ESCUELA SUPERIOR POLITÉCNICA DEL CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

TESIS DE GRADO

Previa la obtención del Título de:

INGENIERO ELECTRÓNICO EN TELECOMUNICACIONES Y REDES

Presentado por:

CARINA VALERIA ESCOBAR VALLEJO

Riobamba – Ecuador

2012

Agradezco a la Escuela de Ingeniería Electrónica por todo el conocimiento adquirido durante la carrera, al Ing. Daniel Haro por la ayuda brindada para realizar este trabajo de investigación.

A todos mis seres queridos entre ellos familiares y amigos por haber caminado junto a mí estos años de estudio y por estar presentes en mi corazón todos los días siendo una razón más para salir adelante.

Y a mi sol personal por aguantar mis días malos mientras las cosas no salían como pensaba, por su constante apoyo y por demostrarme que las cosas mejoran con el tiempo.

A Dios por brindarme la oportunidad y la dicha de la vida, por acompañarme en cada paso que he dado sin dejarme perder la esperanza, y a mi Virgen Auxiliadora que ha sido mi apoyo incondicional, mi pared en los momentos difíciles, la que ha colocado amor, amistad, ánimo y compañía en mi vida y me ha ayudado a cumplir cada sueño.

NOMBRE	**FIRMA**	**FECHA**
Ing. Iