementación de alguno de estos para comprobar su funcionamiento.

Muchos algoritmos de ruteo han sido propuestos [5] [6] [7] [8] [9] [10], pero han surgido pocas comparaciones [11] [12] [13] [14], sin embargo, estos trabajos se enfocan en la simulación. La simulación se basa en modelos aproximados del funcionamiento del sistema en ambientes reales. Para garantizar su funcionamiento en un ambiente real, es requerida la implementación experimental. Algunas implementaciones realizadas anteriormente son la del National Institute of Standards and Technology (NIST) [15], la de University of California, Santa Barbara (UCSB) [16], la de Uppsala University en Suecia (UU) [17], la University of Illinois at Urbana-Champaign (UIUC) [18], el común denominador de estas implementaciones es que emplean el mismo OS (Linux). En contraste al trabajo de University of Dublin [19], en Irlanda, que utilizó Windows como sistema operativo.

Por lo anterior en este trabajo, el **objetivo** general se basa en revisar los algoritmos de ruteo para redes móviles Ad-Hoc proactivos, reactivos e híbridos más importantes que se emplean en la actualidad, así como los estándares para redes inalámbricas haciendo un énfasis en la normatividad IEEE 802.11x, además implementar experimentalmente una red inalámbrica aplicando específicamente el algoritmo reactivo de vector distancia para redes móviles ad-hoc (AODV, *Ad-Hoc On demand Distance Vector*) [5].

El análisis de la normatividad IEEE 802.11x, permitirá conocer los parámetros que se utilizan para establecer una comunicación con dispositivos que se encuentran en el área de cobertura. Mientras que el estudio de los algoritmos de ruteo proporcionará una experiencia en protocolos multisaltos.

Para alcanzar el objetivo, fue necesario realizar diferentes objetivos particulares, los cuales son:

- Comprobar la información que intercambian los dispositivos que están a un salto, mediante el estándar IEEE 802.11x.

- Proponer una topología de red y realizar un análisis de ruta utilizando el algoritmo proactivo de estado de enlace optimizado (OLSR).

- Proponer una topología de red y realizar el análisis correspondiente utilizando el algoritmo reactivo de vector distancia (AODV).

- Realizar una comparación de ambos protocolos mediante un simulador de red.

- Realizar una implementación experimental del algoritmo que mejores resultados presente. Para lograr este objetivo se propone implementar en tres computadoras portátiles el algoritmo, separándolas de manera que la computadora uno está conectada con la computadora dos y la computadora dos está conectada con la tres, así la computadora dos tiene conexión con la uno y la tres.

Los objetivos se cumplieron con los siguientes capítulos. En el capítulo 2 se trata del estándar IEEE 802.11x, se describen las principales diferencias en la capa física y así como también se aborda en extenso la subcapa de control de acceso al medio (MAC). En el capítulo 3 se presentan las redes inalámbricas ad-hoc, las características de operación y principalmente se presentan algunos algoritmos de ruteo para estas redes. En el capítulo 4 se describe el funcionamiento del algoritmo proactivo de estado de enlace (OLSR), así como también el formato de paquetes y se realiza un análisis de ruta de una topología propuesta. De la misma manera, en el capítulo 5 se lleva a cabo la descripción del funcionamiento del protocolo reactivo de vector distancia (AODV), el formato de los mensajes utilizados y por último el análisis de ruta en una topología de red propuesta. En el capítulo 6 se muestra la metodología para realizar la simulación mediante NCTUns. También muestra los resultados de los escenarios. En el capítulo 7 se presenta la implementación experimental del algoritmo. Y por último en el capítulo 8 se presentan las conclusiones del trabajo.

2

ESTÁNDAR IEEE 802.11 EN UNA RED AD-HOC

En este capítulo se aborda el estándar IEEE 802.11 en modalidad Ad-Hoc. Principalmente se hace un énfasis en la subcapa de acceso al medio (MAC). También se describen los diferentes tipos de mensajes que se utilizan para establecer una comunicación entre dispositivos móviles. Además se presenta la configuración en un sistema operativo, para obtener un dispositivo en Ad-Hoc.

El estándar 802.11 para WLAN se enfoca en la capa Física (PHY) y en la subcapa MAC (*Medium Acces Control*, Control de Acceso al Medio) para redes que utilizan algún punto de acceso (AP, *access point*) y/o redes ad hoc.

El estándar original soportaba tres tecnologías en la capa Física: infrarrojo (IR), Espectro Disperso de Saltos de Frecuencia (FHSS) y Espectro Disperso de Secuencia Directa (DSSS). Posteriormente una extensión del estándar llamada 802.11b fue diseñado para DSSS utilizando la banda de 2.4 GHz con tasas de datos de 1, 2, 5.5 y 11 Mbps. Las últimas dos son alcanzadas a través de modificación por código complementario (CCK, complementary code keying). Otra extensión del estándar llamada 802.11a usada para grandes tasas de bits utiliza modulación OFDM proporcionando tasas de bits desde 6 Mbps hasta 54 Mbps en la banda de 5 GHz. Todas estas tecnologías utilizan la misma subcapa MAC [20], [21].

Como todos los estándares del IEEE 802, el estándar 802.11 se enfoca en los primeros dos niveles del modelo de Referencia OSI, la capa física y la capa de enlace de datos, como lo muestra en la figura 2.1 [21].

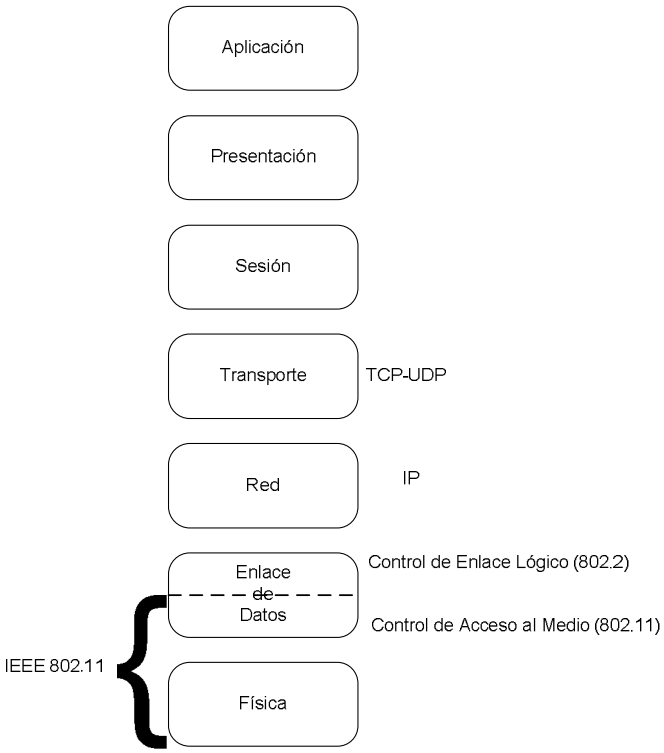


Figura 2. 1 Relación IEEE 802.11 con el Modelo OSI

En la figura 2.2 se muestra como se ha ido desarrollando el estándar y continúa su evolución [22].

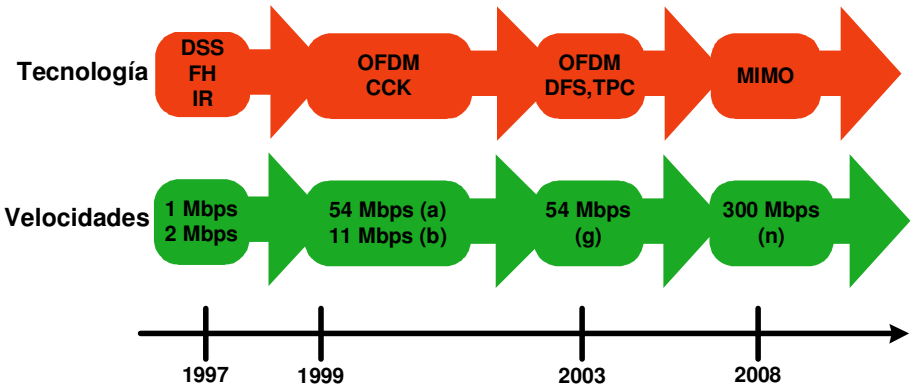


Figura 2. 2. Evolución de 802.11.

La tabla 2.1 muestra un resumen de las características físicas de los estándares aprobados [20] [21] [22] [23] [24] [25] [26].

Tabla 2. 1. Resumen del estándar 802.11

Estándar	**802.11**	**802.11a**	**802.11b**	**802.11g**	**802.11n**
Fecha Aprobado	Julio 1997	Septiembre 1999	Septiembre 1999	Julio 2007	*Draft 7 Noviembre 2008
Frecuencia de Operación	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz / 5 GHz
Cobertura Típica Máxima	100 m	100 m	100 m	100 m	150 m
Tasa de Datos	2 , 1 Mbps	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Número de Canales No Traslapados	3	23	3	3	3 / 23

Cabe resaltar que la capa física es igual para redes que utilizan un punto de acceso y las redes ad-hoc, que es el caso que aquí se presenta.

2.1. SUBCAPA DE MECANISMO DE ACCESO AL MEDIO (MAC)

La capa de enlace de datos, se divide en dos subcapas, el control de enlace lógico (LLC) que se especifica en el estándar IEEE 802.2 y el control de acceso al medio (MAC) que entra dentro de las especificaciones del 802.11 como se puede observar en la figura 2.1. MAC define dos tipos de acceso al medio diferentes, el Distributed Coordination Function (DCF) y Point Coordination Function (PCF). PCF se utiliza solo para redes de tipo infraestructura y es opcional. DCF es básicamente un mecanismo de Múltiple Acceso con sensado de Portadora con Colisión Evitada

(Carrier Sense Multiple Access with Collision Avoidance CSMA/CA), este se utiliza en ambos tipos de redes tanto para infraestructura y ad-hoc.

2.1.1. Funcionamiento del MAC en Modalidad Ad-Hoc

Existen dos intervalos de tiempo especificados dentro del estándar 802.11 para el acceso al medio en una red ad-hoc, los cuales son el intervalo corto entre tramas "SIFIS" (Short Inter Frame Space) y su valor es fijo y esta dado por cada tipo de enlace físico, para Espectro Disperso con Saltos de Frecuencia el valor típico es de 28μs y para Espectro Disperso de Secuencia Directa (DSSS) es de 10 μs. Y también se tiene el intervalo de tiempo distribuido entre tramas "DIFS" (Distributed Inter Frame Space), el cual su valor es calculado por la ecuación 1 [25].

$$DIFS = SIFS + 2 \times Bloque\ de\ Tiempo \qquad \text{Ec. 1}$$

Donde el *Bloque de Tiempo* es un valor definido en la capa física y sus valores dependen del tipo de tecnología que se utiliza, así para FHSS el valor es igual a 50 μs y para DSSS es igual a 20 μs.

Para iniciar una transmisión, el nodo interesado espera a que el canal este libre por un intervalo de tiempo distribuido (DIFS), si está ocupado el canal, se espera un tiempo aleatorio (backoff), donde su valor esta dado por la ecuación 2 [25].

$$Backoff = Aleatorio(\ \ ) \times Bloque\ de\ Tiempo \qquad \text{Ec. 2}$$

Donde *Aleatorio*( ) es un valor entero entre [0,CW], donde CW es un valor entero entre los valores definidos en la capa física como aCWmin≤CW≤aCWmax, donde aCWmin para FHSS es 15 y para DSSS es 31 y el valor para aCWmax en ambos caso es 1023.

Si esta libre el canal, el nodo puede transmitir. Al terminar de recibir los datos, el nodo receptor checa el número de redundancia cíclica (CRC) para saber si ocurrió una colisión, si no la hubo, envía un mensaje de enterado (ACK) después de un intervalo de tiempo corto (SIFIS).

Para reducir la probabilidad de colisión entre dos nodos se utiliza el sensado de portadora virtual, el cual su funcionamiento es agregar un vector de asignación de red NAV (Network Allocation Vector) en un nodo "n", el cual recibe una transmisión que no le corresponde, con el fin de señalizar el canal ocupado. El vector se refiere a un segmento de tiempo, el cual deshabilitará cualquier transmisión en el nodo. La duración de esta deshabilitación temporal dura aproximadamente el tiempo especificado en la trama que se recibió.

La figura 2.3 muestra la transmisión de una trama del nodo 1 al nodo 2, donde el nodo 1 espera un tiempo DIFS para enviar la trama X, una vez enviada la trama, todos los nodos que recibieron la trama, agregan un vector con el tiempo especificado en la trama X, excepto el nodo destino (nodo 2). El nodo 2 envía una trama Y, por lo que los nodos que no recibieron la trama X se deshabilitan con la trama Y durante el tiempo especificado dentro de la trama Y. Una vez finalizada la transmisión se habilitan todos los nodos.

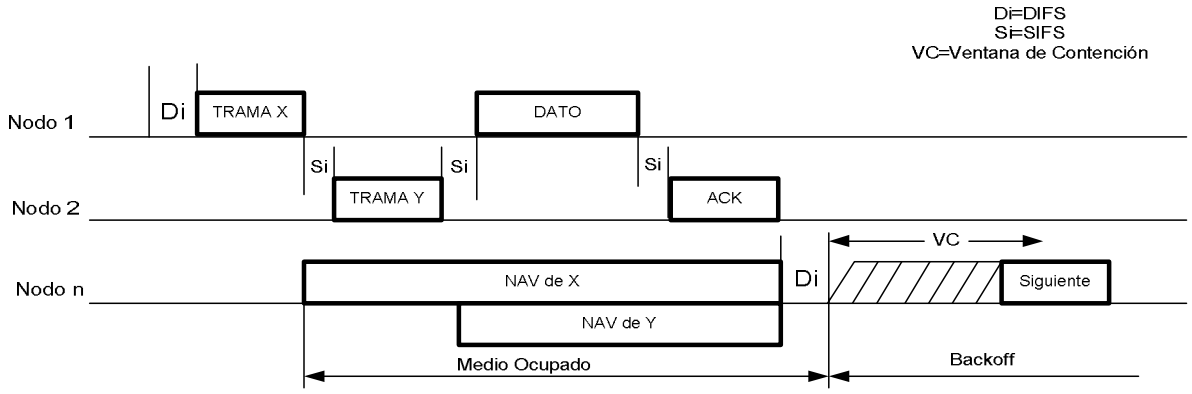


Figura 2. 3. Ejemplo de MAC usando NAV.

2.2. FORMATO DE TRAMAS

El formato general de una trama MAC se muestra en la figura 2.4. Cada trama MAC está compuesta por un encabezado MAC, un cuerpo de trama y el checksun. Los campos de la dirección 2, dirección 3, control de secuencia (seq), dirección 4 y cuerpo de la trama se presentan en ciertas tramas.

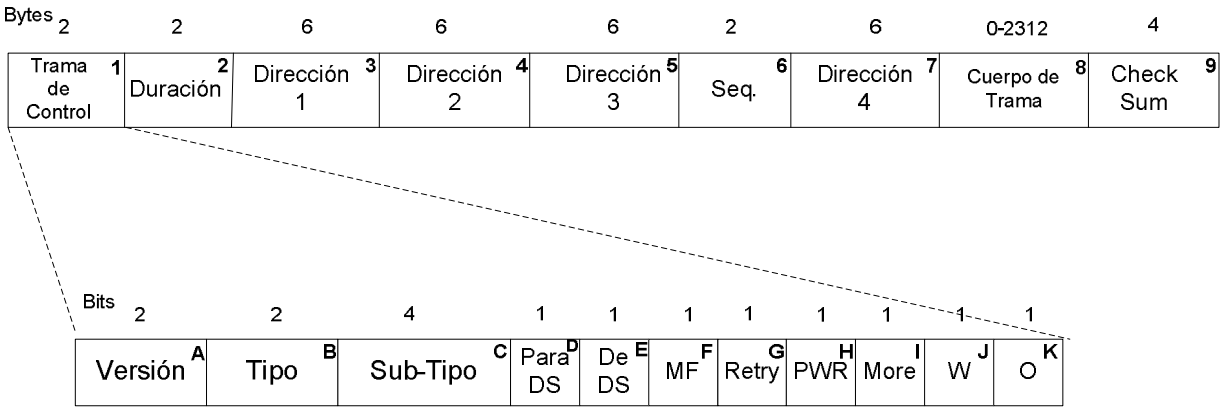


Figura 2. 4. Formato general de Trama MAC.

Algunos de los campos sobresalientes son Tipo (Campo 1B), específica el tipo de mensaje (Datos, Control o Administración). Sub-Tipo (Campo 1C), este campo indica las funciones principales de los diferentes tipos de mensajes. Para/De DS (Campos 1D, 1E) son banderas que indican si la trama "va" (Para) o "viene" (De) de un sistema de distribución. MF (Campo 1F) indica si existen más fragmentos del mensaje detrás de él. Retry (Campo 1G) indica si la trama será retransmitida. W (Campo 1J) se habilita si cuenta con clave WEP. O (Campo 1K), este bit indica que las tramas serán procesadas por estricto Orden.

Duración (Campo 2) se refiere al tiempo que tardará en transmitirse la trama y esté es usado para calcular el vector NAV. Control de Secuencia (Campo 6) permite ordenar diferentes fragmentos de tramas en una sola, también para reconocer paquetes duplicados. CheckSum (Campo 9) contiene un número de 32 bits que se utiliza para checar la redundancia cíclica (CRC) con el fin de conocer si la trama llego completa.

2.2.1. Tramas de Administración

Para que un nodo sea capaz de realizar una comunicación con otro nodo, el nodo que quiere transmitir necesita tener información de sincronización de los otros nodos vecinos, esta información la puede obtener mediante dos procedimientos básicos de Administración: Escaneo Pasivo o Escaneo Activo.

En el Escaneo Pasivo, el nodo recibe tramas de sensado y las contesta, utilizado generalmente para redes en modo infraestructura. En cambio en el Escaneo Activo, el nodo intenta buscar a los nodos vecinos enviando mensajes de petición de sondeo (Probe Request) y respondiendo los nodos que lo recibieron con una contestación de sondeo (Probe Response), este es el utilizado en modalidad ad-hoc. El tiempo mínimo en el que puede llegar un Probe Response es DIFS y el tiempo máximo en el que puede llegar un Probe Response esta dado por la ecuación 3 [25]:

$$2 \times DIFS + 2 \times Probe\_Response + SIFIS + ACK + aCWmax \qquad \text{Ec. 3}$$

Este tipo de mensajes se envían mediante las tramas de administración o Management Frames, el cual en su formato general, cuenta con los campos 1, 2, 3, 4, 5, 6, 8 y 9 de la figura 2.4. Estos elementos los podemos observar en la figura 2.5.

Bytes	2	2	6	6	6	2	0-2312	4
	Frame Control 1	Duración 2	DA 3	SA 4	BSSID 5	Seq. 6	Cuerpo de Trama 8	Check Sum 9

Figura 2. 5. Tramas de Administración

Así el campo 8 contendrá los diferentes sub-campos para cada tipo de trama de administración. En este caso solamente se requiere conocer las tramas para realizar el Escaneo Activo, por ser una red Ad-Hoc. Por lo tanto para un mensaje PROBE REQUEST la información que se agrega dentro del campo 8 es un identificador de red Ad-Hoc (SSID) y un sub-campo con las velocidades Soportadas que muestra las velocidades permitidas por el nodo. Por lo tanto, el formato de un mensaje Probe Request está definido en la figura 2.6.

Bytes	2	2	6	6	6	2	34	10	4
	Frame Control	Duración	DA	SA	BSSID	Seq.	SSID	Velocidades Soportadas	Check Sum

Figura 2. 6. Formato PROBE REQUEST

Donde SSID indica la identificación de una red ad-hoc. La figura 2.7 está formada por un byte de Identificador de Elementos, 1 byte de longitud si es cero esto indica que será una difusión a todos los elementos y hasta 32 bytes del identificador.

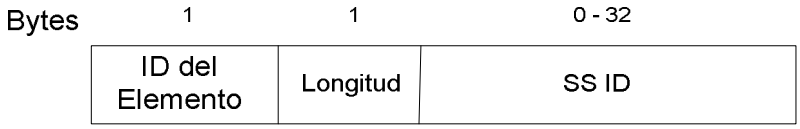


Figura 2. 7. Formato SSID

El elemento de Velocidades Soportadas, muestra las velocidades permitidas por el nodo. Está formado por el byte del Identificador de Elemento, el byte de la longitud y por 8 bytes de la información de las tasas soportadas, la figura 2.8 muestra la distribución de este elemento.

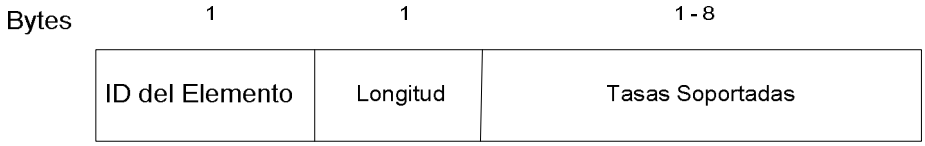


Figura 2. 8. Formato de Tasas Soportadas

Para una trama PROBE RESPONSE la información que se agrega dentro del campo 8 es el campo TimeStamp que contiene el valor para sincronizar del reloj. Un intervalo Beacon que corresponde al número de unidades de tiempo (TUs) que serán enviadas las tramas. Un TUs equivale a 1,024 µs y su valor común es de 100 TUs ó 0.1 s. También se agrega el campo de Capacidades que muestra las capacidades que tiene el nodo emisor. Además del identificador de Red Ad-Hoc y el campo de Velocidades Soportadas. Una trama Probe Response tiene el formato de la figura 2.9.

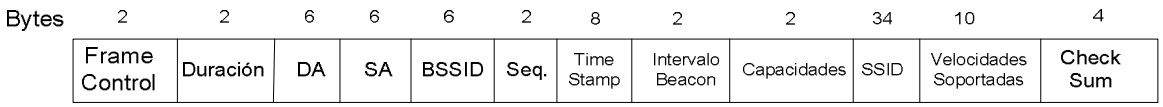


Figura 2. 9. Formato de PROBRE RESPONSE

El campo TimeStamp representa el valor del reloj de la función de reloj de sincronización Timing Synchronization Function "TSF". El TSF mantiene a todos los relojes de los nodos sincronizados. Todos los nodos mantienen un reloj TFS local que es el número en microsegundos que fue activada la red. Se compone de 64 Bits.

El intervalo Beacon representa el número en unidades de tiempo (TUs) de la frecuencia que serán enviadas las tramas Beacon. Un TUs equivale 1,024 microsegundos aproximadamente 1 milisegundo. Este valor comúnmente se pone en 100 TUs lo que equivale a 100 milisegundos o 0.1 segundo. Está formado por 16 bits.

La figura 2.10 representa el campo de información de capacidades, que contiene una serie de subcampos que se utilizan para indicar al nodo las capacidades requeridas o las capacidades que tiene. Se compone de 16 bits de los cuales solo se utilizan 4.

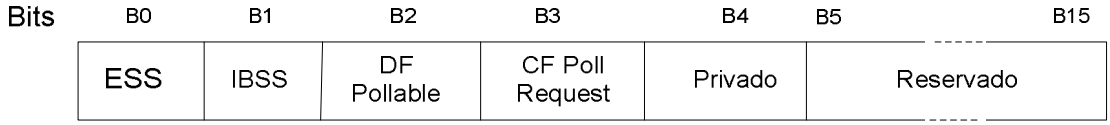


Figura 2. 10. Formato de la información de Capacidades

El campo de los parámetros IBSS está presentado en la figura 2.11, contiene la información necesaria para soportar una red ad-hoc. El campo de la información contiene la duración en TUs de la ventana del Mensaje de Indicación de Aviso de Trafico (Announcement Traffic Indication Message "ATIM"). Formado por un byte del ID del elemento, un byte de la longitud y 16 bits para la ventana ATIM.

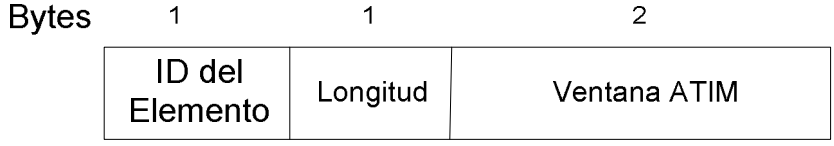


Figura 2. 11. Formato de Parámetros IBSS

El valor del identificador de elementos que se utilizan para cada elemento que se envía se enlista en la tabla 2.2 junto con su correspondiente descripción del elemento.

Tabla 2. 2. Elementos de una trama

Tipo de Elemento	ID del Elemento
SSID	0
Tasa Soportada	1
Parámetros FH	2
Parámetros DS	3
Parámetros CF	4
TIM	5
Parámetros IBSS	6
Reservado	7 – 15
Pruebas de Texto	16
Reservado para Pruebas de Texto	17 – 31
Reservado	32 – 255

2.2.2. Tramas de Control

Una vez sensado el medio y obtenida la información de nodos cercanos, se puede comunicar con un nodo, utilizando las tramas de control. En este caso las tramas que se necesitan para establecer una comunicación son petición de envió (Request to Sent "RTS"), Libre para el envió (Clear to Sent "CTS") y Enterado (Acknowledgment "ACK").

La trama RTS se utiliza para realizar una petición a los nodos para poder transmitir y saber si está libre el canal. Los campos de la figura 2.4 que contiene una petición son los campos 1, 2, 3, 4 y 9. Donde la dirección 1 (campo 3) y la dirección 2 (campo 4) son las direcciones de los nodos destino y nodos fuentes respectivamente, esta información se obtiene de las tramas de administración. El campo de duración (campo 2) se asocia al valor del tiempo requerido para transmitir 4 tramas (RTS, CTS, ACK, Datos o de Administración) además de 3 intervalos cortos (SIFS). El formato del RTS es mostrado en la figura 2.12.

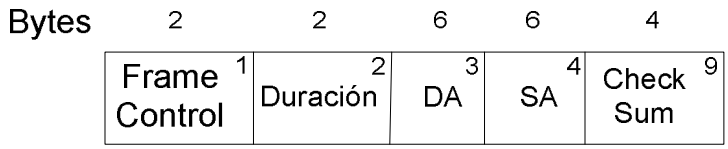


Figura 2. 12. Formato RTS

El CTS, se utiliza para responder a un mensaje de petición (RTS) solo si esta libre el canal de comunicación. El formato de una trama libre para el envió (CTS) mostrado en la figura 2.13 cuenta con los campos 1, 2, 3 y 9 de la figura 2.4. Donde el campo de destino (Campo 3), es la dirección del nodo que se quiere alcanzar, esta se obtiene de la trama inmediata anterior del campo de la dirección fuente (Campo 4).

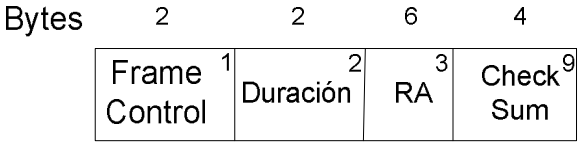


Figura 2. 13. Formato CTS

El formato de la trama ACK mostrado en la figura 2.14 contiene los campos 1, 2, 3 y 9 de la figura 2.4. Donde la dirección destino (Campo 3) es la dirección del nodo que envía la trama inmediata anterior.

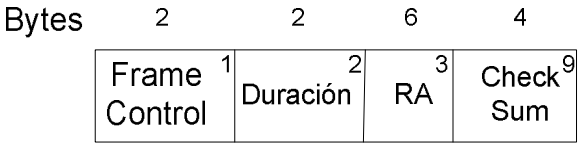


Figura 2. 14. Formato ACK

2.2.3. Tramas de Datos

Cuando se requiere enviar Datos de una aplicación, se utilizan las tramas de Datos. El formato de la trama contiene los 9 campos de la figura 2.4, donde el valor característico de tipo y subtipo es Datos [25]. El cuerpo de la trama (Campo 8) contiene los datos encapsulados de las aplicaciones o una parte fragmentada en el caso que sea mayor al valor máximo de 2312 Bytes [25].

2.3. EJEMPLO DE COMUNICACIÓN

A continuación se presenta un ejemplo del establecimiento de comunicación entre dos nodos vecinos que aun no pertenecen a ninguna red, por lo tanto no tienen información almacenada previa. Este establecimiento de red, se realiza para el caso particular de una red ad-hoc.

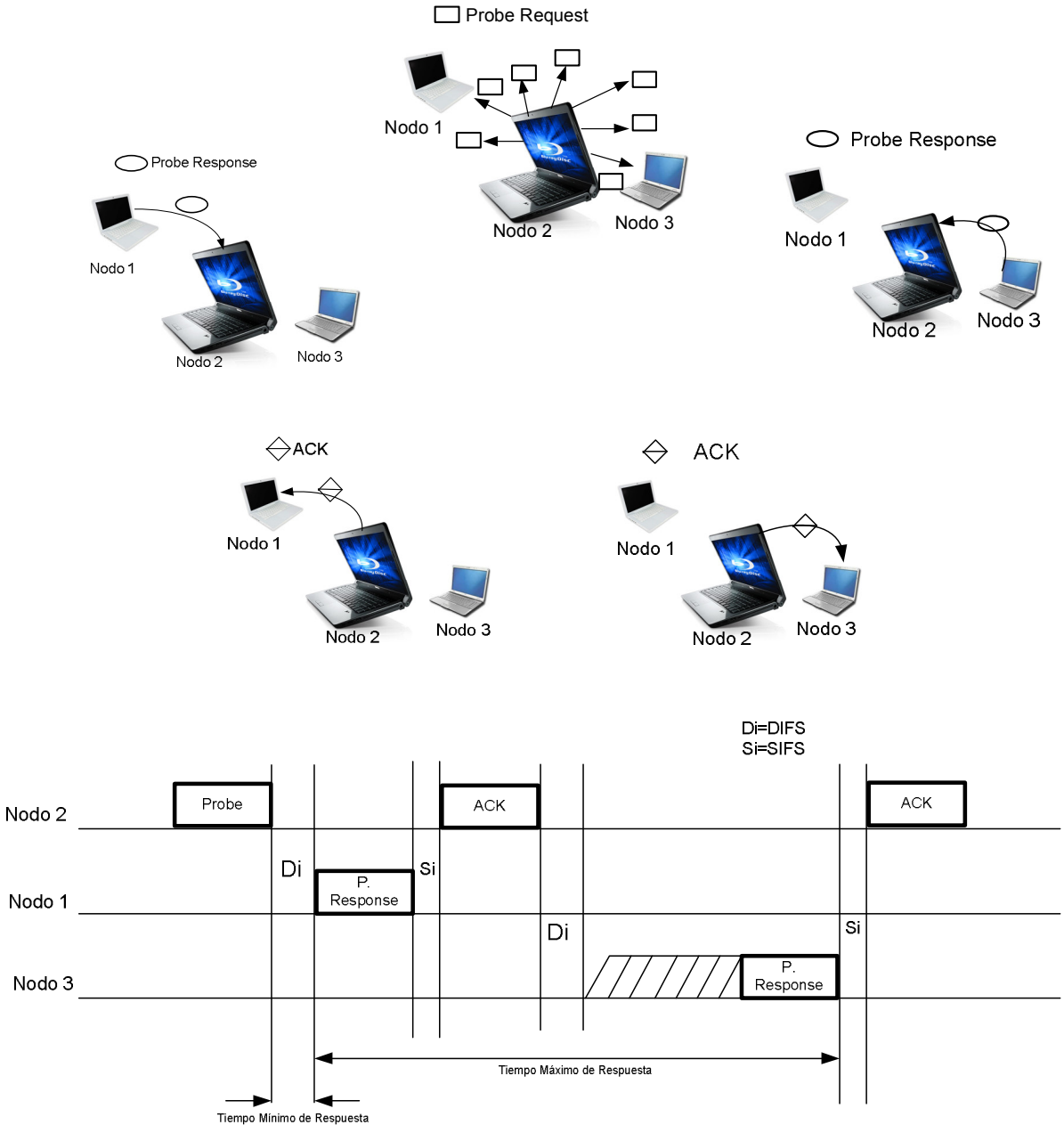
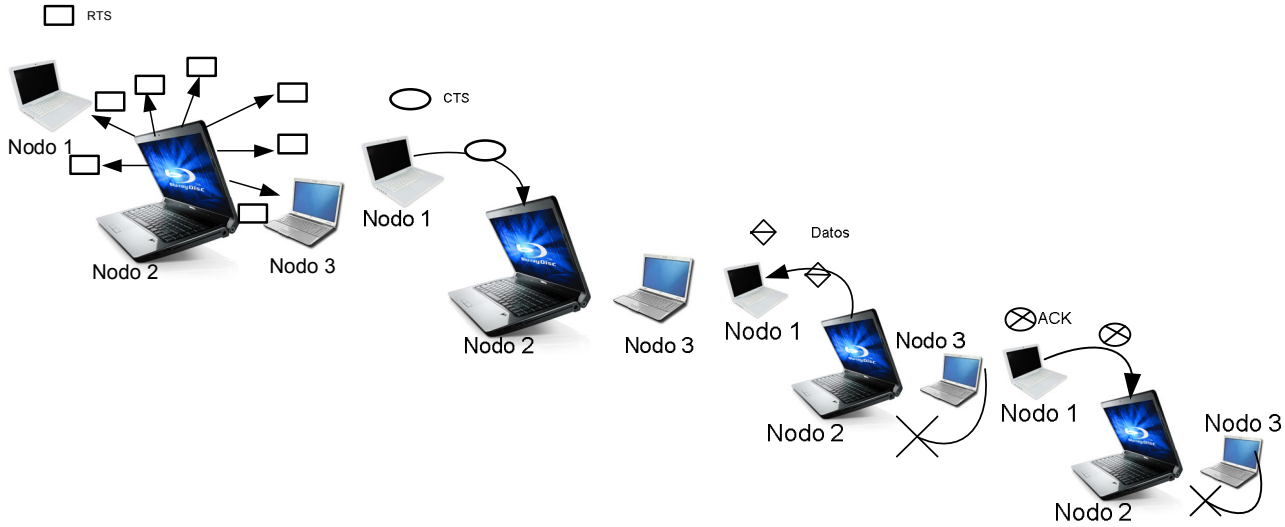


Figura 2. 15. Transmisión de Probe Request y Probe Response

En la figura 2.15 se muestra que el nodo 1 envía una trama Probe Request, los nodos que estén en el área de cobertura enviarán una trama de Probe Response, tomando los parámetros necesarios para sincronizar ambos nodos y finaliza con una trama ACK para certificar que los datos llegados en Probe Response fueron correctos.

Una vez sincronizados los nodos de la red y guardados los parámetros de las direcciones de los vecinos, es posible mantener una comunicación de acuerdo al esquema de control de acceso al medio.



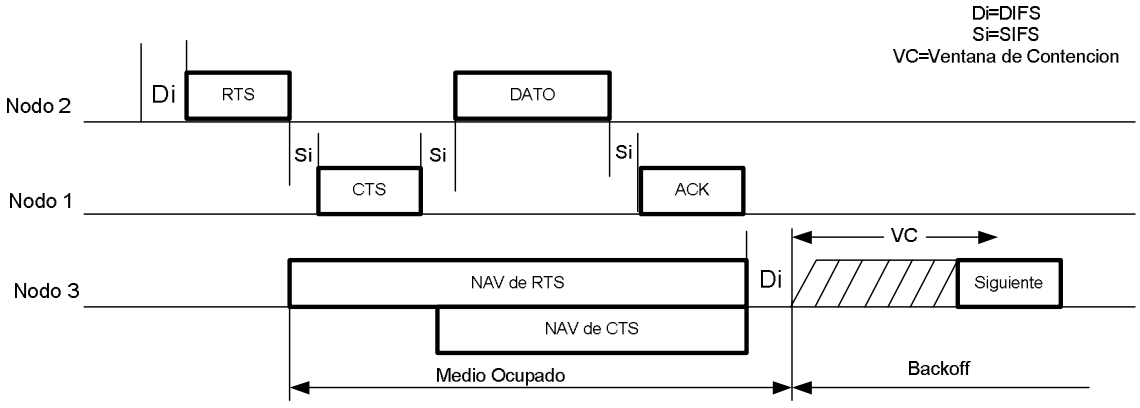


Figura 2. 16. Funcionamiento CSMA/CA con NAV.

En la figura 2.16 se muestra el funcionamiento CSMA/CA con NAV. El nodo 2 requiere comunicarse con el nodo 3, por tal motivo el nodo 2 envía una petición de envío RTS y todos los nodos que escuchan esta petición excepto el nodo destino reservan el medio el tiempo de duración según el campo de duración en RTS y el nodo 3 envía un CTS y todos los nodos que escuchen este mensaje reservan el medio el tiempo según la duración en CTS excepto el nodo fuente, que CTS es la señal que está libre el medio para que empiece a transmitir los datos, al finalizar el nodo destino envía un ACK certificando que el dato se envió correctamente, al finalizar esta trama se libera el medio y cualquier otro nodo puede empezar a transmitir de acuerdo al tiempo que se obtuvo aleatoriamente de la Ventana de Contención.

2.4. IMPLEMENTACIÓN EN UN DISPOSITIVO

Ya se tiene la teoría del establecimiento de una red, ahora es necesario conocer como se realiza físicamente. En este caso particular, se utiliza una computadora portátil con sistema operativo Windows XP, esta computadora cuenta con una tarjeta de red inalámbrica Atheros AR5005G y soporta modalidad Ad-Hoc e Infraestructura. El sistema operativo cuentan con una interfaz para poder realizar cambios en la tarjeta de red, ya que por default se encuentra habilitada la modalidad Infraestructura, por lo tanto es necesario habilitarla en modalidad ad-hoc. Este procedimiento se realiza de la siguiente manera:

Entrar en Panel de Control, hacer doble clic en Conexiones de Red, posteriormente ubicamos a la tarjeta de red inalámbrica y se le da un clic derecho para desplegar un menú emergente donde se selecciona la opción de Propiedades, como lo muestra la figura 2.17

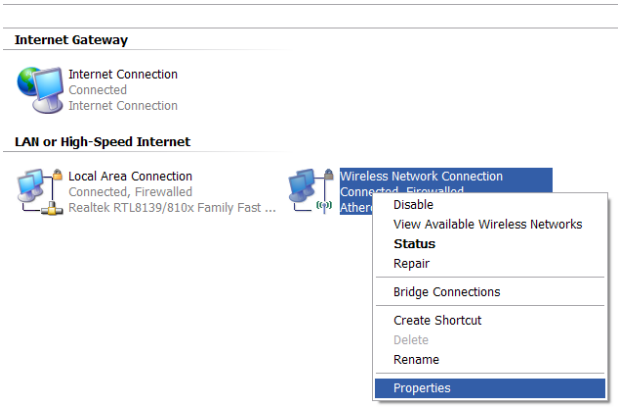


Figura 2. 17. Selección de propiedades de la tarjeta de red Inalambrica

Una vez que se le dio clic, se abre la ventana de propiedades de la tarjeta de red. Se ubica la pestaña Redes Inalámbricas y se le da clic en Avanzado, estos pasos se muestran en la figura 2.18 marcados en un recuadro rojo.

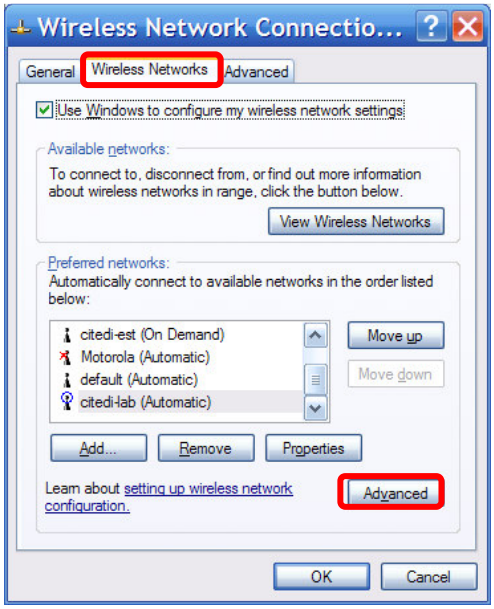


Figura 2. 18. Propiedades de la Tarjeta de Red.

Finalmente se selecciona la modalidad ad-hoc en las propiedades avanzadas, como se muestra en la figura 2.19.

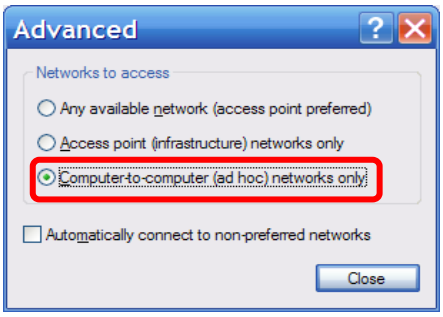


Figura 2. 19. Selección de modo Ad-Hoc

En este momento la computadora esta lista para acceder a una red ad-hoc sencilla a un solo salto, que no necesita alguna ruta, en cambio para el proceso de ruteo se explicará en los capítulos siguientes, primeramente se tendrá que familiarizar con el concepto de ruteo y sus algoritmos.

3

REDES INALÁMBRICAS AD-HOC

Las comunicaciones móviles e inalámbricas han tenido un crecimiento exponencial en los últimos años. Lo anterior se debe a que por un lado se han logrado avances en la microelectrónica, al mejor uso del conocimiento, utilización y aprovechamiento del espacio electromagnético, lo cual ha permitido el desarrollo de dispositivos portátiles de tamaño reducido. Además, la gran potencia de procesamiento y cómputo a extendido el uso de los mismos por parte de usuarios, que día a día requieren más capacidades y facilidades de comunicación y acceso a redes de datos.

La transmisión de datos a través del espectro de frecuencia está regulada por agencias gubernamentales. En México, la Secretaria de Comunicaciones y Transportes (SCT) es la encargada de regular estas frecuencias. Estas regulaciones controlan la banda de frecuencia y la potencia de transmisión que puede ser usada por la señal. Sin embargo, no se regulan el tipo de transmisión o la arquitectura de las redes inalámbricas y principalmente las de área local (WLAN).

En el ambiente de las WLAN, cada dispositivo que requiere comunicarse a través del aire tiene un adaptador WLAN. Este adaptador incluye una antena y proveen una interfaz entre el sistema operativo del dispositivo y las ondas electromagnéticas.

A continuación se describirá la arquitectura y topologías para las redes inalámbricas ad-hoc, así como las principales características de operación. También en este capítulo se presentan los algoritmos de ruteo más importantes que se utilizan para redes móviles ad-hoc.

3.1. ARQUITECTURA

Hablando del estándar 802.11 [25] [26] del IEEE, se distinguen dos tipos de configuraciones diferentes, en las que se utilizan puntos de acceso llamadas redes de de infraestructura y las redes ad-hoc que no cuentan con algún punto de coordinación.

La configuración más sencilla son las redes AD-HOC, en donde las terminales móviles se comunican directamente. La red se divide en celdas de servicio básico "BSS" (*Basic Service Set*), las cuales son zonas de cobertura alcanzadas por el dispositivo. Ya que la comunicación se realiza directamente, no se necesita ningún dispositivo que coordine las funciones de comunicación, las redes ad-hoc también son llamadas IBSS (*Independent BSS*). La única limitación es que la comunicación entre los dispositivos solo se hace mediante los dispositivos que se encuentran dentro de sus respectivas áreas de cobertura, así para comunicar dispositivos fuera del área de cobertura se requieren técnicas de ruteo. En la figura 3.1 se muestra la configuración ad-hoc para redes inalámbricas.

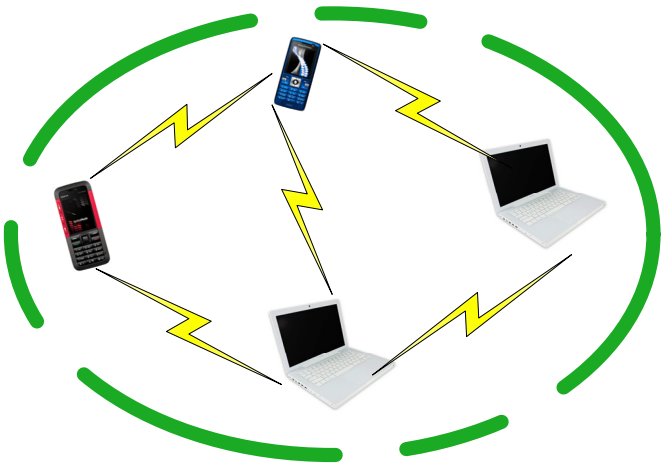


Figura 3. 1. Configuración Ad-Hoc.

La otra alternativa utiliza un dispositivo base que coordina la comunicación entre los dispositivos, este dispositivo base recibe el nombre de punto de acceso (AP, *Access Point*). Este tipo de redes, se les denomina como redes *de infraestructura*. Para formar una red en modalidad de infraestructura, requiere de una planificación muy cuidadosa y compleja, ya que los puntos de

acceso (AP) deben de distribuirse estratégicamente para evitar que algunas zonas se queden sin cobertura, evitar obstáculos para que todos los usuarios tengan cobertura. Un solo AP puede soportar un grupo de usuarios de 253 [27] y alcanzar un rango comprendido entre los 30m y varios cientos de metros [27], esto en función de las condiciones de propagación. En la figura 3.2 se muestra la topología de una red de infraestructura típica.

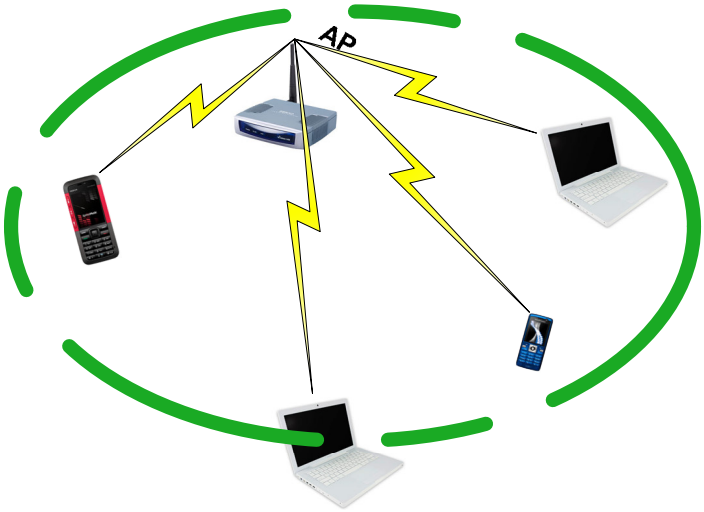


Figura 3. 2. Configuración de Infraestructura

La tabla 3.1 muestra un resumen donde se observa que existen dos posibles configuraciones para tener redes inalámbricas, Ad-Hoc y redes con Infraestructura.

Tabla 3. 1. Topología de redes inalámbricas.

Nombre	Descripción
Ad-Hoc	No se utiliza ningún AP centralizado; todas las comunicaciones son entre usuarios.
Infraestructura	Cuenta con un AP que es el agente de comunicación central para todos los usuarios.

Un factor importante en el desempeño de las redes en modalidad ad hoc es la movilidad, la cual determina cambios periódicos en las rutas establecidas entre fuente y destino conforme pasa el tiempo. Una ruta ya establecida, durante cierto período de tiempo, puede volverse inaccesible cuando los nodos que participan en la ruta establecida cambian de posición.

Algunas características que hacen interesante la conformación de redes ad-hoc, son la rapidez y facilidad con la que son instaladas y de su independencia de una infraestructura fija, lo cual en algunos casos resulta económicamente costoso instalar el cableado y equipo. Algunas áreas de aplicación de las redes ad-hoc se enlistan en la tabla 3.2.

Tabla 3. 2. Aplicaciones comunes de redes Ad-Hoc

ÁREA	EJEMPLOS
Ambientes Militares	Comunicación entre Soldados, Tanques, Aviones y Base en el campo de batalla.
Ambientes Civiles	Red de taxis, sala de reuniones, estadios deportivos, conferencias, botes.
Operaciones de Emergencia	Cuerpos de bomberos, policiacos, de búsqueda y rescate, desastres naturales.

3.2. CARÁCTERÍSTICAS DE OPERACIÓN

Una red que trabaja en configuración ad-hoc, posee condiciones de operación muy particulares en comparación con una red de datos convencional, e incluso, si se le compara también con una red inalámbrica de infraestructura. Una red ad-hoc tiene las siguientes características de operación:

a) Ambiente completamente similares: Todos los nodos poseen capacidades y responsabilidades idénticas. Todo nodo tiene la responsabilidad de participar en la transmisión de paquetes dentro de la red que pertenece, sirviendo como nodo base o punto de acceso al dirigir los paquetes e incluso descubrir nuevas rutas para la entrega más rápida o confiable de la información, contando a cambio con funciones recíprocas de los demás nodos de la red.

b) Capacidades asimétricas: Los rangos de transmisión y los radios en sí mismos pueden ser diferentes. Debido a que los equipos son móviles y poseen como fuente de energía una batería con capacidades limitadas, su tiempo de vida y carga puede variar entre los nodos, también su capacidad de procesamiento puede ser distinta. Finalmente, se debe de

considerar que la velocidad con la que se mueven los usuarios móviles varía constantemente.

c) Las características del tráfico puede ser diferente en las redes ad-hoc. Debido a las variaciones en la velocidad de transmisión, requerimientos de confiabilidad, transmisiones del tipo unicast y multicast.

d) Una red ad-hoc puede convivir con una red de infraestructura: Al realizar esta operación se le denomina red hibrida.

Como consecuencia, existen algunos factores que son determinantes en el funcionamiento de una red ad-hoc. Por ejemplo, en este tipo de red, los patrones de movilidad pueden ser diferentes dependiendo de la aplicación: personas esperando en una sala de un aeropuerto, grupo de personas en una cafetería, grupos de servicios de taxis en una ciudad, movimientos de personal militar o simplemente personas caminando en la calle. Por otro lado también varían la velocidad, dirección así como la falta de uniformidad de la movilidad entre diferentes nodos.

Trabajar con redes Ad-Hoc presenta algunos retos que se tienen que considerar para realizar un mejor análisis de ellas. Algunos de los retos a considerar son los siguientes:

1. Rango de transmisión inalámbrica limitada: El rango de transmisión es reducido, principalmente debido a que las unidades son móviles y utilizan baterías de tamaño pequeño, esto permite transmisiones de potencia baja. También podemos adjudicar esto a las regulaciones de la Unión Internacional de Telecomunicaciones (ITU) en todo el mundo, de la Comisión Federal de Comunicaciones (FCC) en los Estados Unidos de Norteamérica y de la Secretaría de Comunicaciones y Transportes (SCT) en México.

2. Naturaleza de multidifusión (broadcast) del medio: La transmisión es “escuchada” por todos los usuarios dentro del rango de transmisión, ocasionando algunos problemas llamados “terminal oculta” y “terminal expuesta”.

3. Pérdidas de paquetes debidas a errores en la transmisión: Colisiones, rupturas de ruta, entre otros eventos, ocasionan que se pierdan paquetes antes de llegar al nodo destino.

4. Cambios de ruta inducidos por la movilidad: El movimiento de los nodos, a cierta velocidad y con dirección aleatoria, ocasionan que aquellas rutas formadas para entregar paquetes entre dos nodos dejen de funcionar, por lo que resulta una topología muy dinámica.

La tabla 3.3 muestra en resumen las problemáticas a considerar en una red ad-hoc.

Tabla 3. 3. Problemática a resolver en una red Ad-Hoc

RETO
Radio de Transmisión limitado
Multidifusión
Errores de Transmisión
Cambio de Ruta

3.3. TERMINALES OCULTAS Y EXPUESTAS

Al utilizar redes inalámbricas ad-hoc se presentan principalmente dos problemas:

1. Terminal oculta: Como se muestra en la figura 3.3, debido a la distancia entre terminales y el alcance del radio de cada una, el nodo A puede enviar paquetes hacia B pero C no puede recibir los paquetes del nodo A, ocasionado por la atenuación que sufre la señal. Por tanto, el móvil C podría transmitir hacia el nodo B, sin detectar una posible transmisión simultánea del nodo A hacia el nodo B, ocasionando una Colisión.

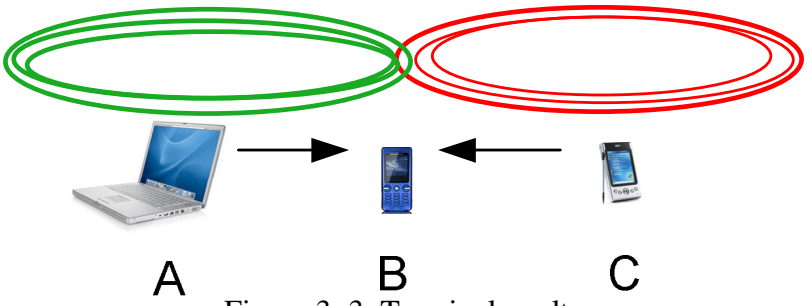


Figura 3. 3. Terminal oculta.

2. Terminal Expuesta: Para el caso que se muestra en la figura 3.4, la terminal B está transmitiendo a la terminal A y por su parte C transmite a D. Al dar lugar las transmisiones simultáneamente, C puede detectar que el canal está ocupado y por tanto debe esperar a su liberación. Sin embargo, A está fuera del alcance de C por lo que es innecesario la espera, ocasionando una detección incorrecta del canal.

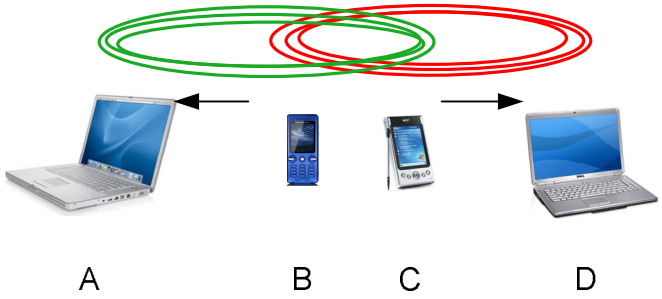


Figura 3. 4. Terminal expuesta.

La solución de algunos de estos problemas se resuelven con la transmisión de mensajes de petición de envío y libre para enviar, que se vieron en el capítulo 2.

3.4. ALGORITMOS DE RUTEO

El ruteo en redes inalámbricas ad-hoc es en muchos aspectos diferentes al enrutamiento en redes cableadas convencionales, debido principalmente a la movilidad de los nodos.

Para redes móviles Ad-Hoc, el ruteo de paquetes entre un par de nodos se convierte en gran reto porque los nodos pueden moverse aleatoriamente dentro de la red. Una trayectoria que consideremos óptima en un punto y momento dado puede no funcionar en pocos momentos después.

Muchos protocolos de enrutamiento se han propuesto para este tipo de redes en particular, algunos inventados específicamente para redes ad hoc y otros adaptados a partir de protocolos existentes en redes cableadas.

En general los protocolos de ruteo se pueden clasificar de la siguiente manera: Protocolos Proactivos, son aquellos donde los nodos mantienen rutas establecidas para cada destino de la red, Protocolos Reactivos son aquellos en donde la ruta para un destino se crea en el tránsito de los mensajes y los Protocolos Híbridos son la combinación de ambos, teniendo rutas establecidas y rutas que se están encontrando al momento del tránsito de los mensajes.

Ejemplos de los protocolos proactivos son el protocolo DSDV (*Destination-Sequenced Distance-Vector Routing*) y OLSR (*Optimized Link State Routing*). Los ejemplos para los reactivos o Sobre Demanda es DSR (*Dynamic Source Routing*) y AODV (*Ad hoc On-Demand Distance Vector*). El protocolo ZRP (*Zone Routing Protocol*) y el protocolo TORA (*Temporally Ordered. Routing Algorithm*) son ejemplos de los híbridos.

La figura 3.5 muestra una diagrama que podemos visualizar mejor los protocolos de enrutamiento así como algunos ejemplos de ellos.

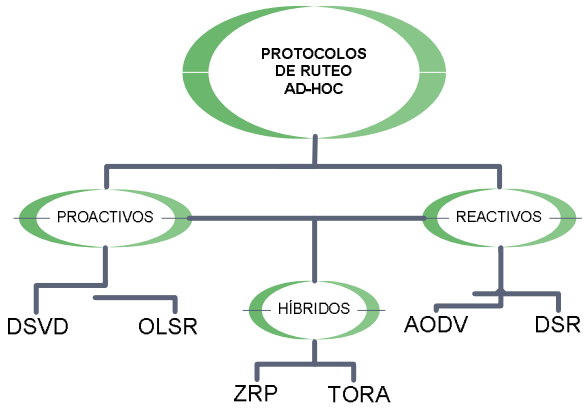


Figura 3. 5. Algunos protocolos de ruteo.

3.4.1. Protocolos proactivos

En los protocolos de ruteo proactivos, la información de ruteo para buscar todos los demás nodos en la red siempre es mantenida en cada nodo. Cuando la topología de la red cambia por ejemplo, nodos existentes se mueven, algunas nuevas conexiones son creadas o existe alguna que se haya caído, tales cambios en los enlaces son anunciados a todos los nodos de la red.

Si el protocolo proactivo es usado un problema que surge de inmediato es que los cambios rápidos en la topología de la red pueden inundar la red con mensajes de control (mensajes para actualizar la tabla de ruteo en cada nodo) y el exceso de mensajes de control pueden comprometer el rendimiento de procesamiento de las transmisiones de los datos.

DSDV

Este algoritmo está basado en el algoritmo Vector de Distancia [28], donde vector hace referencia a una Dirección y distancia a una longitud [29].

La tabla de ruteo en el protocolo DSDV [30] [31] [32] está compuesta por cuatro elementos: Destino, dirección del nodo destino, Siguiente Salto, dirección del nodo siguiente, Métrica, la métrica puede ser la cantidad de saltos, el retardo en mseg o el número total de paquetes enviados por la trayectoria seleccionada [1]. Y por último el Número de Secuencia, esta se utiliza para definir qué tan nuevo es el mensaje, a mayor número de secuencia será más nuevo el mensaje. En general, procedimientos de su funcionamiento consta de 2 procesos básicos, Actualizar Ruta y Seleccionar Ruta, los cuales siempre se están realizando [33].

La actualización de ruta inicia con el descubrimiento de nodos vecinos a 1 salto, después, intercambia las tablas de ruteo con su nodo vecino, así obtendrá las direcciones de sus vecinos a 2 saltos, al siguiente intercambio de tablas se conocerán los vecinos a 3 saltos, y así sucesivamente hasta conocer toda la red. Cada vez que se conozca un nuevo destino, se incrementa en 2 el número de secuencia de ese nodo. Si llega un momento en que no se alcanza a ese nodo, se incrementa en una unidad y la métrica se establece a ∞. Cada cambio en la tabla es difundido a través de la red.

La selección de una ruta se realiza checando en su tabla de ruteo, si la métrica del destino es diferente a ∞. De ser verdadera esta condición, selecciona un puerto para empezar a transmitir. En el caso de que existan dos rutas hacia el destino, primero selecciona la ruta que tenga mayor número de secuencia y empieza a transmitir. En el caso de tener el mismo número de secuencia, selecciona aquella ruta donde la métrica es mejor, en el caso de saltos, la métrica con menor valor es la que se selecciona.

El funcionamiento del algoritmo se muestra mediante un diagrama a flujo en la figura 3.6:

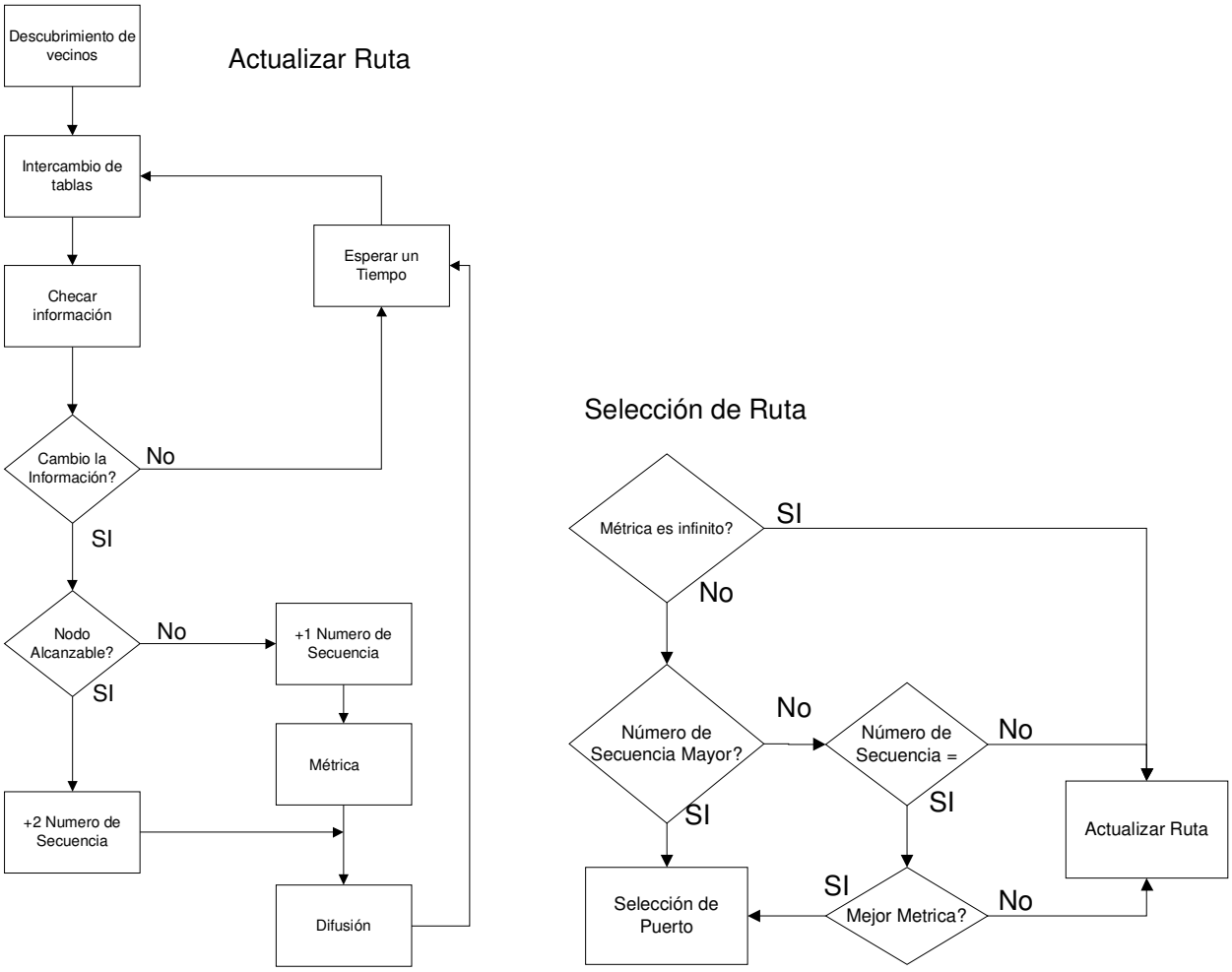


Figura 3. 6. Diagrama de flujo del algoritmo DSDV.

OLSR

Este algoritmo de Estado de Enlace Optimizado (Optimized Link Sate Routing) [34] se basa en el intercambio periódico de mensajes para actualizar la información topológica de cada nodo en la red. Contiene 4 elementos generales: descubrimiento de vecinos a uno y dos saltos, selección de retransmisores de multipuntos (MPR) [35], descubrimiento de la red y cálculo de ruta.

Un diagrama a bloques del algoritmo se presenta en la figura 3.7:

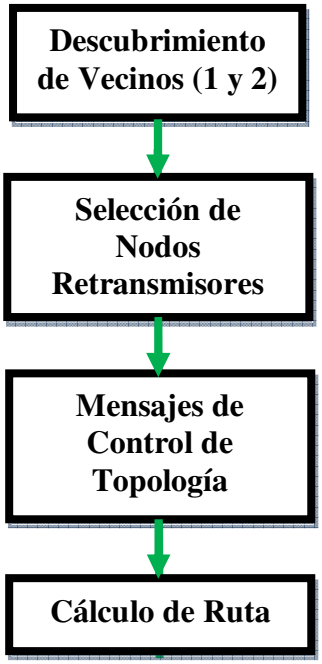


Figura 3. 7. Diagrama a bloques de OLSR.

La descripción detallada del protocolo OLSR se deja para ser abordada en el capítulo 4.

3.4.2. Protocolos reactivos

Este tipo de protocolos descubren una ruta solo cuando ocurre una transmisión de datos. Cuando un nodo quiere mandar información a otro nodo de la red, el nodo fuente inicia el proceso de búsqueda de la ruta. Una vez que la ruta es descubierta, es mantenida en un archivo temporal en

el nodo fuente a menos que expire o algún evento ocurra (por ejemplo, un enlace caído) que requiera de otra búsqueda de ruta empezará del principio.

Los protocolos de ruteo Reactivos requieren mínima información de ruteo de cada nodo, comparada con el protocolo proactivo, aquí no es necesario obtener ni mantener información de ruteo para todos los nodos en la red.

Una obvia desventaja es los protocolos reactivos es el tiempo que tarda en descubrir una ruta, llamado retraso de adquisición de ruta. Actualmente los protocolos reactivos más populares son el protocolo DSR (ruteo de fuente dinámica) y AODV (vector distancia sobre demanda ad hoc).

DSR

DSR [29] es un protocolo de ruteo que inicia en la fuente [30] [32] lo que quiere decir es que una secuencia completa de nodos intermedios desde la fuente hasta el destino es determinada por el nodo fuente y todos los paquetes transmitidos por la fuente hasta el destino siguen la misma trayectoria. El funcionamiento del protocolo realiza dos mecanismos importantes, Descubrimiento de ruta y Mantenimiento de ruta [36].

El procedimiento de descubrimiento de ruta inicia en la fuente buscando el destino en memoria, si encontró al destino empieza a transmitir de otra manera difunde un paquete de petición de ruta (RRP- *Route Request Paquet*). El nodo que recibe el RRP compara con el destino para saber si ya se ha alcanzado, de ser así se agrega la dirección en una tabla de ruta aprendida y se envía a la fuente. De otra manera agrega la dirección a la tabla de ruta aprendida y se compara para evitar nodos repetidos. Si ya existe el nodo, se aborta el procedimiento y si no existe el nodo se transmite nuevamente el RRP. Este procedimiento se realiza hasta alcanzar al nodo destino. Una vez llegada la ruta aprendida al nodo fuente, este comienza a transmitir a través de la ruta aprendida.

El mantenimiento de ruta se realiza desde que se envía el primer dato. Este funciona esperando una contestación de recibido (ACK) para poder transmitir el siguiente dato. En el caso de que no se haya recibido un ACK el nodo que envía el dato borra de la memoria al nodo que no contesto, asumiendo que se ha caído el enlace. Inmediatamente después se envía un mensaje de error para anunciar a la fuente que hay un error en la ruta para que ya no envíe datos. Por el paso del mensaje de error se borra de la memoria el nodo caído hasta llegar a la fuente. En este caso la fuente decide si quiere reiniciar el descubrimiento de ruta o abortar la transmisión.

El diagrama de flujo de la figura 3.8 representa el funcionamiento del procedimiento de descubrimiento de ruta y el mantenimiento de ruta.

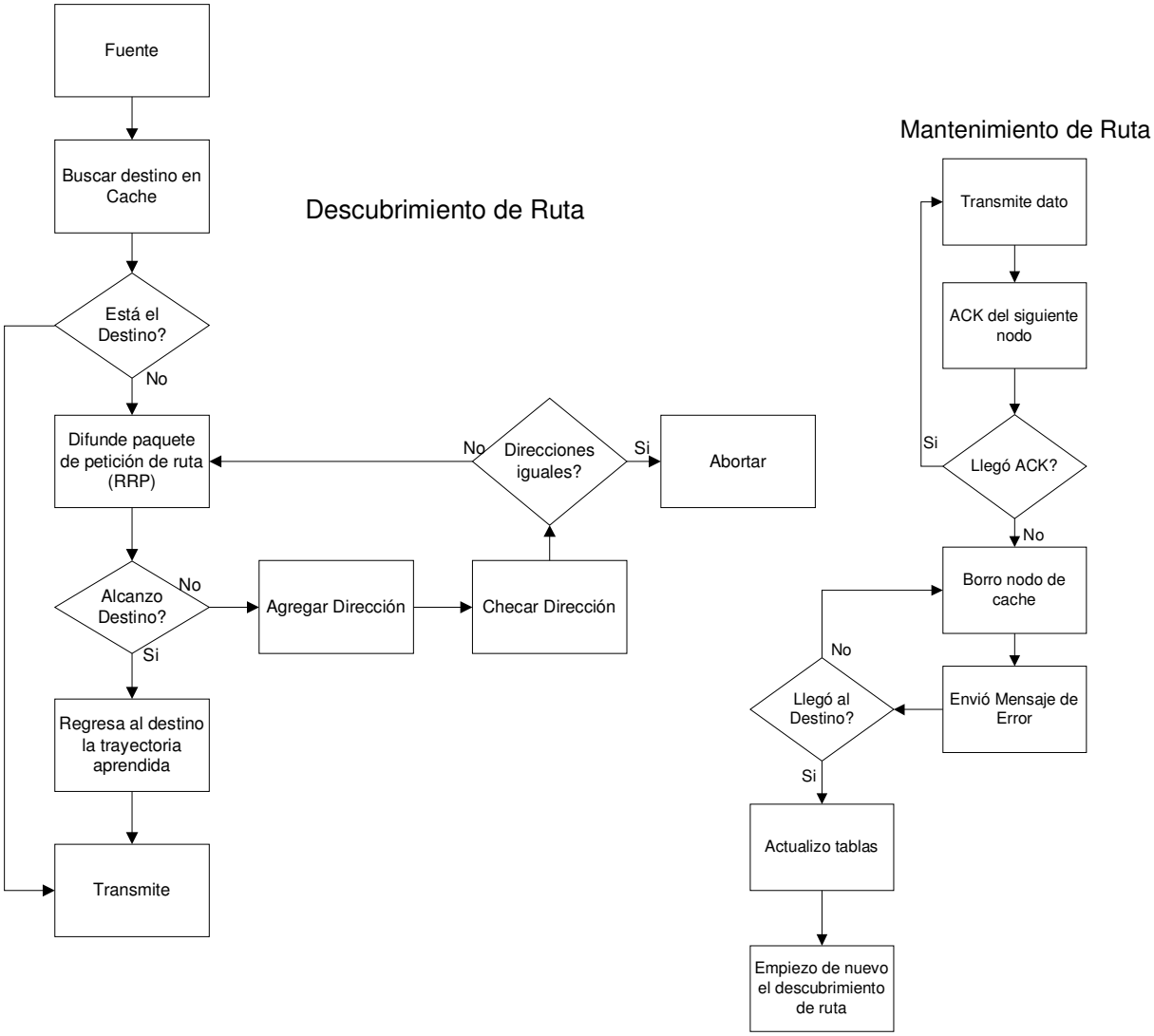


Figura 3. 8. Diagrama de flujo del algoritmo DSR

Una ventaja obvia de DSR es que los nodos fuentes son enterados de la existencia de trayectorias alternas, que implica que se recupere fácil y rápidamente de un enlace que haya fallado. Otra ventaja es que no tiene oportunidad de un lazo de ruteo (o es fácil de detectar y evitar uno). Además, los nodos no tienen que mantener una tabla de ruteo.

La desventaja en DSR es el largo retardo de adquisición de ruteo debido al descubrimiento de ruta. Un retardo de adquisición largo puede no ser aceptable en algunas situaciones, como comunicaciones móviles en el campo de batalla. Otra desventaja es que el paquete puede también causar baja utilización de carga útil, ya que cada paquete tiene que contener una lista de todas las rutas intermedias para llegar a un destino.

AODV

Este protocolo se compone de dos mecanismos básicos, Descubrimiento de ruta y el Mantenimiento de ruta. Para su funcionamiento se utilizan tres tipos de mensajes RREQ (mensaje de petición de ruta), RREP (mensaje de contestación de ruta) y el RERR (mensaje de error) [36].

Cuando un nodo fuente quiere mandar información a un nodo destino, primero busca en su tabla de ruteo si existe una comunicación previa, antes del Periodo de Borrado (DELETE_PERIOD), este tiempo está dado por la ecuación 4 y permite establecer el tiempo máximo que el nodo guarda en memoria la información. Si la comunicación no existe, el nodo fuente transmite un mensaje de petición de ruta (RREQ) que contiene la siguiente información: Tipo de Mensaje, Dirección IP de la fuente, Dirección IP destino, número secuencial de respuesta del destino (*Destination Sequence Number*), identificador (ID) del mensaje (*RREQ ID*) y conteo de saltos (*Hop Count*).

$$DELETE\_PERIOD = K + \max(ACTIVE\_ROUTE\_TIMEOUT, HELLO\_INTERVAL) \quad \text{Ec. 4}$$

donde K=5, ACTIVE_ROUTE_TIMEOUT es el tiempo que una ruta esta activa = 3,000 milisegundos y HELLO_INTERVAL es el intervalo de mensajes HELLO = 1,000 milisegundo.

El tipo de mensaje distingue entre los tres tipos de mensajes, Petición de Ruta (RREQ), Contestación de Ruta (RREP) y Error de Ruta (RERR) y sus valores son 1, 2 y 3 respectivamente asignados por la *Internet Assigned Numbers Authority* (IANA) [37]. La dirección IP de la fuente es el número que asigna el Protocolo de Internet (IP) cuyo valor pertenece al nodo que origina el mensaje. La dirección IP destino es el número asignado por IP asociado al nodo destino. El *Destination Sequence Number* es el número consecutivo de respuesta del destino a una misma fuente, permitiendo a la fuente saber si el mensaje llegó a su destino y que puede transmitir el siguiente mensaje. El RREQ ID es el número que permite distinguir entre dos mensajes diferentes enviados por una misma fuente.

Durante el tránsito del RREQ cada nodo intermedio incrementa en uno el número de saltos. Además modifica las tablas de los nodos, estas tablas son llenadas con información recolectada por el estándar 802.11 en modalidad Ad-Hoc una de ellas relacionada con las IP de los vecinos (aquellos nodos que se encuentran en el área de cobertura) también almacena la información del campo TTL de la cabecera IP. En esta tabla se encuentra también información que lleva el mensaje como es el tipo de mensaje, IP de la fuente, IP del Destino y RREQ ID.

Cuando el mensaje RREQ llega al destino, éste incrementa el valor *Destination Sequence Number* y estructura un mensaje RREP con la información mencionada anteriormente, agregando la dirección IP del Receptor en la trama del 802.11 que equivale a la dirección IP del transmisor almacenada al momento del paso del mensaje RREQ. Almacenándose en las tablas las direcciones IP de los nodos transmisores de ida (RREQ) y direcciones IP de los nodos transmisores de vuelta (RREP). El mensaje RREP llega hasta el nodo fuente y comienza a enviar la información almacenada en memoria temporalmente.

Cuando el nodo detecta que algún nodo vecino, que involucre la utilización de la ruta, sale fuera del área de cobertura emite un mensaje de error (RERR), este mensaje se transmite para que llegue hacia el destino por un lado y hacia la fuente por el otro lado, la finalidad de enviarlo al

destino es para restablecer el número de secuencia de respuestas y a la fuente le sirve para buscar otra ruta enviando un RREQ nuevo.

Un diagrama a bloques del funcionamiento de los mecanismos que utiliza AODV se muestra en la figura 3.9.

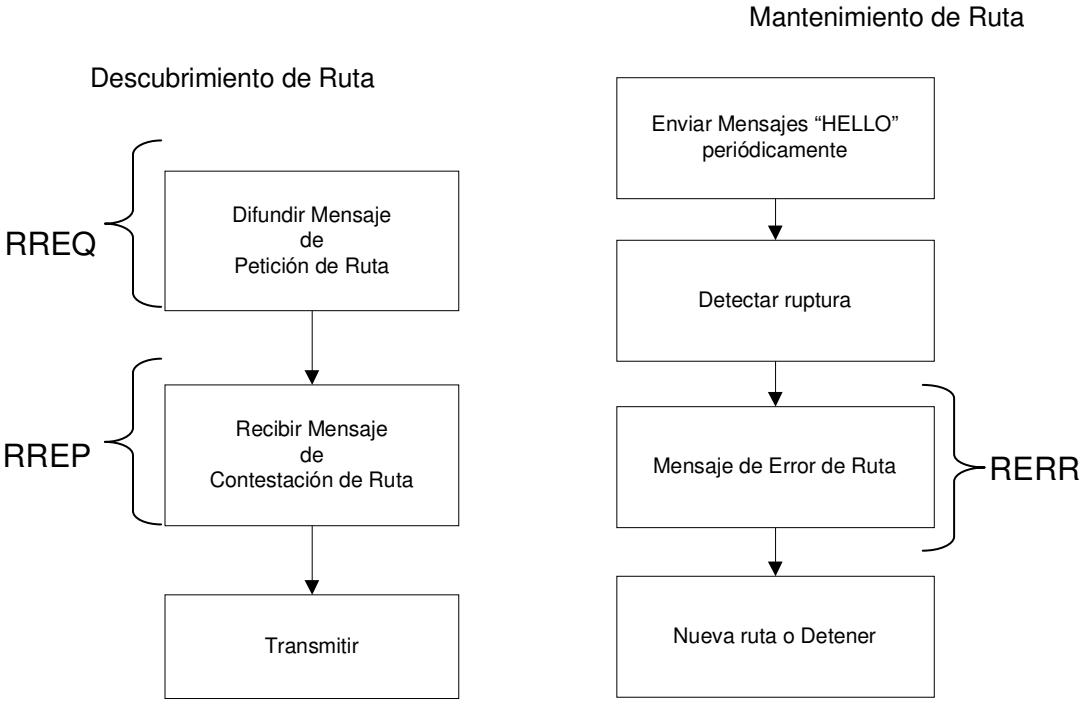


Figura 3. 9. Diagrama a bloques de AODV

En el capítulo 5 se detalla el funcionamiento del algoritmo AODV así como el formato de los mensajes.

3.4.3. Protocolos Híbridos

Un protocolo reactivo puro no es la mejor solución para ruteo en redes Ad Hoc Móviles (MANET), debido al descubrimiento de ruta y el alto control de overhead. Por el otro lado, un protocolo proactivo puro usado para una red grande puede no ser factible por la necesidad de mantener una larga tabla de ruteo todo el tiempo. Un protocolo que usa las mejores características de ambos protocolos, reactivo y proactivo, puede ser la mejor solución. Un

ejemplo es el protocolo de ruteo de zona (ZRP) [28]. Otro protocolo hibrido es el TORA (Algoritmo de Ruteo Temporalmente Ordenado) [38].

ZRP

El protocolo ZRP [28] es un hibrido que la característica principal es que utiliza el concepto de divide y vencerás, ya que divide la red en zonas como lo muestra la figura 3.10, utilizando dos tipos de protocolos para comunicarse entre los nodos [28]. El protocolo IARP (IntrA-zone Routing Protocol) es utilizado para buscar destinos dentro de una zona [30]. El protocolo IERP (IntEr-zone Routing Protocol) se utiliza para comunicarse entre diferentes zonas [31]. El uso recomendado es que un protocolo IARP sea proactivo mientras que para salir de la zona se haga sobre demanda [32].

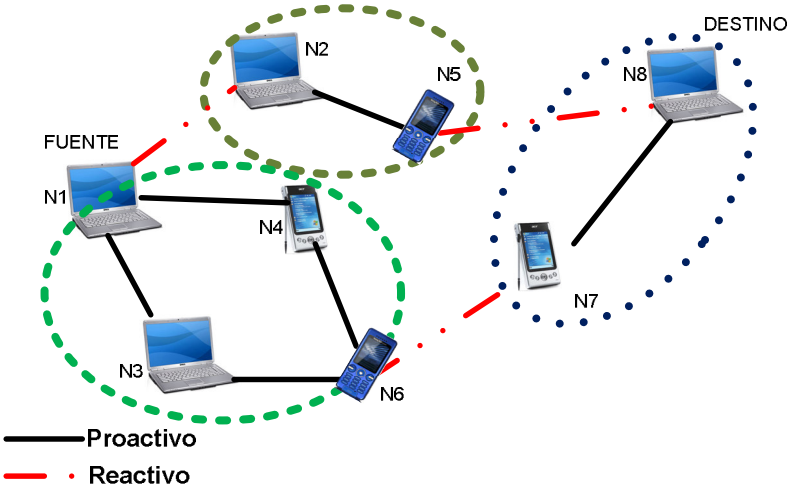


Figura 3. 10. División de la red en zonas.

La zona de ruteo tiene un radio ρ expresado en saltos. Los nodos que incluyen esta zona es tiene un máximo de ρ saltos. Por ejemplo en la figura 3.11 definimos un nodo fuente como S donde su radio de ruteo es 2 y todos los nodos desde *A* hasta *I* excepto *K* están dentro de la zona de ruteo. Dentro de esta zona, los nodos se dividen en nodos bordes y nodos interiores donde los nodos bordes son aquellos que están exactamente igual a ρ saltos. Mientras que los nodos interiores son aquellos que su distancia es menor que ρ saltos.

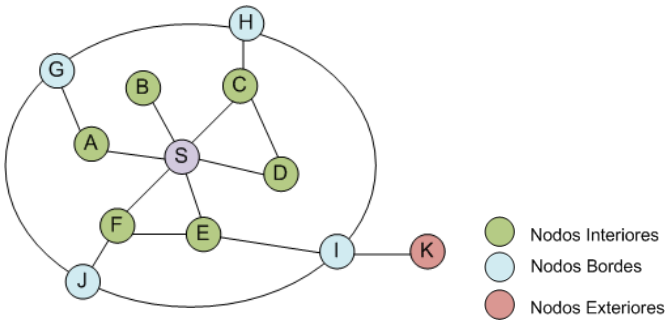


Figura 3. 11.Ejemplo de ZRP.

Básicamente realiza dos mecanismos muy parecidos a los ya vistos, Descubrimiento de ruta y mantenimiento de ruta. Un diagrama a bloques de su funcionamiento es el mostrado en la figura 3.12.

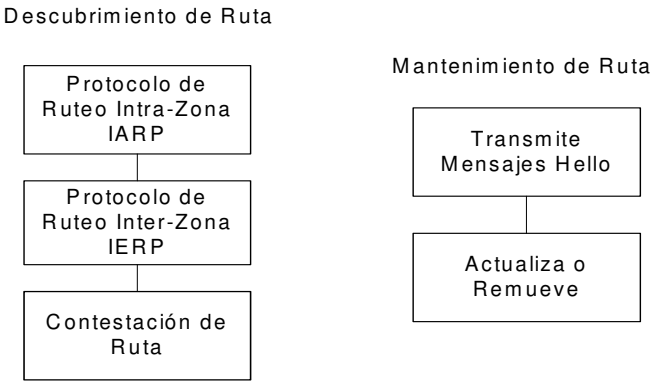


Figura 3. 12. Diagrama a bloques de ZRP.

El descubrimiento de ruta depende de que algoritmo proactivo y reactivo se está utilizando para IARP e IERP respectivamente. Al tener un algoritmo proactivo en IARP se conocen todos los posibles destinos de la zona y la comunicación se da al instante. Por otro lado si el destino no se encuentra en la lista de IARP, utiliza una petición de ruta en los nodos que están en el borde de la zona. Estos buscan en su tabla IARP y si no se encuentra el destino, se reenvía a los otros nodos bordes de la otra zona hasta llegar al nodo destino.

TORA

La característica principal de este algoritmo es que ordena temporalmente la red de acuerdo a pesos específicos que les son asignados por el nodo fuente mientras realiza la ruta [38]. Los

mecanismos en los que se compone este protocolo es en Creación de Ruta, Mantenimiento de Ruta y Borrado de ruta [29]. Para esto se utilizan los mensajes de petición "QRY", de actualización "UPD" y el de borrado "CLR" [30]. El diagrama a bloques del descubrimiento, mantenimiento y borrado de rutas se muestra en la figura 3.13.

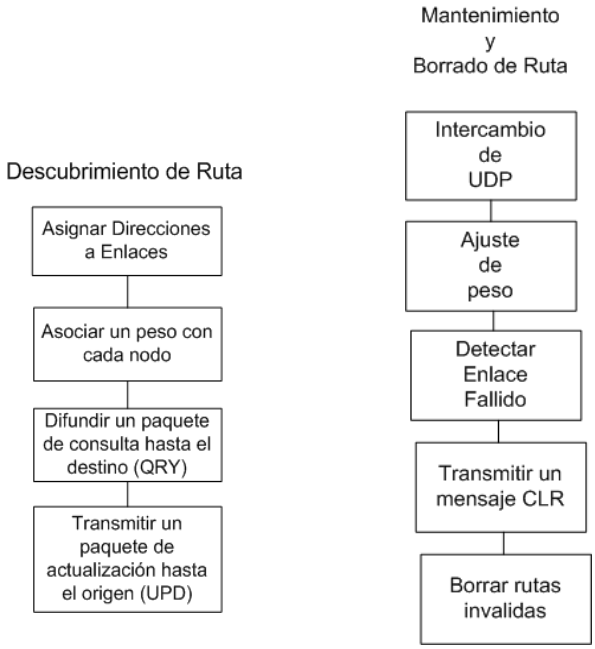


Figura 3. 13. Diagrama a bloques de TORA

En este capítulo se introdujo a las redes inalámbricas ad-hoc, presentando la topología característica, las características de operación, el problema de la terminal oculta y la terminal expuesta así como también se presentó una explicación de los algoritmos de ruteo que se utilizan para este tipo de redes clasificados en proactivos, reactivos e híbridos.

Se presentaron 6 algoritmos (2 proactivos, 2 reactivos y 2 hibrido) de los cuales 2 algoritmos (1 algoritmo proactivo y 1 algoritmo reactivo) se explicarán ampliamente en los capítulos 4 y 5, comenzando con el algoritmo proactivo de estado de enlace optimizado (OLSR).

4

ALGORITMO DE ESTADO DE ENLACE OPTIMIZADO (OLSR)

El algoritmo de ruteo de Estado de Enlace Optimizado (OLSR, Optimized Link State Routing) [34], pertenece a la clasificación de algoritmos de ruteo proactivos. Como un protocolo proactivo este cuenta con las rutas hacia todos los posibles destinos de la red [39], caso contrario a los protocolos reactivos específicamente a AODV donde la ruta se va descubriendo de acuerdo a las necesidades de comunicación de los nodos [40].

En este capítulo se muestra el funcionamiento del algoritmo OLSR, el formato de los paquetes y su transmisión a través de la red. Se eligió el algoritmo OLSR por ser un algoritmo proactivo y realizar una comparación posterior con un algoritmo reactivo. Además, utiliza la técnica de puntos de retransmisión, lo que evita que la red se congestione con una gran cantidad de datos, aprovechando al máximo el ancho de banda asignada.

4.1. FUNCIONAMIENTO

El algoritmo OLSR puede funcionar de dos maneras: de núcleo y auxiliares. Dentro de las funciones de núcleo se encuentra el formato y reenvío de paquete, la información en las tablas, los mensajes Hello, el sensado de enlace, detección de vecinos, descubrimiento de Topología y cálculo de las tablas de ruteo. Y en las funciones auxiliares se encuentran las interfaces que no son OLSR, la notificación de la capa de enlace, el sensado de enlace avanzado, redundancia de

topología y redundancia de inundación de retransmisores de multipunto (MPR). Este trabajo solo se enfoca a las funciones núcleo.

El procedimiento de descubrimiento de rutas se basa en el descubrimiento de vecinos a uno y dos saltos, selección de retransmisores de multipuntos (MPR) [35], descubrimiento de la red y cálculo de ruta.

El procedimiento de descubrimiento de vecinos se lleva a cabo mediante la difusión de mensajes de inicio HELLO. Los mensajes de inicio son generados por cada nodo de la red, limitados a un salto. Estos mensajes contienen el estado del enlace con el nodo. Este se caracteriza por 4 estados: simétrico, asimétrico, perdido y el estado de retransmisor (MPR). Mediante el procedimiento de mensajes HELLO, es posible el descubrimiento de vecinos a un salto, al igual que vecinos a dos saltos. Esta información permite seleccionar al nodo retransmisor (MPR) el cual se rectifica o se agregan otros retransmisores dependiendo de los mensajes HELLO.

El proceso para seleccionar los nodos de retransmisión inicia con un conjunto vacio de retransmisores (MPR), después se seleccionan aquellos nodos en el conjunto de vecinos a un salto, que proporcionen el único camino de comunicación con el nodo vecino a 2-saltos. Estos nodos de un salto se van agregando al conjunto de retransmisores (MPR). Mientras existan nodos en el conjunto de vecinos de 2-saltos se calcula el número de nodos de 2-saltos para cada nodo vecino de un salto, el nodo de un salto que cubra más nodos de 2-saltos se agregara a la lista de retransmisores (MPR), se eliminarán las direcciones de los vecinos que ya han sido utilizadas.

Una vez seleccionados los nodos retransmisores, cada uno de ellos, y solo ellos, transmiten y retransmiten mensajes de Control de Topología (TC) para descubrir la red [41]. La información asociada con este mensaje es la tabla de nodos vecinos que seleccionaron a dicho retransmisor por el cual se está enviando el mensaje.

Cuando llega un mensaje de control de topología (TC) a un nodo de la red, permite conocer al nodo retransmisor y a los nodos vecinos asociados a éste. Así la información guardada en cada

nodo es la dirección IP del nodo Retransmisor y la dirección IP del nodo vecino correspondiente, etiquetado de la siguiente manera:

T_Dest_Addr = Dirección IP del Vecino
T_Last_Addr = Dirección IP del MPR transmisor

En el procedimiento para calcular las tablas de ruteo, se emplea información contenida en la lista de vecinos y de la topología, la tabla de ruteo se actualiza cuando detecta algún cambio en los mensajes Hello o en los mensajes de control de topología. El procedimiento para el cálculo de la ruta inicia agregando nuevas entradas identificando a los vecinos a un salto y se registran de la siguiente forma:

R_Dest_Addr = Dirección IP del Nodo Vecino
R_Next_Addr = Dirección IP del Nodo Vecino
R_Dist = 1
R_Iface_Addr = Dirección de la Interfaz Local

El segundo proceso es la detección de los vecinos a 2 saltos y se registran de la misma forma con los parámetros adecuados e incrementando el valor de la distancia en *R_Dist* = 2, como se muestra a continuación:

R_Dest_Addr = Dirección IP del Nodo Vecino a 2-Saltos
R_Next_Addr = Dirección IP del Nodo Vecino
R_Dist = 2
R_Iface_Addr =R_Next_Addr

Una vez que no hay vecinos a 2 saltos, se crean las rutas para aquellos vecinos que están a una distancia ***R_Dist > h*** saltos, donde el valor de ***h*** inicial es 2. Si no existe una ruta creada en los pasos anteriores para algún nodo faltante y si la dirección de un nodo retransmisor (*T_Last_Addr*) corresponde a una entrada en la tabla de ruteo creada anteriormente donde ***R_Dist*** es igual a ***h***, entonces se crea una nueva entrada donde:

R_Dest_Addr = T_Dest_Addr
R_Next_Addr = R_Next_addr del T_Last_Addr
R_Dist = h + 1

$$R\_Iface\_Addr = T\_Last\_Addr$$

Se incrementará ***h*** ya que no exista alguna iteración que corresponda con lo especificado anteriormente. Una vez que se incrementa ***h*** se realiza el paso anterior hasta que no existan más nodos destinos que agregar.

4.2. FORMATO DE PAQUETES

Todo el tráfico se envía en paquetes. Estos paquetes están formados por un encabezado de algoritmo, un encabezado de mensaje y el mensaje. Gracias al encabezado de mensaje un paquete puede contener diferentes tipos de mensajes. La estructura básica de un paquete OLSR se muestra en la figura 4.1.

Figura 4. 1. Formato general de un Paquete OLSR.

Algunos de los campos más importantes son: *Tipo de Mensaje* define el tipo de mensaje que se envía y puede ser mensajes de Inicialización (Hello) y mensajes de Topología (TC). *Tiempo Valido* indica cuanto tiempo después de la recepción, un nodo puede considerar la información como válida, a menos que una actualización se reciba y se representa por la ecuación 5.

$$Tiempo\ Valido = C \times \left(1 + \frac{a}{16}\right) \times 2^b \text{ Segundos} \qquad \text{Ec. 5}$$

Donde *a* representa los 4 bits más significativos del campo de 8 bits de *Tiempo Valido*, *b* representa los 4 bits menos significativos del campo de 8 bits de *Tiempo Valido* y *C* un valor constante de 1/16 segundos (0.0625 segundos).

El *Tamaño del mensaje* se utiliza para definir el tamaño del mensaje en bytes y se mide desde el inicio del campo "Tipo de Mensaje" hasta el inicio del siguiente campo "Tipo de Mensaje" o si no existen más mensajes, hasta el fin del paquete. Y el campo del *Mensaje* que se conforma de los formatos de cada mensaje.

4.2.1. Formato de Iniciación (HELLO).

El formato del mensaje HELLO está formado por los campos del paquete general de la figura 4.1, además el campo *Tiempo de Iniciación* el cual define el intervalo de emisión entre mensajes de iniciación (HELLO), el valor recomendado es de 2 y se obtiene igual que *Tiempo Valido* por la ecuación 5.

También contiene el campo de *Disponibilidad* que indica la disponibilidad que tiene un nodo para reenviar tráfico a otros nodos, los parámetros que puede tomar son 5 diferentes (Nunca, Poca, Inicial, Alta y Siempre). El campo *Código de Enlace* especifica el tipo de enlace y tipo de vecino que tiene con el nodo vecino que se agrega a la lista. Los valores que puede tomar el tipo de vecino son 3 (Sin Vecino, Vecino de Retransmisión, Vecino Simétrico) y los valores que puede tomar el tipo de enlace son 4 (Inespecífico, Asimétrico, Simétrico y Perdido). También cuenta con el campo de *Dirección de la interfaz* del nodo vecino, donde se almacenan las dirección IP de los nodos vecinos.

"Simétrico" se refiere a que la conexión a ese nodo vecino, fue comprobada para tener una comunicación bi-direccional. En el caso de "Asimétrico" esto indica que se ha recibido un mensaje HELLO de un nodo, sin embargo, no se ha confirmado que este pueda recibir mensajes.

4.2.2. Formato del Mensaje de Control de Topología (TC).

El formato del mensaje de control de topología (TC) está formado por los campos obligatorios de la figura 4.1, agregando el campo *Advertised Neighbor Sequence Number (ANSN)* donde se define el número de secuencia asociado con los vecinos que seleccionaron a este retransmisor. Además contiene el campo de *Direcciones de Selectores del MPR* que contiene la o las direcciones de los nodos que conforma la lista de los nodos selectores del nodo retransmisor.

4.2.3. Parámetros Configurables

En esta sección se describen los valores sugeridos de los parámetros más comunes como los tiempos de intervalos de Inicio (Hello) y los de control de topología (TC) de acuerdo al RFC 3626 [34].

En la tabla 4.1 se muestran los valores para los intervalos de emisión.

Tabla 4. 1. Valores para intervalos de emisión

Descripción	Valor
HELLO_INTERVALO	2 Segundos
REFRESH_INTERVALO	2 Segundos
TC_INTERVALO	5 Segundos
MID_INTERVALO	TC_INTERVALO

Los valores de tiempos de retención se muestran en la tabla 4.2

Tabla 4. 2. Tiempos de retención.

Descripción	Valor
NEIGHB_HOLD_TIME	3 X REFRESH_INTERVALO
TOP_HOLD_TIME	3 X TC_INTERVALO
DUP_HOLD_TIME	30 Segundos
MID_HOLD_TIME	3 X MID_INTERVALO

En la tabla 4.3 se muestran los valores para los tipos de mensajes.

Tabla 4. 3. Tipos de Mensajes.

Descripción	Valor
HELLO_MESSAGE	1
TC_MESSAGE	2
MID_MESSAGE	3
HNA_MESSAGE	4

Los tipos de enlaces se muestran en la tabla 4.4

Tabla 4. 4. Valores para tipos de enlaces.

Descripción	Valor
ENLACE_SIN_ESPECIFICAR	0
ENLACE_ASYM	1
ENLACE_SYM	2
ENLACE_PERDIDO	3

En la tabla 4.5 se muestran los valores para los tipos de vecinos.

Tabla 4. 5. Valores para los tipos de Vecinos.

Descripción	Valor
NINGUN_NODO	0
NODO_SYM	1
NODO_MPR	2

Los valores para los parámetros de disponibilidad se muestran en la tabla 4.6

Tabla 4. 6. Valores para disponibilidad.

Descripción	Valor
WILL_NUNCA	0
WILL_POCA	1
WILL_DEFAULT	3
WILL_ALTA	6
WILL_SIEMPRE	7

4.3. DISEÑO DE TOPOLOGÍA

Se diseñó la topología de la figura 4.2 con el fin de potencializar al algoritmo y conocer todas las posibilidades en la obtención de las tablas de ruteo, en la figura se observa que las líneas representan la conexión inalámbrica [77]. Al ser un algoritmo proactivo, no se requiere de tener una comunicación entre un par de nodos para crear las rutas, las rutas se crean aun y cuando no sean necesarias en ese momento. El análisis se centra en la obtención de las tablas de ruteo en los nodos. Para el análisis de este trabajo donde se requiera de establecer una comunicación se eligen el nodo 1 y el nodo 8 como fuente y destino respectivamente.

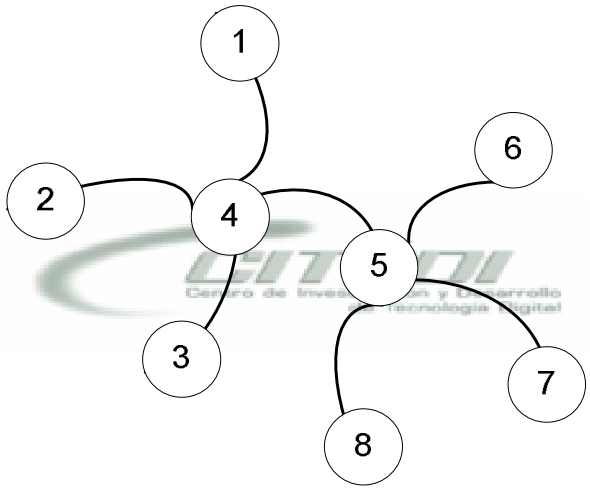


Figura 4. 2. Topología de Red Ad-Hoc Inalámbrica

La tabla 4.7 muestra la asignación de direcciones IP en la red.

Tabla 4. 7. Asignación de IP

Nodo	Dirección IP
1	1.0.0.1
2	1.0.0.2
3	1.0.0.3
4	1.0.0.4
5	1.0.0.5
6	1.0.0.6
7	1.0.0.7
8	1.0.0.8

4.4. ANÁLISIS DE RUTA

4.4.1. Descubrimiento de Vecinos

Se asume que el algoritmo se inicia en el nodo 1. El procedimiento inicia con el envío de mensajes HELLO [77].

Paso 1:

El nodo 1 inicia el procedimiento del descubrimiento de vecinos ajustando el contador de saltos (Hop Count) en 0. Además incrementa una unidad el Número de Secuencia del paquete (1), especifica el tipo de mensaje a 1 (HELLO), el tiempo valido es 2 segundo de acuerdo a la ecuación 2 a=0 y b=5. También agrega la dirección IP del Originador, TTL a 1 esto para que no se retransmita, el tipo de vecino y enlace en 0, la disponibilidad es puesta como Default (3), se incrementa el número de secuencia del mensaje. Por último se calcula el tamaño del mensaje de enlace, el tamaño del mensaje y el tamaño del paquete y se agregan al mensaje. Por esta razón el paquete toma la forma de la figura 4.3.

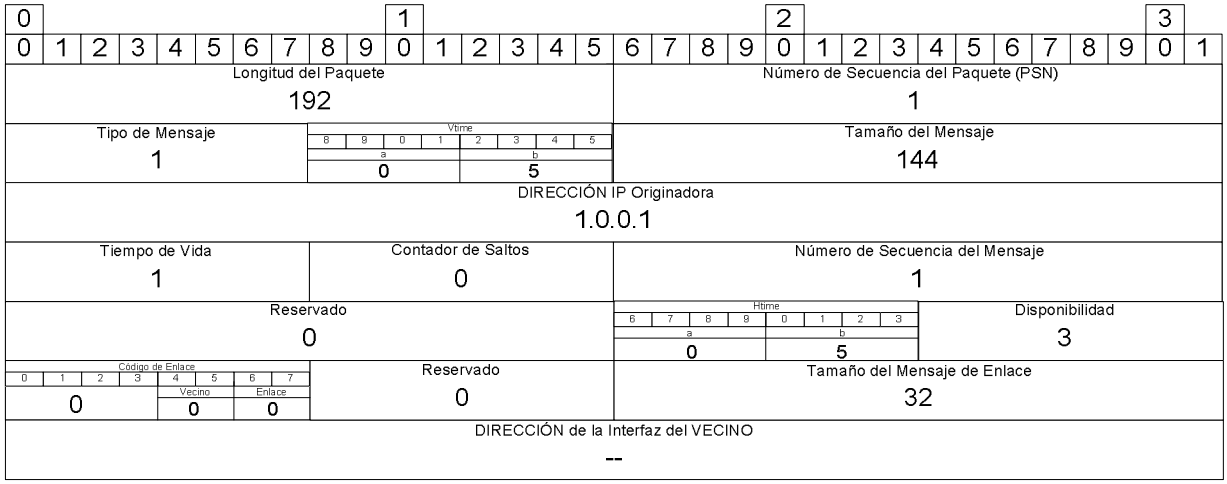


Figura 4. 3. Creación de paquete por el nodo 1.

Este paquete es transmitido a todas las direcciones, alcanzando solamente al nodo 4, como lo muestra la figura 4.4, la flecha indica la dirección del paquete que se envía.

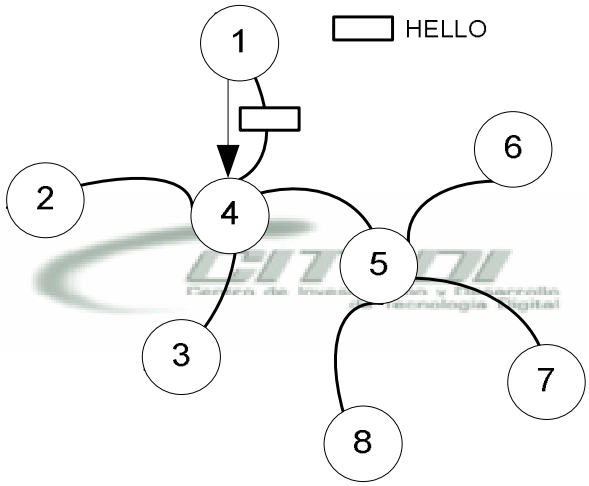


Figura 4. 4. Transmisión de Mensaje Hello

Paso 2:

Cuando el nodo 4 recibe el mensaje, este compara el tipo de mensaje y lo procesa, guardando la información del enlace (prefijo L) y del Vecino (prefijo N):

L_Neighbor_Iface_Addr = 1.0.0.1

L_Local_Iface_Addr = 1.0.0.1

N_Neighbor_Main_Addr =1.0.0.1

N_Willingnes = 3 (Default)

Una vez almacenada la información 4 procede a contestar este mensaje, creando un mensaje nuevo HELLO con la siguiente información (figura 4.5):

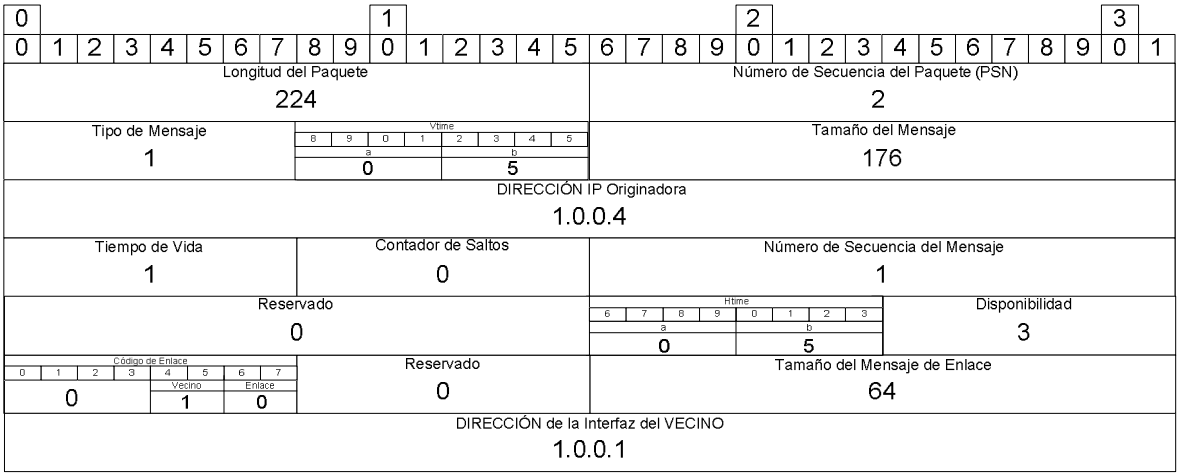


Figura 4. 5. Creación de mensaje por el nodo 4.

El paquete se envía a todos los nodos que están en el área de cobertura del nodo 4, alcanzando a los nodos 2, 3, 5 y 1 (quien originó este proceso). La figura 4.6 muestra la transmisión del nodo 4.

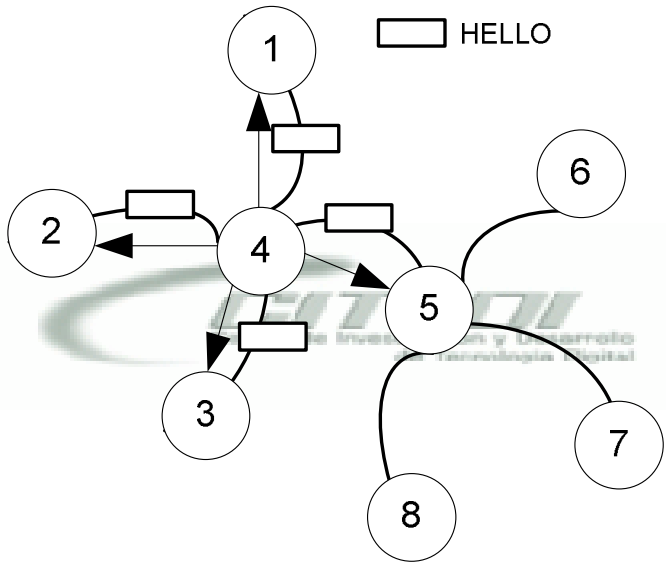


Figura 4. 6. Transmisión del mensaje por el nodo 4.

Paso 3:

Los nodos vecinos del nodo 4 que recibieron el paquete identifican el tipo de mensaje y crean las listas correspondientes a los enlaces y a los vecinos guardando la siguiente información cada nodo.

L_Neighbor_Iface_Addr = 1.0.0.4
L_Local_Iface_Addr = 1.0.0.4
N_Neighbor_Main_Addr =1.0.0.4
N_Willingnes = 3 (Default)

Ahora los nodos 1,2,3 y 5 saben que tienen a un vecino, mas no tiene una disponibilidad alta por lo tanto no es confiable, para conocer si el nodo sigue presente y tener una respuesta bidireccional cada nodo construye un mensaje HELLO el cual se compone de la siguiente manera.

Nodo 1:

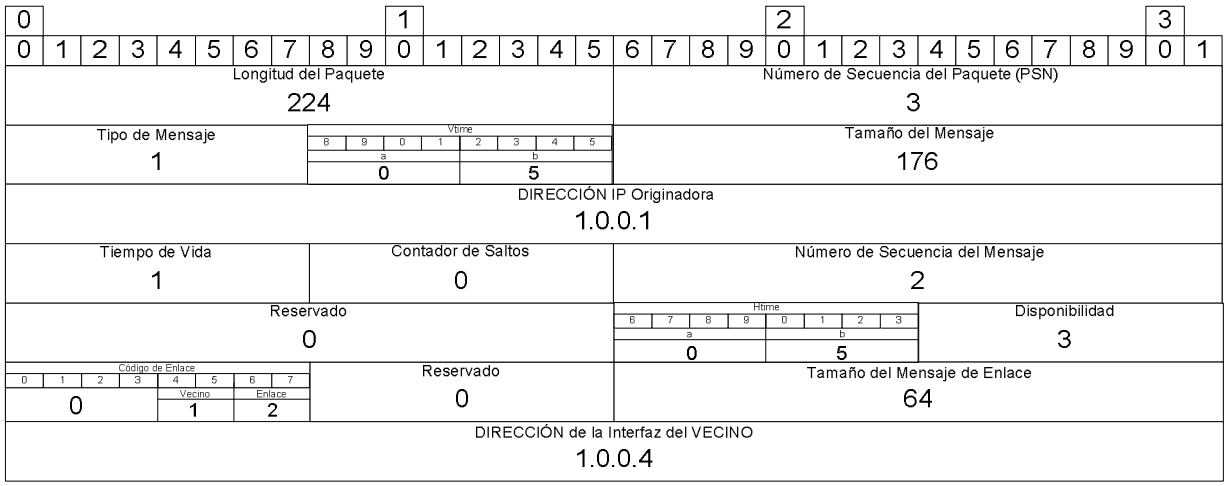


Figura 4. 7. Creación de Paquete en Nodo 1.

Nodo 2:

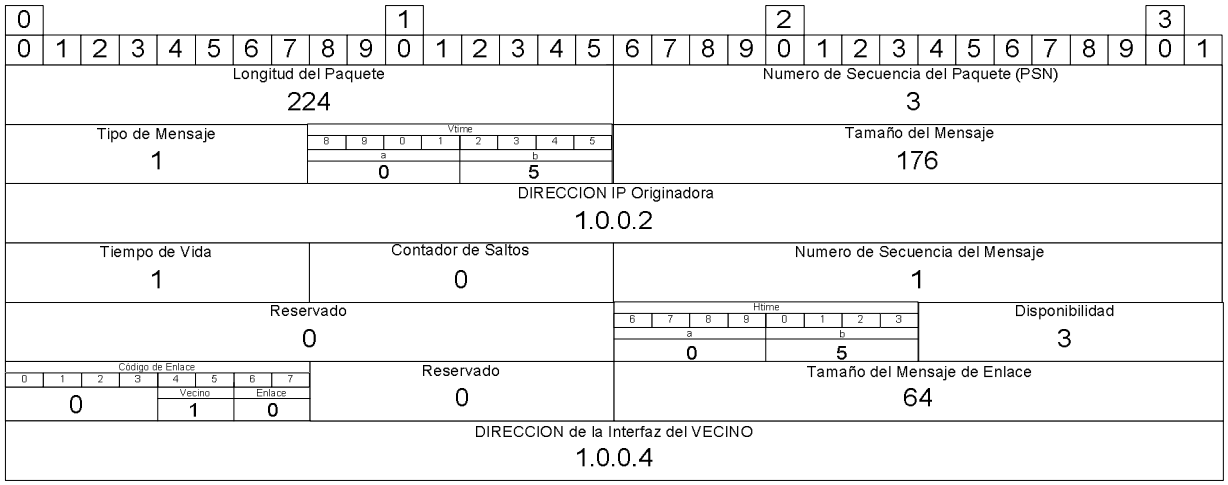


Figura 4. 8. Creación de paquete en el nodo 2.

Nodo 3:

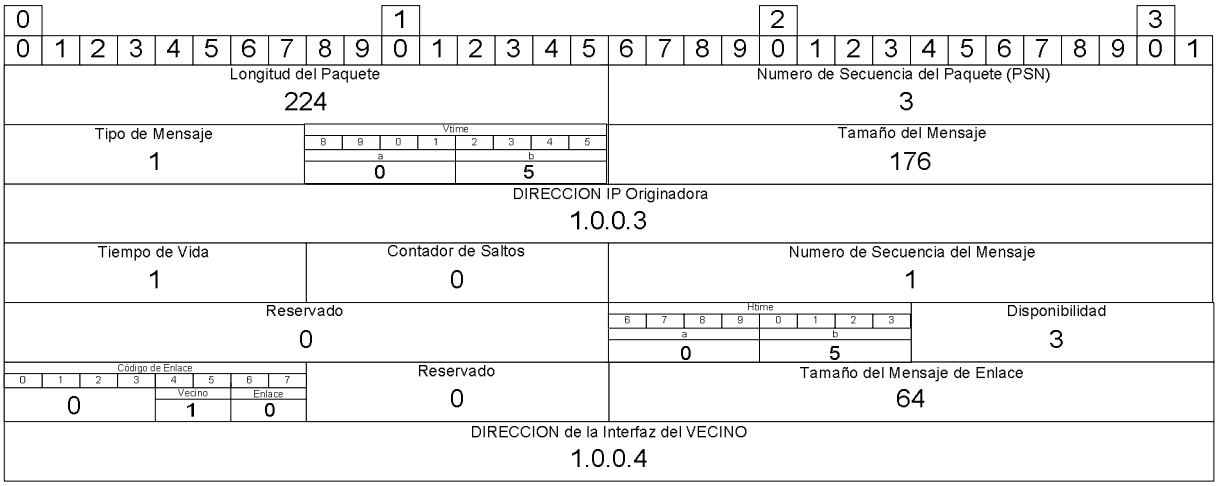


Figura 4. 9. Creación de paquete en el nodo 3.

Nodo 5:

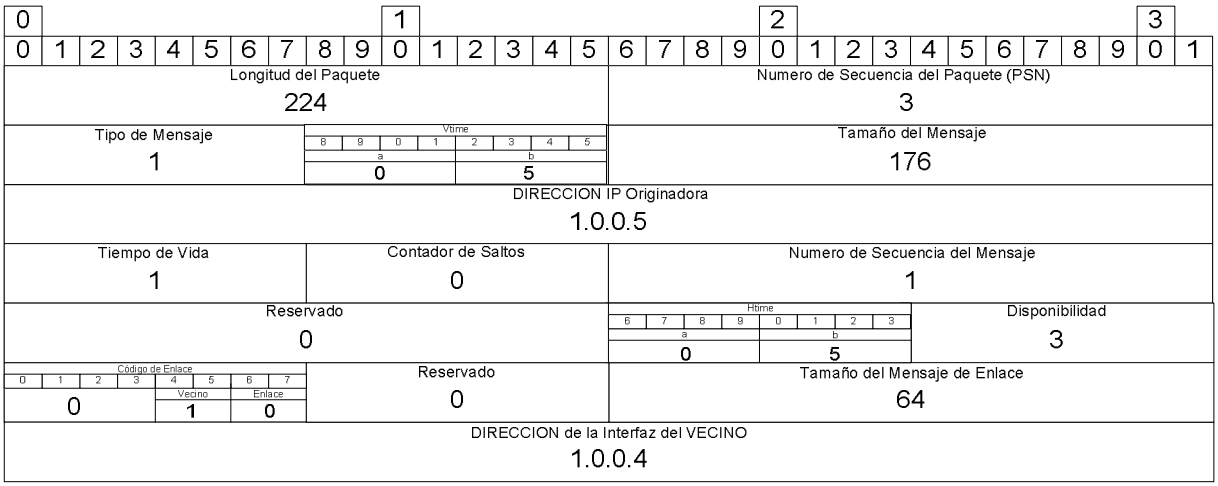


Figura 4. 10. Creación del paquete en el nodo 5.

Y la red queda como lo muestra la figura 4.11:

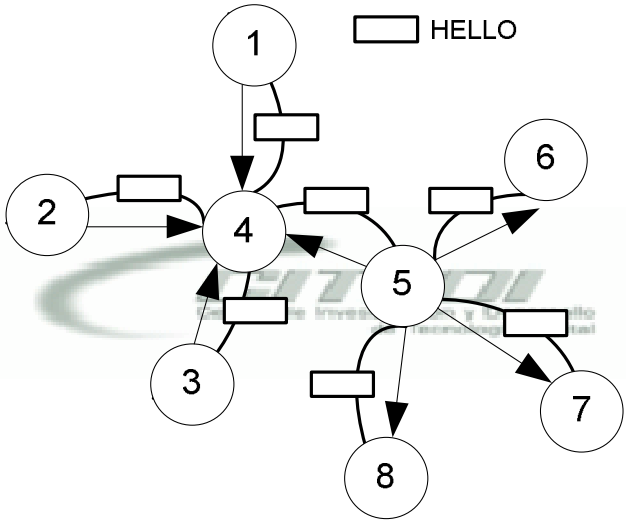


Figura 4. 11. Transmisión de paquetes de los nodos 1, 2, 3 y 5.

Paso 4:

Al nodo 4 le llegan los paquetes procedentes de los nodos 1, 2, 3 y 5, mientras que al nodo 6, 7, y 8 reciben el paquete del nodo 5, como se muestra en la figura 4.11. El nodo 4 procesa el mensaje enviado por el nodo 1 y actualiza sus tablas, cambiando el tipo de nodo "ASIMÉTRICO" a nodo "SIMÉTRICO" y agregando el procedimiento de la tabla de vecinos a 2 saltos. Esta tabla compara las direcciones de los vecinos del vecino y aquella dirección que no corresponda a su misma dirección IP la guardara como vecino a 2-saltos, en este caso el único vecino que envía el nodo 1 es 1.0.0.4 que es la misma del nodo 4. Crea entradas para los vecinos nuevos.

L_Neighbor_Iface_Addr = 1.0.0.1
L_Local_Iface_Addr = 1.0.0.1
N_Neighbor_Main_Addr = 1.0.0.1
N_Willingnes = 7 (Siempre)

L_Neighbor_Iface_Addr	= 1.0.0.2	1.0.0.3	1.0.0.5
L_Local_Iface_Addr	= 1.0.0.2	1.0.0.3	1.0.0.5
N_Neighbor_Main_Addr	= 1.0.0.2	1.0.0.3	1.0.0.5
N_Willingnes	= 3 (Default)	3	3

Una vez almacenados los datos se crean los paquetes en cada nodo con la información de la figura 4.12

Nodo 4:

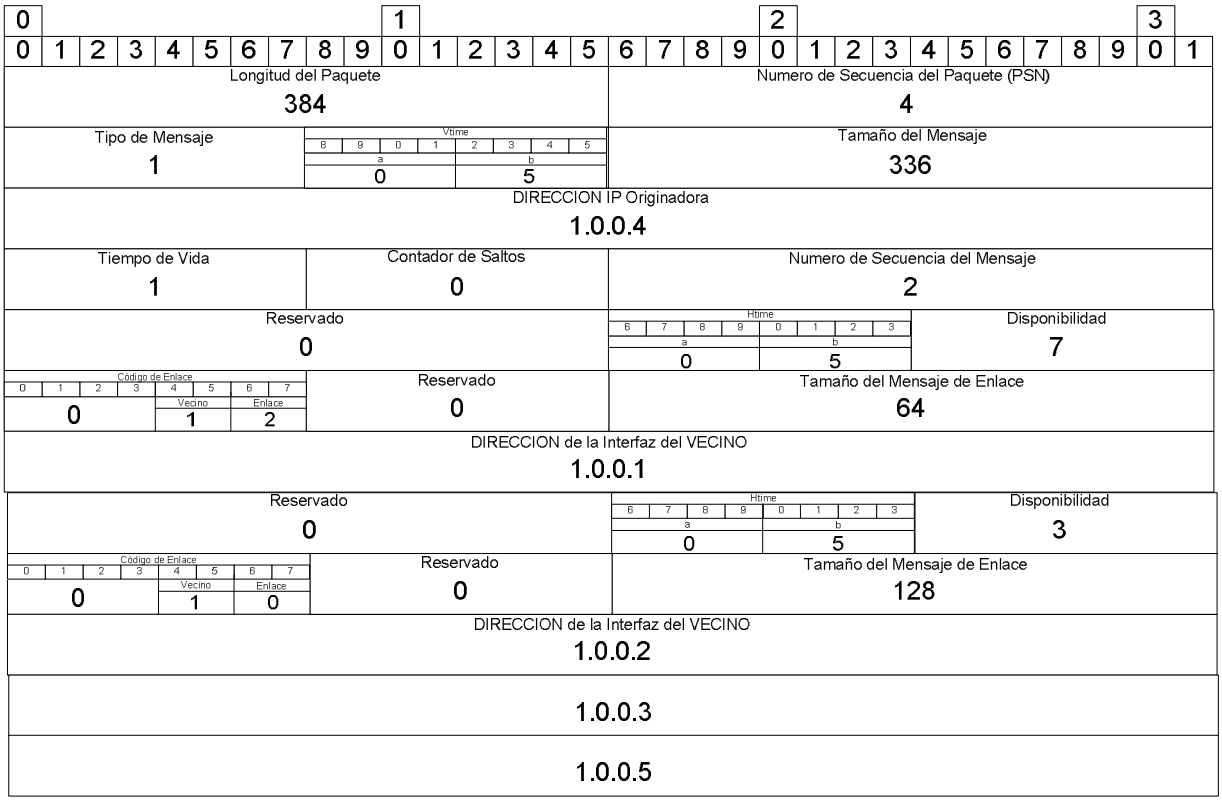


Figura 4. 12. Paquete creado por el nodo 4, con dos tipos de vecinos.

Cabe señalar que el paquete del nodo 4, tiene dos tipos de vecinos, los que tienen un enlace simétrico y enlace asimétrico es por eso que los vecinos están distribuidos en dos secciones del paquete.

Nodo 6, 7 y 8

0										1						2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Longitud del Paquete 224																Número de Secuencia del Paquete (PSN) 4															
Tipo de Mensaje 1										Vtime 8 9 0 1 2 3 4 5 a: 0 b: 5																Tamaño del Mensaje 176					
DIRECCIÓN IP Originadora 1.0.0.6 (7 y 8)																															
Tiempo de Vida 1										Contador de Saltos 0																Número de Secuencia del Mensaje 1					
Reservado 0																Htime 6 7 8 9 0 1 2 3 a: 0 b: 5												Disponibilidad 3			
Código de Enlace 0 1 2 3 4 5 6 7 0				Vecino 1		Enlace 0				Reservado 0																Tamaño del Mensaje de Enlace 64			
DIRECCIÓN de la Interfaz del VECINO 1.0.0.5																															

Figura 4. 13. Paquete creado por el nodo 6

El paquete que se envía por los nodos 6, 7 y 8 son similares, la diferencia radica en la dirección IP del originado, de la figura 4.13 la información que cambia es la que se encuentra entre paréntesis, la figura 4.14 ilustra el envió de los paquetes del nodo 4, 6, 7 y 8.

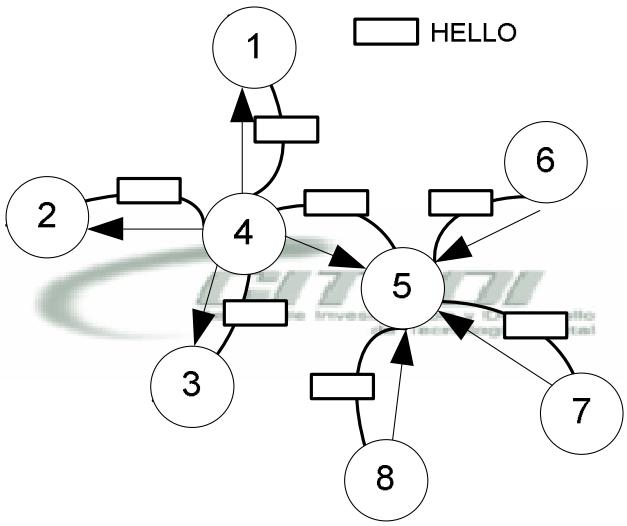


Figura 4. 14. Transmisión de paquetes de los nodos 4, 6, 7 y 8.

Paso 5:

El nodo 1 confirma que es nodo simétrico, 2, 3 y 5 comparan la lista de vecinos con sus direcciones IP, asegurándose que son vecinos simétricos proceden a cambiar el estado del enlace y cambiando la disponibilidad a la más alta (7-Siempre). Además comparan un nodo (el nodo 1) simétrico y con disponibilidad aceptada para almacenarlo como nodo vecino a 2-saltos, almacenando la siguiente información en la tabla de vecinos a 2-saltos:

N_Neighbor_main_Addr = 1.0.0.4
N_2Hop_Addr = 1.0.0.1

Por otra parte el nodo 5 guarda las direcciones de los nodos vecinos:

L_Neighbor_Iface_Addr = 1.0.0.4
L_Local_Iface_Addr = 1.0.0.4
N_Neighbor_Main_Addr =1.0.0.4
N_Willingnes = 7 (Siempre)

L_Neighbor_Iface_Addr =	1.0.0.6	1.0.0.7	1.0.0.8
L_Local_Iface_Addr =	1.0.0.6	1.0.0.7	1.0.0.8
N_Neighbor_Main_Addr =	1.0.0.6	1.0.0.7	1.0.0.8
N_Willingnes =	3 (Default)	3	3

Una vez guardada la información se crean los mensajes con la siguiente información actualizada, para el caso de los nodos 2, 3 y 5 la información que cambia es el tipo de enlace, el tipo de vecino, la disponibilidad y los números de secuencia, este cambio se ve reflejado en las figuras 4.15 y 4.16.

Nodo 1, 2 y 3

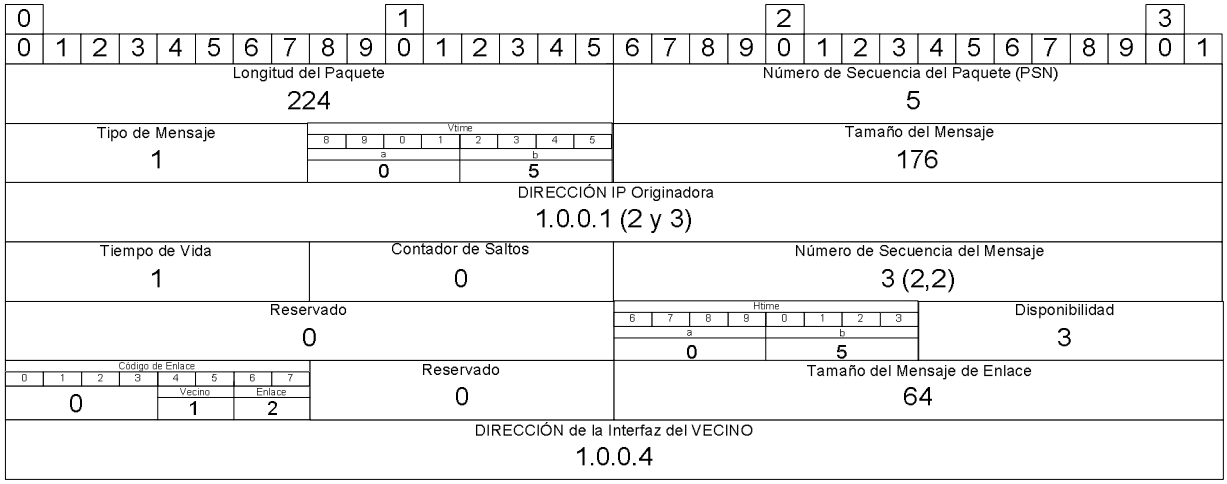


Figura 4. 15. Paquete creado por los nodos 1, 2 y 3.

Nodo 5

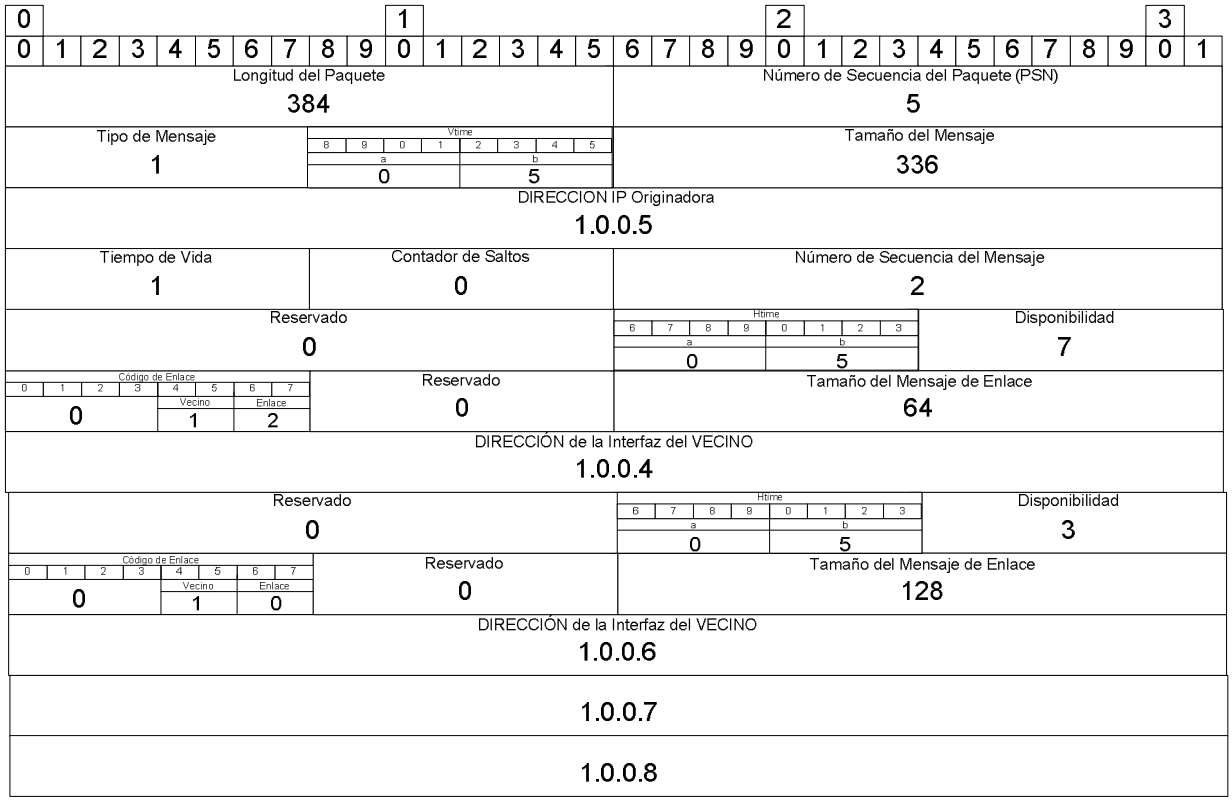


Figura 4. 16. Paquete creado por el nodo 5.

La figura 4.11 ilustra el envió de los paquetes del nodo 1, 2, 3 y 5.

Paso 6:

El nodo 4 realiza las actualizaciones pertinentes como ajustar la disponibilidad de los vecinos a 7. La información que llega a los nodos 6, 7 y 8 sirve para asegurar los enlaces simétricos además para conocer a los vecinos a 2-saltos, esto lo logran comparando las direcciones IP de los vecinos del vecino y guardando todas aquellas diferentes a la dirección local. Este proceso da como resultado el almacenamiento del nodo 4 en cada nodo.

N_Neighbor_main_Addr = 1.0.0.5

N_2Hop_Addr = 1.0.0.4

Una vez actualizada la información se generan los paquetes de los mensajes HELLO para cada nodo.

Nodo 4

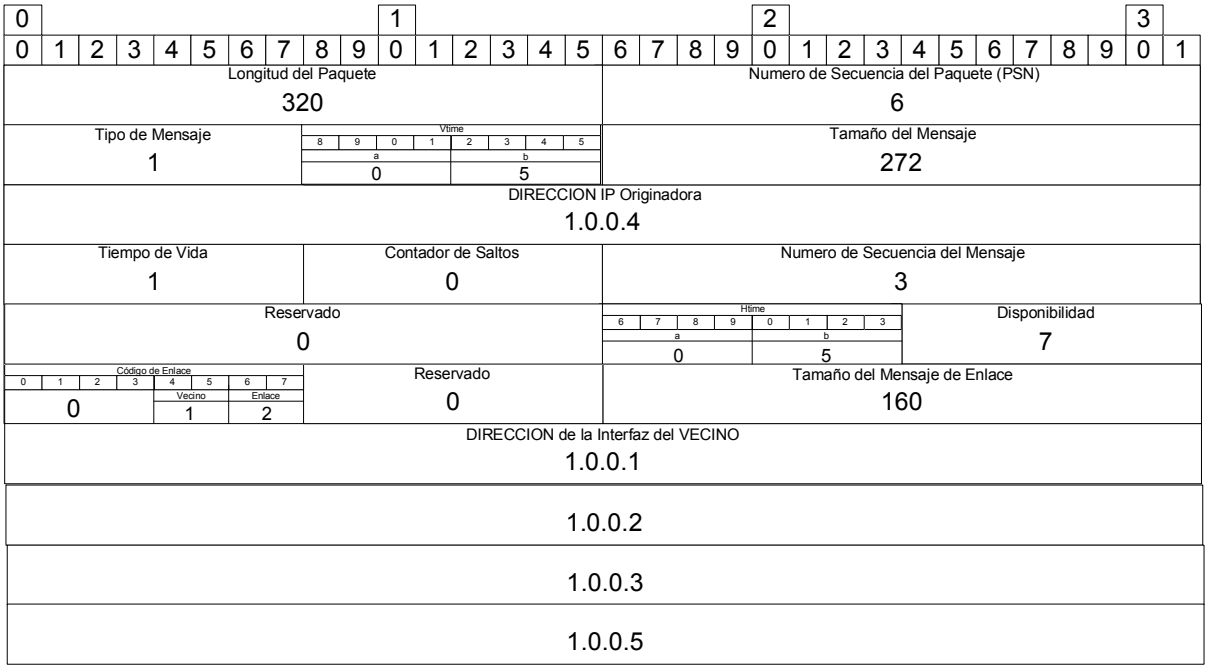


Figura 4. 17. Paquete creado por el nodo 4 con información de 4 vecinos.

Nodo 6, 7 y 8.

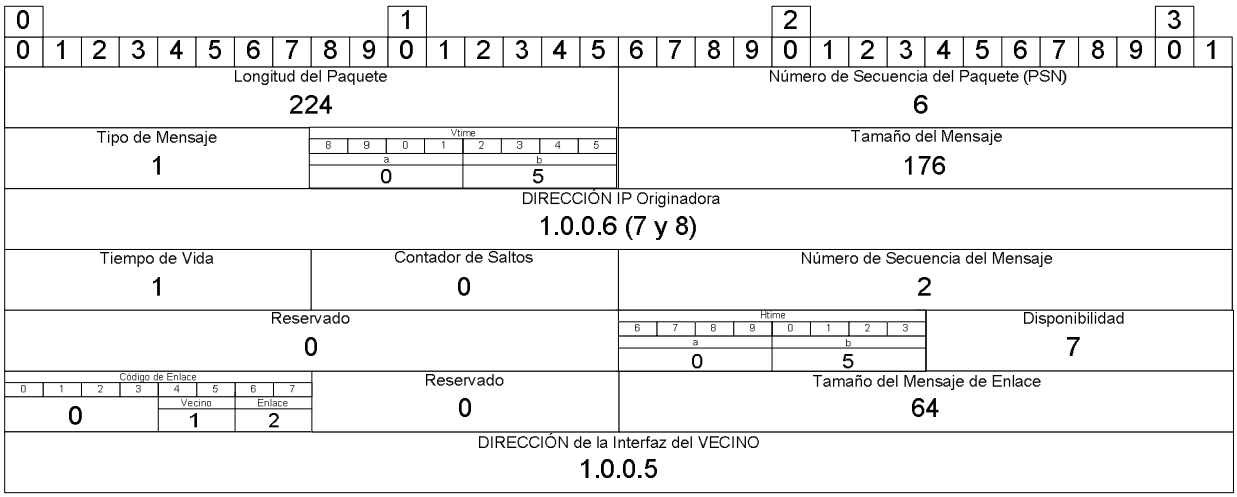


Figura 4. 18. Valores generados por el nodo 6, 7 y 8.

La figura 4.14 ilustra la transmisión de los paquetes del los nodo 4, 6, 7 y 8.

El paquete que se envía por el nodo 4 llega a los nodos 1, 2, 3 y 5 mientras que el enviado por los nodos 6, 7 y 8 llegan al nodo 5.

Paso 7:

El nodo 1 actualiza sus tablas, en este caso checa las direcciones de los vecinos del vecino para agregar más direcciones a la tabla de vecinos a 2-saltos. Toda dirección diferente a la del nodo 1, es almacenada como vecino a 2-salto, creando una entrada para cada nodo, como lo muestran las siguientes tablas.

Nodo 1

N_Neighbor_main_Addr	=	1.0.0.4	1.0.0.4	1.0.0.4
N_2Hop_Addr	=	1.0.0.2	1.0.0.3	1.0.0.5

El nodo 2 realiza el mismo procedimiento de comparación para agregar entradas en la lista de vecinos a 2-saltos

Nodo 2

N_Neighbor_main_Addr	=	1.0.0.4	1.0.0.4	1.0.0.4
N_2Hop_Addr	=	1.0.0.1	1.0.0.3	1.0.0.5

Nodo 3

N_Neighbor_main_Addr	=	1.0.0.4	1.0.0.4	1.0.0.4
N_2Hop_Addr	=	1.0.0.1	1.0.0.2	1.0.0.5

Al nodo 5 le llegan paquetes de los nodos 4, 6, 7 y 8 estos se utilizan para actualizar la información de los vecinos y cambiarlas a simétricos y con disponibilidad alta (7-Siempre), además agrega los nodos a 2-saltos.

Nodo 5

N_Neighbor_main_Addr	=	1.0.0.4	1.0.0.4	1.0.0.4
N_2Hop_Addr	=	1.0.0.1	1.0.0.2	1.0.0.3

Una vez almacena la información se crean los paquetes “HELLO” para informar de la actualización en los nodos, el mensaje se crea en los nodo 5, 1, 2 y 3, para este caso la información en los nodos 1, 2 y 3 no sufrió algún cambio, por lo que para el análisis se omite esta transmisión que en la realidad si se realiza ya que se tienen que actualizar los tiempos de los vecinos y el tiempo de vida de los nodos. El paquete que se envía del nodo 5 a los nodos 4, 6, 7 y 8 es el de la figura 4.19.

Nodo 5

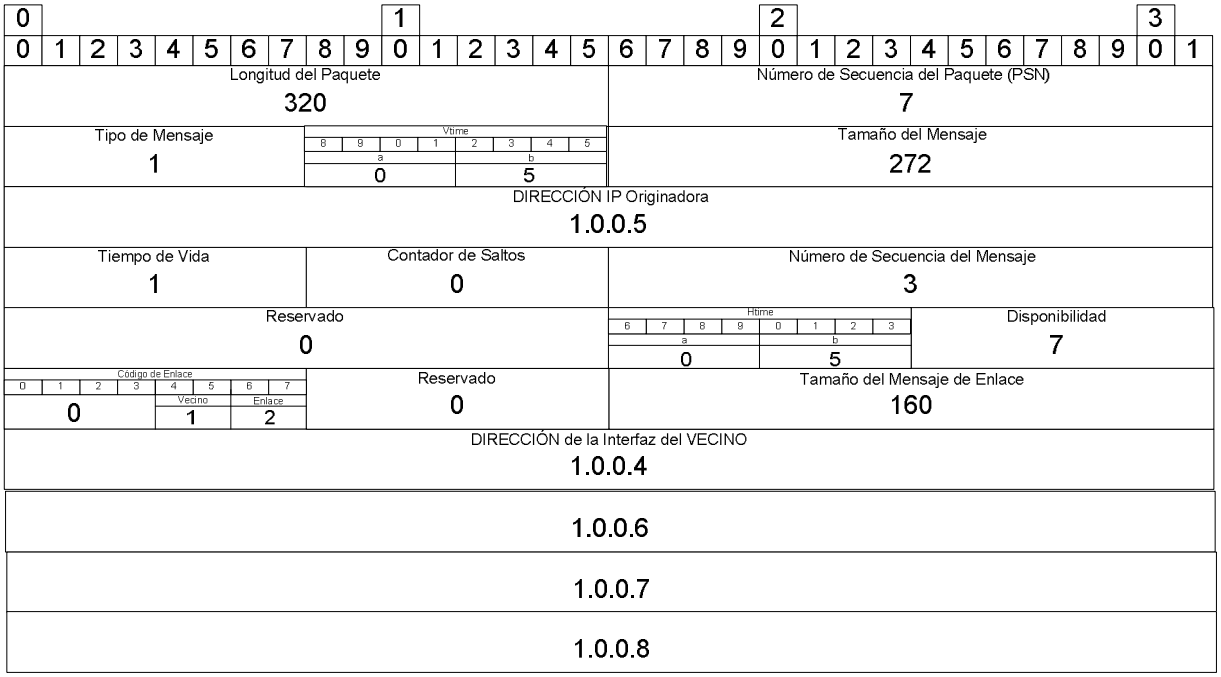


Figura 4. 19. Paquete realizado por el nodo 5.

La ilustración de la transmisión del paquete por la red es como la que se muestra en la figura 4.11.

Paso 8:

El paquete llega a los nodos 4, 6, 7 y 8, estos realizan las actualizaciones necesarias una de las más importantes es la tabla de vecinos a 2-saltos. El proceso es comparar las direcciones IP de los vecinos guardados en el paquete y se almacenará todo vecino que no corresponda a la dirección IP local. Por lo tanto la información que se almacena en los nodos es la siguiente:

Nodo 4

N_Neighbor_main_Addr	=	1.0.0.5	1.0.0.5	1.0.0.5
N_2Hop_Addr	=	1.0.0.6	1.0.0.7	1.0.0.8

Nodo 6

N_Neighbor_main_Addr	=	1.0.0.5	1.0.0.5	1.0.0.5
N_2Hop_Addr	=	1.0.0.4	1.0.0.7	1.0.0.8

Nodo 7

N_Neighbor_main_Addr	=	1.0.0.5	1.0.0.5	1.0.0.5
N_2Hop_Addr	=	1.0.0.4	1.0.0.6	1.0.0.8

Nodo 8

N_Neighbor_main_Addr	=	1.0.0.5	1.0.0.5	1.0.0.5
N_2Hop_Addr	=	1.0.0.4	1.0.0.6	1.0.0.7

En este momento todos los nodos conocen a sus vecinos inmediatos y a sus vecinos a 2 saltos, con solo enviar los mensajes HELLO. El siguiente procedimiento que se recomienda realizar es la selección de los nodos MPR.

4.4.2. Selección de Nodos MPR

Siguiendo el algoritmo para la selección de MPR, cada nodo selecciona a sus nodos MPR.
El Nodo 1 tiene 3 vecinos a 2 saltos y para ello se requiere solamente del nodo 4 para llegar a ellos por lo tanto Nodo 1 selecciona al nodo 4 como MPR. El nodo 2 compara sus tablas de vecinos a 2-saltos y verifica que exista el único camino para llegar a los destinos de 2 saltos, por lo tanto selecciona al nodo 4 como MPR. En resumen tenemos la siguiente tabla que muestra la selección de nodos MPR.

Tabla 4. 8. Relación de selección de MPR.

Nodo Selector	Nodo MPR
Nodo 1	Nodo 4
Nodo 2	Nodo 4
Nodo 3	Nodo 4
Nodo 4	Nodo 5
Nodo 5	Nodo 4
Nodo 6	Nodo 5
Nodo 7	Nodo 5
Nodo 8	Nodo 5

Por último se envía un mensaje "HELLO" cambiando el tipo de enlace de los nodos que fueron seleccionados como MPR. El formato de los paquetes y la transmisión de los paquetes de muestra en la figura 4.20 a la figura 4.24.

Nodo 1, 2 y 3.

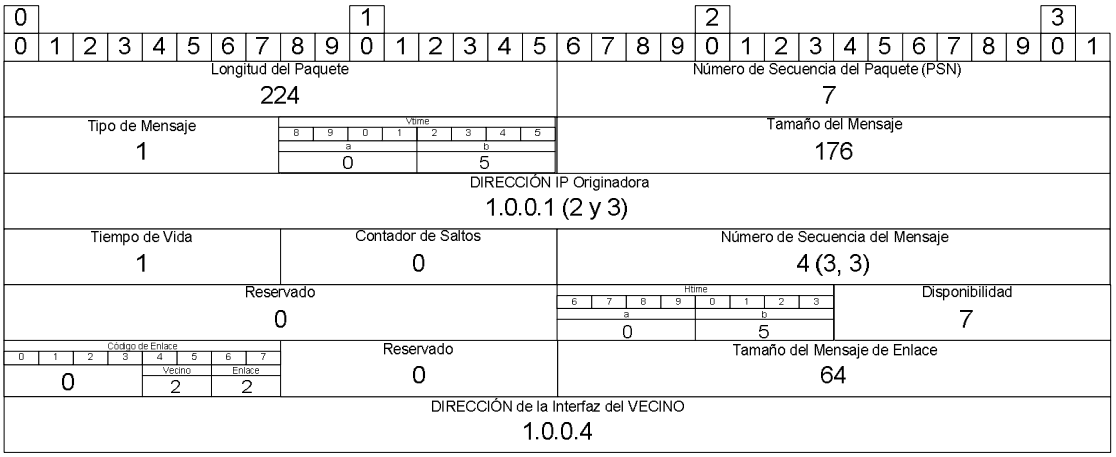


Figura 4. 20. Paquete creado por los nodos 1, 2 y 3, informando el MPR.

Nodo 4

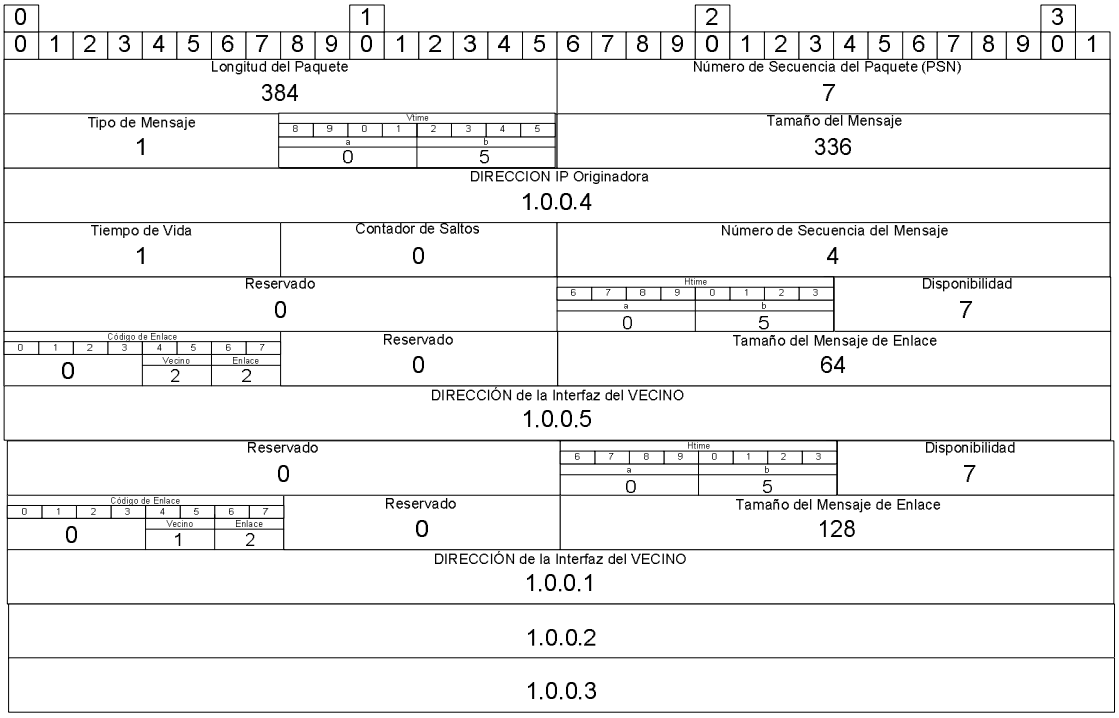


Figura 4. 21. Paquete creado por el nodo 4, informando al MPR.

Nodo 5

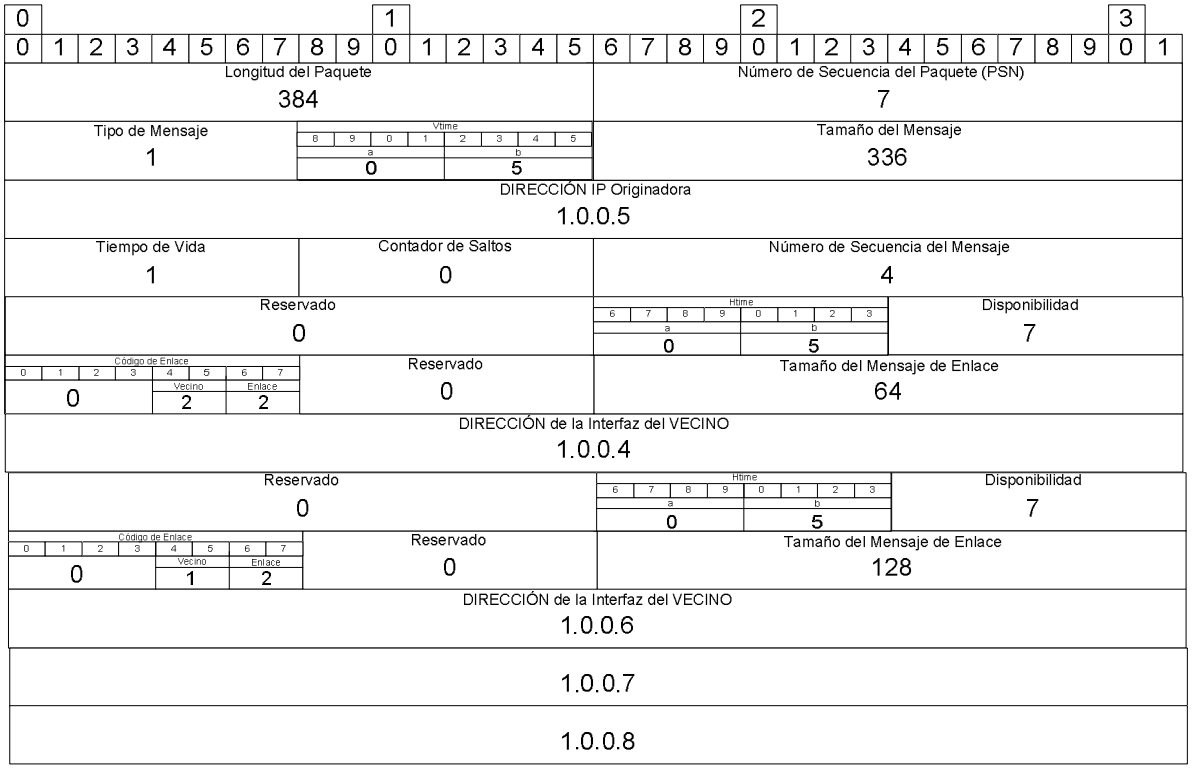


Figura 4. 22. Paquete creado por el nodo 5, informando al MPR.

Nodo 6, 7 y 8

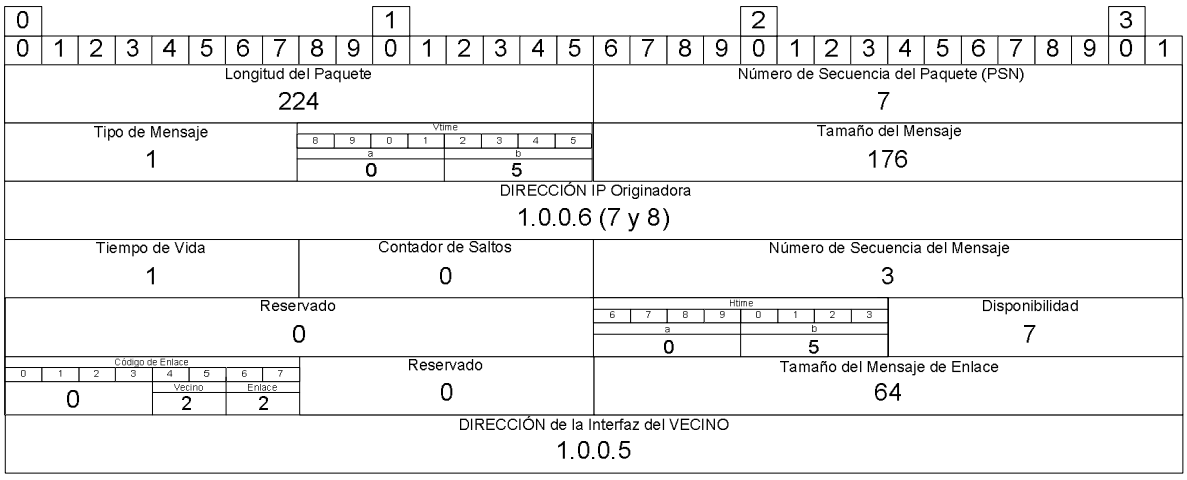


Figura 4. 23. Paquete creado por los nodos 6. 7 y 8, Informando al MPR.

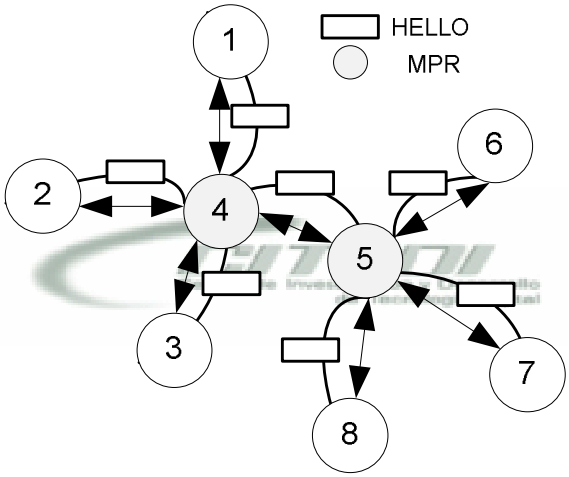


Figura 4. 24. Transmisión de la Selección de nodos MPR.

4.4.3. Difusión de Topología

Una vez notificados los nodos que son MPR y conocer a los nodos que lo seleccionaron, los MPR crean el mensaje de control de acuerdo a la siguiente estructura.

TC del MPR 4

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ANSN																Reservado															
1																0															
DIRECCION del Selector MPR																															
1.0.0.1																															
1.0.0.2																															
1.0.0.3																															
1.0.0.5																															

Figura 4. 25. Mensaje TC creado por el nodo MPR 4.

TC del MPR 5

Figura 4. 26. Mensaje TC creado por el nodo MPR 5.

La transmisión de los mensajes TC se muestra en la figura 4.27.

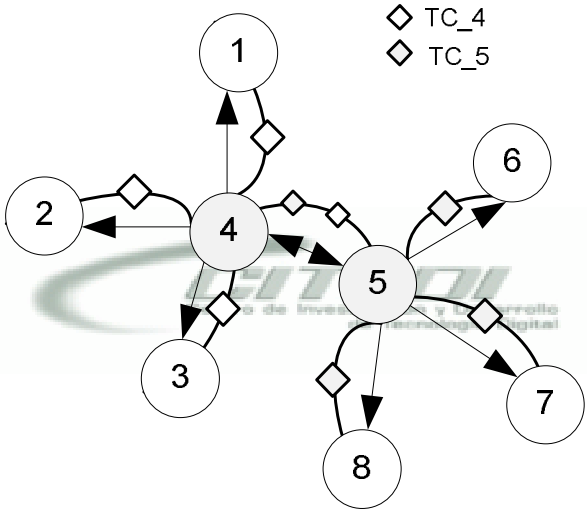


Figura 4. 27. Transmisión de los mensajes TC.

Una vez que el paquete llega a los nodos MPR procedente del otro MPR, estos retransmiten el paquete para que se cubra por completo la topología con esta información. La retransmisión del mensaje TC se observa en la figura 4.28, identificando el paquete del MPR del nodo 4 como rombo y el paquete del MPR del nodo 5 como rombo relleno.

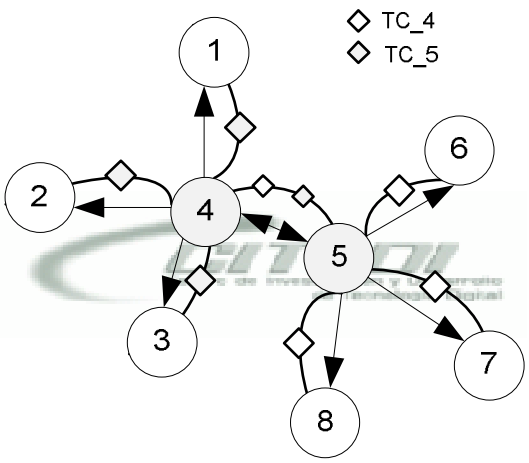


Figura 4. 28. Retransmisión de TC.

Al paso de los mensajes TC se almacena la información de un par de enlaces relacionada con los nodos selectores y el nodo que originó el mensaje TC. Por lo tanto al cubrir toda la red con los mensajes TC tenemos en los nodos la información de la tabla 4.9.

Tabla 4. 9. Tablas de descubrimiento de la Topología y su último nodo conocido.

Nodo 1	
T_Dest_Addr	T_Last_Addr
1.0.0.2	1.0.0.4
1.0.0.3	1.0.0.4
1.0.0.5	1.0.0.4
1.0.0.6	1.0.0.5
1.0.0.7	1.0.0.5
1.0.0.8	1.0.0.5

Nodo 2	
T_Dest_Addr	T_Last_Addr
1.0.0.1	1.0.0.4
1.0.0.3	1.0.0.4
1.0.0.5	1.0.0.4
1.0.0.6	1.0.0.5
1.0.0.7	1.0.0.5
1.0.0.8	1.0.0.5

Nodo 3	
T_Dest_Addr	T_Last_Addr
1.0.0.1	1.0.0.4
1.0.0.2	1.0.0.4
1.0.0.5	1.0.0.4
1.0.0.6	1.0.0.5
1.0.0.7	1.0.0.5
1.0.0.8	1.0.0.5

Nodo 4	
T_Dest_Addr	T_Last_Addr
1.0.0.6	1.0.0.5
1.0.0.7	1.0.0.5
1.0.0.8	1.0.0.5

Nodo 6	
T_Dest_Addr	T_Last_Addr
1.0.0.1	1.0.0.4
1.0.0.2	1.0.0.4
1.0.0.3	1.0.0.4
1.0.0.4	1.0.0.5
1.0.0.7	1.0.0.5
1.0.0.8	1.0.0.5

Nodo 5	
T_Dest_Addr	T_Last_Addr
1.0.0.1	1.0.0.4
1.0.0.2	1.0.0.4
1.0.0.3	1.0.0.4

Nodo 7	
T_Dest_Addr	T_Last_Addr
1.0.0.1	1.0.0.4
1.0.0.2	1.0.0.4
1.0.0.3	1.0.0.4
1.0.0.4	1.0.0.5
1.0.0.6	1.0.0.5
1.0.0.8	1.0.0.5

Nodo 8	
T_Dest_Addr	T_Last_Addr
1.0.0.1	1.0.0.4
1.0.0.2	1.0.0.4
1.0.0.3	1.0.0.4
1.0.0.4	1.0.0.5
1.0.0.6	1.0.0.5
1.0.0.7	1.0.0.5

Estos mensajes se envían con un intervalo de 6 segundos con la finalidad de tener actualizados la topología de la red. Una vez obtenidos estos datos el siguiente procedimiento es el cálculo de la ruta.

4.4.4. Calculo de Tablas de Ruteo

El formato de las tablas de ruteo es el siguiente:

1.- R_Dest_Addr R_Next_Addr R_Dist R_Iface_Addr

2.- R_Dest_Addr R_Next_Addr R_Dist R_Iface_Addr

3.- R_Dest_Addr R_Next_Addr R_Dist R_Iface_Addr

:

:

Cada entrada en la tabla consiste de la dirección de un nodo destino (R_Dest_Addr), dirección del siguiente nodo (R_Next_Addr), el número de saltos (R_Dist) y la dirección del nodo por donde es alcanzado R_Dest_Addr (R_Iface_Addr).

De acuerdo al algoritmo de obtención de ruta [34], cada nodo crea una entrada para los nodos vecinos, y luego para los nodos vecinos a 2-saltos y posteriormente para los nodos mayores a 3 saltos.

Tabla 4. 10. Tablas de ruteo de toda la red.

Nodo 1				
Número	Destino	Siguiente	Distancia	Interfaz
1.-	1.0.0.4	1.0.0.4	1	1.0.0.4
2.-	1.0.0.2	1.0.0.4	2	1.0.0.4
3.-	1.0.0.3	1.0.0.4	2	1.0.0.4
4.-	1.0.0.5	1.0.0.4	2	1.0.0.5
5.-	1.0.0.6	1.0.0.4	3	1.0.0.5
6.-	1.0.0.7	1.0.0.4	3	1.0.0.5
7.-	1.0.0.8	1.0.0.4	3	1.0.0.5

Nodo 2				
Número	Destino	Siguiente	Distancia	Interfaz
1.-	1.0.0.4	1.0.0.4	1	1.0.0.4
2.-	1.0.0.1	1.0.0.4	2	1.0.0.4
3.-	1.0.0.3	1.0.0.4	2	1.0.0.4
4.-	1.0.0.5	1.0.0.4	2	1.0.0.5
5.-	1.0.0.6	1.0.0.4	3	1.0.0.5
6.-	1.0.0.7	1.0.0.4	3	1.0.0.5
7.-	1.0.0.8	1.0.0.4	3	1.0.0.5

Nodo 3				
Número	Destino	Siguiente	Distancia	Interfaz
1.-	1.0.0.4	1.0.0.4	1	1.0.0.4
2.-	1.0.0.2	1.0.0.4	2	1.0.0.4
3.-	1.0.0.1	1.0.0.4	2	1.0.0.4
4.-	1.0.0.5	1.0.0.4	2	1.0.0.5
5.-	1.0.0.6	1.0.0.4	3	1.0.0.5
6.-	1.0.0.7	1.0.0.4	3	1.0.0.5
7.-	1.0.0.8	1.0.0.4	3	1.0.0.5

Nodo 4				
Número	Destino	Siguiente	Distancia	Interfaz
1.-	1.0.0.1	1.0.0.1	1	1.0.0.1
2.-	1.0.0.2	1.0.0.2	1	1.0.0.2
3.-	1.0.0.3	1.0.0.3	1	1.0.0.3
4.-	1.0.0.5	1.0.0.5	1	1.0.0.5
5.-	1.0.0.6	1.0.0.5	2	1.0.0.5
6.-	1.0.0.7	1.0.0.5	2	1.0.0.5
7.-	1.0.0.8	1.0.0.5	2	1.0.0.5

Nodo 5				
Número	Destino	Siguiente	Distancia	Interfaz
1.-	1.0.0.4	1.0.0.4	1	1.0.0.4
2.-	1.0.0.6	1.0.0.6	1	1.0.0.6
3.-	1.0.0.7	1.0.0.7	1	1.0.0.7
4.-	1.0.0.8	1.0.0.8	1	1.0.0.8
5.-	1.0.0.1	1.0.0.4	2	1.0.0.4
6.-	1.0.0.2	1.0.0.4	2	1.0.0.4
7.-	1.0.0.3	1.0.0.4	2	1.0.0.4

Nodo 6				
Número	Destino	Siguiente	Distancia	Interfaz
1.-	1.0.0.5	1.0.0.5	1	1.0.0.5
2.-	1.0.0.4	1.0.0.5	2	1.0.0.5
3.-	1.0.0.7	1.0.0.5	2	1.0.0.5
4.-	1.0.0.8	1.0.0.5	2	1.0.0.5
5.-	1.0.0.1	1.0.0.5	3	1.0.0.4
6.-	1.0.0.2	1.0.0.5	3	1.0.0.4
7.-	1.0.0.3	1.0.0.5	3	1.0.0.4

Nodo 7				
Número	Destino	Siguiente	Distancia	Interfaz
1.-	1.0.0.5	1.0.0.5	1	1.0.0.5
2.-	1.0.0.4	1.0.0.5	2	1.0.0.5
3.-	1.0.0.6	1.0.0.5	2	1.0.0.5
4.-	1.0.0.8	1.0.0.5	2	1.0.0.5
5.-	1.0.0.1	1.0.0.5	3	1.0.0.4
6.-	1.0.0.2	1.0.0.5	3	1.0.0.4
7.-	1.0.0.3	1.0.0.5	3	1.0.0.4

Nodo 8				
Número	Destino	Siguiente	Distancia	Interfaz
1.-	1.0.0.5	1.0.0.5	1	1.0.0.5
2.-	1.0.0.4	1.0.0.5	2	1.0.0.5
3.-	1.0.0.6	1.0.0.5	2	1.0.0.5
4.-	1.0.0.7	1.0.0.5	2	1.0.0.5
5.-	1.0.0.1	1.0.0.5	3	1.0.0.4
6.-	1.0.0.2	1.0.0.5	3	1.0.0.4
7.-	1.0.0.3	1.0.0.5	3	1.0.0.4

Las tablas de ruteo se actualizan cuando se detecta algún cambio en:

1. La tabla de enlaces
2. La tabla de vecino
3. Tabla de vecinos a 2-saltos

Esto conlleva a modificar las tablas de ruteo en la topología. Aun así se puede modificar las rutas para los vecinos de 1 y 2 saltos ya que esta información es obtenida a través de los mensajes "HELLO" mientras que la información para nodos mayores a 2 saltos se encuentra en los mensajes "TC", por lo tanto las tablas de ruteo se actualizan mínimo cada 2 segundos en los intervalos de los mensajes "HELLO" y máximo 5 segundos en los intervalos "TC".

Una vez analizado el funcionamiento teórico del algoritmo OLSR y realizar la implementación teórica en una red inalámbrica ad-hoc propuesta, se procederá a realizar el estudio y análisis de un algoritmo reactivo.

5

ALGORITMO VECTOR DISTANCIA SOBRE DEMANDA AD-HOC (AODV)

En este capítulo se presentará el funcionamiento del algoritmo reactivo de vector distancia "AODV", el formato de los paquetes y su proceso de transmisión a través de los nodos de la red. Se selecciona AODV entre los reactivos, por la ventaja de no guardar toda la ruta en el paquete de transmisión, utilizando menos memoria de almacenamiento.

5.1. Formato de mensajes

Para llevar a cabo con éxito el procedimiento de Descubrimiento de ruta y mantenimiento de ruta, AODV define tres tipos de mensajes: Petición de Ruta (RREQ), Contestación de Ruta (RREP) y Error de Ruta (RERR), estos mensajes son recibidos vía UDP [5, 43].
El primer formato que se muestra es:

RREQ

El formato de mensaje de petición de ruta (RREQ) se muestra en la figura 5.1. Se agregó un identificador de fila y columna a los formatos de los mensajes AODV, todos ellos basados en [5]. Además facilita la ubicación de los campos en el formato para el análisis de ruta, así para ubicar a la bandera J se dice que está ubicada en la fila "a", sección "0" en el numero "7" (a0-7).

Figura 5. 1. Formato de mensaje RREQ.

La descripción de algunos de los campos más sobresalientes es:

Tipo: Indica el tipo de mensaje de acuerdo a la Agencia de Asignación de números de Internet (IANA) (ver tabla 5.1) [37]. **J y R**: Son Banderas para señalar Unión y Reparar respectivamente **G**: Es la Bandera de RREP Gratuito; Indica cuando un mensaje de respuesta gratuita debe ser unicast hacia el nodo especificado en el campo de Dirección IP Destino.

D: Es la bandera de solo Destino; indica que solo el destino debe responder a este RREQ. **U**: es la bandera de Número de Secuencia Desconocido; indica que número de secuencia destino es desconocido. **Contador de Saltos**: es el Número de saltos desde la dirección IP Origen hacia el nodo que está manejando la petición. **RREQ ID**: es un número de secuencia único que identifica particularmente al RREQ. La **Dirección IP Destino**: es la dirección IP del destino.

El **Número de Secuencia Destino**: Es la última secuencia recibida por el origen para cualquier ruta que alcance el destino. **Dirección IP Origen**: es la dirección IP del nodo que origina la petición de ruta. Y finalmente **Número de secuencia Origen**: es la secuencia actual del origen que será usada en la ruta.

Tabla 5. 1. Tipos de mensajes de acuerdo a IANA.

Tipo de Mensaje	Valor
RREQ	1
RREP	2
RERR	3
RREP-ACK	4

El siguiente formato de mensaje es para:

RREP

La figura 5.2 muestra el formato de mensaje de contestación de ruta (RREP).

	0										1										2										3	
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
a	TIPO								R	A	RESERVADO										TAMAÑO PREFIJO				CONTADOR DE SALTOS							
b	DIRECCIÓN IP DESTINO																															
c	NÚMERO DE SECUENCIA DESTINO																															
d	DIRECCIÓN IP ORIGEN																															
e	TIEMPO DE VIDA																															

Figura 5. 2. Formato de mensaje RREP.

La descripción de algunos de los campos más sobresalientes es:
La bandera **A**: Indica que se requiere una contestación de enterado. El **Tamaño Prefijo**: Si no es cero, los 5 bits especifican que el próximo salto puede utilizarse por cualquier nodo con el mismo prefijo de ruteo como el del destino solicitado. El **Tiempo de Vida**: Es el tiempo en milisegundos para que el nodo que reciba la RREP considere la ruta valida.

RERR

El Formato para el mensaje de error de ruta (RERR) se presenta en la figura 5.3.

	0										1										2										3	
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
a	TIPO								N		RESERVADO														CONTADOR DE DESTINOS							
b	DIRECCIÓN IP DESTINO INALCANZABLE (1)																															
c	NÚMERO DE SECUENCIA DESTINO INALCANZABLE (1)																															
d	DIRECCIÓN IP DESTINO ADICIONAL INALCANZABLE (si es necesario)																															
e	NÚMERO DE SECUENCIA DESTINO ADICIONAL INALCANZABLE (si es necesario)																															

Figura 5. 3. Formato de mensaje RERR.

La bandera **N**: es la Bandera de NO borrar; se activa cuando un nodo pide una reparación local de un enlace y los nodos de la ruta de ida no deben borrar la ruta. El **Contador de Destinos**: es el número de destinos inalcanzados, este debe contener al menos 1. La **Dirección IP Destino Inalcanzable**: es la dirección IP del destino que se ha convertido en inalcanzable debido a un enlace caído y el **Número de Secuencia Destino Inalcanzable**: es el número de secuencia del destino.

De manera adicional, se presenta el formato para el mensaje de respuesta de ruta-enterado (RRE-ACK):

RREP-ACK

El Formato de mensaje de respuesta de ruta-enterado (RREP-ACK) se muestra en la figura 5.4.

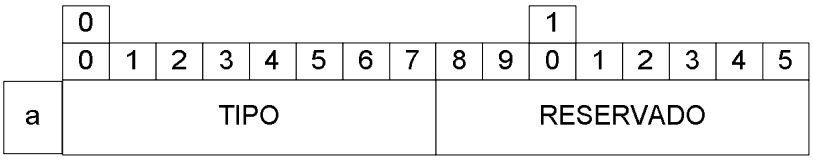


Figura 5. 4. Formato de mensaje RREP-ACK.

El **Tipo**: Indica el tipo de mensaje de acuerdo a la IANA (tabla 5.1) y **Reservado**: es para uso futuro; se envía como 0.

Este mensaje debe ser enviado en respuesta al mensaje RREP con la bandera "A" encendida. Esto típicamente se realiza cuando hay un riesgo de un enlace unidireccional previniendo un ciclo de descubrimiento de ruta.

5.2. Proceso de Funcionamiento

En esta sección se presenta el proceso de funcionamiento de AODV, por ejemplo; cuando generar un RREQ, un RREP o un RERR. Todos los mensajes de AODV son enviados por el puerto 654 usando UDP [5].

5.2.1. Uso del Número de Secuencia

En cada nodo se debe incluir la última información disponible acerca del número de secuencia para la dirección IP del nodo destino. Este número de secuencia es llamado "número de secuencia destino" y se incrementa cuando un nodo recibe información nueva de los mensajes RREQ, RREP o RERR.

Un nodo destino incrementa su número de secuencia en dos situaciones: La primera se hace antes que un nodo realice un descubrimiento de ruta (RREQ) y la segunda es antes de que el nodo envié un mensaje RREP en respuesta de un RREQ.

El formato del número de secuencia puede contener números enteros sin signos de 32 bits o utilizando números con signo de 32 bits. En el caso de utilizar 32 bits sin signo, el número máximo es 4,294,967,295, el siguiente valor es cero (0). Y en el otro caso el número máximo utilizando 32 bits con signo es el 2,147,483,647, solamente se utilizan 31 bits + 1 bit para el signo, el siguiente número será 2,147,483,648 que resulta el número más negativo utilizando el complemento a 2, es decir -2,147,483,647. Aunque la representación de números negativos en una secuencia de números para el caso de AODV no es recomendable [5].

5.2.2. Entradas de tablas

Cuando un nodo recibe paquetes de control (RREQ, RREP, RERR) de sus vecinos, crea o actualiza una ruta para un destino particular, primero revisa en su tabla de ruteo la información del destino. En caso de que no corresponda alguna entrada, se crea una nueva. El número de secuencia es determinado por la información contenida en el paquete de control. La ruta solo se actualiza si el nuevo número de secuencia contenido en el paquete:

- Es más grande que el número de secuencia en la tabla de ruteo.
- El número de secuencia es igual, pero el contador de saltos más uno, es menor que el contador de saltos de la tabla de ruteo.

El campo de tiempo de vida de la tabla de ruteo también se determinada del paquete de control o es inicializado como ACTIVE_ROUTE_TIMEOUT. Este tiempo de ruta es actualizado cada vez que se envía un paquete de datos.

5.2.3. Generando una Petición de Ruta

Cuando el nodo necesita una ruta a un destino y no tiene una disponible, se genera un mensaje de petición de ruta (RREQ) con el formato de la figura 5.1. El número de secuencia destino es el último número de secuencia conocido para ese destino. Si no se conoce ningún número de secuencia, la bandera de número de secuencia desconocido se habilita. El campo de RREQ ID es incrementado por unidad desde el último RREQ ID usado para el mismo nodo. Cada nodo mantiene solo una RREQ ID. El Contador es puesto a cero.

Antes de que se difunda el mensaje RREQ, el nodo almacena la RREQ ID y la dirección IP origen (su propia dirección) por un tiempo PATH_DISCOVERY_TIME. De esta manera cuando le lleguen los mensajes de los vecinos estos serán ignorados.

El número máximo de mensajes RREQ que se pueden crear por segundo esta dado por RREQ_RATELIMIT. Después de mandar el RREQ, el nodo espera un RREP (o cualquier otro mensaje de control). Si la respuesta no se recibe dentro de NET_TRAVERSAL_TIME milisegundos, el nodo envía otro RREQ, hasta un máximo de RREQ_RETRIES veces para un máximo valor TTL.

Los datos que esperan llegar a un destino son almacenados temporalmente hasta obtener una ruta, esto se hace de manera FIFO. Si la búsqueda de ruta pasa las RREQ_RETRIES veces sin ninguna respuesta de RREP, todos los paquetes de la FIFO se eliminan.

Para reducir la congestión en la red, se utiliza el método retroceso exponencial binario (BEB - *Binary Exponential Backoff*). La primera vez que el nodo envía el mensaje RREQ espera un RREP NET_TRAVERSAL_TIME milisegundos. Si este no llega vuelve a mandar otro RREQ

donde el tiempo de espera se realiza utilizando el BEB, por lo que para el segundo RREQ el tiempo de espera es 2*NET_TRAVERSAL_TIME milisegundos. Si no se recibe dentro de este nuevo periodo, otro mensaje RREQ deberá se mandando, hasta RREQ_RETRIES veces, adicional a la primera RREQ. Cada mensaje adicional deber ser multiplicado por 2 para obtener el nuevo tiempo de espera.

El nodo originador utiliza una técnica de búsqueda de expansión de anillo, para prevenir la propagación innecesaria de RREQs en la red. En la búsqueda de expansión de anillo, el nodo originador inicialmente usa un tiempo de vida TTL=TTL_START tomado del encabezado IP y además pone un tiempo máximo para recibir un RREP en RING_TRAVERSAL_TIME milisegundos. El TTL_VALUE es puesto al valor del campo TTL en el encabezado IP. Si el RREQ termina su tiempo sin novedades de RREP, el originador envía el RREQ de nuevo con el TTL incrementado por TTL_INCREMENT. Esto continúa hasta que TTL alcanza el valor máximo (TTL_THRESHOLD) antes de que llegue a TTL=NET_DIAMETER.

Un nodo que espera un RREP tiene un tiempo máximo de vida antes de ser eliminado, el cual está dado por (current_time+2*NET_TRAVERSAL_TIME). El tiempo máximo de vida antes de ser eliminada una ruta expirada está dada por un periodo de borrado, el cual está dado por (current_time+DELETE_PERIOD).

Cabe mencionar que los valores recomendados para los parámetros utilizados arriba se especifican en la sección 5.2.6.

Cuando un nodo recibe un mensaje RREQ, primero, según sea el caso, crea o actualiza la tabla de ruteo. Después determina si esta dentro del tiempo PATH_DISCOVERY_TIME para poder ser procesado, de otra manera, el mensaje RREQ se elimina. Si el mensaje RREQ es aceptado, primero se incrementa el contador de salto en 1. Después el nodo crea una ruta de regreso hacia el nodo Fuente, guardando la dirección IP del nodo que envió el mensaje, a este nodo se le conoce como Transmisor. El nodo transmisor es el nodo que reenvía un mensaje de control (RREQ, RREP, REER), de tal manera que solo un nodo fuente será Fuente-Transmisor y el resto de los nodos de la red son solamente Transmisores. La ruta de regreso se utiliza para enviar un

mensaje RREP a la fuente, también conocido como “siguiente salto”. Después el nodo compara en su tabla de ruteo la petición del nodo destino para saber si existe.

Para poder crear un RREP, el nodo debe ser el destino o tener una ruta hacia el destino que no haya expirado y con un número de secuencia mayor al indicado en el mensaje de petición de ruta, con el fin de tener la ruta más reciente. En el caso de tener la ruta más reciente o ser el nodo destino, se crea un mensaje de contestación de ruta (RREP) que será enviado a través de la ruta de regreso creada al inicio del proceso. En cambio si no se genera el RREP se reenvía la petición de ruta.

Un nodo puede recibir varios paquetes RREQ, en este caso para evitar un sobre flujo de paquetes cuando se recibe un RREQ se guarda la dirección IP del transmisor y el ID del mensaje. Así, cuando vuelva a recibir un RREQ con la misma información se omite el procedimiento, puesto que se asume que ya se trabajo en ese mensaje.

5.2.4. Generando Respuesta de Ruta

Como ya se mencionó, un nodo responde a una petición de ruta solo en el caso de que sea el nodo destino o si tiene una ruta hacia el nodo destino. Cuando se cumple estos requisitos, se crea un mensaje RREP hacia el nodo fuente. El formato de este mensaje se encuentra en la figura 5.2.

El nodo que esta creando el mensaje, enruta el mensaje hacia el nodo fuente enviandolo solo al siguiente salto. El siguiente salto es el nodo que envió la petición de ruta, guardada en la ruta de regreso por el RREQ.

El procedimiento que realiza el nodo que recibe el mensaje RREP es incrementar el contador de saltos en uno y despues crea o actualiza su tabla de ruteo. Tambien, establece un ruta de ida hacia el nodo destino. Esto lo hace guardando la dirección IP del nodo que le envio el RREP. Como en el caso del RREQ que se guarda la dirección que le envia el RREQ, ahora en el nodo se tienen

dos rutas establecidas, la de regreso, formada por el RREQ y la de ida, formada por el RREP. La primera se se utiliza para llegar al nodo fuente y la segunda se utiliza para llegar al nodo destino.

Continuando con el proceso, el mensaje RREP se envia por la ruta de regreso hasta llegar al nodo fuente. A los nodos que no les llega el mensaje RREP, eliminan la ruta de regreso despues del tiempo de vida asociado en su tabla.

Una vez que el nodo fuente recibe el mensaje RREP, ya puede utilizar la ruta para enviar los paquetes de datos hacia el destino. En el caso de que posteriormente se reciba un mensaje RREP con el número de secuencia destino mayor o igual que el primer RREP y además el contador de saltos sea menor, el nodo fuente actualiza su tabla de ruteo e inmediatamente utiliza la nueva ruta.

5.2.5. Generando Error de Ruta

Cuando uno nodo detecta un enlace caído con algún vecino que participe en la ruta, el nodo primero copia la distancia en saltos hacia el destino en el contador de último salto para ese nodo. Este dato se usa por si se requiere redescubrir la ruta. Después, el nodo marca el enlace como inválido actualizando la distancia hacia el destino en "∞" e incrementando el número de secuencia. El siguiente paso es revisar en su tabla si existe alguna otra ruta hacia el nodo destino. Si existe tal ruta, el nodo crea un mensaje de error de ruta (RERR). El formato del mensaje se observa en la figura 5.3.

El nodo que generó el RERR transmite este mensaje hacia toda la red mediante la dirección IP destino 255.255.255.255. Cuando los nodos reciben el mensaje RERR, deshabilitan las rutas que contienen al nodo inalcanzado solo si el nodo es usado como siguiente salto. Si existen más nodos en la ruta de regreso o ruta de ida, se generarán mensajes RERR hasta llegar al nodo fuente, por el lado de la ruta de regreso y al nodo destino, por el lado de la ruta de ida.

También se genera un mensaje de error (RERR) si un nodo recibe un paquete de datos para el cual no tiene alguna ruta establecida.

5.2.6. Parámetros Configurables

Algunos parámetros que se utilizan con sus valores, se muestran en la tabla 5.2.

Tabla 5. 2. Configuración de los parámetros en el protocolo AODV.

PARÁMETRO	VALOR
ACTIVE_ROUTE_TIMEOUT	3,000 Milisegundos
ALLOWED_HELLO_LOSS	2
BLACKLIST_TIMEOUT	RREQ_RETRIES * NET_TRAVERSAL_TIME
DELETE_PERIODO	K * max (ACTIVE_ROUTE_TIMEOUT,HELLO_INTERVAL) (Se recomienda K = 5)
HELLO_INTERVAL	1,000 Milisegundo
LOCAL_ADD_TTL	2
MAX_REPAIR_TTL	0.3 * NET_DIAMETER
MIN_REPAIR_TTL	La última cuenta de salto conocida al destino
MY_ROUTE_TIMEOUT	2 * ACTIVE_ROUTE_TIMEOUT
NET_DIAMETER	35
NET_TRAVERSAL_TIME	2 * NODE_TRAVERSAL_TIME * NET_DIAMETER
NEXT_HOP_WAIT	NODE_TRAVERSAL_TIME + 10
NODE_TRAVERSAL_TIME	40 Milisegundos
PATH_DISCOVERY_TIME	2 * NET_TRAVERSAL_TIME
RERR_RATELIMIT	10
RING_TRAVERSAL_TIME	2 * NODE_TRAVERSAL_TIME * (TTL_VALUE + TIMEOUT_BUFFER)
RREQ_RETRIES	2
RREQ_RATELIMIT	10
TIMEOUT_BUFFER	2
TTL_START	1
TTL_INCREMENT	2
TTL_THRESHOLD	7
TTL_VALUE	El valor del campo TTL en la cabecera IP

5.3. DISEÑO DE TOPOLOGÍA

Se propone una topología que muestre todas las facetas del algoritmo AODV, principalmente los mensajes RREQ, RREP y RERR, así como el reenvió de los mensajes, la omisión de mensajes repetidos, la eliminación de mensajes, eliminación de ruta, restablecimiento de ruta, entre otras. La topología propuesta se muestra en la figura 5.5.

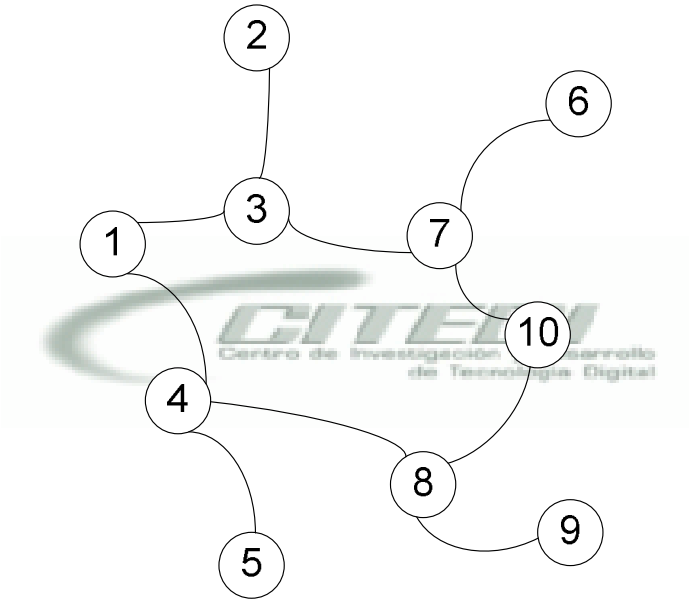


Figura 5. 5. Topología de una red experimental.

Consideraciones

Se tiene la topología de la figura 5.5, donde las líneas representan la conexión inalámbrica con dicho nodo y no representa una conexión física directa por medio de un cable. El problema inicia cuando se requiere una comunicación entre un par de nodos. Para el caso de ejemplificar se eligen los nodos 1 y el nodo 10, siendo el nodo 1 la fuente y destino el nodo 10.
La asignación de las direcciones IP para la red, se muestran en la tabla 5.3.

Tabla 5. 3. Relación de nodos con dirección IP.

Nodo	Dirección IP
1	1.0.0.1
2	1.0.0.2
3	1.0.0.3
4	1.0.0.4
5	1.0.0.5
6	1.0.0.6
7	1.0.0.7
8	1.0.0.8
9	1.0.0.9
10	1.0.0.10

5.4. ANÁLISIS DE RUTA

El algoritmo inicia solo cuando se requiere una comunicación entre un par de nodos. El procedimiento inicia con la petición de ruta o búsqueda de ruta, le sigue la contestación de ruta y finalmente para este caso en particular se realiza el error de ruta.

5.4.1. Petición de Ruta

Paso 1:

El nodo 1 inicia el procedimiento de petición de ruta del nodo 10. Pone el contador de saltos (Hop Count) en 0. Además incrementa una unidad el RREQ ID (1), almacena IP y RREQ IP de la fuente y transmite el mensaje RREQ hacia todos los nodos vecinos. Los valores de los campos del mensaje se muestran en la tabla 5.4.

Tabla 5. 4. Valores para RREQ nodo 1.

Descripción	Valor	Ubicación
Tipo	1	a0-0 al a0-7
Contador de Salto	0	a2-4 al a3-1
RREQ ID	1	B
IP Destino	1.0.0.10	C
Núm. Secuencia Destino	0	D
IP Fuente	1.0.0.1	E
Núm. Secuencia Fuente	1	F
Banderas: U	1	a1-1

De acuerdo al formato del mensaje para RREQ de la figura 5.1 y la asignación de los valores de la tabla 5.4, la información que se envía codificada en hexadecimal, donde cada par de números representa 8 bits, es la siguiente:

01 08 00 00 00 00 00 01 01 00 00 10 00 00 00 00 01 00 00 01 00 00 00 01

La información que no se presenta en la tabla se considera 0.

La figura 5.6 muestra la transmisión del mensaje RREQ.

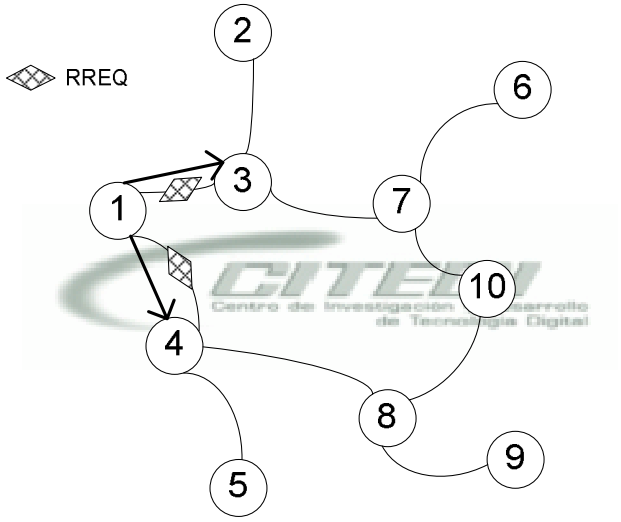


Figura 5. 6. Transmisión de RREQ.

Paso 2:

El mensaje transmitido llega a los nodos 3 y 4, estos almacenan en su tabla el IP Fuente, RREQ ID, el IP del nodo transmisor (nodo fuente o retransmisor). Busca si tuvo comunicación previa con el destino, en caso de encontrar una ruta previa, copia el número de saltos en un nuevo mensaje de respuesta de ruta y retransmite hacia el nodo fuente dicha información (informando que conoce al destino). En caso de no tener comunicación previa con el destino, incrementa contador en una unidad (1) y retransmite.

De acuerdo al formato del mensaje para RREQ, la información que se modifica es el contador de saltos ubicada en los campos a2-4 al a3-1 como se muestra en el cuarto par de números hexadecimales que estaba en 00 y cambio a 01. La información que se imprime en el estándar 802.11 es:

01 08 00 01 00 00 00 01 01 00 00 10 00 00 00 00 01 00 00 01 00 00 00 01

Paso 3:

El mensaje enviado por el nodo 3 llega a los siguientes nodos, 1, 2 y 7, mientras que el mensaje retransmitido por el nodo 4 llega a los nodos 1, 5 y 8. En este momento al nodo 1 le llega una petición de búsqueda para el nodo 10, la cual él originó, es el momento en el que consulta en su tabla la información que tenia almacenado en el paso 1 (la dirección IP y el RREQ ID) como estos son iguales, el nodo considera que es la misma información, por lo que descarta inmediatamente el mensaje de petición de ruta. El siguiente procedimiento lo realizan los nodos 2, 7, 5 y 8 que recibieron el mensaje de petición de ruta excepto el nodo 1. Primero le llega el mensaje. Posteriormente almacena IP y RREQ ID de la fuente así como IP del nodo Transmisor. Busca una ruta para el destino en sus tablas, inmediatamente si la encontró copia el número de saltos y lo retransmite a la fuente y si no encontró ruta, incrementa contador (2) y retransmite. La información que se envía es similar al paso 3 solo que incrementa el campo del contador de saltos a 2.

Paso 4:

De la misma manera, para los nodos que ya tengan la información del mensaje de petición de ruta, este nuevo mensaje no se considera, para evitar un lazo cerrado. Descartando al nodo 3 y 4, los nodos que reciben la petición de ruta son 6 y 10 por parte del nodo 7 y por parte del nodo 8 reciben el mensaje 9 y 10. En este caso, 6 y 9 se comportan de la misma manera que en el paso 3, por lo tanto se describe el procedimiento del nodo 10, que es el nodo Destino. En este caso le llegan dos peticiones al nodo 10, las cuales son las mismas, el nodo elige la que llegue primero, ya que los datos se almacenan en la tabla y cuando llega la otra petición reconoce que es una repetida (fig. 5.7).

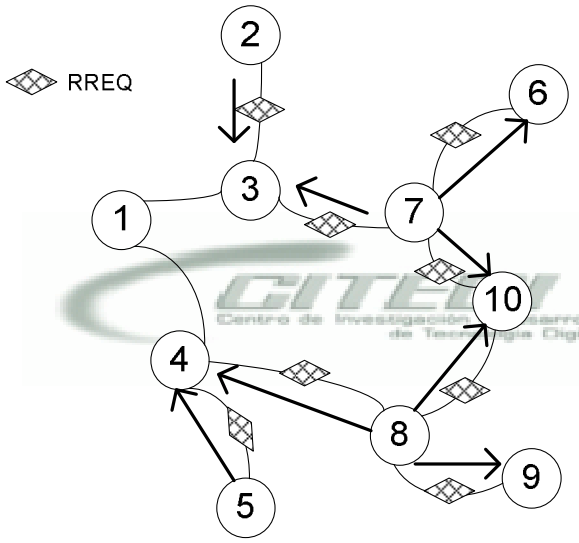


Figura 5. 7. Retransmisión de REEQ de los nodos 7 y 8.

El procedimiento es el siguiente, recibe el mensaje, almacena RREQ ID, IP de la Fuente e IP del transmisor. Busca ruta para destino en las tablas, por medio de los bits de la dirección destino, reconoce que es él el destino, por lo tanto inicia la creación de una respuesta de ruta (RREP).

5.4.2. Contestación de Ruta

Paso 5:

El proceso comienza cuando al nodo destino llega un mensaje de RREQ. El destino utiliza el mensaje RREQ para copiar la dirección Destino IP y el número de secuencia de la fuente del mensaje RREQ, en el nuevo mensaje RREP. Además, copia la IP del nodo transmisor y la incrusta en la trama del 802.11 como la dirección IP receptor. Además pone el contador de saltos en 0 y envía el mensaje RREP. Los valores de los campos del mensaje de acuerdo al formato de la figura 5.2 se muestran en la tabla 5.5.

Tabla 5. 5. Valores para el mensaje RREP en nodo 10.

Descripción	**Valor**	**Ubicación**
Tipo	2	a0-0 al a0-7
Contador de Salto	0	a2-4 al a3-1
IP Destino	1.0.0.10	b
Núm. Secuencia Destino	1	c
IP Fuente	1.0.0.1	d
Lifetime	6	e

El Tiempo de Vida (Lifetime) se calcula mediante la ecuación 6 y 7 [5].

Lifetime=MY_ROUTE_TIMEOUT Ec. 6

MY_ROUTE_TIMEOUT=2*ACTIVE_ROUTE_TIMEOUT Ec. 7

ACTIVE_ROUTE_TIMEOUT=3,000 milisegundos

La información que se incrusta a la trama 802.11 de acuerdo con el formato de mensaje de la figura 5.2 y la ubicación en la tabla 5.5 es:

02 00 00 00 01 00 00 10 00 00 00 01 01 00 00 01 00 00 00 06

La figura 5.8 muestra la transmisión del mensaje RREP.

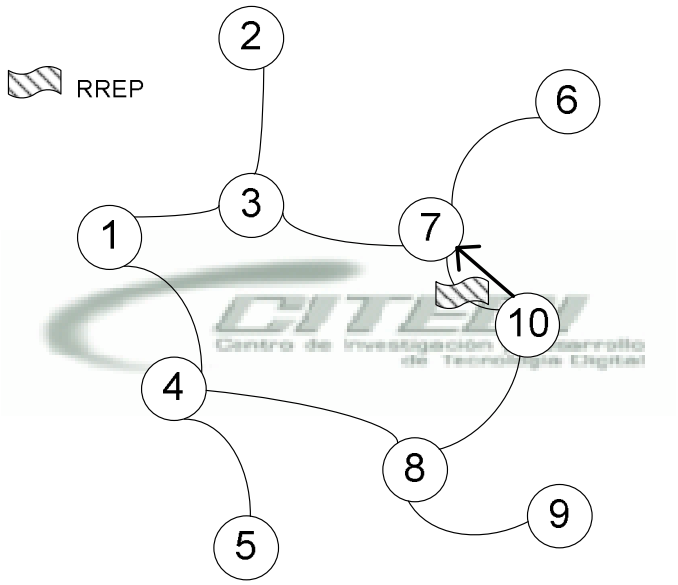


Figura 5. 8. Transmisión de RREP del nodo 10.

Paso 6:

Aquí, el nodo 7 y 8 reciben la petición de ruta, de los nodos 6 y 9 respectivamente, la cual en su tabla ya tenían almacenada la información, por lo tanto, descartan la operación, así mismo el nodo 7 recibe del nodo 10 una respuesta de ruta por lo que realiza el siguiente procedimiento: Compara el tipo de mensaje, después incrementa el contador (1). Guarda la IP del nodo transmisor, compara los bits de la dirección IP de la fuente con su propia dirección para saber si es el nodo fuente. Si coincide inicia la transmisión de la información almacenada en la memoria del nodo temporalmente, al no coincidir, reenvía el mensaje RREP al nodo siguiente (dirección IP guardada en el paso 3, la dirección IP del transmisor que se convierte en dirección IP del receptor). La información que se envía contenida del mensaje es idéntica a la información del paso 5 salvo el incremento en el campo del contador de salto a 1, ubicada en a2-4 al a3-1.

Paso 7:

En el paso número 7 el mensaje llega al nodo 3, verifica el tipo de mensaje, incrementa contador (2). Guarda la dirección IP del nodo transmisor, compara su dirección IP y la de la Fuente, al no coincidir, reenvía el mensaje RREP al siguiente nodo (guardado en el paso 2). Envía la misma información modificando a2-4 al a3-1 en 2.

Paso 8:

Durante este paso llega el mensaje RREP al nodo 1 (fuente). Identifica el tipo de mensaje e incrementa el contador (3). Compara los bits de la dirección IP con su Dirección, en este caso coinciden, por lo tanto almacena en su tabla la dirección IP Destino, Número de Saltos, Número de Secuencia y la IP del nodo transmisor.

En este momento inicia el proceso de Transmisión utilizando la ruta obtenida. La tabla 5.6 muestra el contenido de la información almacenada en el nodo 1.

Tabla 5. 6. Información almacenada en nodo 1.

Nodo 1

Destino	Receptor	Saltos	No. de Secuencia
1.0.0.10	1.0.0.3	3	1

La transmisión de los paquetes se realiza utilizando la ruta encontrada; pero ¿qué pasará si los nodos móviles cambian de ubicación? Suponiendo que después de un tiempo *t* la topología se va moviendo hasta que la conexión, entre el nodo 7 y el nodo 3, pierda conectividad, lo que tendríamos una topología como la de la figura 5.9. La flecha en la figura 5.9, indican el movimiento que sigue el nodo.

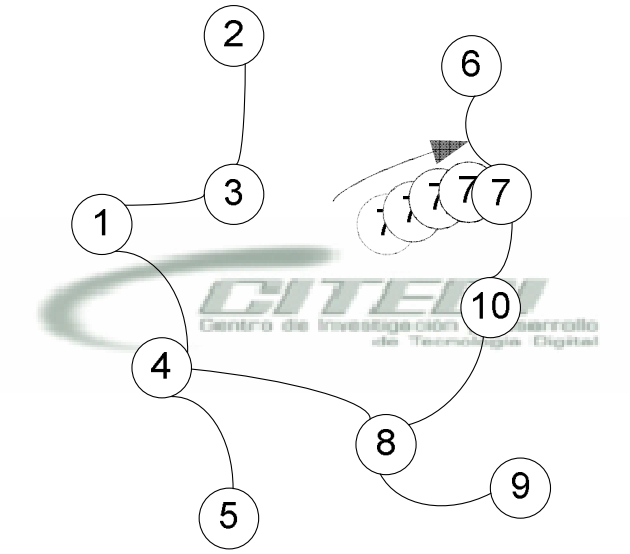


Figura 5. 9. Movimiento del nodo 7 después de un tiempo *t*.

El nodo 7 y 3 detectan la ruptura del enlace y empieza un proceso de reparación local. El cual tiene el siguiente procedimiento: Incrementa el número de secuencia para el destino (2). Después envía un RREQ para este destino. El TTL de este Mensaje RREQ está dado por la ecuación 8.

TTL=max(MIN_REPAIR_TTL,0.5*#hops)+LOCAL_ADD_TTL Ec. 8

donde MIN_REPAIR_TTL = el último número de saltos hacia el destino, #hops es el número de saltos de la fuente del paquete que no se ha alcanzado y LOCAL_ADD_TTL=2.

El nodo espera el periodo de búsqueda, dado por la ecuación 9, para recibir algún mensaje RREP en respuesta al RREQ que envió.

PATH_DISCO VERY_TIME = 2 * NET_TRAVER SAL_TIME Ec. 9
NET_TRAVER SAL_TIME = 2 * NODE_TRAVE RSAL_TIME * NET_DIAMET ER Ec. 10
NODE_TRAVE RSAL_TIME = 40 milisegund os
NET_DIAMET ER = 35
Sustituyen do Valores en Ec.10 y posteriorm ente en Ec.9
PATH_DISCO VERY_TIME = 5,600 milisegund os

El procedimiento y los mensajes son los mismos como se vieron al principio con la característica que se incrementa el número de secuencia.

5.4.3. Error de Ruta

Al no tener una respuesta después de 5,600 milisegundos, se realiza el procedimiento de mensaje de error RERR. La información que requiere el RERR de acuerdo con el formato de la figura 5.3 se tiene en la tabla 5.7:

Tabla 5. 7. Valores para RERR.

Descripción	**Valor**	**Ubicación**
Tipo	3	a0-0 al a0-7
Destinos no alcanzados	1	a2-4 al a3-1
Dirección IP Destino	1.0.0.10	b
Núm. Secuencia Destino	1	c

La información enviada de acuerdo al formato del mensaje RERR y a la ubicación de los valores es:

03 00 00 01 01 00 00 10 00 00 00 01 00 00 00 00 00 00 00 00

Se envía a todos los nodos y en cada nodo se actualiza la información necesaria, marcando como inválido las entradas que utilicen al nodo inalcanzable. Una vez eliminada la ruta, si existen más paquetes para el mismo destino, se realiza de nuevo el procedimiento de petición de ruta, de lo contrario simplemente se queda la red en reposo. Para este caso vamos a ejemplificar que simplemente se tiene más información que enviar al nodo 10. Por lo tanto el nodo 1 realiza el procedimiento necesario para buscar al nodo 10, y al finalizar el procedimiento tenemos la tabla 5.8 del nodo 1.

Tabla 5. 8. Información Actualizada del nodo 1.

Nodo 1			
Destino	Receptor	Saltos	No. de Secuencia
~~**1.0.0.10**~~	~~1.0.0.3~~	~~3~~	~~1~~
1.0.0.10	1.0.0.4	3	2

Inmediatamente después de tener el mensaje de notificación de ruta (RREP), el nodo fuente comienza la retransmisión hacia el nodo destino.

En este capítulo se presentó el formato de los mensajes de control que utiliza algoritmo reactivo de vector distancia AODV. También se realizó un análisis del procedimiento que realiza el algoritmo para establecer una comunicación.

Una vez explicado el funcionamiento del algoritmo, en el capítulo 6 se procederá a realizar las comparaciones mediante simulación utilizando NCTUns.

6

SIMULACIÓN Y COMPARACIÓN DE OLSR vs AODV

En este capítulo se presenta la metodología para realizar la simulación y las comparaciones de los protocolos especificados en los capítulos 4 y 5, así como los resultados de dichas simulaciones.

Para poder hacer una comparación realista del algoritmo se definieron 5 escenarios para la simulación de cada protocolo. Cada escenario corresponde a un área rectangular 5000 m^2 (100m x 50m) sin obstáculos, se asume que se utiliza el mismo ancho de banda, el mismo tiempo de respuesta y la misma área de cobertura de cada nodo. Los escenarios difieren en tres parámetros importantes que se utilizan para conocer el desempeño del algoritmo, población (número de nodos), tráfico (transmisión simultánea en otros nodos) y tamaño del paquete enviado por el nodo fuente al nodo destino. En la tabla 6.1 se muestra la descripción de los escenarios.

Tabla 6. 1. Descripción de los Escenarios de Simulación

	Población		**Tráfico**		**Tamaño**	
	30	**90**	**No**	**Si**	**1400**	**15000**
Escenario 1	X		X		X	
Escenario 2	X		X			X
Escenario 3	X			X	X	
Escenario 4	X			X		X
Escenario 5		X	X		X	

6.1. CARACTERIZACIÓN DE PARÁMETROS

6.1.1. Población

La población se creó en un área mencionada de 100m x 50m, los nodos móviles fueron distribuidos aleatoriamente. El 80% de los escenarios se realizaron con 30 nodos y el otro 20% se triplicó la población dando como resultado 90 nodos, esto se hace con el fin de observar los efectos que tiene el tamaño de la población en una comunicación. Como se puede apreciar en la figura 6.1 y 6.2 la distribución de las redes en ambos casos.

Figura 6. 1. Escenario con 30 nodos.

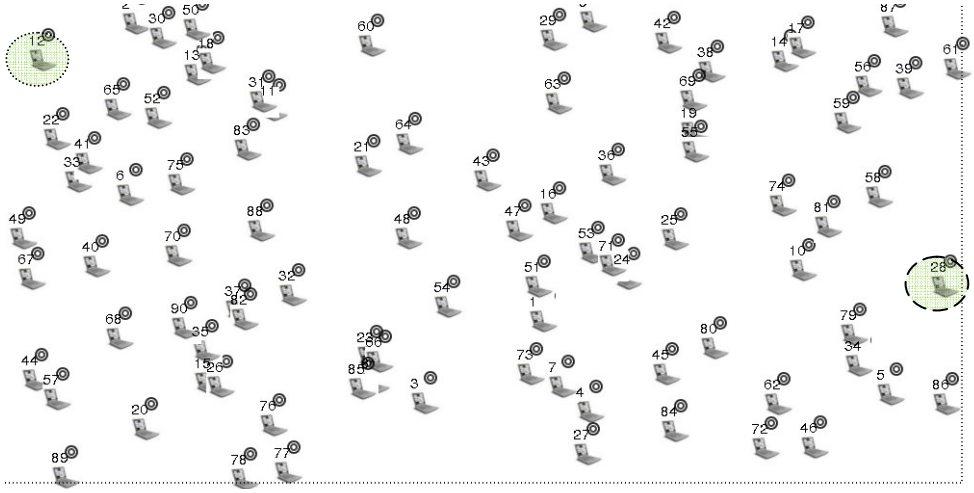


Figura 6. 2. Escenario con 90 nodos.

6.1.2. Tráfico

Se considera tráfico en la red, cuando otros nodos están transmitiendo al mismo tiempo que el nodo fuente. Los escenarios con tráfico se especificaron con un 66.66% de la población que están manteniendo una comunicación (Transmisión o Recepción) por lo tanto en el caso de un tráfico con población de 30 nodos, existen 20 nodos activos de los cuales 10 en Tx y 10 en Rx (10 parejas de nodos). De la misma manera, en el caso de población de 90 nodos, 60 nodos (66.66%) están activos (30 parejas). El tamaño de los paquetes, de los nodos que están transmitiendo simultáneamente que el nodo fuente, es de 512 bits por un periodo de 80 segundos empezando 1 segundo después de establecerse la comunicación. En la tabla 6.2 se observan los nodos que se encuentran activos para los escenarios con 30 nodos y para escenarios con 90 nodos.

Tabla 6. 2. Pares de Nodos Activos

Fuente	06	21	05	27	29	22	09	16	17	14	31	50	60	35	75	65	72	69	45	43	71	02	63	85	23	14	77	35	06	90
Destino	11	30	10	01	19	15	17	26	15	30	40	51	33	41	39	38	88	89	72	48	55	81	73	47	24	63	88	59	66	44
Escenarios con 30 Nodos																														
Escenarios con 90 Nodos																														

6.1.3. Tamaño de Paquetes

El tamaño de los paquetes que envía el nodo fuente varía en cada escenario teniendo como valores de 1400 bits y 15000 bits, que corresponden a una transmisión de un mensaje de información corto o un archivo pequeño para el primer caso y para un mensaje de información largo o un archivo grande.

6.2. INICIALIZANDO EL SIMULADOR DE RED

La simulación de la red Ad Hoc es realizada utilizando el simulador de red NCTUns [44]. Algunos parámetros importantes para la simulación en NCTUns son: Capa Física, Propagación y Protocolo de Ruteo.

6.2.1. Capa Física

El simulador NCTUns trae por default el estándar IEEE 802.11b para dispositivos móviles inalámbricos. Los parámetros más importantes se muestran en la tabla 6.3.

Tabla 6. 3. Parámetros en NCTUns.

Parámetro	Valor
Estándar	IEEE 802.11b
Frecuencia	2.4 GHz
Tasa de Datos	11 Mbps

6.2.2. Propagación

Para tener un modelo real de la señal de propagación se usa el modelo de pérdida de trayectoria de dos rayos. Teniendo que un valor aproximado real medido para uso interior un rango de comunicación de 25 mts.

6.2.3. Protocolo de Ruteo

De acuerdo a la investigación realizada de los protocolos más populares para redes inalámbricas ad hoc se utilizan los protocolos AODV y OLSR. Teniendo la siguiente configuración en el simulador. En la tabla 6.4 muestra los parámetros más importantes para AODV, los que tienen relación con el tiempo, la unidad es en milisegundos.

Tabla 6. 4. Parámetros para AODV en NCTUns.

Parámetro	Valor
Intervalo Hello	1000
Hello permitidos perdidos	2
Tiempo de ruta activa	3000
Periodo de Borrado	3000
Diámetro de Red	15
Tiempo de cruzar un nodo	40
Intentos RREQ	5
Limite de RREQ	10
Limite de RERR	10

En la tabla 6.5 se muestran los valores típicos para OLSR en NCTUns.

Tabla 6. 5. Parámetros para OLSR.

Parámetro	Valor
Intervalo Hello	2000
Hello Hold	6000
Intervalo TC	5000
TC Hold	15000
Cobertura MPR	5

6.3. ESCENARIO DE COMUNICACIÓN

El principal objetivo de la simulación de la red Ad Hoc en NCTUns es para investigar la influencia de la población, tráfico y el tamaño de paquetes del nodo en los protocolos de ruteo.

Cada nodo fuente genera paquetes de datos de tamaño dependiendo cada escenario, 1400 y 15000 bits durante un periodo de 100 segundos. El tiempo entre generación de dos paquetes sucesivos es de 0.5 segundos. La transmisión del primer paquete de datos empieza a partir de 1 segundo después de haber iniciado la simulación, subsecuentemente los pares fuentes-destino empiezan con el intercambio de la transmisión de paquetes por un corto tiempo, para evitar un numero grande de RREQ cuando se usa AODV. El máximo número de pares activos fuente-destino permanece constante. El tráfico es generado usando el generador de tráfico de NCTUns la cual emplea el protocolo de transporte UDP.

6.3.1. Distancia

La distancia entre dos nodos *1* y *2* está definida por la distancia Euclidiana entre estos nodos. Esto se muestra mediante la ecuación 11:

$$distancia(1,2) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \qquad \text{Ec. 11}$$

Donde x_1 y y_1 son las coordenadas del punto 1, mientras que x_2 y y_2 son las coordenadas del punto 2.

Para poder utilizar la ecuación 11 se tiene la siguiente información:

Posición
Nodo 12 (45,61)
Nodo 28 (982,296)

Utilizando la Ec. 11, y sustituyendo los datos necesarios se tiene:

$$distancia(12,28) = \sqrt{(982 - 45)^2 + (296 - 61)^2}$$
$$distancia(12,28) = 966.01967$$

Esto no quiere decir que la distancia es de 966 mts, de acuerdo a [45], los nodos se encuentran a una proporción de 0.1 Metros por Pixel [45], lo que significa que:

$$distancia(12,28) \times 0.1 = 96.601967$$

Esto indica que los nodos no se encuentran dentro del área de transmisión, lo que permite utilizar un algoritmo de ruteo al no estar conectadas directamente.

6.4. PROGRAMACIÓN EN NCTUNS

A continuación se presenta el pseudocódigo requerido para la definición de los nodos en NCTUns [46].

Create Node 1 as MOBILE with name = MOBILE1
Define port 1
Module Interface : Node1_Interface_LINK_1
Set Node1_Interface_LINK_1.ip = 1.0.1.1
Set Node1_Interface_LINK_1.netmask = 255.255.255.0

Module AODV : Node1_AODV_LINK_1
Set Node1_AODV_LINK_1.HELLO_INTERVAL = 1000
Set Node1_AODV_LINK_1.ALLOWED_HELLO_LOSS = 2
Set Node1_AODV_LINK_1.ACTIVE_ROUTE_TIMEOUT = 3000
Set Node1_AODV_LINK_1.DELETE_PERIOD = 3000
Set Node1_AODV_LINK_1.NET_DIAMETER = 15
Set Node1_AODV_LINK_1.NODE_TRAVERSAL_TIME = 40
Set Node1_AODV_LINK_1.RREQ_RETRIES = 5
Set Node1_AODV_LINK_1.RREQ_RATELIMIT = 10
Set Node1_AODV_LINK_1.RERR_RATELIMIT = 10

Module FIFO : Node1_FIFO_LINK_1
Set Node1_FIFO_LINK_1.max_qlen = 50
Set Node1_FIFO_LINK_1.log_qlen = on
Set Node1_FIFO_LINK_1.log_option = FullLog
Set Node1_FIFO_LINK_1.samplerate = 1

Module MAC80211 : Node1_MAC80211_LINK_1
Set Node1_MAC80211_LINK_1.mac = 0:1:0:0:0:2
Set Node1_MAC80211_LINK_1.PromisOpt = off
Set Node1_MAC80211_LINK_1.RTS_Threshold = 3000

```
Module Wphy : Node1_Wphy_LINK_1
        Set Node1_Wphy_LINK_1.BeamWidth = 360
        Set Node1_Wphy_LINK_1.PointingDirection = 90
        Set Node1_Wphy_LINK_1.AngularSpeed = 0
        Set Node1_Wphy_LINK_1.Bw = 11
        Set Node1_Wphy_LINK_1.freq = 3
        Set Node1_Wphy_LINK_1.BER = 0.0
        Set Node1_Wphy_LINK_1.TransRange = 25
        Set Node1_Wphy_LINK_1.InferRange = 35

    EndDefine

EndCreate
```

Se observa que un nodo está conformado principalmente por 5 módulos, el módulo de la interface, el del algoritmo de ruteo, módulo de la memoria, el módulo del mac y por último el módulo de la capa física. De la misma forma se procede para los 30 o 90 nodos según sea el cado del escenario.

Después de tener todos los nodos, se requiere que exista una comunicación entre un par de nodos. El pseudocódigo para conectar dos nodos es el siguiente:

```
#nctuns traffic generator file
$node_(12) 1.000000 100.000000 stg -u 1400 100 1.0.1.28
$node_(28) 0.000000 100.000000 rtg -u -w log
```

Se utiliza el generador de tráfico de NCTUns para crear un enlace con un par de nodos, donde los comandos “rtg” y “stg” se utilizan para Recibir y Enviar tráfico respectivamente.

En el caso de los escenarios con "tráfico" el pseudocódigo es el siguiente, donde el tamaño de paquete se mantiene constante a un valor de 512 bits mientras que el par de nodos principal cambia de 1400 bits a 15000 bits.

#nctuns traffic generator file
$node_(1) 0.000000 100.000000 rtg -u -w log
$node_(5) 1.000000 100.000000 stg -u 512 80 1.0.1.10
$node_(6) 1.000000 100.000000 stg -u 512 80 1.0.1.11
$node_(9) 1.000000 100.000000 stg -u 512 80 1.0.1.17
$node_(10) 0.000000 100.000000 rtg -u -w log
$node_(11) 0.000000 100.000000 rtg -u -w log
$node_(12) 1.000000 100.000000 stg -u 1400 100 1.0.1.28
$node_(14) 1.000000 100.000000 stg -u 512 80 1.0.1.30
$node_(15) 0.000000 100.000000 rtg -u -w log
$node_(15) 0.000000 100.000000 rtg -u -w log
$node_(16) 1.000000 100.000000 stg -u 512 80 1.0.1.26
$node_(17) 0.000000 100.000000 rtg -u -w log
$node_(17) 1.000000 100.000000 stg -u 512 80 1.0.1.15
$node_(19) 0.000000 100.000000 rtg -u -w log
$node_(21) 1.000000 100.000000 stg -u 512 80 1.0.1.30
$node_(22) 1.000000 100.000000 stg -u 512 80 1.0.1.15
$node_(26) 0.000000 100.000000 rtg -u -w log
$node_(27) 1.000000 100.000000 stg -u 512 80 1.0.1.1
$node_(28) 0.000000 100.000000 rtg -u -w log
$node_(29) 1.000000 100.000000 stg -u 512 80 1.0.1.19
$node_(30) 0.000000 100.000000 rtg -u -w log
$node_(30) 0.000000 100.000000 rtg -u -w log

6.5. RESULTADOS DE LAS SIMULACIONES

En esta sección se presenta una evaluación de la simulación de la red ad-hoc realizada en el simulador de red NCTUns usando los algoritmos de ruteo AODV y OLSR. Ya que lo interesante en este caso es saber qué algoritmo tiene mayor efectividad en entregar paquetes a su destino, la evaluación está restringida a la siguiente métrica: el número de paquetes perdidos.

El resultado de cada nodo en cada escenario de los paquetes perdidos se muestra en las siguientes figuras. En la figura 6.3 se muestran los resultados de cada nodo para el escenario 1.

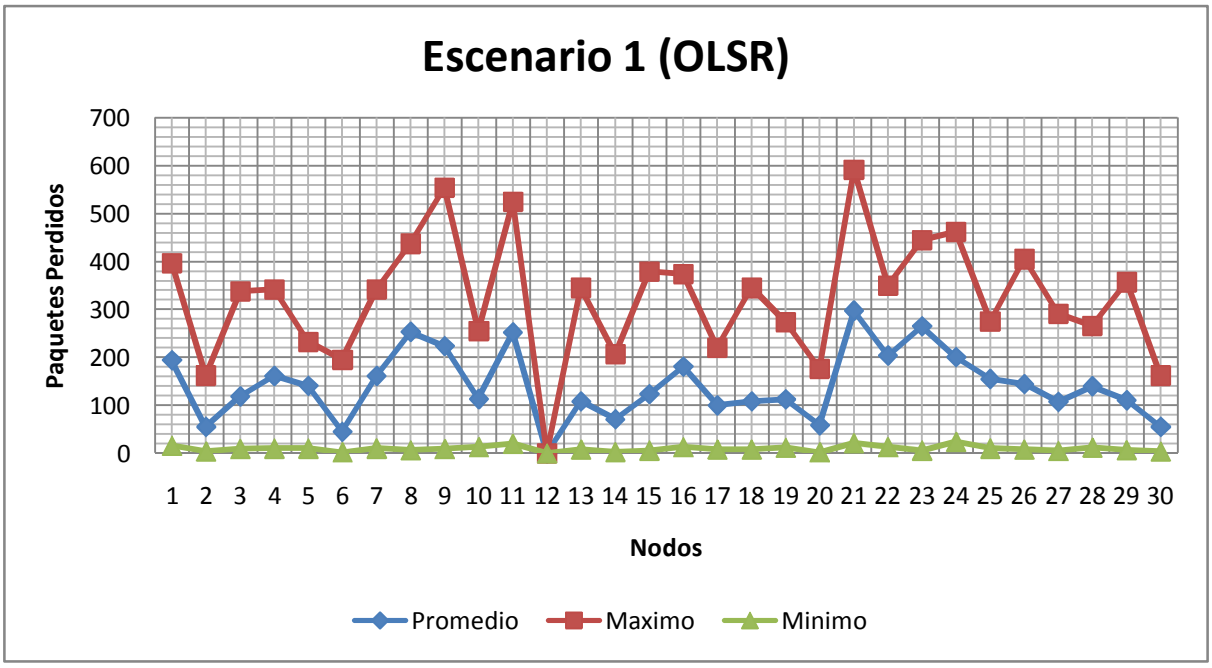


Figura 6. 3. Grafica de resultados de cada nodo del escenario 1 con OLSR, población de 30 nodos, sin tráfico y tamaño de paquete de 1400 bits.

Se observa en la figura 6.3 el comportamiento de cada nodo, durante el tiempo de simulación (100 segundos). Se infiere que el promedio de paquetes perdidos del nodo 1 es aproximadamente 200 paquetes, mientras que el máximo número de paquetes que llegó a perder el nodo 1 es aproximadamente 400. También se observa que el nodo que perdió más paquetes es el nodo 21. En el caso del nodo 12, se observa que no tiene paquetes perdidos, por lo que se concluye que este nodo entrego todos sus paquetes correctamente.

En promedio, se puede decir que en toda la red se perdió un total de 141.7 paquetes. Algunos datos generales del escenario se presentan en la tabla 6.6

Tabla 6. 6. Resultados del escenario 1 con OLSR.

Promedio del Escenario	141.7
Promedio Max	323.3
Promedio Min	9.333

En la figura 6.4 se muestran los resultados del escenario 2, donde se incrementa el tamaño del paquete a 15000 bits.

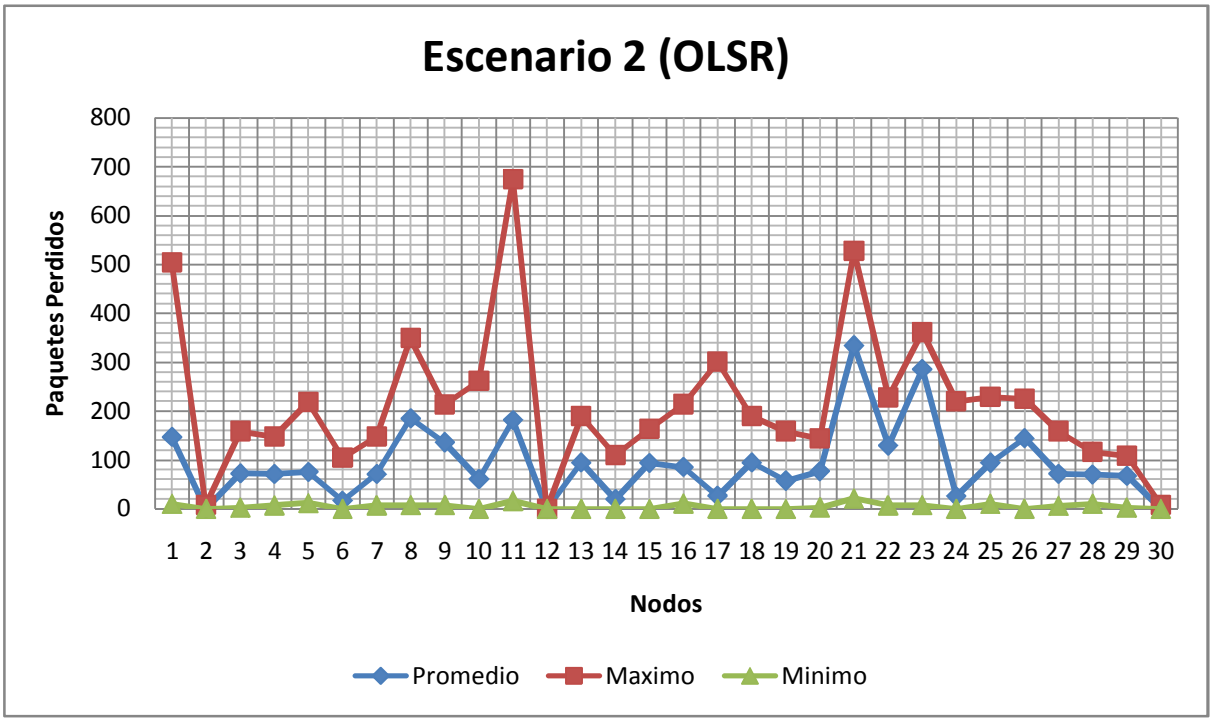


Figura 6. 4. Gráfica de resultados de cada nodo del escenario 2 con un paquete de 15000 bits, sin tráfico, población de 30 nodos usando OLSR.

De la misma manera, en la figura 6.4 se observa el comportamiento de cada nodo. Mostrando drásticamente que el nodo 11 tuvo el mayor número de paquetes perdidos en un instante de tiempo con aproximadamente 700. Pero en promedio general, el nodo 21 tuvo el mayor número de paquetes perdidos, lo que se asume que el nodo 21 fue el que perdió más paquetes. En general el escenario tuvo una pérdida de 93.1 paquetes, como se muestra en la tabla 6.7.

Tabla 6. 7. Resultados del escenario 2 con OLSR

Promedio del Escenario	93.128
Promedio Max	214.7
Promedio Min	4.93333333

En la figura 6.5 se muestran los resultados para el escenario 3. Donde las condiciones de población son las mismas (30 nodos), el tamaño del paquete de fuente a destino es de 1400 bits y con una afluencia de 10 pares de nodos con tráfico de 512 bits.

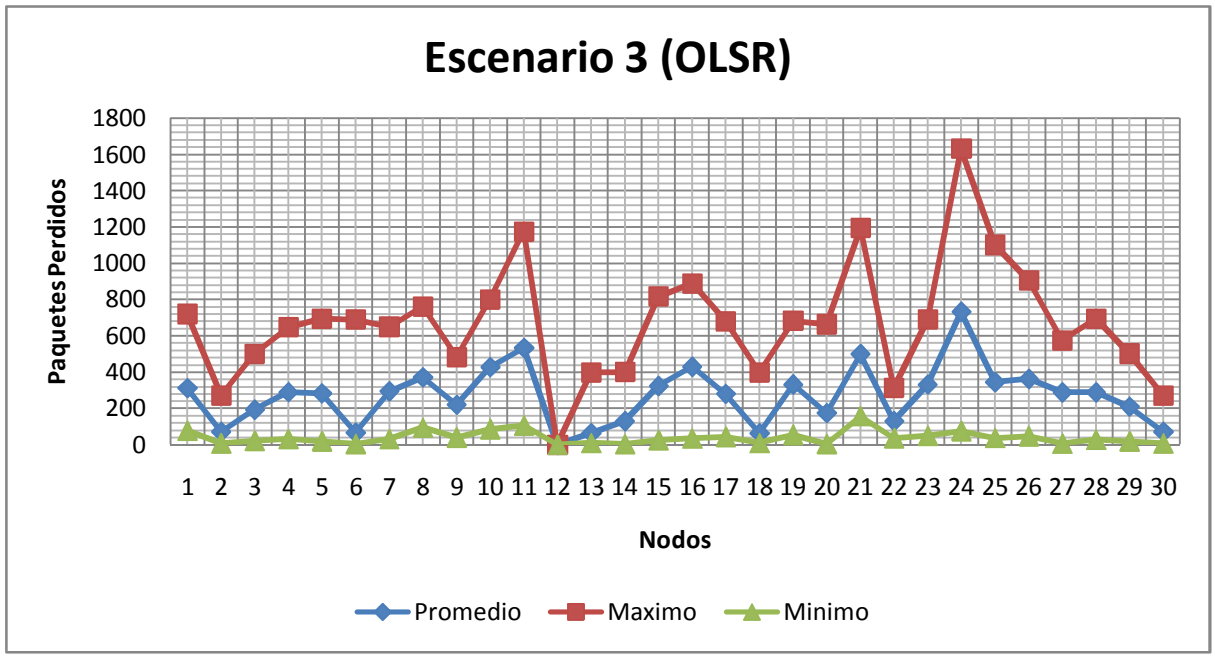


Figura 6. 5. Resultados de cada nodo del escenario 3, con población de 30 nodos, con el 66.66% de los nodos activos con tráfico de 512 bits, paquete de transmisión de 1400 bits, usando OLSR.

En general para este escenario, se perdieron 270.6 paquetes, como lo presenta la tabla 6.8.

Tabla 6. 8. Resultados del escenario 3 con OLSR.

Promedio del Escenario	270.6
Promedio Max	673.2
Promedio Min	38.6

En el escenario 4 se modificó el parámetro del tamaño del paquete que se envía. Mientras que la población permanece en 30 nodos con tráfico. Los resultados de esta simulación se presentan en la figura 6.6.

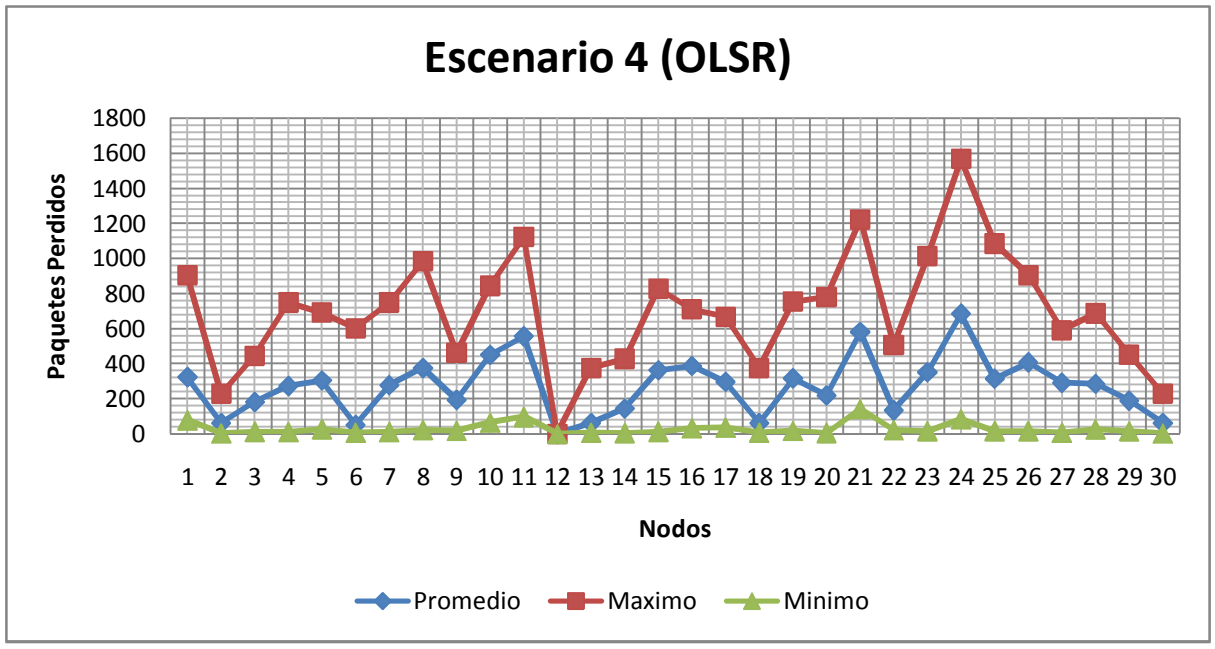


Figura 6. 6. Grafica de Resultados de cada nodo del escenario 4, usando OLSR, una población de 30 nodos, con el 66.66% nodos activos con trafico de 512 bits, con un paquete de 15000 bits.

En promedio para el escenario se perdió 272.84 paquetes, como se muestra en la tabla 6.9.

Tabla 6. 9. Resultado del escenario 4 con OLSR.

Promedio del Escenario	272.8436667
Promedio Max	698.3
Promedio Min	26.56666667

En el escenario 5, se incrementa el número de nodos a 90. Con el tamaño de paquete entre fuente destino de 1400 bits y sin tráfico. Los resultados de cada nodo se muestran en la figura 6.7

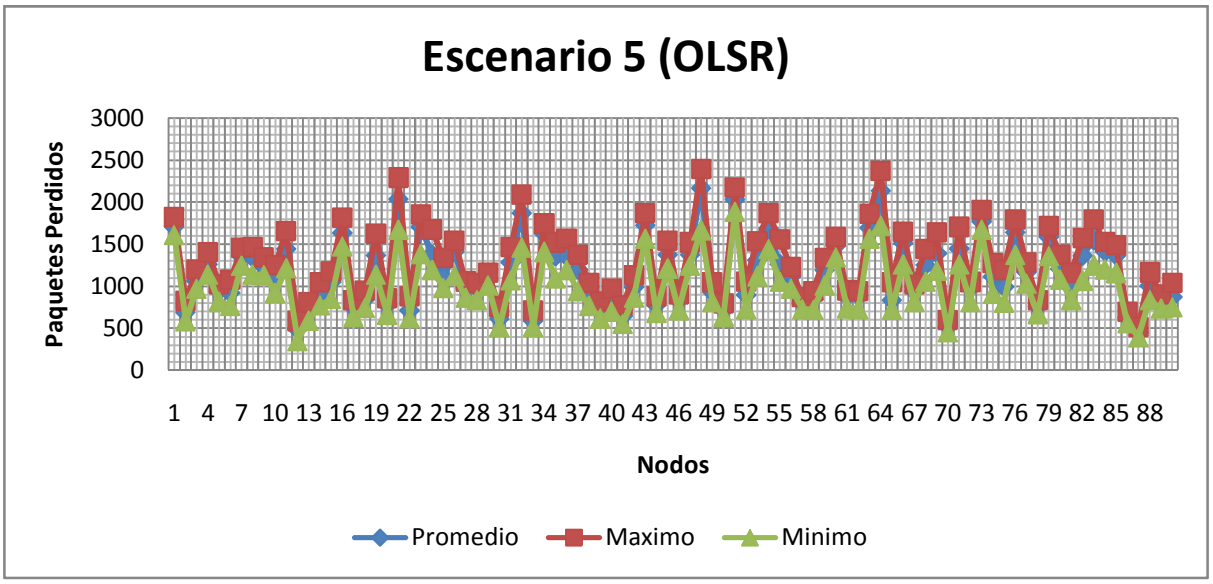


Figura 6. 7. Grafica de resultados de cada nodo del escenario 5; con una población de 90 nodos, sin tráfico, enviando un paquete de 1400 bits, usando OLSR.

Se observa que se incrementó el número de paquetes perdidos, a consecuencia del incremento del número de nodos. El promedio general del escenario y el promedio de los máximos y mínimos esta mostrado en la tabla 6.10.

Tabla 6. 10. Resultados del escenario 5 con OLSR.

Promedio del Escenario	372.15
Promedio Max	419.7
Promedio Min	322.12

El escenario con AODV, tiene las mismas características de población, tráfico y tamaño de paquete del nodo fuente al nodo destino que el escenario 1 con OLSR. Cambiando el algoritmo de ruteo de OLSR a AODV. En la figura 6.8, se muestran los resultados de la simulación. Se observa que el número de nodos que entregan todos sus paquetes es mayor al escenario donde se utiliza el algoritmo OLSR.

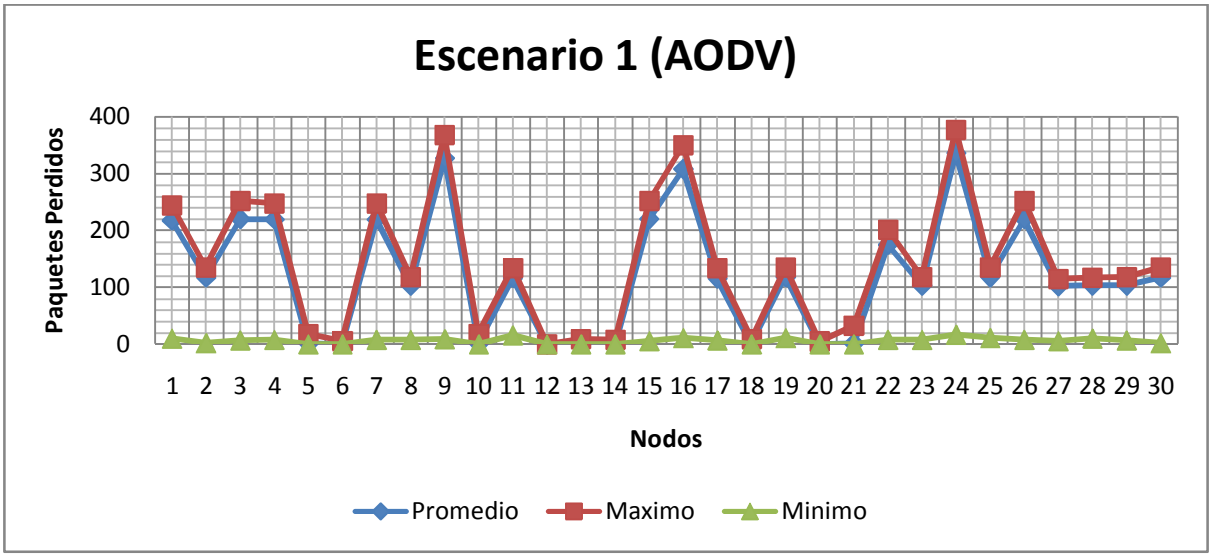


Figura 6. 8. Grafica Grafica de resultados de cada nodo del escenario 1 con AODV, población de 30 nodos, sin tráfico y tamaño de paquete de 1400 bits.

En promedio, el escenario tuvo una pérdida de 122.85 paquetes, mientras que el promedio máximo de paquetes que se perdió fue de 143. Estos datos se presentan en la tabla 6.11.

Tabla 6. 11. Resultados del escenario 1 con AODV.

Promedio del Escenario	122.856333
Promedio Max	143.066667
Promedio Min	6

De la misma manera, el escenario 2 con AODV, equivale al escenario 2 con OLSR, solo que utilizando el protocolo AODV. La figura 6.9 muestra el comportamiento de los nodos durante el tiempo de simulación.

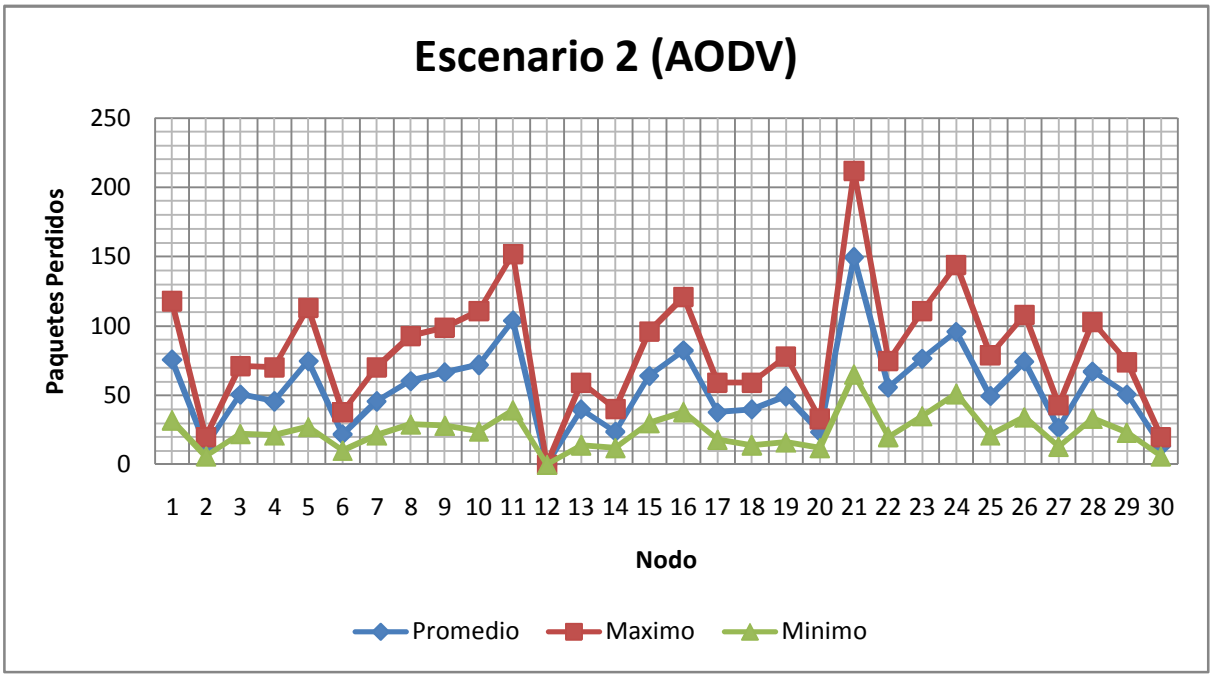


Figura 6. 9. Gráfica de resultados de cada nodo del escenario 2 con un paquete de 15000 bits, sin tráfico, población de 30 nodos usando AODV.

Se puede observar que el nodo 21 en promedio ha perdido aproximadamente 150 paquetes. En general el desempeño de la red se muestra en la tabla 6.12.

Tabla 6. 12. Resultados del escenario 2 con AODV.

Promedio del Escenario	55.03066667
Promedio Max	82.3
Promedio Min	23.8

En el escenario 3 con AODV, se agrega tráfico a la red, utilizando 1400 bits como el tamaño de los paquetes del nodo fuente. Los resultados de la simulación de cada nodo se muestran en la figura 6.10.

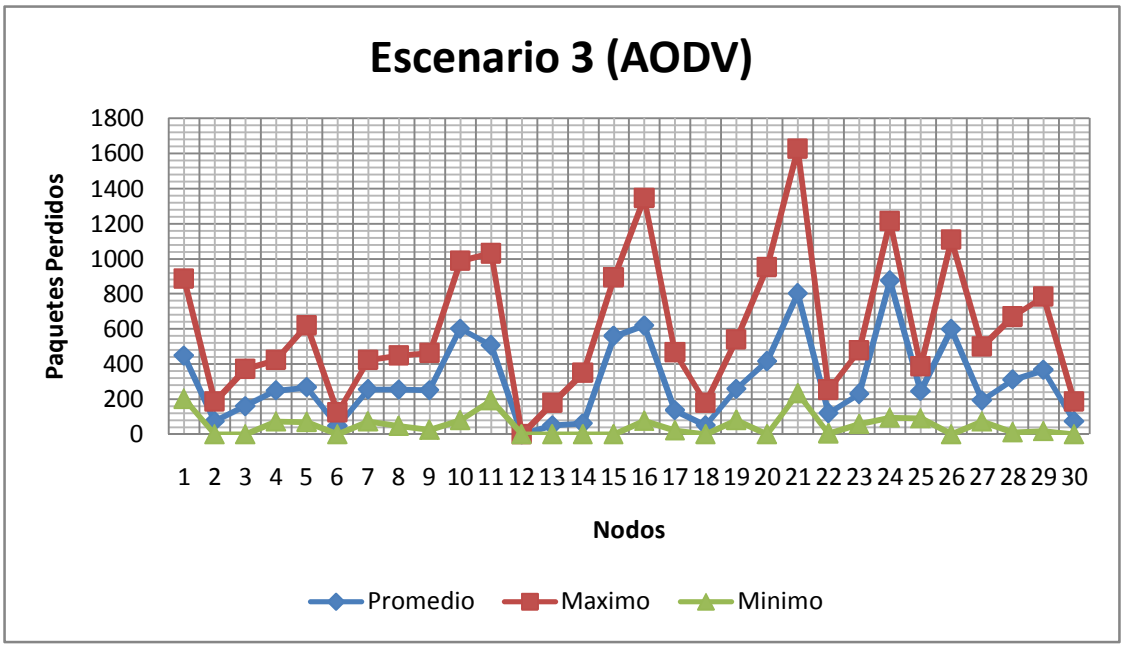


Figura 6. 10. Resultados de cada nodo del escenario 3, con población de 30 nodos, con el 66.66% de los nodos activos con tráfico de 512 bits, paquete de transmisión de 1400 bits, usando AODV.

Se observa que al introducir tráfico a la red, se incrementa el número de paquetes perdidos en cada nodo. En general, los resultados del escenario se muestran en la tabla 6.13.

Tabla 6. 13. Resultados del escenario 3 con AODV.

Promedio del Escenario	301.969333
Promedio Max	602.4
Promedio Min	51.1

El comportamiento de cada nodo del escenario 4 utilizando AODV, se presenta en la figura 6.11. En este caso el escenario se caracteriza con una población de 30, con tráfico y con un tamaño del paquete de 15000.

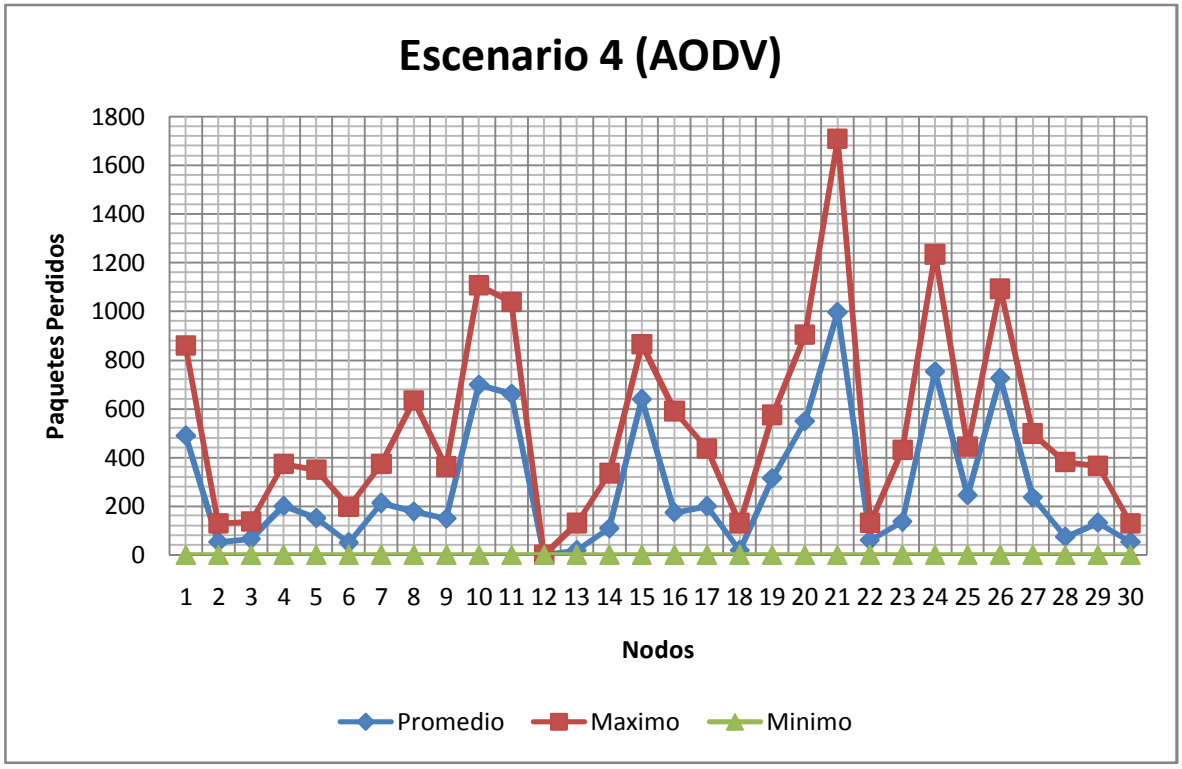


Figura 6. 11. Grafica de Resultados de cada nodo del escenario 4, usando AODV, una población de 30 nodos, con el 66.66% nodos activos con trafico de 512 bits, con un paquete de 15000 bits

Algunos datos generales del escenario se presentan en la tabla 6.14.

Tabla 6. 14. Resultados del escenario 4 con AODV.

Promedio del Escenario	278.135
Promedio Max	530.966667
Promedio Min	0

En el escenario 5 con AODV, se incrementa el número de nodos de la red. Eliminando el tráfico de los nodos restantes y con un tamaño de paquetes de nodo fuente a destino de 1400 bits. La figura 6.12 muestra los resultados de cada nodo durante el tiempo de simulación.

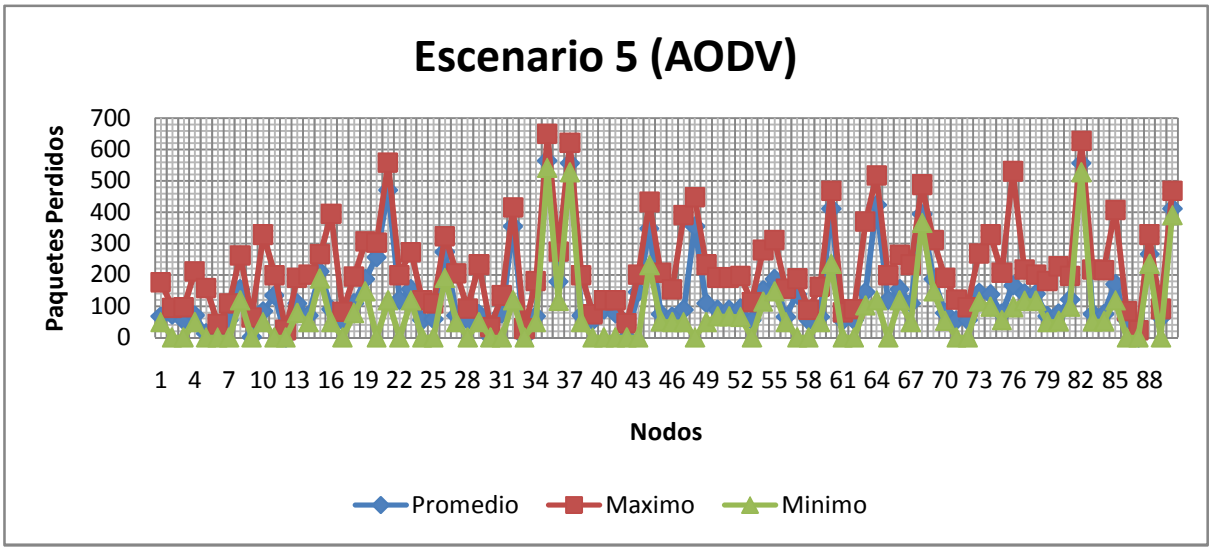


Figura 6. 12. Grafica de resultados de cada nodo del escenario 5; con una población de 90 nodos, sin tráfico, enviando un paquete de 1400 bits, usando OLSR.

En general, el promedio de pedida de paquetes para este escenario es de 137.36, lo que hace pensar que AODV no presenta grandes pérdidas al incrementar el número de nodos en comparación con OLSR.

Tabla 6. 15. Resultados escenario 5 con AODV.

Promedio del Escenario	137.36
Promedio Max	231.69
Promedio Min	79.1

De acuerdo con los valores obtenidos, se realiza la comparación de cada escenario con los dos protocolos. En la figura 6.13 se muestra las comparaciones de OLSR con AODV en el desempeño de los 5 diferentes escenarios.

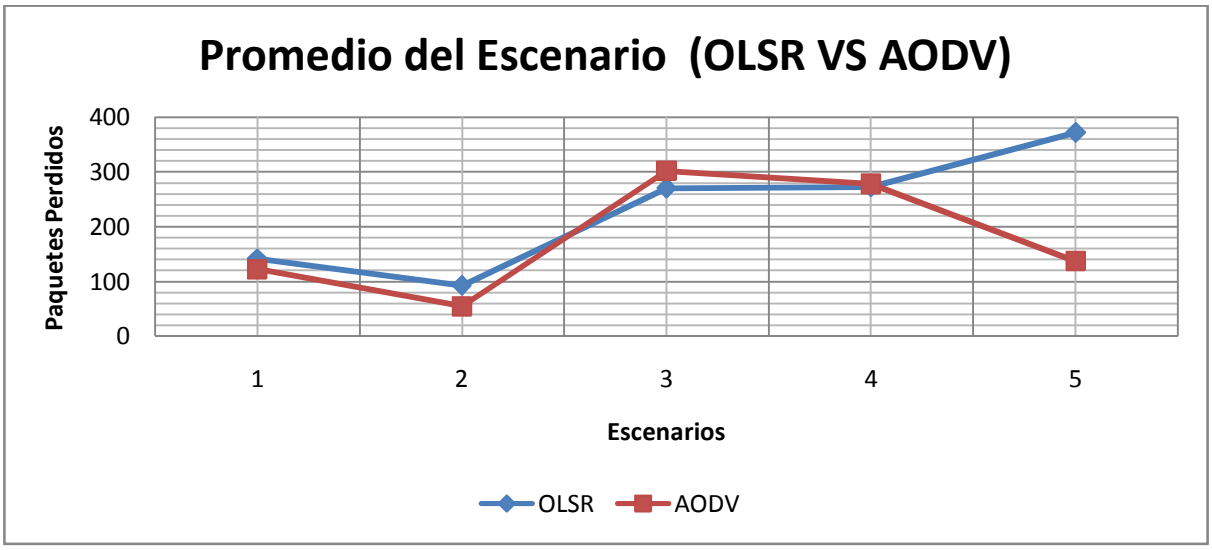


Figura 6. 13. Promedio de los Escenario con OLSR y AODV

En la figura 6.13, se observa claramente que el protocolo OLSR en general tiene más perdidas de paquetes que el protocolo AODV.

Para conocer el promedio máximo de paquetes perdidos en cada escenario se muestra la figura 6.14.

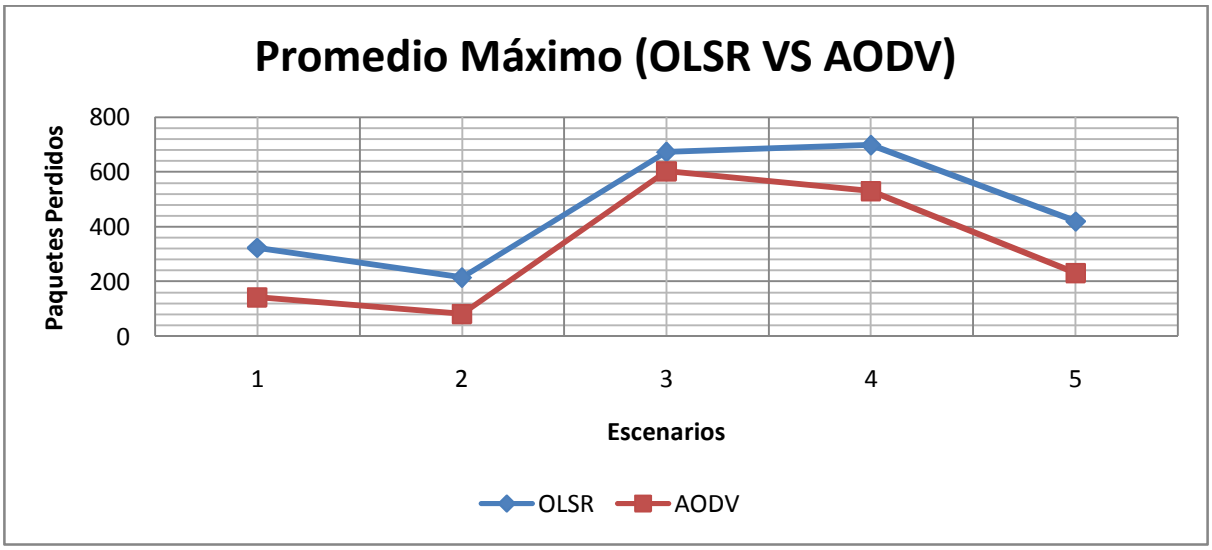


Figura 6. 14. Promedio Máximo de cada escenario usando OLSR y AODV.

Se observa, en la figura 6.14, el máximo número de paquetes se pierden en el escenario 4, el cual es un escenario con una población de 30 nodos, con 10 pares de nodos transmitiendo o recibiendo, con el tamaño del paquete de nodo fuente a nodo destino de 15000, además de que se utiliza OLSR.

La figura 6.15, muestra los valores para el promedio mínimo en cada escenario, usando los protocolos OLSR y AODV.

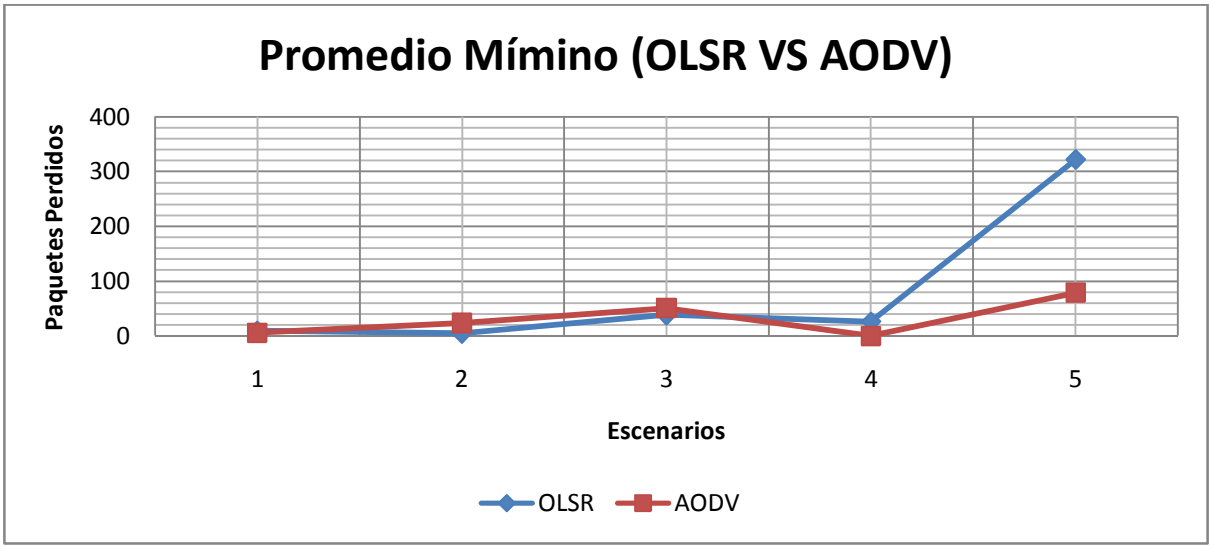


Figura 6. 15. Promedio mínimo de cada escenario usando OLSR y AODV.

En este capítulo se presentó la metodología para realizar la simulación de dos algoritmos para redes móviles ad-hoc. Al término de las simulaciones se logra observar que el algoritmo AODV tiene menos pérdidas de paquetes, esto quiere decir, que entrega más paquetes a sus destinos. Es por este motivo que en el capítulo 7 se realiza la implementación del algoritmo AODV, teniendo como antecedentes el mejor funcionamiento en una red ad-hoc que OLSR.

7

IMPLEMENTACIÓN DEL ALGORITMO REACTIVO VECTOR DISTANCIA ADHOC (AODV)

La simulación de protocolos es una pieza clave para el desarrollo de una comunicación [47], evitando gastos innecesarios, además proporciona un excelente ambiente para experimentar y probar nuevos modelos. Sin embargo, la simulación se basa en modelos aproximados del funcionamiento del sistema en ambientes reales. Para garantizar su funcionamiento en un ambiente real, es requerida la implementación experimental.

Realizar la implementación experimental del protocolo de ruteo AODV [5] [43] requiere del conocimiento de los protocolos de red, del sistema operativo (OS) en el cual se hará la implementación, de las funciones de interconectividad entre procesos y también de la interface de red.

En este capítulo se abordan las posibilidades de implementación como Snooping, Modificación de Kernel y Netfilter. Se presenta la metodología de implementación de WinAODV [48] en el sistema operativo Windows. Ya que [42] muestra que Windows tiene más del 90% del mercado mundial como sistema operativo.

7.1. DISEÑO DE LA IMPLEMENTACIÓN

De acuerdo con las necesidades del protocolo se deben de determinar que eventos son los que se llevaran a cabo, como por ejemplo:

- Cuando iniciar una petición de ruta (RREQ)
- Cuando y como almacenar paquetes durante el descubrimiento de ruta
- Cuando actualizar el tiempo de vida de una ruta activa
- Cuando generar un mensaje de error de ruta (RERR) si una ruta valida no existe.

Para realizar una implementación en una computadora móvil existen diferentes métodos de diseño las cuales son:

Snooping

Una posibilidad para determinar la necesidad de los eventos es husmear promiscuamente todos los paquetes que entran y salen. La figura 7.1 muestra la arquitectura básica del método de snooping.

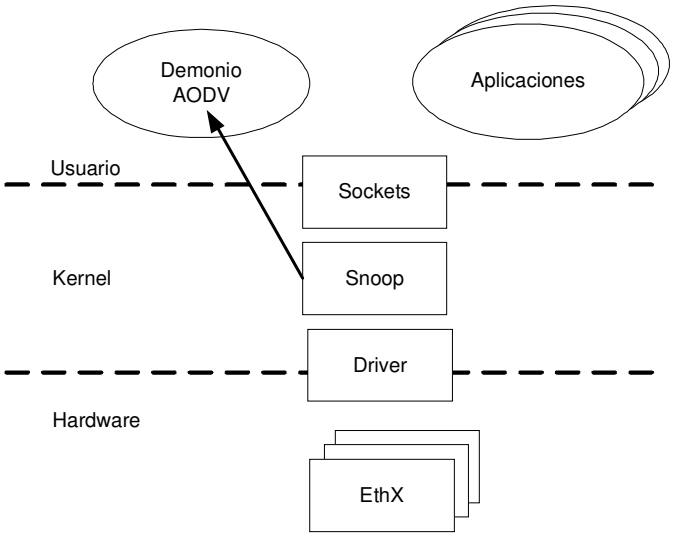


Figura 7. 1. Arquitectura de snooping.

Modificación de Kernel

Otra posibilidad de determinar eventos AODV es modificando el kernel. El código se puede poner en el kernel para comunicar los eventos mencionados anteriormente. La figura 7.2, muestra la arquitectura del método de modificación de kernel.

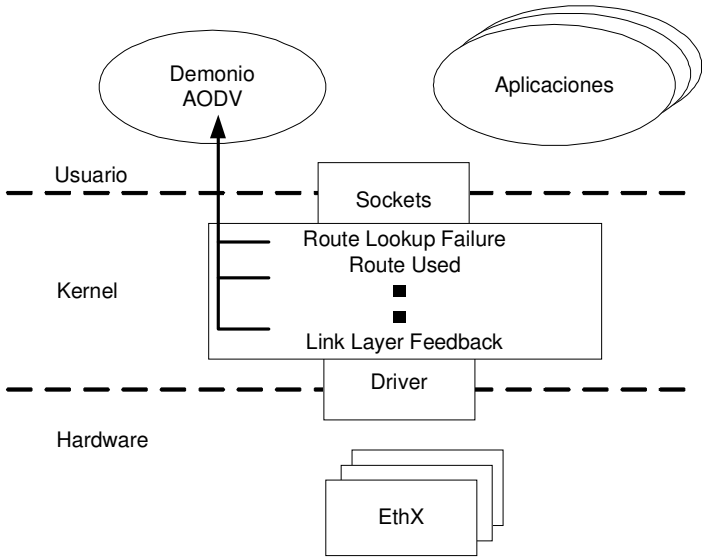


Figura 7. 2. Arquitectura de modificación de kernel.

Netfilter

Netfilter es un conjunto de ganchos a varios puntos dentro de la pila de protocolos de Linux. Netfilter redirecciona paquetes de flujo sobre código definido del usuario, lo que se puede examinar, descartar, eliminar, modificar o mantener en espera los paquetes para el espacio de usuario. Es muy similar al método de snooping. La arquitectura del este método se muestra en la figura 7.3. Se seleccionó esta arquitectura ya que no se requiere de escribir algún código en el kernel del dispositivo, solamente se hace mediante una instalación y su ejecución.

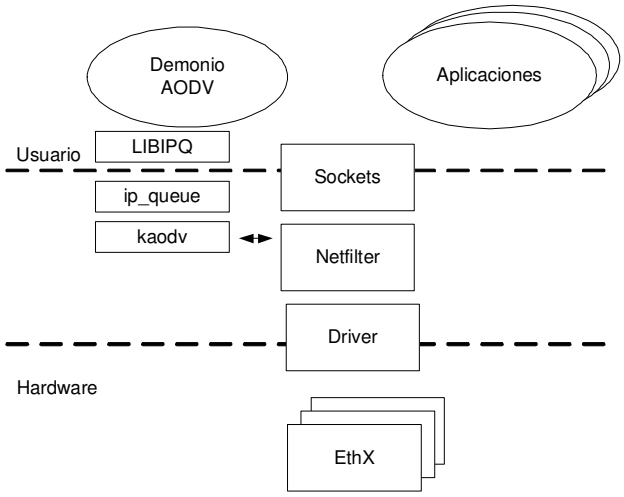


Figura 7. 3. Arquitectura Netfilter.

7.2. CARACTERÍSTICAS ESPECIALES

Para las pruebas experimentales se utilizaron 3 computadoras con las siguientes características:

Laptop 1
Sistema Operativo: Microsoft Windows XP SP2
Procesador: AMD Turio ™ 64x2 Mobile
Tecnología TL-50
1.60 GHz, 1.87 GB en RAM
Adaptador de Red: Atheros AR5005G Wireless Network Adapter
Grupo de Trabajo: LABTELECOM

Laptop 2
Sistema Operativo: Microsoft Windows XP SP2
Procesador: AMD Turion ™ 64x2 Mobile
Tecnología TL-50
1.60GHz, 960 MB en RAM
Adaptador de Red: Realtek RTL8185 54M Wireless Lan Network Adpater
Grupo de Trabajo: LABTELECOM

Laptop 3
Sistema Operativo: Microsoft Windows XP SP2
Procesador: Intel® Celeron® M
1.60 GHz, 1.24 GHz en RAM
Adaptador de Red: Intel® Pro/Wireless 2200 BG Network Connection
Grupo de Trabajo: LABTELECOM

De las características de cada computadora las que interesan son el tipo de sistema operativo, ya que todas cuentan con Windows XP y el tipo de adaptador de red que en este caso todos son de diferentes fabricantes pero con las mismas características, a continuación algunas de ellas para cada tarjeta de red.

Atheros AR5005G

Banda de Frecuencia: 2.4 GHz

Estándar: 802.11b / 802.11g

Velocidad de Transferencia de datos:

802.11b – 1-11 Mbps

802.11g – 1-54 Mbps

Modalidad: Ad-Hoc / Infraestructura

Realtek RTL8185 54M

Banda de Frecuencia: 2.4 GHz

Estándar: 802.11b / 802.11g

Velocidad de transferencia de datos:

1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 y 54 Mbps

Modalidad: Ad-Hoc / Infraestructura

Intel® Pro/Wireless 2200 BG

Banda de Frecuencia: 2.4 GHz

Estándar: 802.11b / 802.11g

Velocidad de transferencia de datos:

802.11b – Hasta 11 Mbps

802.11g – Hasta 54 Mbps

Alcance: 30m en Interiores

Modalidad: Ad-Hoc / Infraestructura

7.3. INSTALACIÓN DE WinAODV

WinAODV [48] de la universidad de Dublín en Irlanda, es un protocolo realizado para Windows CE que de acuerdo con Microsoft "Windows CE es una plataforma libre, escalable, con un amplio rango de dispositivos de comunicación, entretenimiento y computación móvil" [19].

Algunas características de WinAODV son las siguientes:

- Utiliza Windows
- Uso del Netfilter
- Utiliza la Especificación de Interface de Controlador de Red (NDIS - *Network Driver Interface Specification*), que es la que facilita la comunicación entre los protocolos de alto nivel como TCP/IP y los controladores de la red.
- Funciona adecuadamente con el RFC 3561 [5].

Antes de instalar el algoritmo AODV en las computadoras, es necesario habilitarlas como routers [78], ya que sin esta opción no podrán trabajar como dispositivos y routers a la vez. Esto se logra modificando el registro "*IpEnableRouter*" de 0 a 1, haciendo click en *Inicio-Ejecutar* y tecleando *regedit* y siguiendo la siguiente ruta: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters* como lo muestra la figura 7.4.

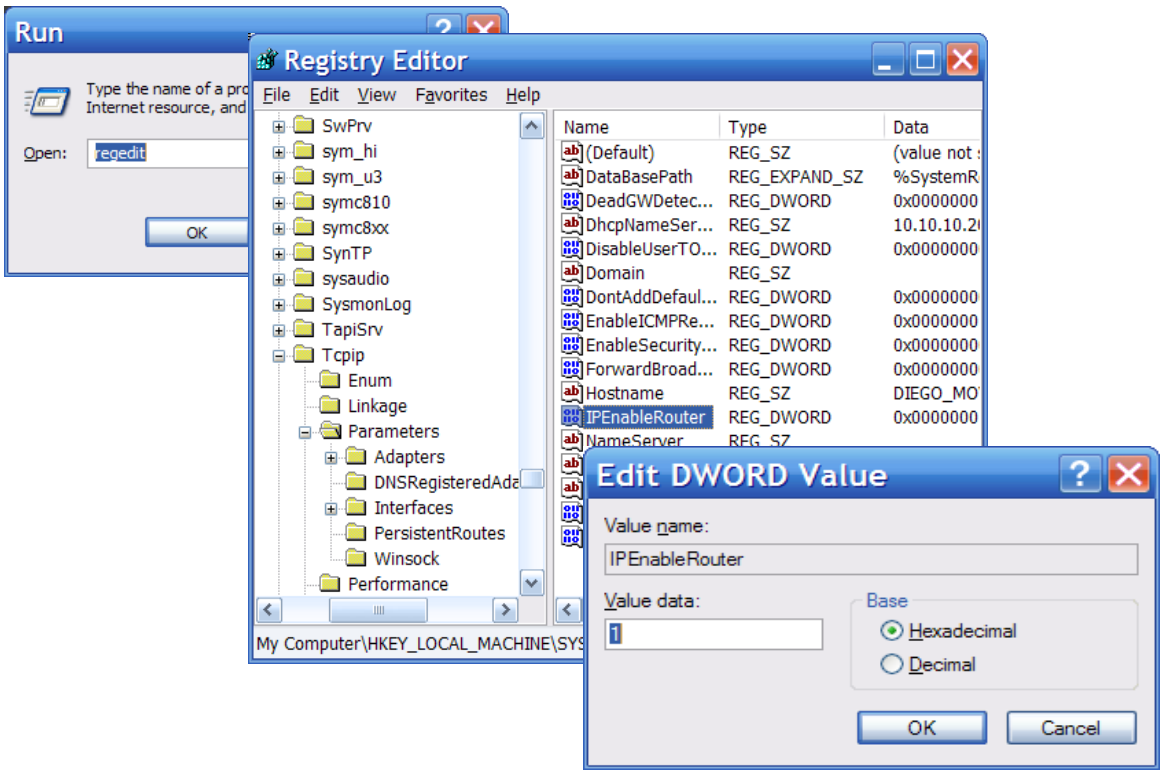


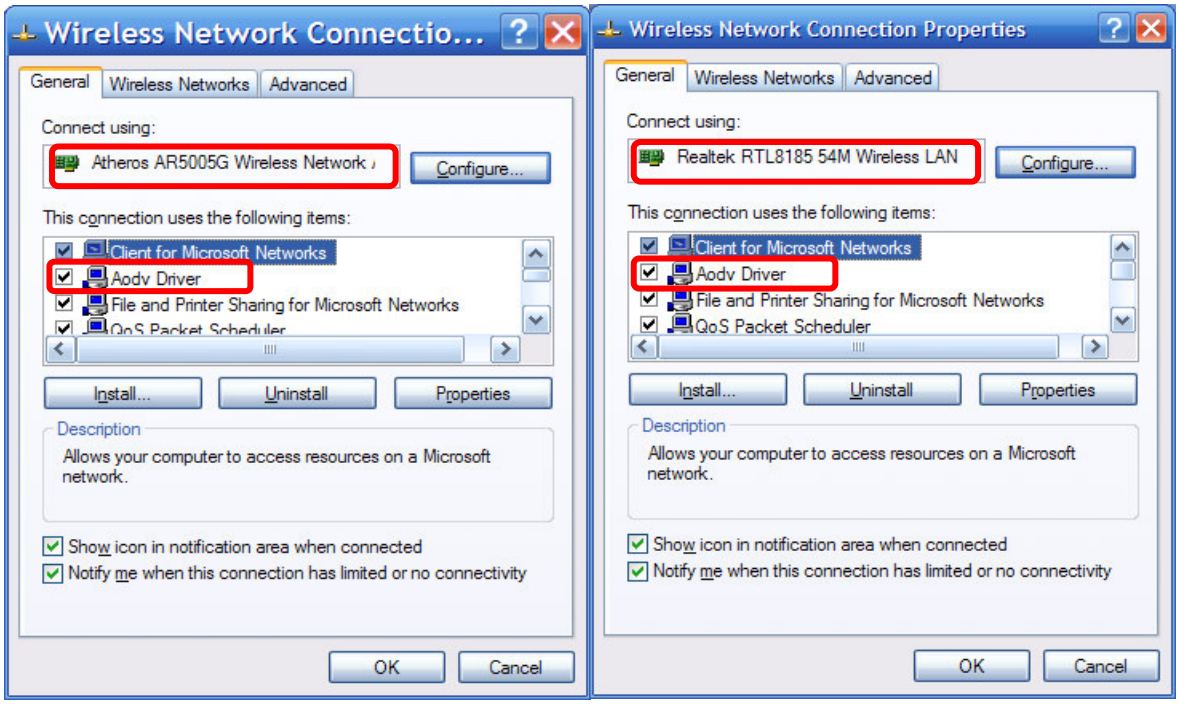
Figura 7. 4. Edición del Registro TCP/IP.

Enseguida en una computadora se crea una red Ad-Hoc con el nombre: AD_HOC_USUARIO, con clave de seguridad de acceso: XXXX.

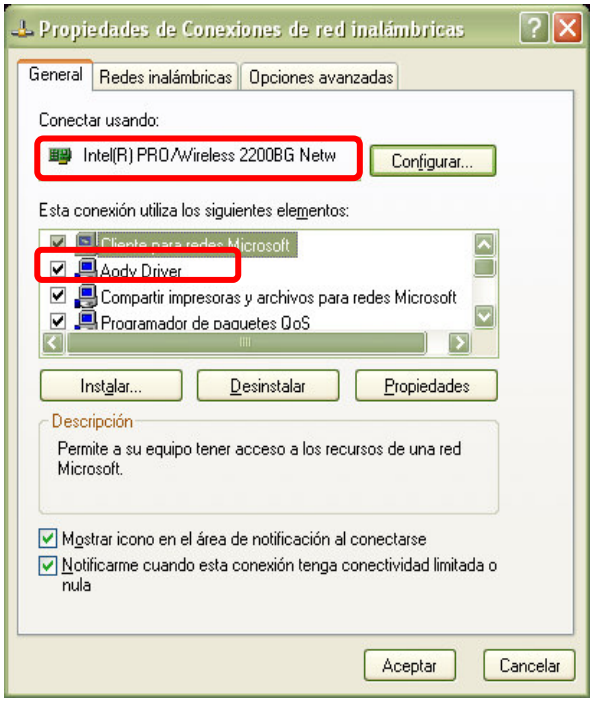
Las computadoras se ubicaron dentro de las instalaciones del CITEDI, estratégicamente en lugares donde no hubiera interferencia con otra red. Además, la cobertura de una computadora solo cubre una computadora y no abarcara ambas. La distancia aproximada entre las computadoras es de 20 mts. La figura 7.5 muestra la ubicación de las computadoras utilizadas en el experimento.

Figura 7. 5. Ubicación de las Computadoras.

Una vez creada la red, se procede a instalar la herramienta WinAODV en cada computadora y se verifica la correcta instalación [78] así como lo muestra la figura 7.6.



a) b)



c)

Figura 7. 6. Comprobación del protocolo AODV: a) Laptop 1, b) Laptop 2 y c) Laptop 3

Una vez reiniciado el equipo, se procede a conectar cada equipo a la red Ad-Hoc que se acaba de crear, con la ayuda del visor de redes inalámbricas de Windows se conecta tecleándole la contraseña, así como se muestra en la figura 7.7.

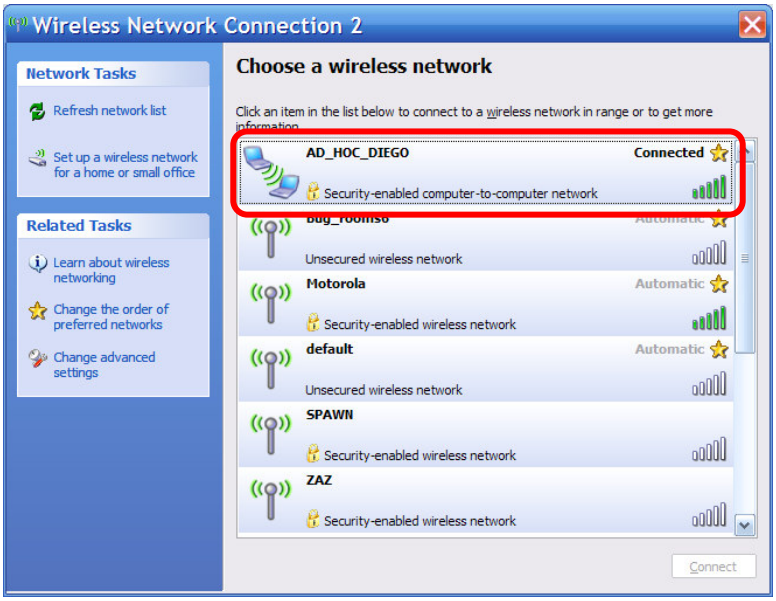


Figura 7. 7. Conexión a la red AD_HOC_DIEGO.

Una vez conectadas las laptops a la misma red, encontramos que tenemos tres objetos (nodos) en un mismo grupo de trabajo (nodos vecinos) (figura 7.8).

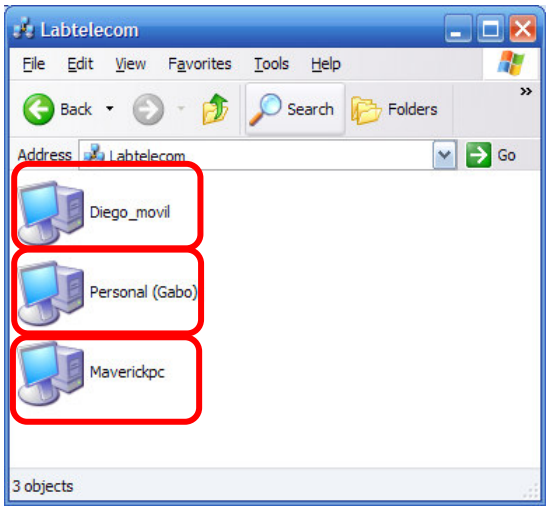


Figura 7. 8. Grupo de trabajo en la red Ad-Hoc

De la figura 6.8 decimos que Diego_movil = Laptop 1, Personal (Gabo) = Laptop 2 y Maverickpc = Laptop 3.

Para seleccionar un nodo simplemente se dan dos clics con el botón izquierdo y aparecerán los archivos que se pueden compartir, en este caso para comprobar el protocolo de ruteo se conectan las computadoras de los extremos (1 y 3) dejando como nodo intermedio a la computadora 2, los archivos de la computadora 1 accesados desde 3 se muestran en la figura 7.9.

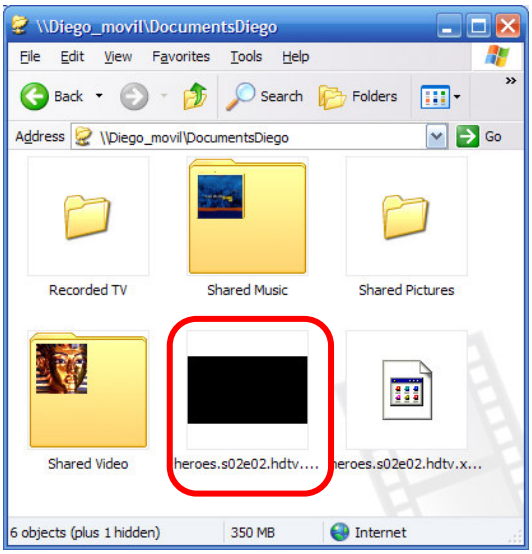


Figura 7. 9. Documentos en Laptop 1.

En este momento se puede decir que la red se encuentra lista para poder compartir archivos con las computadoras y principalmente utilizar la comunicación de la computadora 1-3, utilizando como nodo intermedio la computadora 2.

Si un usuario quiere abrir un archivo, en este caso de ejemplo se trata de un video, solo es cuestión de tener instalados los drivers correspondientes de video y disfrutar del archivo. Incluso se pueden estar viendo al mismo tiempo, como sería un ejemplo para el caso de alguna exposición en un auditorio y necesitamos distribuir el archivo de la presentación para que todos

tengan la presentación y la pueden visualizar mejor. Este ejemplo lo podemos observar en la figura 7.10, la reproducción del video se realiza en las tres computadoras simultáneamente.

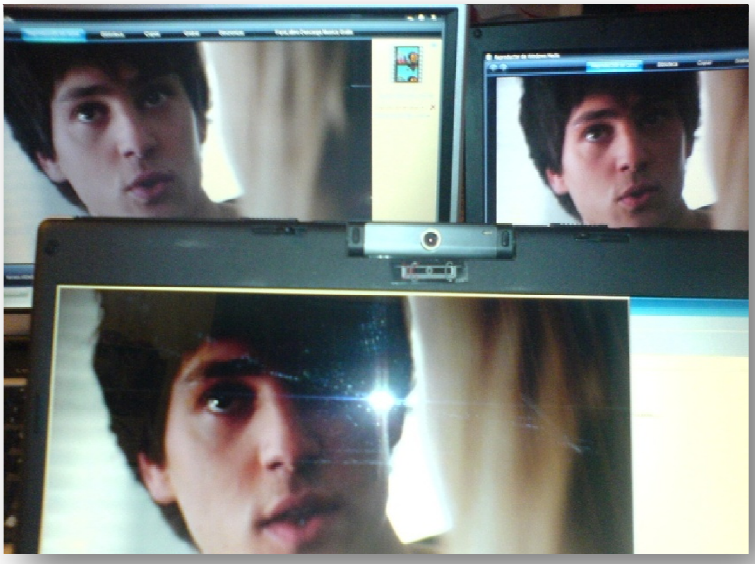


Figura 7. 10. Reproducción en las tres laptops.

Se observó que existen diferentes formas de realizar una implementación experimental de un protocolo de ruteo, el principal objetivo de hacerlo es que funcione adecuadamente de acuerdo al estándar que pertenece.

Se logró la comunicación entre computadoras de una red ad-hoc inalámbrica que se encontraban fuera del área de cobertura utilizando un nodo intermedio.

Con este capítulo se terminan las pruebas físicas y de laboratorio, simplemente resta por realizar las conclusiones.

8
CONCLUSIONES

A través de este trabajo se ha adquirido el conocimiento sobre el funcionamiento de las redes móviles ad-hoc utilizando el estándar IEEE 802.11 [25]. Se analizó el proceso de obtención de rutas mediante dos algoritmos diferentes. El primer análisis se realizó mediante el algoritmo OLSR [34], un algoritmo proactivo, cuyas rutas hacia un destino siempre son conocidas. Mientras que el estudio del algoritmo AODV [5], condujo al entendimiento de una obtención sobre demanda, lo que implica que solo se conocen las rutas para los destinos cuando son necesarias.

Además del estudio, se presentó la metodología para realizar la simulación de estos algoritmos en 5 escenarios particulares, donde las topologías cambiaban el número de nodos, el tamaño del paquete de datos y el tráfico en la topología. Los resultados muestran que el algoritmo de ruteo AODV tiene menos pérdidas de paquetes, es decir, la efectividad de entrega de paquetes es mayor que OLSR. En el caso particular donde el escenario presenta una población de 90 nodos sin tráfico y transmitiendo un paquete de 1400 bits, se observa que el promedio de paquetes perdidos por OLSR es el doble que el número de paquetes perdidos por el algoritmo AODV.

Mediante la implementación experimental del algoritmo de ruteo reactivo de vector distancia (AODV) con WinAODV, se logró realizar la comunicación entre computadoras de una red inalámbrica ad-hoc que se encontraban fuera del área de cobertura.

De acuerdo a las observaciones realizadas mediante los experimentos, AODV tiene potencial en las aplicaciones, ya que las rutas hacia los destinos son descubiertas solo cuando es necesaria una comunicación, evitando tener rutas que no se utilizan. Por otro lado, tiene la ventaja de que cada nodo es independiente y puede realizar la mejor ruta hacia un destino sin depender del nodo fuente. Otra ventaja es que en memoria no se almacena la ruta por completo, utilizando menos espacio en memoria y aprovechándola para uso del dispositivo.

Se ha visto que este tipo de algoritmos tiene aplicaciones en áreas como la militar, civil, casos de desastres y sociales, ya que se establece la comunicación solo donde es requerido, disminuyendo el número de nodos ocupados, obteniendo mejor utilización del Ancho de Banda y Conservación de la Energía.

Es por eso que se propone como trabajo a futuro, diseñar e implementar un sistema que permita enviar y recibir información en un entorno de poco ancho de banda (celulares) con requerimiento de gran cantidad de ancho de banda (audio, video y texto) a través de una red ad-hoc utilizando AODV, con el fin de tener redes dinámicas, sin tener que utilizar puntos de acceso. Esto lograría reducir los costos de los servicios ya que no se utilizarán para su comunicación.

REFERENCIAS

[1]. TANENBAUM, Andrew. *Computer Networks,* Fourth Edition, P. Hall PTR, Upper Saddle River, NJ, 2005.

[2]. Real Academia Española, *diccionario de la lengua española* [en línea] [consulta: Abril 2007] Disponible en:
< http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=ad%20hoc>.

[3]. WENCHAO, Ma and YUGUANG, Fang. Dynamic hierarchical mobility management strategy for mobile IP networks. In *IEEE Journal on Selected Areas in Communications*. 22(4): 664-676, 2004.

[4]. National Institute of Standards and Technology (NIST) [en línea] [consulta: Abril 2007]. Disponible en <http://www.itl.nist.gov/div892/wahn_mahn.shtml, Abril 2007>.

[5]. PERKINS, Charles, ROYER, Elizabeth and DAS, Samir. "Ad hoc On-Demand Distance Vector (AOVD) Routing". *RFC 3561*, July 2003.

[6]. RAMASUBRAMANIAN V., HAAS Z. and SIRER E. 2003. "SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks," In *Proc. 4th International Symp. on Mobile Ad Hoc Networking and Computing* (MobiHoc 2003), Annapolis, MD, June 3-6, 2003

[7]. JOHNSON, David, MALTZ, David and HU, Yih-Chun. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). *RFC 4728*, February 2007.

[8]. JOHNSON D. and MALTZ D. “Dynamic source routing in ad-hoc wireless networks”. In *Computer Communication Review – Proceedings of SIGCOMM ’96*, pp 153-181, 1996.

[9]. MURTHY S. and GARCIA J. “A Routing Protocol for Packet Radio Networks”. In *1st ACM Int’l Conference on Mobile Computing and Networking (Mobicom’95)*, pp 86-95, November 1995.

[10]. HAAS Z and PEARLMAN Marc, "The Performance of Query Control Schemes for the Zone Routing Protocol," In *Proceedings of the ACM SIGCOMM '98*, pp 167-177, September 1998.

[11]. JOHNSON, David and MALTZ, David. Protocols for adaptive wireless and mobile computing. In *IEEE Personal Communications*. 3(1): 34-42, February 1996.

[12]. BANDYOPADHYAY S. and PAUL K., "Evaluating the Performance of Mobile Agent-Based Message Communication among Mobile Hosts in Large Ad Hoc Wireless Networks," *Proc. 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, pp. 69-73, 1999.

[13]. PERKINS, Charles, ROYER, Elizabeth, DAS, Samir and MARINA, Mahesh. Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks. In *IEEE Personal Communications*. 8(1): 16-28, February 2001.

[14]. RAMANATHAN S. and STEENSTRUP M., "A survey of routing techniques for mobile communications networks," Baltzer/ACM *Mobile Networks and Applications*, vol. 1, pp. 89-104, 1996.

[15]. L. Klein-Berndt. Kernel AODV from National Institute of Standards and Technology (NIST). [en linea] [consulta: Diciembre 2007]. Disponible en: <http://w3.antd.nist.gov/wctg/aodv_kernel/index.html. Diciembre 2007>.

[16]. I. D. Chakeres. AODV-UCSB Implementation from University of California Santa Barbara. [en linea] [consulta: Diciembre 2007]. Disponible en: <http://moment.cs.ucsb.edu/AODV/aodv.html. Diciembre 2007>.

[17]. LUNDGREN H., NORDSTROM E. and TSCHUDIN C., "Coping with Communication Gray Zones in IEEE 802.11b based Ad hoc Networks" In *Proceedings of the 5th ACM International Workshop on Wireless Mobile Multimedia (WOWMOM'02),* pages 49-55, Atlanta, Georgia, USA, September 2002.

[18]. KAWADIA V., ZHANG Y. and GUPTA B. "System Services for Implementing Ad-Hoc Routing: Architecture, Implementation and Experiences". In *Proceedings of the 1st International Conference on Mobile Systems, Applications, and Services (MobiSys'03),* pages 99-112, San Francisco, CA, June 2003.

[19]. WEST, David. "An Implementation and Evaluation of the Ad-Hoc On-Demand Distance Vector Routing Protocol for Windows CE", Directed by Jim Dowling, Master in Science in Computer Science, University of Dubblin, September 2003.

[20]. STALLINGS, William. *Data and Computer Communications,* Eighth Edition, P. Hall PTR, Upper Saddle River, Nj, 2007.

[21]. STALLINGS, William. *Redes e Internet de Alta Velocidad,* Rendimiento y Calidad de Servicio*,* Segunda Edición, P. Hall PTR, Madrid, 2004.

[22]. MICROSOFT-TECHNET, "*El Modelo TCP/IP"*, Microsoft Corporation, España, 2005.

[23]. ROLDAN, David, *Comunicaciones Inalámbricas: un enfoque aplicado*. Alfaomega Grupo Editor. México, 2005.

[24]. CARBALLAR, José. *WiFi, Cómo construir una red inalámbrica*. Segunda Edición. Alfaomega Grupo Editor. México. 2005.

[25]. IEEE. *802.11*, Information technology Telecommunications and information Exchange between systems Local and metropolitana area networks Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 1999 Edition.

[26]. ETOH, Minoru. *Next Generation Mobile Systems:* 3G and Beyond. John Wiley and Sons. England. 2005.

[27]. 3COM, "Enterprise-Class 3Com Wireless Lan Access Points 7250/8250/8750", *Data Sheet*, 2005.

[28]. BROCH J., MALTZ D., JOHNSON D., HU Y. and JETCHEVA J. "A performance Comparasion of Multi-Hop Wireless Ad-Hoc Network Routing Protocolos". In *Proceedings of the Fourth Annual ACM/IEEE International on Mobile Computing and Networking (Mobicom'98)*, pp 85-97, October 1998.

[29]. LARSSON, Tony and HEDMAN Nicklas, Routing Protocols in Wireless Ad-Hoc Networks – A Simulation Study, Master in Science in Computer Science and Engineering, Luleâ University of Technology, Stockholm, Sweden 1998.

[30]. HAAS, Zygmunt, DENG, Jing, LIANG, Ben, Panagiotis Papadimitatos, and S. Sajama. "Wireless ad hoc networks". *Encyclopedia of Telecommunications*. John Wiley, December 2002.

[31]. LIU C. and KAISER J. “A Survey of Mobile Ad Hoc Network Routing Protocols”. *Technical Report Series*, University of Ulm, Nr. 2003-08, October 2005.

[32]. CORDEIRO C. and AGRAWAL D., "Mobile Ad Hoc Networking," Tutorial/Short Course in *20 th Brazilian Symposium on Computer Networks*, pp. 125-186, May 2002.

[33]. PERKINS C. and BHAGWAT P. “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”. In *Proc. of the ACM SIGCOMM*, pp 234-244, October 1994.

[34]. CLAUSEN, Thomas and JACQUET, Philippe. “Optimized Link State Routing Protocol (OLSR)”. *RFC 3626*, October 2003.

[35]. QAYYUM A., VIENNOT L. and LAOUITI A. “Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks”, In *Proceedings of the 35th Hawaii International Conference on System Sciences 2002 (HICSS 35’02)*, pages 298-307, Hawaii, USA, 2002.

[36]. TRUJILLO D., ÁLVAREZ G., SÁNCHEZ M. and ÁLVAREZ M. “Estudio de Algoritmos de Ruteo para Redes Móviles Ad-Hoc (Manet’s), In *Proceedings of III Encuentro Regional Académico (ERA’07),* paginas 37-42, Tijuana, B.C. México, Octubre 2007.

[37]. Internet Assigned Numbers Authority (IANA) [en linea] [consulta: Noviembre 2007]. Disponible en:
<http://www.iana.org/ assignments/aodv-parameters/aodv-parameters.xhtml>.

[38]. PARK V. and CORSON M. “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks”. In *Proceedings of 1997 IEEE Conference on Computer Communications (Infocom’97)*, pp 1405-1413, Japan, April. 1997.

[39]. TRUJILLO D., ÁLVAREZ G., SÁNCHEZ M. and ÁLVAREZ M. "A Survey on Routing Protocols For Manet", In *Proceedings of International Technology, Education and Development Conference (INTED 2008),* page 412, Valencia, Spain, March 2008.

[40]. TRUJILLO D., SÁNCHEZ M. and ÁLVAREZ M. "Análisis de Ruta Implementando el Algoritmo Reactivo de Vector Distancia (AODV) en una Red Ad-Hoc 802.11", En el *5to Congreso Internacional de Ingeniería Electromecánica y de Sistemas (5CIIES)*, pp 1105-1110, Distrito Federal, México, Noviembre 2008.

[41]. BENZAID M., MINET P. and KHALDOOUN A., "Integrating fast mobility in the OLSR routing protocol", In Proceedings of the 4th IEEE Conference on Mobile and Wireless Communications Networks (MWCN), pp 377- 388, Stockholm Sweden, September 2002.

[42]. Market Share, *global market share statistics* [en linea] [consultado: Diciembre 2007]. Disponible en: <http://marketshare.hitslink.com/report.aspx?qprid=8>

[43]. ROYER, Elizabeth.*"Routing in Ad hoc Mobile Networks: On-Demand and Hierarchical Strategies"*, Directed by Michael Melliar-Smith, Doctor of Philosophy in Electrical and Computer Engineerign, University of California, Santa Barbara, December 2000.

[44]. NCTUNS, [en línea] [consulta: Marzo 2008]. Disponible en: <http://nsl10.csie.nctu.edu.tw/>.

[45]. WANG S., CHOU C. and LIN C. "*The GUI User Manual for the NCTUns 4.0 Network Simulator and Emulator"*. Network and System Laboratory, Department of Computer Science, National Chiao Tung University, Taiwan. July 2007.

[46]. WANG S., HUANG C., LIN C., CHOU C. and LIAO K. *"The Protocol Developer Manual for the NCTUns 4.0 Network Simulator and Emulator"*. Network and System Laboratory, Department of Computer Science, National Chiao Tung University, Taiwan. July 2007.

[47]. CHAKERES D. and ROYER E., "AODV Routing Protocol Implementation Design", in *Proceedings of the 24th International Conference on Distributed Computing Systems Workshop (ICDCSW'04)*, pages 698-703, Volume 7, Tokyo, Japan, March 2004.

[48]. WEST D, *WinAODV Implementation from Trinity College Dublin* [en línea] [consulta: Marzo 2008]. Disponible en: <http://www.dsg.cs.tcd.ie/dynamic/?category_id=379>.

[49]. STALLINGS, William. *Comunicaciones y Redes de Computadores.* Séptima Edición. Prentice Hall PTR, Madrid. 2004.

[50]. IEEE. *802.15.1*, IEEE Standard for Information technology Telecommunications and information Exchange between systems Local and metropolitan area networks Specific requirements – Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). June 2005.

[51]. PRASAD, Neeli and PRASAD, Anand. *WLAN Systems and Wireless IP for Next Generation Communications*. Artech House, Universal personal communications. USA, 2002.

[52]. AHMAD, Aftab. *Wireless and Mobile Data Networks*. John Wiley and Sons. NJ, 2005.

[53]. SANCHEZ Garcia, Jaime. "Comunicaciones Inalámbricas de 4ta Generación". *Electro2001*. Instituto Tecnológico de Chihuahua. pp 61-66.

[54]. EKLUND Carl, MARKS Roger B., STANWOOD Kenneth L. and WANG Stanley. "IEEE Standard 802.16: A Technical Overview of the WirelessMAN^{TM}". IEEE Communications Magazine, June 2002, pp. 98-107.

[55]. IEEE 802.20 – PD-02: *Mobile Broadband Wireless Access Systems*: Approved PAR 2002 – 12 – 11.

[56]. IEEE 802.20 – PD-04: *Introduction to IEEE 802.20* - Technical and Procedural Orientation. 2003 – 03 – 10.

[57]. ITU-R. *Recomendación UIT-R F.1763*: Normas de interfaz radioeléctrica para sistemas de acceso inalámbrico de banda ancha que funcionan en el servicio fijo por debajo de 66 GHz. 2006.

[58]. IEEE, *work group 22* [en línea] [consulta: Abril 2007]. Disponible en: <www.ieee802.org/22>

[59]. IEEE 802.22. PAR FORM: *Wireless Regional Area Networks.* 2004 – 09 – 23.

[60]. CRC, Communications Research Center. *Wireless Regional Area Network (WRAN):* Initial System Concept and IEEE 802 undertaking. 2004 – 11 – 29.

[61]. IEEE 802.22. *Wireless Regional Area Network (WRAN)*: Initial System Concept. 2004.

[62]. CRC, Communications Research Center. *Broadband landscape in North-America. Broadwan Workshop*. 2005 – 05 – 24.

[63]. CHAPLIN Kevin. "Wireless LANs vs. Wireless WANs". Sierra Wireless. White Paper 2130273. November 2002.

[64]. TOSHIBA. *Conozca la banda ancha WWAN*: ¿qué supone para el profesional móvil?. Toshiba Europe GmbH. 2006.

[65]. JENKINS Gareth. *Brillian past, bright future*. Deutsche Bank, Global Telecommunications. GSM White Paper GRCM2004PROD002566. 2004.

[66]. GSM [en línea] [consulta: Abril 2007]. Disponible en: <www.gsmworld.com>

[67]. DODD Annabel. *The Essential Guide to Telecommunications*. Fourth Edition. Prentice Hall PTR. NJ, 2005.

[68]. ARENAS Matías, BETTANCOURT Rolando, GROTE Alex, SOTO Marcelo y GROTE Walter. *"Análisis de Tasa Efectiva de Servicio y Retardo de GPRS y EDGE"*. Congreso SENACITEL 2004, Ciudad de Valdivia, Chile. Noviembre 2004.

[69]. MAYORAL Palacios Erick. *"Redes Inalámbricas de 2G, 2.5G y 3G"*. Tesis profesional. Universidad de las Américas Puebla. Mayo 2004.

[70]. DUBENDORF, Vern A. *Wireless Data Technologies*: Reference HandBook. John Wiley and Sons. England. 2003.

[71]. WONG Daniel. *Wireless Internet Telecommunications*. Artech House mobile communications series. MA, 2005.

[72]. HSPA [en línea] [consulta: Abril 2007]. Disponible en: <hspa.gsmworld.com>

[73]. ARTHUR D., *"HSPA and mobile WiMax for Mobile Broadband Wireless Access"*. An independent report prepared for the GSM Association. Reference 21239. UK. 27 March 2007.

[74]. QUALCOMM. “Release 7 HSPA+ For Mobile Broadband Evolution”. November 2007.

[75]. ERICSSON. *“HSPA, the undisputed choice for mobile broadband”*. White paper 284 23-3119 Uen. May 2007.

[76]. HSPA. *“Network Update October 2007”*. GSMA, 22 October 2007.

[77]. TRUJILLO D., SÁNCHEZ M. and ÁLVAREZ M. “Análisis de Ruta Implementando el Algoritmo Proactivo OLSR en una Red Ad-Hoc 802.11”, Por aparecer en el *IV Encuentro Regional Académico (ERA’08)*, Tijuana, B.C. México, Noviembre 2008.

[78]. TRUJILLO D., SÁNCHEZ M. and ÁLVAREZ M. “Implementación Experimental de AODV en una Red Ad-Hoc Inalámbrica 802.11x”, En el *XXX Congreso Internacional de Ingeniería en Electrónica (ELECTRO’08)*, pp 139-144, Chihuahua, Chihuahua. México, Octubre 2008.

A

APÉNDICE

CLASIFICACIÓN Y ESTANDARES DE REDES INALÁMBRICAS DE DATOS

A.1. REDES INALÁMBRICAS DE ÁREA PERSONAL

Se les llaman de área personal porque se utilizan dentro de un espacio operativo personal. Este espacio tiene una cobertura de varios metros, del orden de 10 mts. La finalidad de estas redes es comunicar cualquier dispositivo personal (computadora, terminal móvil, PDA, entre otros) con sus periféricos, así como establecer una comunicación directa a corta distancia entre otros dispositivos [49].

Tradicionalmente, la comunicación de estos dispositivos con sus periféricos se había hecho mediante cables. Pero tener pequeños dispositivos llenos de cables alrededor no resulta de lo más confortable, por lo que la comunicación inalámbrica ha dado un paso gigantesco en esta área.

El uso necesario de una comunicación inalámbrica a muy corta distancia y con necesidades de velocidades menores a 1 Mbps ha incrementado su demanda. Estos tipo de red son muy útiles en aplicaciones de domótica, en seguridad, iluminación, aire acondicionado; Electrónica de consumo en TV, VCR, DVD, CD; en periféricos para la computadora, ratón, teclado, impresora, joystick; en Medicina como en la monitorización, sensores; en entretenimiento como videojuegos, juguetes; y un sin fin de mercados donde las WPAN son utilizadas, estos ejemplos se observan en la figura A.1.

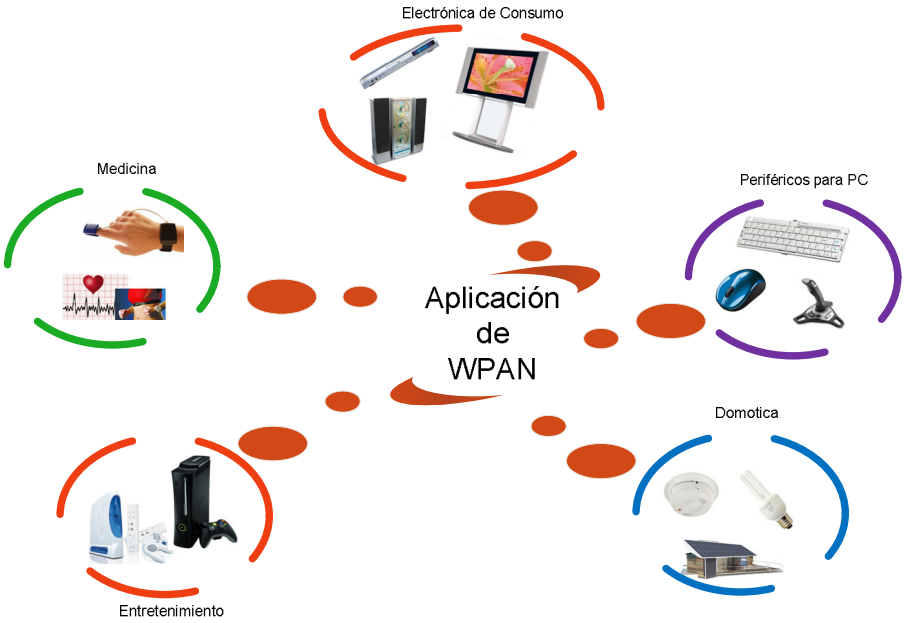


Figura A. 1. Aplicaciones de Redes de Área Personal

Cada una de las aplicaciones presentadas anteriormente, requieren de diferentes necesidades del sistema de comunicación. Por lo general en los entornos de WPAN la velocidad de 1 Mbps es suficiente. En la figura A.2 se muestran algunas aplicaciones más comunes y la velocidad de transmisión que requieren.

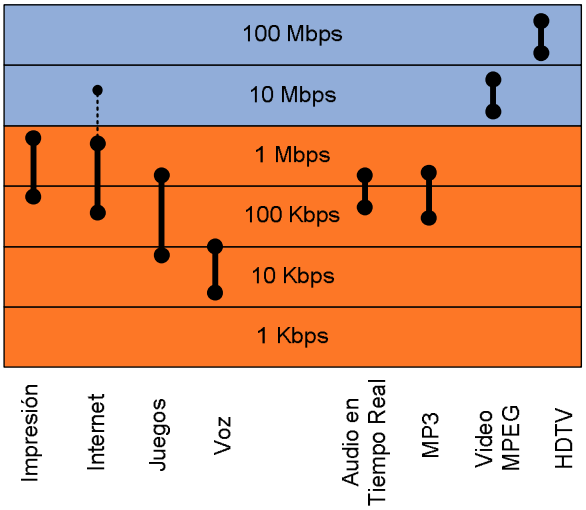


Figura A. 2. Velocidades de aplicaciones WPAN

Con la finalidad de soportar este tipo de comunicaciones se desarrollaron algunas tecnologías para redes inalámbricas de área personal como Bluetooth (IEEE 802.15.1), WiMedia (IEEE 802.15.3), Zigbee (IEEE 802.15.4), DECT (*Digital Enhanced Cordless Telecommunications*, "Telecomunicaciones Digitales Inalámbricas Mejoradas") y luz infrarroja.

A.1.1. Bluetooth

De todas las tecnologías de redes inalámbricas de área personal la más conocida es la de Bluetooth (IEEE 802.15.1 [50]). Esta tecnología no está pensada para soportar redes de computadoras sino, más bien, para comunicar una computadora o cualquier otro dispositivo con sus periféricos dentro de un pequeño alcance (10 mts).

La comunicación de Bluetooth se lleva a cabo mediante el modelo maestro-esclavo. Un terminal maestro puede comunicarse hasta con siete esclavos simultáneamente. La figura A.3 muestra la estructura maestro-esclavo [24].

Figura A. 3. Esquema Maestro-Esclavo

No obstante, el maestro siempre puede suspender las comunicaciones con un esclavo (la técnica usada se le conoce como *parking*) y activar la comunicación con un nuevo dispositivo esclavo. Con este sistema un maestro puede establecer comunicación con un máximo de 256 esclavos, donde sólo siete se encuentran activos, el resto se dice que están aparcados (*parked*). A cada uno de los esclavos activos se les asigna un número de 3 bit que recibe el nombre de dirección AMA

(*Active Member Address*) mientras que para los *parked* la dirección es de 8 bits y se le denomina PMA (*Parked Member Address*). A este conjunto de relaciones maestro-esclavo se le llama ***piconet***. La figura A.4 muestra la relación de una piconet.

Figura A. 4. Esquema de una *piconet*

Dentro del entorno piconet, un dispositivo puede ser a la vez maestro de un piconet y esclavo de otra piconet. Cuando esto ocurre, al conjunto se le conoce como ***scatternet*** (red dispersa), como se puede observar en la figura A.5. Scatternet utiliza un esquema TDM de multiplexación por división en el tiempo. Cada una de las piconet opera con una secuencia de salto distinta.

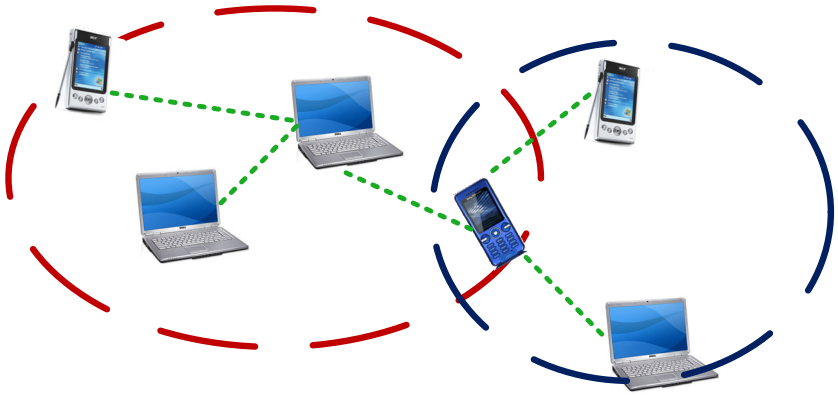


Figura A. 5. Esquema de una *Scatternet*.

Bluetooth utiliza la tecnología FHSS (*Frequency Hopping Spread Spectrum, "Espectro Disperso por Salto de Frecuencia"*) en la banda de frecuencias de 2.4 GHz. Puede establecer comunicaciones asimétricas donde la velocidad máxima de bajada es de 721 Kbps y 57.6 Kbps de subida o comunicaciones simétricas de 432.6 Kbps. Por otro lado, puede transmitir voz como datos. En resumen algunas de las características más importantes de Bluetooth [24] se muestran en la tabla A.1:

Tabla A. 1. Características de Bluetooth.

Tecnología	FHSS
Banda de Frecuencia	2.4 GHz (Banda ISM)
Modulación	GFSK
Potencia del Transmisor	1 mW
Canales Máximos	• De voz: 3 por piconet • De datos: 7 por piconet
Velocidad de datos	Hasta 721 Kbps por piconet
Distancia máxima	10 m
Número de dispositivos	8 por piconet y hasta 10 piconets
Consumo de Potencia	Desde 30 µA hasta 30 mA transmitiendo

A.1.2. WIMEDIA/UWB

Algunas aplicaciones, como las comunicaciones multimedia o la transmisión de imágenes digitales de alta resolución, requieren anchos de banda y calidad de servicio con mayor grado de garantía del que Bluetooth es capaz de ofrecer. En estos casos, la solución es WiMedia, estandarizado por la IEEE como 802.15.3 [51].

WiMedia actúa en la misma banda de frecuencias que Bluetooth (2.4 GHz) y permite seleccionar cinco tasas binarias: 11 Mbps, 22 Mbps, 33 Mbps, 44 Mbps y 55 Mbps [26]. La potencia transmitida es, aproximadamente, de 8 dBm y el alcance de las comunicaciones está comprendido entre 5 y 55 m. además, proporciona características como el control de potencia,

seguridad, coexistencia con Bluetooth y WLAN y QoS, que la hacen ideal para transporte multimedia de alta calidad, la interconexión de dispositivos.

Ultrawideband (UWB) es una tecnología basada en la transmisión de pulsos muy cortos. La consecuencia principal es que la expansión del ancho de banda de la señal y la disminución de la densidad espectral de potencia permiten la coexistencia con otro tipo de tecnologías de radio. Los principales beneficio de UWB en comparación con otra tecnologías son mayor robustez frente a la propagación multicamino, menor potencia de transmisión, localización de dispositivos y flexibilidad en la relación distancia y ancho de banda. Sin embargo, requieren de antenas de gran ancho de banda y relojes muy precisos.

A.1.3. ZIGBEE

En algunas aplicaciones en las que participan pequeños dispositivos como sencillos sensores o actuadores no suelen ser necesarias tasas binarias altas. Estos sistemas se caracterizan por comunicaciones esporádicas en las que el mayor volumen de información apenas supera unas pocas decenas o centenas de Kbps y por requerir un alcance limitado a pocas decenas de metros, lo que facilita la portabilidad de la red y la instalación de este tipo de dispositivos. En estos entornos, por otra parte, resulta más crítico minimizar costes, tamaño y consumo de potencia de los dispositivos.

El estándar IEEE 802.15.4, más conocido como Zigbee, es una especificación para aplicaciones de control remoto de dispositivos, juguetes y, en general, cualquier equipo que requiere un bajo coste y un bajo consumo de potencia en entornos reducidos como un hogar.

Zigbee puede trabajar a tres bandas de frecuencias diferentes: 868 MHz, 915 MHz y 2.4 GHz. La topología que soporta esta tecnología puede ser de Estrella, punto a punto y mallada. Las velocidades de transmisión 868 MHz es 20 Kbps, 40 Kbps para 915 MHz y 250 Kbps para 2.4 GHz. Estas y otras características [26] se mencionan en la tabla A.2.

Tabla A. 2. Características de *Zigbee*.

Bandas de Frecuencia	868 MHz 915 MHz 2.4 GHz
Velocidad de Transmisión	20 Kbps (868 MHz), 40 Kbps (915 MHz) y 250 Kbps (2.4 GHz)
Acceso al Medio	CSMA-CA
Topologías	Estrella, Punto a Punto y Mallada
Espacio de Direccionamiento	64 Bits
Alcance	Entre 5 y 500 m dependiendo del entorno, aunque el valor típico es de 50 m.

Zigbee diferencia entre dispositivos completamente funcionales (FFD, *Full Function Device*) y dispositivos parcialmente funcionales (RFD, *Reduced Function Device*). Las características de estos dispositivos se muestran en la tabla A.3.

Tabla A. 3. Características de FFD y RFD.

FFD	Funciona en cualquier topología. Puede ser el coordinador de la red. Capacidad para comunicarse con cualquier otro dispositivo.
RFD	Únicamente en topologías en estrella. No puede ser el coordinador de la red. Sólo se puede comunicar con el coordinador de la red. Implementación sencilla

En una red Zigbee, al menos, debe existir un dispositivo FFD que haga las veces de coordinador de red y, el resto, suele ser RFD, mucho más sencillo, ya que, de este modo, se reduce el costo económico del sistema.

A.1.4. DECT

El estándar DECT [24] (*Digital Enhanced Cordless Telecommunications, "Telecomunicaciones Digitales Inalámbricas Mejoradas"*) existe desde 1992 desarrollado por ETSI (*European Telecommunications Standards Institute, "Instituto Europeo de Normalización en Telecomunicaciones"*). El objetivo de DECT es facilitar las comunicaciones inalámbricas entre terminales telefónicos (teléfonos inalámbricos y centrales inalámbricas).

DECT trabaja en la banda de frecuencias de 1.9 GHz y utiliza la técnica TDMA (*Time Division Multiple Access, "Acceso Múltiple por División del Tiempo"*). La velocidad máxima a la que trabaja DECT es de 2 Mbps. Algunas características importantes de DECT [49] se enlistan en la tabla A.4.

Tabla A. 4. Características de DECT.

Naturaleza de Transmisión	Digital
Acceso al Medio	FDMA/TDMA
Modulación	GFSK
Banda de Frecuencia	1.880-1.990 GHz
Portadoras por Canal	12
Numero de Portadoras	10
Canales	120
Alcance Máximo	300 m
Duración de Trama	10 ms

A.1.5. INFRARROJO

La luz infrarroja es un tipo de radiación electromagnética invisible para el ojo humano. Los sistemas de comunicaciones con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja. La radiación infrarroja (IR) tiene longitudes de ondas entre 1 mm y 750 nm. La radiación infrarroja oscila con frecuencias entre 300 GHz (Gigahertz ó 10^9 Hertz) y 400 THz (Terahertz ó 10^{12} Hertz). La mayoría de los mandos a distancia de los aparatos domésticos

(televisión, vídeo, equipos de música, entre otros) utilizan comunicación por infrarrojo. Por otro lado, la mayoría de las PDA, algunos teléfonos celulares y muchas computadoras portátiles incluyen un dispositivo infrarrojo como medio de comunicación entre ellos.

Los sistemas de comunicaciones de infrarrojo pueden ser clasificados en dos categorías:

1. Infrarrojo de haz Directo. Esta comunicación necesita una visibilidad directa sin obstáculos entre ambas terminales.
2. Infrarrojo de haz Difuso. En este caso el haz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. En este caso no se necesita visibilidad directa entre terminales.

Las ventajas que ofrecen las comunicaciones de infrarrojo es que no están reguladas, son de bajo costo e inmunes a interferencia de los sistemas de radio de alta frecuencia. Sus principales inconvenientes son su corto alcance, el hecho de que no puedan traspasar objetos y que no son utilizables en el exterior debido a que agentes naturales como la lluvia o la niebla les producen grandes interferencias.

IrDA (*Infrared Data Association*) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Cuenta con varios estándares:

IrDA-Control. Es un protocolo de baja velocidad optimizado para ser utilizado en los dispositivos de control remoto inalámbricos. Éste es el caso de dispositivos como los mandos a distancia, ratones de computadoras o joysticks.

A.2. REDES INALÁMBRICAS DE ÁREA LOCAL

Se llaman redes inalámbricas de área local, WLAN (*Wireless Local Area Networks*) a aquellas redes que tienen una cobertura máxima de unos cientos de metros en un ambiente libre de

obstáculos. Estas redes están pensadas parea crear un entorno de red local entre computadoras o terminales situados en un mismo cuarto, edificio o grupo de edificios [24].

Los principales estándares que compiten en esta categoría son el Estándar IEEE 802.11, esta se usa para América y el HiperLAN/2 para Europa.

A.2.1. HIPERLAN/2

HIPERLAN (**HI**gh **PE**rformance **R**adio **LAN**) es una solución de redes de área local basadas en radio (RLAN, radio-based LAN). Está destinado para la conexión inalámbrica entre PC's, Laptops, estaciones de trabajo, servidores, impresoras y otros equipos de red para la conexión de redes de datos dentro de un edificio, proveyendo más flexibilidad y posiblemente un ahorro de economía en la instalación, reconfiguración y uso de estas redes dentro de los negocios y la industria. HIPERLAN ha sido desarrollado por el Instituto de Estándares en Telecomunicaciones Europeo (ETSI, European Telecommunications Standards Institute) [51] [52].

HIPERLAN/2 es uno de cuatro estándares especificados por la ETSI dentro de la familia de estándares BRAN (Broadband Radio Access Networks, "redes de acceso de radio de banda ancha"), el alcance de HIPERLAN/2 es proveer de servicios a las redes inalámbricas con infraestructura o redes ad hoc con poca movilidad (< 1.5 m/s) y un alcance pequeño (<50m). Los estándares de HIPERLAN incluyen a HIPERLAN/1 (alta velocidad en WLAN), HIPERLAN/2, HIPERACCESS (acceso remoto punto-multipunto para redes inalámbricas fijas), HIPERLINK (interconexión ancho de banda inalámbrico) asi como lo muestra la figura A.6.

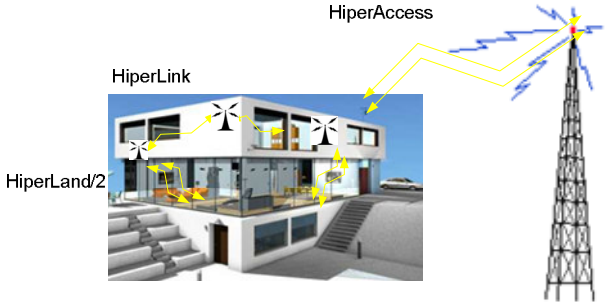


Figura A. 6. Ejemplo de HiperLAN.

HIPERLAN/1 y /2 operan en la banda de frecuencia de 5GHz mientras que HIPERLINK opera en 17GHz. La tabla A.5 resume estas características del estándar [51] [52] [53].

Tabla A. 5. Características de HIPERLAN

Estándar	HIPERLAN/1	HIPERLAN/2	HIPERACCES	HIPERLINK
Tipo	WLAN	WLAN	Acceso Remoto	Interconexión de Ancho de Banda
Banda de Frecuencia	5 GHz	5 GHz	Variada	17 GHz
Tasa de Datos Física	19 Mbps	54 Mbps	25 Mbps	155 Mbps

El modelo de capas de HIPELAN está compuesto por tres capas, la capa física, capa de control de enlace de datos y una capa de convergencia.

La capa física está basada en el esquema de modulación de Multiplexación por División de Frecuencias Ortogonales (OFDM). Además, para mejorar la capacidad de enlace por las diferentes situaciones de interferencia y distancias de terminales de los puntos de acceso, se utiliza un esquema de adaptación de enlace, por ejemplo usando varios esquemas de modulación en la subportadora y puntualizando códigos de convolución o también cambiando la tasa de datos. Los parámetros más importantes de la capa física se encuentran resumidos en la tabla A.6 [51] [52].

Tabla A. 6. Parámetros la capa Física de HIPERLAN/2

Parámetros	Valor
Número de Subportadoras	64
Número de Subportadoras usadas	52, donde 48 son para datos y 4 pilotos
Espacio de Canal	20 MHz
Tasa de Muestreo	20 Mmuestras/s
Intervalo de Guarda	80 ns correspondientes a 16 tiempos de muestras

Modulación de Subportadora	BPSK, QPSK, 16QAM y 64QAM(opcional)
Corrección de Error	Una tasa de ½ de código convolucional original (9/16 y 3/4 para código puntualizado)
Tasa de Datos	6, 9, 12, 18, 27, 36, y 54 Mbps
Oscilador	+/- 20 ppm con un oscilador de referencia para la generación de RF y un reloj de tiempo base.

A.3.REDES INALÁMBRICAS DE ÁREA METROPOLITANA

Se llaman redes inalámbricas de área metropolitana, WMAN (*Wireless Metropolitan Area Networks*), a aquellas redes que tienen una cobertura desde unos cientos de metros hasta varios kilómetros. El grupo de trabajo del IEEE 802.16 [54] ha desarrollado una serie de recomendaciones para WMAN en el rango del espectro de 10-66 GHz, cubriendo alguna de los estándares existentes. El grupo presenta los aspectos de las capas MAC y PHY para este espectro como IEEE 802.16. Más tarde, IEEE 802.16a una extensión del grupo agregó especificaciones para WMAN para 2-11GHz de tal manera que modifican las especificaciones MAC y PHY del IEEE 802.16 [54]. Otro grupo de la IEEE se dedica para el caso de la movilidad, el IEEE 802.20 en 3.5GHz, para velocidades excediendo los rangos vehiculares.

Adicionalmente, la infraestructura de acceso de banda ancha de la ETSI tiene especificada HIPERACCES para la familia del estándar BRAN. También cuentan con el estándar para el caso donde no se requiera línea de vista como el caso de la movilidad, HIPERMAN

A.3.1. IEEE 802.16

El WMAN del IEEE consta de dos partes, una basada para el rango de 10-66GHz, que fue el interés principal, y la otra de 2-11GHz que quedo aprobada en el estándar IEEE 802.16a en marzo del 2000. El proyecto 802.16a implica el desarrollo de una nueva capa física, con mejoras de la capa básica MAC [52] [54].

Estas versiones del estándar son especificadas para la comunicación fija, por lo que surgió la necesidad de crear otro grupo para desarrollar estándares para movilidad, el cual se llama IEEE 802.16e.

En resumen se muestra la tabla A.7 con las principales características del estándar IEEE 802.16.

Tabla A. 7. Parámetros del estándar IEEE 802.16

Estándar	IEEE 802.16	IEEE 802.16a	IEEE 802.16e
Espectro	10 – 66 GHz	< 11 GHz	< 6 GHz
Funcionamiento	En Línea de Vista	En Línea de Vista	Sin Línea de Vista
Tasa de Bit	32 – 134 Mbit/s	75 Mbit/s	15 Mbit/s
Modulación	QPSK, 16 y 64 QAM	OFDM con 256 subportadoras QPSK, 16 y 64 QAM	OFDM con 256 subportadoras QPSK, 16 y 64 QAM
Movilidad	No	No	Pedestre
Ancho de Banda	20, 25 y 28 MHz	1.25 – 20 MHz	1.25 – 20 MHz
Cobertura	2 – 5 Km	5 – 10 Km	2 – 5 Km

A.3.2. IEEE 802.20

Tradicionalmente, el acceso inalámbrico de ancho de banda ha sido asociado con ser sistemas fijos. Sin embargo, dos desarrollos han sido destinados para cambiar el panorama de este escenario. Estos son, el IEEE 802.16e del mismo grupo de trabajo de WirelessMAN (802.16) visto en A.3.1 y otro grupo de trabajo el IEEE 802.20 [55].

El alcance del IEEE 802.20 es la especificación de las capas físicas y MAC de una interface aérea para sistemas de acceso inalámbrico de ancho de bandas móviles interoperables. Operando en bandas con licencia por debajo de 3.5GHz y optimizado para el transporte de de datos IP con tasas de datos por usuarios de máximo 1 Mbps. Soporta varias clases de movilidad hasta una velocidad de 250 Km/h en una ambiente MAN [55] [56].

La tabla A.8 resume algunas de las características del estándar 802.20 [52] [55] [56].

Tabla A. 8. Características del estándar IEEE 802.20.

Característica	Valor
Movilidad	Movilidad vehicular hasta 250 Km/Hrs
Máxima tasa de transmisión de bajada	1 Mbps
Máxima tasa de transmisión de subida	300 Kbps
Máxima tasa de bajada por celda	4 Mbps
Máxima tasa de subida por celda	800 Kbps
Ancho de Banda	1.25 – 5 MHz
Frecuencia	<3.5 GHz

A.3.3. HIPERACCESS e HIPERMAN

La norma HiperMAN trata del interfuncionamiento para sistemas BWA (Broadband wireless Access) fijos que funcionan en las frecuencias de 2-11 GHz, usando un enlace descendente OFDM y un enlace ascendente OFDMA, para proporcionar células de gran tamaño cuando se trabaja sin línea de vista directa (NLoS). La norma permite la compatibilidad con la transmisión en dos sentidos con división de frecuencia (DDF) y con división de tiempo (DDT), eficiencia espectral y velocidades de datos elevadas, modulación adaptativa, gran radio de célula, compatibilidad con sistemas avanzados de antenas y algoritmos de encriptado de alta seguridad. Sus perfiles apuntan a las separaciones de canales de 1,75 MHz, 3,5 MHz y 7 MHz, adecuados para la banda de 3,5 GHz [57].

HiperACCESS especifica la interfaz radioeléctrica de los sistemas de acceso radioeléctrico de banda ancha que trabajan en el servicio fijo con una topología punto-multipunto (P-MP). La norma está optimizada para redes centrales basadas en paquetes y en células. Las principales aplicaciones son las redes de reserva que trabajan en condiciones de línea de vista directa (LoS), las PYME (pequeñas y medianas empresas) y las pequeñas oficinas en el hogar (SOHO, *small office home office*). La especificación HiperACCESS consta de varias partes: capa física basada

en transmisión de portadora única, optimizada para enlaces de LoS por encima de 10 GHz, DLC (capa de control de enlaces de datos) con un conjunto bien controlado de características optativas y previsiones para la evolución futura, varias capas de convergencia, un conjunto completo de especificaciones de prueba para asegurar la interoperabilidad entre equipos de diferentes fabricantes. El concepto adaptativo HiperACCESS permite un elevado caudal de tráfico de más de 100 Mbit/s en condiciones normales de propagación, permite factores elevados de reutilización de frecuencias, y garantiza que la interferencia con otros sistemas es pequeña y controlable así como densidades de flujo de potencia ajustables según la reglamentación de cada país [57].

A.4. REDES INALÁMBRICAS DE ÁREA REGIONAL

A.4.1. IEEE 802.22

El grupo de trabajo 22 de la IEEE de las redes inalámbricas (IEEE 802.22) [58] se encuentra realizando una propuesta para redes inalámbricas de largo alcance, para llevar acceso de banda ancha a áreas rurales y/o remotas, tomando las mejores características de VHF y L-UHF, utilizando canales de TV no utilizados.

Este estándar no tiene alcance de una red de área metropolitana ya que es mayor la cobertura que los estándares 802.16 y 802.20 que son los que están dentro de este alcance y también no se puede decir que es una red de área extensa ya que no cubre grandes distancia como lo hacen las redes de área extensa por lo que se le ha denominado Redes Inalámbricas de Área Regional (WRAN, *Wireless Regional Area Networks*).

Como se observa en la figura A.7, los diferentes tipos de redes y sus estándares, tanto los propuestos por la IEEE y la IETF. Se observa que el 802.22 está entre WAN y MAN.

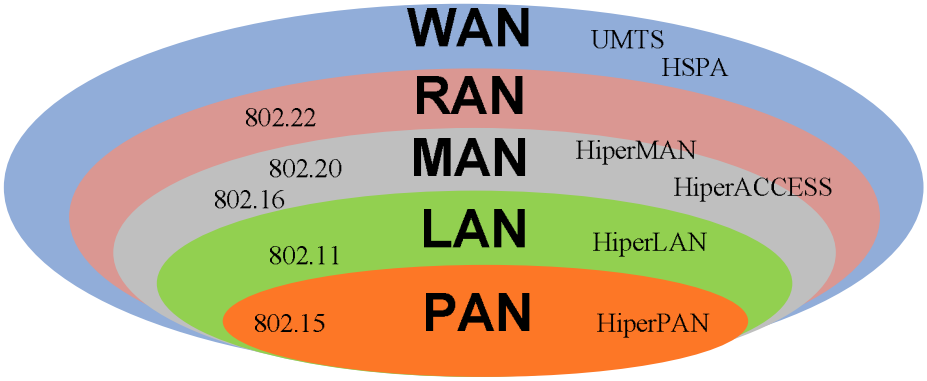


Figura A. 7. Clasificación de redes inalámbricas.

Este estándar (IEEE 802.22) especifica la interface aérea, incluyendo la capa de control de acceso al medio (MAC) y la capa física (PHY), de redes inalámbricas de área regional estáticas de punto-multipunto operando en las bandas de difusión de VHF/UHF TV entre las frecuencias 54 MHx y 862 MHz [59] [60]. Algunas de las características se resumen en la tabla A.9 [60] [61] [62].

Tabla A. 9. Características de 802.22.

Característica	Valor
Rango	40 Km
Máxima Tasa de Datos	18 Mbps
Ancho de Banda	6,7,8 MHz (dependiendo el país)
Frecuencia	54-862 MHz
Modulación	64 QAM Adaptiva
Población por área cubierta	4500 personas
Mínima Densidad de población cubierta	1.5 personas/km^2

A.5.REDES INALÁMBRICAS DE ÁREA EXTENSA

Una vez visto las tecnologías anteriores, pensar que existan redes inalámbricas con más cobertura parece imposible. Aquí es donde entra el concepto de Redes inalámbricas de área extensa (WWAN, *Wireless Wide Area Networks*), o también conocidas como redes de área global, las cuales tienen cobertura de un estado, un país, un continente o incluso a nivel mundial.

La WWAN se aprovecha de la infraestructura de red de los teléfonos móviles para proporcionar conexión de red inalámbrica en cualquier lugar. Gracias a la WWAN, el usuario puede mantener una conexión de red incluso si está en movimiento, como el caso del estándar 802.16e y 802.20. Se aprovecha de diferentes tipos de tecnologías, entre las tecnologías más importantes que ofrecen WWAN son las siguientes [63] [64]:

- 2G – GSM (Sistema Global para las Comunicaciones Móviles, *Global System for Mobile communications*)
- 2.5G – GPRS (Servicio General de Radio Paquetes, *General Packet Radio Services*)
- 2.75G – EDGE (Entorno GSM de Datos Mejorados, *Enhanced Data GSM Environment*)
- 3G – UMTS (Sistema Universal de Telecomunicaciones Móviles, *Universal Mobile Telecommunications Service*)
- 3.5G – HSDPA (Acceso a Paquetes de Descarga de Alta Velocidad, *High Speed Downlink Packet Access*)

La figura A.8 muestra la evolución de las tecnologías mencionadas y el futuro en redes extensas.

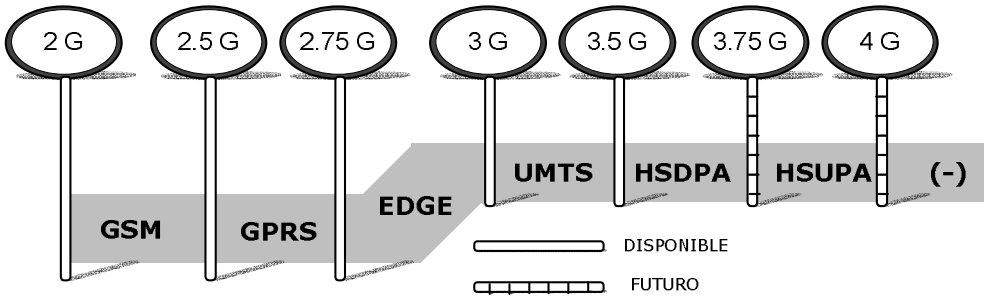


Figura A. 8. Evolución de WAN.

A.5.1. GSM

Es un estándar de telecomunicaciones establecido por iniciativa Europea que rápidamente fue adoptada por todo el mundo [65]. Hoy en día, la tecnología GSM es usada por más de uno de cada cinco de la población mundial, para Junio del 2006 había un poco más de 2 billones de subscriptores GSM [66]. GSM utiliza tecnología digital y métodos de transmisión de acceso

múltiple por división de tiempo. Es un sistema de conmutación de circuito que divide cada canal de 200 KHz en 8 ranuras de tiempo en 25 KHz. Opera en las bandas frecuencias de 900 MHz y 1.8 GHz en Europa y 850 MHz y 1.9 GHz en Estados Unidos. GSM soporta velocidades de transferencia de datos arriba de 9.6 Kbps, permitiendo la transmisión de servicios de datos básicos como SMS (Servicio de Mensajes Cortos, *Short Message Service*) [66].

La tabla A.10 resume las características importantes para la banda de frecuencia de 900 MHz.

Tabla A. 10. Características de GSM.

Característica	Valor
Técnica de Acceso Múltiple	FDMA / TDMA
Frecuencia de Subida	933 – 960 MHz
Frecuencia de Bajada	890 – 915 MHz
Espacio entre Canales	200 KHz
Modulación	GMSK
Canales de Voz por Canales de RF	8
Tasa de transmisión de Canal	270.833 Kbps

A.5.2. GPRS

GPRS es el servicio de datos inalámbricos más ubicuo en el mundo, disponible ahora con la mayoría de las redes GSM. GPRS es una solución basada en protocolos de internet (IP) que soporta un amplio rango de empresas y aplicaciones de consumidor.

Las velocidades de transmisión teóricas posibles son arriba de 171.2 Kbps cuando son asignadas 8 ranuras al mismo tiempo [66]. Utiliza las mismas frecuencias que GSM [67].

Con el propósito de contrarrestar los efectos de un medio de transmisión adverso como lo es el medio inalámbrico, GPRS considera transmisiones a diversas tasas de bit que se seleccionan en forma dinámica de acuerdo a las condiciones del canal. Esto se logra cambiando el sistema de codificación convolucional, y el proceso de perforación (*puncturing*)

Por lo tanto se definieron cuatro esquemas de codificación diferentes CS-1 (Coding Sequence 1), este corresponde al esquema de codificación más robusto, pero a la vez, de menor tasa de transferencia efectiva. A su vez, CS-4 posee una tasa de transferencia efectiva mayor, pero no soporta interferencias en el canal, ya que no posee correcciones de errores [68] [69].

La tabla A.11 nos muestra un resumen de las principales características de GPRS [69].

Tabla A. 11. Características de GPRS.

Característica	Valor
Modulación	GMSK
Velocidad de Símbolo	270 ksimb/s
Velocidad de modulación de bit	270 Kbps
Velocidad de datos de radio por intervalo de tiempo	22.8 Kbps
Velocidad de datos de usuario por intervalo de tiempo	20 Kbps (CS4)
Velocidad de datos de usuario (8 intervalos de tiempo)	160 Kbps (182.4 Kbps)

A.5.3. EDGE

Otra mejora para las redes GSM es proporcionada por la tecnología EDGE. Esta tecnología proporciona tres veces más la capacidad de datos que GPRS. EDGE utiliza la misma estructura de TDMA, el canal lógico y la portadora de ancho de banda 200 KHz que hasta hoy en día utiliza GSM, lo que permite ser puestas directamente en redes GSM existentes. Para muchas redes GSM/GPRS, EDGE es simplemente una actualización de software [66].

El objetivo de esta tecnología es la de ofrecer tasas de transmisión superior, una mejor eficiencia espectral y facilitar nuevas aplicaciones y mayor capacidad para el usuario móvil [69].

EDGE se diferencia de GPRS en el sistema de modulación de portadora, utilizando codificación 8-PSK (*Phase Shift Keying*) lineal para incrementar la tasa de transmisión de datos. además se utilizan en forma adicional los bits de bandera (F, *Stealing Flag*) de una trama GSM.

Al igual que GPRS, EDGE considera transmisiones a diversas tasas de transmisión efectivas seleccionadas en forma dinámica de acuerdo a las condiciones del canal. La mayor eficiencia espectral que se logra al utilizar 8-PSK, es a cambio de hacer la información más vulnerable a las malas condiciones de canal, por lo que EDGE considera también la reducción de tasa de transmisión a modulación a GMSK [68].

La máxima tasa efectiva (*Throughput*) de servicio alcanzable con EDGE es de 59.2 Kbps, si solamente se utiliza una ranura de tiempo (*timeslot*) de GSM. Por lo tanto teóricamente para 8 intervalos de tiempo la velocidad seria 473.6 Kbps [68] [69]. La tabla A.12 muestra en resumen las características más importantes de EDGE [69].

Tabla A. 12. Características de EDGE.

Característica	Valor
Modulación	8-PSK / GMSK
Velocidad de Símbolo	270 ksimb/s
Velocidad de modulación de bit	810 Kbps
Velocidad de datos de radio por intervalo de tiempo	69.2 Kbps
Velocidad de datos de usuario por intervalo de tiempo	59.2 Kbps (MCS9)
Velocidad de datos de usuario (8 intervalos de tiempo)	473.6 Kbps (553.6 Kbps)

A.5.4. UMTS

La ITU (*Unión Internacional de Telecomunicaciones*) inicio actividades hacia la creación de un sistema de tercera generación. Inicialmente iba a tener el nombre de FPLMTS (*Futuro Sistema Público Terrestre de Telecomunicaciones Móviles*). Este sistema tuvo gran apoyo por parte de la unión europea pero después de los estudios se requería que se estableciera un estándar mundial para la tercera generación. Esto se conoce como IMT-2000 (Comunicaciones Móviles Internacionales, *International Mobile Communicactions*) [24] [69] [70].

UMTS es la propuesta de ETSI para tercera generación, siendo el sucesor de GSM. Utiliza CDMA como técnica de acceso múltiple, ofreciendo servicios de voz, fax, mensajes multimedia, asi como servicios de datos de hasta 2Mbps [24] [69].

Las frecuencias que se utilizan son las siguientes [70]:

1920 – 1980 y **2110 – 2170 MHz**: División de Frecuencia Dúplex (FDD, W-CDMA). Pares de enlace de bajada y enlace de subida, ancho de banda del canal 5MHz y rastreo es de 200 KHz. Un operador necesita de tres a cuatro canales (2 x 15 MHz o 2 x 20 MHz) para ser capaz de tener alta velocidad y redes de alta capacidad.

1900 – 1920 y **2010 – 2025 MHz**: División de Tiempo Dúplex (TDD, TD/CDMA). Sin pareces, mismo ancho de banda y rastreo. Transmisión (Tx) y Recepción (Rx) no están separadas en frecuencia.

1980 – 2010 y **2170 – 2200 MHz:** Enlace ascendente y descendente de satélite.

En la tabla A.13 se muestran las características más importantes del sistema UMTS [24] [69] [70] [71]:

Tabla A. 13. Características de UMTS.

CARACTERISTICA	UMTS
Método de acceso	CDMA
Ancho de banda del canal	5 MHZ
Velocidad de chip	3.84 Mchip/s
Longitud de trama	10 mseg
Factor de expansión	4-512
Modulación	QPSK
Codificación del canal	Convolución, turbo codificado y sin codificación

A.5.5. HSPA

La banda ancha móvil típicamente se refiere a la entrega de usuarios finales tasa de descarga de datos de 500 Kbps o mas proporcionando completa movilidad. La tecnología de Acceso a Paquetes de Alta Velocidad (HSPA, *High Speed Packet Access*) tiene disponibles la entrega de servicios de banda ancha móvil comercial en excesos de tales velocidades y están proporcionando servicios de banda ancha a la elección de consumidores rurales y urbanos y usuarios de empresas.

HPSA [72] es un término común para referirse a los acrónimos para HSDPA y HSUPA conocidos como Envolvente HSPA. Las redes son desarrolladas principalmente en 1.9GHz y 2.1GHz con pocos operando en el espectro más ventajoso de 85MHz.

Algunos términos importantes que se tienen que discutir son:

HSPDA: Acceso a Paquetes con Descarga de Alta Velocidad – Es prácticamente una actualización de software del estándar UMTS. Esta actualización es para incrementar la eficiencia y reducir la latencia del enlace y esto se logra utilizando un número de técnicas en paralelo [73].

Código y Modulación Adaptivo – Software donde el nodo B (estación base) analiza cada usuario en la celda para señales de calidad y usando esta información y también la capacidad de la celda en el tiempo determina que esquema de modulación usara para cada dispositivo. Entonces, para una buena señal y una celda de carga ligera, el nodo B asignara modulación 16 QAM permitiendo tasas pico mayor a 3.6 Mbps y regresando con QPSK con tasas asociadas de datos bajas si las condiciones son menos favorables [72] [74].

Calendarización de paquetes rápidos – Nuevamente depende del dispositivo del reporte de lo fuerte de la señal. El nodo B puede determinar cual dispositivo para mandar datos en la próxima trama de tiempo de 2ms así tomar el mejor ancho de banda disponible. El nodo B también puede determinar cuanta cantidad de datos mandar a un dispositivo basándose en su presupuesto de

enlace. El sistema HSPA usa 16 códigos de los cuales 15 son asignados para HSPA. El nodo B después determina cuantos códigos asignara a un dispositivo individual dentro de la celda en cualquiera de la ranura de tiempo de 2ms dada que en turno determina la velocidad de datos general que es enviada. El nodo B puede asignar todas las ranuras de tiempo y los 15 códigos a un solo dispositivo de la celda y si ese dispositivo reporta condiciones de buena señal, la tasa de transmisión máxima puede ser alcanzada [72] [75].

Petición de reenvío automático híbrido: (Hybrid Automatic Repeat reQuest, HARQ) – Esta técnica es empleada para corregir errores en la transmisión de paquetes entre el nodo B y el usuario. El dispositivo pide una retransmisión de cualquier paquete que tiene error mientras que se almacenan todos los paquetes erróneos viejos. El dispositivo después suavemente re-combina todos los paquetes para corregir el error. Como almacena todo los paquetes en error y los usa después para corregir la transmisión, un método más confiable y eficiente es alcanzado [73].

HSUPA: Acceso a Paquetes con Carga de Alta Velocidad – Utiliza las mismas técnicas que HSDPA en términos de adaptación de enlace en el desarrollo de la modulación y HARQ para mejorar la carga y después crear transmisiones de datos síncronas mayores de 5.7 Mbps. Una pequeña diferencia es en la manera calendarizar el trabajo de manera que "sirva" a todos los dispositivos que se están cargando y el esquema de modulación reducido [72] [73].

Calendarización – Este es un mecanismo de petición de asistencia similar a la calendarización de paquetes rápida pero iniciada por el dispositivo. El dispositivo solicita permiso para enviar datos y el nodo B determina, basado en la carga de celda, peticiones y niveles de poder dentro de la celda, cuando y cuantos dispositivos serán auxiliados y a qué velocidad, entre otras [73] [74].

Sin calendario – Para ciertas aplicaciones donde el retraso basado en la petición de calendario y el overhead del nodo B podría ser también grande como VoIP, hay otro método donde el dispositivo inicia la transmisión. En este caso el nivel de potencia es puesto por el dispositivo y típicamente es constante. Con la asistencia de petición de calendario, el nodo B determina el nivel de potencia de los dispositivos de transmisión y es controlada dinámicamente para asegurar máxima eficiencia para todos los dispositivos en la celda [72] [75].

Envolvente HSPA – Algunas veces se refiere a HSPA+ o I-HSPA (ligeramente diferentes pero tienen el mismo reto final para el usuario. Este sistema mejora la descarga para proveer 42 Mbps utilizando modulación 64 QAM y la carga de 11.5 Mbps a través de 16 QAM [72] [74] [75].

En total existen hasta octubre 2008, 278 HSPA operadoras comprometidas en 122 países/territorios. México cuanta con dos empresas, Movistar y Telcel, las cuales tienen en servicio la tecnología HSDPA con una velocidad de 1.8Mbps [76]. La figura A.9 muestra la distribución en el mundo de esta tecnología.

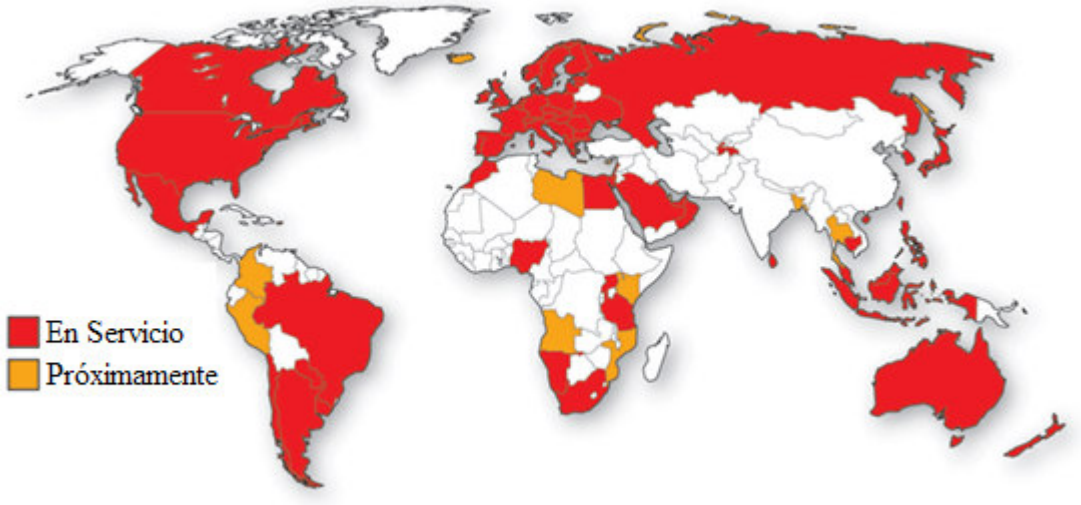


Figura A. 9. Cobertura de HSDPA.

B

APÉNDICE

PRODUCTIVIDAD DURANTE LA ESTANCIA EN LA MAESTRÍA

En este apéndice se mostrarán los artículos publicados, tanto en Congresos Nacionales e Internacionales, que gracias a ellos me dieron la oportunidad de conocer nuevos lugares en diferentes ciudades, países e incluso continentes.

Cabe mencionar que se realizaron trabajos relacionados con el tema de tesis y además se realizaron trabajos en paralelo con otros temas de investigación de interés.

Por lo anterior la sección B.1 contiene los artículos relacionados al tema de tesis y la sección B.2 contiene la productividad adicional.

B.1. PRODUCTOS DE LA TESIS

En resumen se realizaron 5 artículos relacionados con la investigación, 3 en congresos internacionales y 2 en un encuentro regional.

Noviembre 17 y 18 2008 — Centro de Investigación y Desarrollo de Tecnología Digital, Tijuana, B.C, México.

IV Encuentro Regional Académico ERA 2008

Análisis de Ruta Implementando el Algoritmo Proactivo OLSR en una Red Ad-Hoc 802.11

- *Trujillo Toledo Diego Armando*, Sánchez Adame Moisés, Álvarez Cabanillas Miguel Agustín.
- ISBN (En trámite)
- Páginas (En trámite)

Análisis de Ruta Implementando el Algoritmo Proactivo OLSR en una Red Ad-Hoc 802.11

Diego Armando Trujillo Toledo, Moisés Sánchez Adame, Miguel Agustín Álvarez Cabanillas.
Centro de Investigación y Desarrollo de Tecnología Digital (CITEDI) - IPN, Tijuana, B.C., México.
Teléfono (664) 623-1344 Fax (664) 623-1388 E-mail: {trujillo, msanchez, malvarez}@citedi.mx

Resumen **Se presenta el análisis de ruta en una red Ad-Hoc inalámbrica 802.11 implementando el algoritmo de ruteo Proactivo de Estado de Enlace Optimizado (OLSR). De este algoritmo se analiza el procedimiento para la obtención de las tablas de ruteo, descubrimiento de vecinos, selección de retransmisores, y cálculo de ruta. Además se analiza el mecanismo de acceso al medio (MAC) y los diferentes tipos de mensajes de señalización, que emplea éste bajo el estándar IEEE 802.11 para redes Ad-Hoc. Se selecciona una topología de red que permite aplicar los parámetros de control característicos del algoritmo de ruteo proactivo optimizado de estado de enlace (OLSR). Se analizan los principales paquetes a nivel cabecera utilizados por el algoritmo, como son los mensajes de iniciación (HELLO) y los mensajes de control de red ("TC" Topology Control).**

Palabras Clave **802.11, Ad-Hoc, Algoritmo, OLSR, Mensajes, Paquetes, Hello, Control de Topologia (TC), MAC, Probe Request, Probe Response, RTS, CTS, ACK, Proactivo, Estado de Enlace.**

I. Introducción

En una red inalámbrica que utiliza el estándar IEEE 802.11 [1] se pueden distinguir dos tipos de configuraciones. La primera de ellas Ad-Hoc consiste de un mínimo de dos nodos capaces de comunicarse directamente [1]. La segunda configuración llamada de Infraestructura [1] en la cual, se agrega un punto de acceso (AP) para administrar la interconexión entre los nodos.

La comunicación en una red Ad-Hoc se lleva a cabo en dispositivos que se encuentren en el mismo rango de cobertura. Para comunicarse con un destino fuera del área de cobertura se requiere de algoritmos de ruteo, los cuales se pueden clasificar en: Protocolos Proactivos, son aquellos donde los nodos mantienen rutas establecidas para cada destino de la red, Reactivos aquellos donde la ruta para un destino se descubren en el tránsito de los mensajes y los Protocolos Híbridos son la combinación de ambos, teniendo rutas establecidas y rutas que se están encontrando al momento del tránsito de los mensajes.

En el caso de los protocolos proactivos algunos ejemplos son el protocolo de Vector Distancia de Secuencia Destino "DSDV" (*Destination-Sequenced Distance-Vector*) y el Ruteo de Estado de Enlace Optimizado "OLSR" (*Optimized Link State Routing*). Los ejemplos para los reactivos son el Ruteo de Fuente Dinámica "DSR" (*Dynamic Source Routing*) y el algoritmo Vector Distancia Sobre Demanda Ad-Hoc "AODV" (*Ad hoc On-Demand Distance Vector*). El protocolo de Ruteo de Zona "ZRP" (*Zone Routing Protocol*) y el Algoritmo de Ruteo Temporalmente Ordenado "TORA" (*Temporally Ordered. Routing Algorithm*) son ejemplos de los híbridos [2].

El objetivo de este trabajo es presentar la metodología que se emplea para el análisis de una ruta en una red inalámbrica Ad-Hoc 802.11 utilizando el Algoritmo proactivo OLSR. Se seleccionó una topología mínima de 8 nodos, distribuidas de tal manera que reflejará el potencial del algoritmo proactivo seleccionado. La figura 1 muestra la topología de red que se utilizó para el análisis.

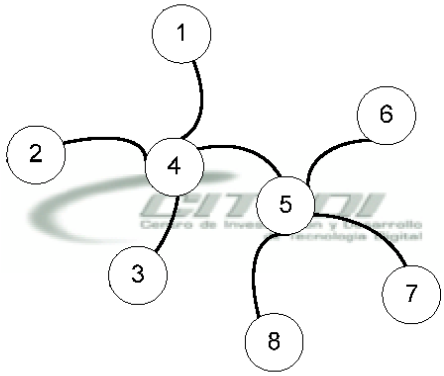


Fig. 1 Topología de Red Ad-Hoc Inalámbrica

El trabajo se divide en las siguientes secciones: en la sección 2 se describe el funcionamiento de la capa MAC del 802.11 en una red Ad-Hoc. En la sección 3 se resume el funcionamiento y formato del algoritmo de estado de enlace optimizado (OLSR). En la sección 4 se presenta la metodología para el análisis de la obtención de las tablas de ruteo utilizando OLSR. En la sección 5 se describe la comunicación entre un par de nodos utilizando las tablas de ruteo obtenidas en la sección 4. En la sección 6 se presentan las conclusiones de este trabajo y trabajos a futuros.

Este trabajo cuenta con el apoyo del proyecto de investigación **SIP 20080845** que pertenece al **Instituto Politécnico Nacional.**

Noviembre 10-14 2008 Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Zacatenco, Distrito Federal, México.

"5to Congreso Internacional de Ingeniería Electromecánica y de Sistemas CIIES 2008"

Análisis de Ruta Implementando el Algoritmo Reactivo de Vector Distancia (AODV) en una Red Ad-Hoc 802.11.

- *Trujillo Toledo Diego Armando*, Sánchez Adame Moisés, Álvarez Cabanillas Miguel Agustín.
- ISSN (En trámite)
- Páginas 1105-1110

5º CONGRESO INTERNACIONAL DE INGENIERÍA ELECTROMECÁNICA Y DE SISTEMAS

5° CONGRESO INTERNACIONAL DE
INGENIERÍA ELECTROMECÁNICA Y DE SISTEMAS
México, D. F. 10-14 de Noviembre 2008

Artículo aceptado por referee
TEL033

Análisis de Ruta Implementando el Algoritmo Reactivo de Vector Distancia (AODV) en una Red Ad-Hoc 802.11

Diego Armando Trujillo Toledo[1], Moisés Sánchez Adame[1], Miguel Agustín Álvarez Cabanillas[1].
[1]Departamento de Telecomunicaciones, CITEDI-IPN, Tijuana, B.C., México.
Teléfono (664) 623-1344 Fax (664) 623-1388 E-mail: {trujillo, msanchez, malvarez}@citedi.mx

Resumen — **Se presenta el análisis de ruta en una red Ad-Hoc inalámbrica 802.11 implementando el algoritmo Reactivo de Vector Distancia (AODV). Se analizó el funcionamiento del algoritmo, específicamente el procedimiento de transmisión de la información que se envía a través de los nodos pertenecientes a la red Ad-Hoc. Se utilizó una topología de red especifica que permite conocer el potencial de AODV al momento de establecer una ruta. Se analizan los principales tipos de mensajes que utiliza el algoritmo como: El Mensaje de Petición de Ruta (*RREQ - Route Request*), Mensaje de Contestación de Ruta (*RREP – Route Replay*) y el Mensaje de Error de Ruta (*RERR – Route Error*). Se logró describir el funcionamiento de AODV resultando un análisis previo para realizar una implementación experimental.**

Palabras Clave – **802.11, Ad-Hoc, Algoritmo, AODV, Mensajes, RERR, RREP, RREQ, Vector Distancia.**

Abstract — **This work presents the analysis of the route in a 802.11 wireless Ad-Hoc network implementing the *Ad hoc On-Demand Distance Vector* algorithm (AODV). We analyzed the function of the algorithm, specifically the procedure for the control of the information that is sent across the nodes in the Ad-Hoc network. It used an specific topology that allows the potential for AODV when the route is established. It discusses the main types of messages used by the algorithm: The Route Request Message (RREQ), Route Reply Message (RREP) and the Route Error Message (RERR). There was describing the operation of AODV resulting in analysis to make a physical implementation.**

Keywords — **802.11, Ad-Hoc, Algorithm, AODV, Distance Vector, Messages, RERR, RREP, RREQ.**

I. Introducción

En una red inalámbrica que utiliza el estándar IEEE 802.11 [1] se pueden distinguir dos tipos de configuraciones, la primera de ellas requiere de un sistema central el cual controla el acceso a los nodos, llamada Infraestructura. La segunda configuración no cuenta con un sistema centralizado y se le conocen como redes Ad-Hoc o redes sin Infraestructura.

Las redes móviles Ad-Hoc están constituidas por un conjunto de dispositivos dinámicos, establecidos arbitrariamente capaces de tener conexión entre ellos. El principal objetivo de los algoritmos de ruteo es la eficiente y correcta conexión entre un par de nodos que requieren mantener una comunicación, se clasifican de la siguiente manera: Protocolos Proactivos, son aquellos donde los nodos mantienen rutas establecidas para cada destino de la red, los Protocolos Reactivos son aquellos donde la ruta para un destino se crea en el tránsito de los mensajes y los Protocolos Híbridos son la combinación de ambos, teniendo rutas establecidas y rutas que se están encontrando al momento del tránsito de los mensajes.

Ejemplos de los protocolos proactivos son el protocolo DSDV (*Destination-Sequenced Distance-Vector Routing*) y WRP (*Wireless Routing Protocol*). Los ejemplos para los reactivos o Sobre Demanda es DSR (*Dynamic Source Routing*) y AODV (*Ad hoc On-Demand Distance Vector*). El protocolo ZRP (*Zone Routing Protocol*) y el protocolo TORA (*Temporally Ordered Routing Algorithm*) son ejemplos de los híbridos.

El objetivo de este artículo es presentar la metodología que se empleó en el análisis de una ruta en una red inalámbrica Ad-Hoc 802.11 utilizando el Algoritmo reactivo AODV. El algoritmo se implementó en un ambiente de diez nodos distribuidos de manera estratégica de tal forma que permita aplicar AODV en diferentes escenarios posibles. La figura 1 muestra la topología de red que se utilizó en el cual se establece la comunicación del nodo 1 al nodo 10.

El artículo se encuentra dividido en las siguientes secciones: sección 2 se resume el funcionamiento del algoritmo AODV. En la sección 3 se describe el formato de los mensajes AODV y la trama 8002.11.

Fig. 1. Topología de Red Ad-Hoc Inalámbrica.

Este trabajo cuenta con el apoyo del proyecto de investigación **SIP 20080845** que pertenece al **Instituto Politécnico Nacional**.

Octubre 29-31 2008

Instituto Tecnológico de Chihuahua,
Chihuahua, México.

"XXX Congreso Internacional de Ingeniería en Electrónica ELECTRO 2008"

Implementación Experimental de AODV en una Red Ad-Hoc Inalámbrica 802.11x.

- *Trujillo Toledo Diego Armando*, Sánchez Adame Moisés, Álvarez Cabanillas Miguel Agustín.
- ISSN 1405-2172 Volumen XXX
- Páginas 139-144

INSTITUTO TECNOLOGICO DE CHIHUAHUA
División de Estudios de Posgrado e Investigación

ELECTRO 2008

XXIX CONGRESO INTERNACIONAL DE INGENIERIA ELECTRONICA

ELECTRO 2008

Octubre del 29 al 31, 2008
Chihuahua, Chih. México

IMPLEMENTACIÓN EXPERIMENTAL DE AODV EN UNA RED AD-HOC INALÁMBRICA 802.11X

Trujillo Toledo Diego Armando, Sánchez Adame Moises, Alvarez Cabanillas Miguel Agustín.

Instituto Politécnico Nacional
Centro de Investigación y Desarrollo de Tecnología Digital
Departamento de Telecomunicaciones
Ave. del Parque #1310, Mesa de Otay, Tijuana B.C 22510
Teléfono: (664) 623-13-44
Fax: (664) 623-13-88
{ trujillo, msanchez, malvarez} @ citedi.mx

RESUMEN.
Se presenta una implementación experimental del algoritmo de ruteo AODV en una red inalámbrica Ad-Hoc utilizando WinAODV. Se resume el funcionamiento del algoritmo Vector Distancia Sobre Demanda Ad-Hoc, posteriormente se describen las posibilidades de implementación como lo son el Snooping, la Modificación de Kernel y el Netfilter. WinAODV entre las características importantes es el empleo de la metodología Netfilter también utiliza el ambiente Windows y lo más importante es que funciona adecuadamente con las especificaciones del RFC 3561 [11]. Se logro establecer una red de computadoras en la modalidad Ad-Hoc utilizando el estándar 802.11 empleando WinAODV.

1. INTRODUCCIÓN

La simulación de protocolos es una pieza clave para el desarrollo de una comunicación [1], evitando gastos innecesarios, además proporciona un excelente ambiente para experimentar y probar nuevos modelos. Sin embargo, la simulación se basa en modelos aproximados del funcionamiento del sistema en ambientes reales. Para garantizar su funcionamiento en un ambiente real, es requerida la implementación experimental.

Realizar la implementación experimental del protocolo de ruteo AODV [2] requiere del conocimiento de los protocolos de red, del sistema operativo (OS) en el cual se hará la implementación, de las funciones de interconectividad entre procesos y también de la interface de red.
Algunas implementaciones realizadas anteriormente son la del *National Institute of Standards and Technology* (NIST) [3], la de *University of California, Santa Barbara* (UCSB) [4], la de *Uppsala University* en Suecia (UU) [5], la *University of Illinois at Urbana-Champaign* (UIUC) [6], el común denominador de estas implementaciones es que emplean el mismo OS (Linux). En contraste al trabajo de *University of Dublin* [7], en Irlanda, que utilizó Windows como sistema operativo.

El objetivo de este artículo es presentar la metodología que se empleó en la implementación experimental de AODV en una red Ad-Hoc inalámbrica 802.11x. Se implementó sobre una red de computadoras móviles en una ambiente Windows en la que al menos cada computadora mantenía la conexión con otra computadora. Se seleccionó una topología de comunicación de tal manera que la computadora fuente (1) no tenia conexión directa con la computadora destino (3), obligando la utilización de los nodos para mantenerse comunicadas. La figura 1 muestra la topología de red que se implementó en la cual se establece la comunicación de la computadora 1 a la computadora 3. Debido a la separación física no pueden comunicarse directamente y lo tienen que hacer a través de la computadora 2, se aseguró que no hubiera comunicación directa entre la computadora 1 y la computadora 3.

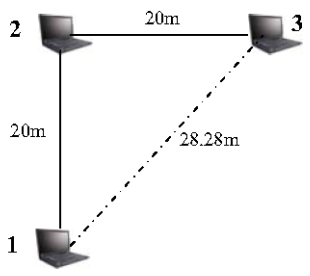


Figura 1. Topología de Red Ad-Hoc Inalámbrica

March 3rd- 5th 2008 International Association of Technology, Education and Development, Valencia, Spain.

"International Technology, Education and Development Conference INTED 2008"

A Survey on Routing Protocols For Manet

- *Trujillo Toledo Diego Armando*, Álvarez Hernández Guadalupe, Sánchez Adame Moisés, Álvarez Cabanillas Miguel A.
- ISBN 978-84-612-0190-7
- Página 412

A SURVEY ON ROUTING PROTOCOLS FOR MANET

D. Trujillo, G. Alvarez, M. Sanchez, M. Alvarez

CITEDI (MEXICO)

trujillo@citedi.mx, alvarez@citedi.mx, msanchez@citedi.mx, malvarez@citedi.mx

The mobile ad hoc network (MANETs) is a group of dynamic devices, supporting peer to peer communication that really doesn't have any pre-existing infrastructure. The nodes or devices can dynamically join or leave the network with the possibility of interrupting any communication among others nodes. The main goals of the routing protocols are the correct connection through the network and an efficient communication among nodes. This article presents a survey of the most important routing protocols in their classifications. The advantage and disadvantage of the proactive protocols, reactive and hybrid are referred. At the end of the study it is concluded that it's not efficient to use a pure proactive protocols or pure reactive protocols, however if we combine the best of both worlds we get the hybrid routing protocols.

Octubre 11-12 2007 Centro de Investigación y Desarrollo de Tecnología Digital, Tijuana, B.C, México.

III Encuentro Regional Académico ERA 2007

Estudio De Algoritmos De Ruteo Para Redes Móviles Ad-Hoc (Manet's)

- *Trujillo Toledo Diego Armando*, Álvarez Hernández Guadalupe, Sánchez Adame Moisés, Álvarez Cabanillas Miguel A.
- ISBN 978-970-36-0460-9
- Páginas 37-42

ESTUDIO DE ALGORITMOS DE RUTEO PARA REDES MOVILES AD-HOC (MANET's)

Trujillo Toledo Diego Armando, Álvarez Hernández Guadalupe, Sánchez Adame Moisés, Álvarez Cabanillas Miguel A.

Instituto Politécnico Nacional
Centro de Investigación y Desarrollo de Tecnología Digital
Departamento de Telecomunicaciones
Ave. Del Parque # 1310, Mesa de otay, Tijuana B.C 22510
Teléfono: (664) 623 – 13 – 44
Fax: (664) 623 – 13 – 88
{ trujillo, alvarez, msanchez, malvarez } @citedi.mx

RESUMEN

Las redes móviles ad hoc son un conjunto de dispositivos dinámicos, establecidos arbitrariamente capaces de tener conexión entre ellos. El principal objetivo de los algoritmos de ruteo es la correcta y eficiente conexión entre un par de nodos que pueden estar mandando un mensaje. Este artículo presenta el estudio de los algoritmos de ruteo más importantes dentro de sus divisiones. Se abordan las ventajas y desventajas para los protocolos proactivos, reactivos e híbridos. Al finalizar el estudio se encuentra que el uso de un protocolo puro, ya sea proactivo o reactivo no es muy eficiente, dando lugar a los protocolos híbridos, que aprovechan las ventajas de ambos.

1. INTRODUCCION

Las comunicaciones móviles e inalámbricas han tenido un gran auge en los últimos años, por un lado los grandes avances obtenidos en el área de la microelectrónica [1], también al conocimiento, utilización y aprovechamiento de los enlaces radio eléctricos, los cuales han permitido el desarrollo de dispositivos portátiles de tamaño reducido y gran potencia de procesamiento; y por supuesto al uso extenso por parte de usuarios que día a día requieren más capacidades y facilidades de comunicación y movimiento. El principal objetivo es el intercambio de información en cualquier lugar y en cualquier momento.

Hoy en día existen varios estándares para redes inalámbricas de área local (Wireless Local Area Network, WLAN) [2], como lo muestra la tabla I.

En una red inalámbrica se pueden distinguir dos tipos de configuraciones diferentes, las que requieren de un sistema central el cual está controlando el acceso a los nodos, y la otra la que no cuenta con este sistema centralizado que comúnmente se conocen como redes Ad-Hoc o redes sin Infraestructura [3,4,5,6]. En este documento se investigan las redes Ad-Hoc, ya que por su importancia ha sido de estudio en recientes años, por la topología que adquieren es un reto establecer comunicación entre los equipos.

TABLA I. Diferentes Estándares para WLAN.

NOMBRE	DESCRIPCION
WiFi	Es un estándar de la IEEE, conocido también como el estándar IEEE 802.11. Cuenta con varias modalidades a, b, g y actualmente n.
HiperLAN	Es un estándar del Instituto Europeo de Estándar de Telecomunicaciones (ETSI). Tiene dos modalidades HiperLAN/1 e HiperLAN/2, el primero opera en la banda de los 5GHz a una velocidad de 24Mbps y el segundo consigue hasta 54 Mbps en la misma banda.
HomeRF SWAP	Protocolo de Acceso Inalámbrico Compartido (SWAP) es un estándar para comunicaciones digitales entre PC y dispositivos electrónicos en entornos de hogares.
Bluetooth	Aunque Bluetooth se considera una red inalámbrica de área personal (WPAN), existen aplicaciones para redes inalámbricas en las que resulta ventajoso su empleo.

Este trabajo se encuentra distribuido de la siguiente manera: en la primera sección se aborda el tema de las redes y sus diferentes topologías, en la sección dos se trata del estudio de los algoritmos de ruteo en redes ad hoc. Posteriormente en la sección tres se habla de los protocolos proactivos y especificamos el protocolo WRP, en la sección cuatro se habla de los protocolos reactivos como el AODV y DSR. Los protocolos ZRP y TORA se mencionan en la sección cinco. Las conclusiones y trabajos a futuro los presentamos en la sección seis y por último las referencias en la sección siete.

B.2. PRODUCTOS ADICIONALES

Adicionalmente se realizaron 6 artículos diferentes al tema de investigación de esta tesis, el 50% se realizaron para congresos internacionales y el otro 50% para encuentros regionales.

Noviembre 17 y 18 2008 — Centro de Investigación y Desarrollo de Tecnología Digital, Tijuana, B.C, México.

IV Encuentro Regional Académico ERA 2008

Sensores de Imagen con Tecnología CMOS

- Sandoval Ibarra Yuma, *Trujillo Toledo Diego Armando*, Álvarez Cabanillas Miguel Agustín.
- ISBN (En trámite)
- Páginas (154-158)

Sensores de Imagen con Tecnología CMOS

Yuma Sandoval Ibarra, Diego Armando Trujillo Toledo, Miguel Agustín Álvarez Cabanillas.
Centro de Investigación y Desarrollo de Tecnología Digital (CITEDI) - IPN, Tijuana, B.C., México.
Teléfono (664) 623-1344 Fax (664) 623-1388 E-mail {sandoval, trujillo, malvarez}@citedi.mx

***Resumen*— Se muestra el funcionamiento de un arreglo de los sensores de imagen implementados con tecnología *Complementary Metal Oxide Semiconductor (CMOS)*. Se describe el funcionamiento de los pixeles tipo pasivo y tipo activo así como la electrónica involucrada en la multiplexión de las señales producidas por varios pixeles y la conversión analógica digital de un arreglo de pixeles.**

***Palabras Claves* — ADC, ASP, CCD, CMOS, PPS,**

I. INTRODUCCIÓN

ACTUALMENTE, los avances y las mejoras en las tecnologías continúan emergiendo en el creciente mundo de las imágenes digitales. Alguna de las aplicaciones las podemos encontrar en maquinas de fax, scanner, cámaras de seguridad, sensores biométricos y automóviles, en productos de consumo tales como cámaras fotográficas digitales, cámaras para computadoras personales, cámaras para teléfonos celulares, *Personal Digital Assistant* (PDAs) y cámaras de video.

Las dos principales tecnologías de sensores de imagen se basan en silicio las cuales son *Charge Cuopled Device (CCD) [1]* y *Complementary Metal Oxide Semiconductor (CMOS) [2]*. Hasta mediado de los años 90´s *[3]* la tecnología *CCD* había sido la tecnología dominante en el mundo de imágenes, mientras los circuitos integrados tradicionales eran fabricados con la tecnología de metal oxido (MOS). El primer sensor *CCD* fue reportado por los laboratorios Bell en 1970 este fue la base para otros sensores imagen en estado sólido [*3*], debido a su tamaño pequeño de integración y bajo nivel de ruido. Desde su creación los sensores de imagen *CCD* han requerido un gran campo de investigación y de desarrollo. Los resultados obtenidos de la investigación y desarrollo, se reflejan en un bajo ruido obtenido en la señal eléctrica de salida y un rango dinámico alto excelente para obtener una respuesta de salida equivalente a una señal de entrada, consiguiendo así un nivel alto de rendimiento [3].

En 1995, surgió un gran interés en el desarrollo de los sensores de imagen *CMOS [3]*, debido a su fácil integración con circuitos. El fotodiodo comúnmente se utiliza en los sensores de imagen *CMOS*, ya que es el dispositivo más simple de detección de luz y es integrado fácilmente. Sin embargo, los sensores de imagen basados en fotodiodos tienen baja respuesta a la luz [4].

Este trabajo cuenta con el apoyo del proyecto de investigación **SIP 20080845** que pertenece al **Instituto Tecnológico Nacional**.

La motivación del presente trabajo es la descripción del funcionamiento electrónico interno de un pixel *CMOS* con tecnología *Active Pixel Sensor (APS)* y también la de *Passive Pixel Sensor (PPS)*.

El artículo se encuentra dividido en las siguientes secciones: en la segunda sección se describen las características de los sensores de imagen CCD y CMOS. En la tercera sección se muestran los circuitos electrónicos de un pixel con tecnología CMOS de tipo Pasivo (PPS) y de tipo Activo (APS) donde se describe su funcionamiento. En la cuarta sección se describe el proceso de multiplexión en un arreglo de pixeles. La conversión de señal analógica a señal digital se muestra en la sección 5 y por último en la sexta sección se muestran las conclusiones obtenidas.

II. SENSORES DE IMAGEN

Un sensor de imagen es un dispositivo que convierte una imagen a una señal eléctrica [3].

Las dos tecnologías de sensores de imagen *(CCD* y *CMOS)* utilizan materiales semiconductores para su fabricación y están estructurados en forma matricial. Ambos sensores responden al acumular una carga eléctrica en cada celda de la matriz en proporción a la intensidad de la luz que incide sobre ella. A cada componente de la matriz se le conoce como pixel.

En un CCD la conversión de luz a una señal eléctrica se realiza cuando la incidencia de fotones llegan al semiconductor y transfieren la carga concentrada en cada pixel en señales discretas proporcionales a la intensidad de fotones que llegan, estas señales salen del pixel en forma secuencial por una salida común. En un CMOS la conversión carga-voltaje se lleva a cabo en cada pixel.

Los factores que caracterizan el funcionamiento de los sensores de imagen son responsividad, rango dinámico, respuesta uniforme, velocidad y saturación.

La responsividad, se define como el nivel de señal que es capaz de ofrecer el sensor por cada unidad de energía óptica incidente [5].

Otros de los factores que caracterizan el funcionamiento es el rango dinámico (RD), el cual está definido como la razón entre el nivel de saturación de los píxeles y el umbral por debajo del cual no captan la máxima cantidad de señal a la

March 3rd- 5th 2008 International Association of Technology, Education and Development, Valencia, Spain.

"International Technology, Education and Development Conference INTED 2008"

An Ontology Application For Veterinary Services

- *Trujillo Toledo Diego Armando*, Sánchez Adame Moisés, Ángeles Valencia Alfonso.
- ISBN 978-84-612-0190-7
- Página 129

AN ONTOLOGY APPLICATION FOR VETERINARY SERVICES

D. Trujillo, A. Angeles, M. Sanchez

CITEDI (MEXICO)

trujillo@citedi.mx, alfang@ieee.org, msanchez@citedi.mx

In this article, we presents the state of the art of ontologies, to the same way an application of veterinary services. The applications consist primarily to built an ontology which contains information about pets, Canines and Felines in this case. Here, we present two types to built the ontology using Protégé. This application is novel in the sense that many differents veterinarians will shared their information, in the sense that one pet could be taken to one veterinarian first and to another one later. This is possible thanks to the proposed RAU (Unique Animal Register). RAU, Age, Sex, Breed, Name (pet), Owner, Vaccination-Date are information contained in the ontology. The results successfully shows that the utilization of the ontologies is of very practical benefits.

Octubre 17-19 2007 Instituto Tecnológico de Chihuahua, Chihuahua, México.

"XXIX Congreso Internacional de Ingeniería en Electrónica ELECTRO 2007"

Aplicación de Ontologías en Servicios Hospitalarios

- *Trujillo Toledo Diego Armando*, Arenas Campis Christian Alonso, Ángeles Valencia Alfonso, Quiroz Morones Ernesto, Sánchez Adame Moisés.
- ISSN 1405-2172 Volumen XXIX
- Páginas 453-458

APLICACIÓN DE ONTOLOGÍAS EN SERVICIOS HOSPITALARIOS

Trujillo Toledo Diego Armando, Arenas Campis Christian Alonso, Ángeles Valencia Alfonso, Quiroz Morones Ernesto, Sánchez Adame Moisés.

Instituto Politécnico Nacional
Centro de Investigación y Desarrollo de Tecnología Digital
Departamento de Telecomunicaciones
Ave. Del Parque # 1310, Mesa de otay, Tijuana B.C 22510
Teléfono: (664) 623 – 13 – 44
Fax: (664) 623 – 13 – 88
{ trujillo, arenas, eequiroz, msanchez } @citedi.mx
alfang@ieee.org

RESUMEN

En este trabajo se presenta el planteamiento y avance de una ontología para servicios hospitalarios. El desarrollo de la ontología se llevó acabo en la plataforma de código libre Protégé 3.2.1 [1]. La información que puede ser consultada en la ontología se relacionada con la situación del paciente, incluyendo datos como Diagnostico, Tratamiento, Edad, Sexo, Peso, Estatura. También se puede buscar por enfermedades. Dando como resultado una recolección y búsqueda de información mas efectiva. La información consultada por el personal medico, será una referencia rápida para diagnosticar al paciente.

1. INTRODUCCION

De acuerdo a la información recolectada, en nuestro país no existen aplicaciones basadas en ontologías. Como lo están haciendo países Europeos y Asiáticos que están trabajando desde un par de años atrás.

En el campo de las aplicaciones actuales, las ontologías capturan conocimiento de modo genérico y formal de tal manera que pueda ser compartido y reutilizado por distintos grupos de personas y/o aplicaciones de software [2].

Algunas aplicaciones de las Ontologías son:

1. Indexación, recuperación y divulgación de la información Web
2. Agentes Inteligentes para encontrar páginas especializadas Web.
3. Herramientas para mejorar la eficiencia de búsquedas en la Web
4. Agentes Inteligentes Notificadores [3].

2. ONTOLOGIAS

2.1. Definición

Semánticamente ontología proviene del griego ontos que significa “el ser” y de logos que significa “estudio de” y si juntamos los significados tenemos “El estudio del Ser” [4].

La ontología trata de describir o proponer las categorías y relaciones básicas del ser o la existencia para definir las entidades y de qué tipo son [5].

En términos computacionales una ontología es una descripción explícita formal de conceptos en un dominio de discusión (clases), las propiedades de cada concepto que describe varias características y cualidades del concepto (propiedades), y restricciones en las propiedades (facetas).

Un ejemplo lo podemos observar en la figura 1, que muestra una ontología de la superclase “OBJETO” y de la clase Vehiculo y así sucesivamente las clases y sus conjuntos de las clases con sus propiedades.

Octubre 17-19 2007

Instituto Tecnológico de Chihuahua,
Chihuahua, México.

"XXIX Congreso Internacional de Ingeniería en Electrónica ELECTRO 2007"

Herramienta Didáctica para Tratamiento de Señales

- *Diego Armando Trujillo Toledo*, Juan Miguel Colores Vargas, Gabriel de Jesús Lizárraga Velarde, Moisés Sánchez Adame, Roberto Herrera Charles.
- ISSN 1405-2172 Volumen XXIX
- Páginas 501-502

HERRAMIENTA DIDÁCTICA PARA TRATAMIENTO DE SEÑALES

Diego Armando Trujillo Toledo, Juan Miguel Colores Vargas, Gabriel de Jesús Lizárraga Velarde, Moisés Sánchez Adame, Roberto Herrera Charles.

Instituto Politécnico Nacional
Centro de Investigación y Desarrollo de Tecnología Digital
Ave. Del Parque # 1310, Mesa de otay, Tijuana B.C 22510

Teléfono: (664) 623 – 13 – 44

Fax: (664) 623 – 13 – 88

{trujillo, colores, lizárraga, msanchez, charles}@citedi.mx

RESUMEN

En este artículo se presenta la propuesta de un software interactivo para el uso de estudiantes de nivel Ingeniería y/o Pos-grado en el área de Electrónica o afines. Con el motivo de apoyar al docente en la impartición de clases, para un fácil entendimiento de la teoría.

La interfaz grafica es un recurso didáctico, que contará con 4 funciones principales, la utilización de Filtros, la Modulación, Mezcla de Audio y la Demodulación.

En toda realización de sistemas de Procesamiento Digital de Señales y de Comunicaciones se debe contemplar tanto el hardware como el software. Aún cuando se pueden realizar en computadores de propósito general, la realización de sistemas de gran velocidad y eficiencia requieren el empleo de circuitería de muy alta escala de integración y de propósito especial. Este campo tecnológico está experimentando un gran crecimiento gracias al desarrollo de la computación y de la microelectrónica al desarrollar circuitos que pueden manejar eficientemente grandes cantidades de información [1].

Es por ello que nuestra herramienta se vuelve interesante, al querer evitar muchas veces por lo complejo o tedioso que resulta trabajar con un manual ya sea en la programación o diseño, los cuales casi siempre están dirigidos a personas más experimentadas, resultando muy frustrante en muchos casos a los estudiantes.
Por esta razón, resulta interesante el desarrollo de utilidades de índole puramente didácticas que faciliten el manejo y la asimilación de los conceptos fundamentales de estas materias y a su vez puedan implementarse sin dificultad las practicas propuestas.

Por otra parte MATLAB, es una plataforma computacional de amplia cobertura, en la que se puede analizar y manipular señales digitales, filtros y espectros, teniendo cierta experiencia en programación [2].

El desarrollo de este trabajo consiste en utilizar el ambiente de desarrollo de Interfaz de Usuario (GUIDE) [2], para así contar con una interacción mas amable y agradable para el estudiante.

Los puntos importantes que se utilizan para el desarrollo son: la creación de ventanas, menús, botones, imágenes, entre otras. Lo cual se realizan programándolas en matlab, generando un archivo .M donde serán editadas las instrucciones para lograr así en conjunto un funcionamiento de nuestra interfaz final.

Nuestra interfaz es un archivo ejecutable que puede ser ejecutada en cualquier computadora, aun y cuando no cuente con Matlab instalado, gracias al desarrollo en GUI que podemos convertir estos programas en archivos ejecutables [3], a demás cuenta con una Función "Filtros" la cual se utiliza para visualizar la utilización de los filtros en una señal de audio, donde nos podemos dar cuenta como se muestra en el

Octubre 11-12 2007 Centro de Investigación y Desarrollo de Tecnología Digital, Tijuana, B.C, México.

III Encuentro Regional Académico ERA 2007

Ontologías: estado del arte y aplicación en servicios veterinarios

- *Trujillo Toledo Diego Armando*, Ángeles Valencia Alfonso, Sánchez Adame Moisés.
- ISBN 978-970-36-0460-9
- Páginas 87-92

ONTOLOGÍAS: ESTADO DEL ARTE Y APLICACIÓN EN SERVICIOS VETERINARIOS

Trujillo Toledo Diego Armando, Ángeles Valencia Alfonso, Sánchez Adame Moisés.

Instituto Politécnico Nacional
Centro de Investigación y Desarrollo de Tecnología Digital
Departamento de Telecomunicaciones
Ave. Del Parque # 1310, Mesa de otay, Tijuana B.C 22510
Teléfono: (664) 623 – 13 – 44
Fax: (664) 623 – 13 – 88
{ trujillo, msanchez } @citedi.mx
alfang@ieee.org

RESUMEN

En este trabajo, se presenta el estado del arte de [1]las ontologías, así mismo una aplicación para servicios de veterinarias. Principalmente la aplicación consiste en realizar una ontología donde se tenga información de mascotas, en este caso, Caninos y Felinos. Esta aplicación es novedosa en el sentido que diferentes veterinarias podrán compartir su información, en el caso que una mascota sea llevada a diferentes veterinarias. Esto es posible gracias a la propuesta del *RAU* (Registro Animal Único). La información contenida en la ontología es, *RAU*, Edad, Sexo, Raza, Nombre (de mascota), Dueño, Vacunas/Fecha y el Nombre de la Veterinaria que fue atendida la mascota.

Satisfactoriamente se realizaron pruebas, y se demuestra que la utilización de ontologías es muy importante. Se verifica que además del RAU, se pueden hacer búsquedas con diferentes parámetros, para tener un resultado especifico.

1. INTRODUCCION

Hoy en día la gente ha tomado conciencia de la responsabilidad que implica tener una mascota y los cuidados que requiere.

Los perros y gatos para muchas personas son como un miembro más en la familia, por lo que esperan para ellos un servicio médico profesional.

La elección del veterinario que atenderá a mascotas, es tan importante como la elección de un médico pediatra. Este debe de proporcionar respuestas a cualquier duda. El cuidado veterinario debe iniciarse desde los primero días de nacido o desde el momento que se adquiere la mascota [1].

Es por ello, que los dueños deberán tener registradas toda la información clínica de la mascota. Dicha información es muy fácil de perder si es impresa, ya que los chequeos de la mascota se recomiendan cada seis meses, los papeles se pueden perder en cualquier momento.

Debido a esta necesidad, se propone la aplicación de ontologías para organizar esta información y tenerla a la mano cuando sea necesario. Esta ontología será muy utilizada en clínicas veterinarias.

De acuerdo a la información recolectada, en nuestro país no existen aplicaciones basadas en ontologías.

En el campo de las aplicaciones actuales, las ontologías capturan conocimiento de modo genérico y formal de tal manera que pueda ser compartido y reutilizado por distintos grupos de personas y/o aplicaciones de software [2].

Algunas aplicaciones de las Ontologías son:

1. Indexación, recuperación y divulgación de la información Web
2. Agentes Inteligentes para encontrar páginas especializadas Web.
3. Herramientas para mejorar la eficiencia de búsquedas en la Web
4. Agentes Inteligentes Notificadores [3].

Este trabajo está distribuido de la siguiente manera: Sección uno se aborda la introducción y motivación de la investigación, sección dos nos muestra el estado del arte de las ontologías, en la sección tres se habla de la aplicación, el desarrollo lo encontramos en la sección cuatro, algunos

[1] Este trabajo está coordinado por el proyecto de investigación: *Mecanismos de Gestión de Servicios Ubicuos: Gestión Autónoma* con registro del IPN **SIP 20070193** dentro del Programa de Comunicaciones Inalámbricas (**SIP 555**)

Octubre 11-12 2007 Centro de Investigación y Desarrollo de Tecnología Digital, Tijuana, B.C, México.

III Encuentro Regional Académico ERA 2007

Sistema Experimental de Voz sobre IP en Servidor TrixBox de Linux

- Álvarez Hernández Guadalupe, *Trujillo Toledo Diego Armando*, Sánchez Adame Moisés, Álvarez Cabanillas Miguel A.
- ISBN 978-970-36-0460-9
- Páginas 49-53

Sistema Experimental de Voz sobre IP en Servidor Trixbox de Linux

Guadalupe Alvarez H., Diego Trujillo T., Moisés Sanches A., Miguel Alvarez C.
alvarez@citedi.mx, trujillo@citedi.mx, msanchez@citedi.mx, malvarez@citedi.mx
Centro de Investigación y Desarrollo de Tecnología Digital (CITEDI-IPN)
Avenida del Parque 1310, Otay, Tijuana, B. C., 22510

***Resumen*—Las tecnología de Voz sobre el Protocolo de Internet (IP: Internet Protocol) hoy en día tiene grandes ventajas frente a la telefonía tradicional. Y es que los costos mínimos que representa en las grandes empresas opacan a la telefonía de conmutación de circuitos. Además, el equipo que se ocupa es robusto y muy caro en comparación con una maquina, dispositivos y software que se utiliza en la tecnología VoIP.**

En este artículo se presenta el desarrollo de una red local de Voz sobre IP bajo la plataforma de Linux en su versión Trixbox como central telefónica, con dos teléfonos implementados por software que utilizan el Protocolo de Inicio de Sesión (SIP: Session Initiation Protocol) para su comunicación, instalados en una plataforma de Windows. Los resultados de los experimentos muestran que fue posible realizar llamadas en tiempo real de un usuario a otro, y se observaron los detalles de dicha llamada en el interfaz de Trixbox. Esta interfaz muestra todos los registros y configuraciones hechas en el servidor y éste a su vez muestra resultados en forma de código en la pantalla.

***Índice de términos*—Asterisk, VoIP y SIP.**

I. Introduccion

La telefonía digital de VoIP (Voice over Internet Protocol) es una tecnología actual que permite el enrutamiento de conversaciones de voz sobre Internet o una red de ordenadores. Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla en forma de circuitos como una compañía telefónica convencional o Red Telefónica Publica Conmutada (PSTN: Public Switched Telephone Network) optimizada para comunicaciones de voz en tiempo real. Para realizar llamadas a través de VoIP, el usuario necesitará de algún dispositivo que funciones con esta tecnología.

En la figura 1 se puede apreciar la arquitectura VoIP que marca tres elementos principales: terminales, gatekeepers y gateway. Las terminales, definidas como los sustitutos de les teléfonos tradicionales los podemos clasificar en tres dispositivos necesarios, teléfono basado en software, teléfono basado en hardware y teléfono VoIP con USB, también podemos utilizar un teléfono analógico mediante un adaptador. En este trabajo se empleó el teléfono basado en software conocido como softphone. El segundo elemento, gatekeepers son el centro de toda la organización VoIP, y serían el sustituto para las actuales centrales. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.

Y por ultimo el gateway, su función es enlazar con la red telefónica tradicional, actuando de forma transparente para el usuario. Es preciso destacar el uso de protocolos en estas aplicaciones, que son un conjunto de reglas que controlan la continuidad de mensajes que suceden durante una comunicación entre entidades que forman una red. VoIP trabaja con varios protocolos por ejemplo el Protocolo de Inicio de Sesión, H.323, IAX (Inter Asterisk Exchange), Protocolo de Control de Entrada de los Medios (MGCP; del ingles Media Gateway Control Protocol), SCCP (Skinny Client Control Protocol). En la tercera sección abordaremos el protocolo SIP que es el que se utiliza en el presente trabajo.

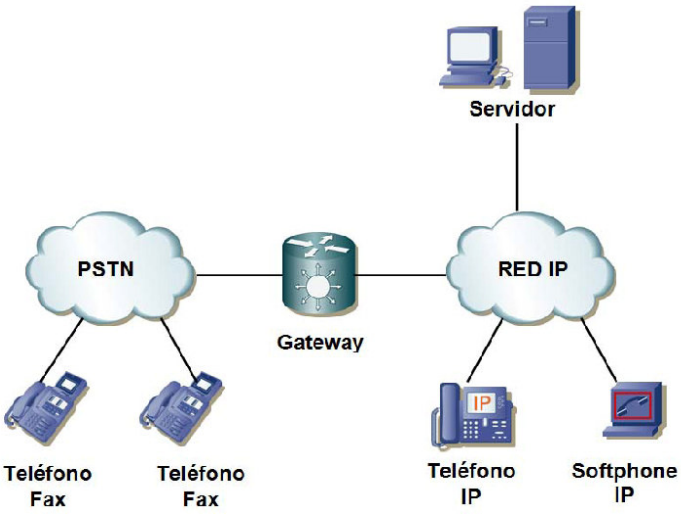


Figura 1 Red VoIP en conexión con una red tradicional.

II. Central Telefónica

Una PBX (Private Branch Exchange) [1] tiene como función compartir de una a varias líneas telefónicas y dar servicio de redirigir llamadas y permitir a un usuario tener acceso a una línea dedicada. La palabra *"private"* da por entendido que es un servicio de un proveedor que es dueño total del sistema y que tiene la opción de brindar el servicio a quien lo desee. Provee varios servicios de valor agregado como transferencia de llamada, conferencia tripartita y buzón.

Este tipo de servicios controlados por una sola compañía benefician a pocos. Actualmente hay muchos proveedores de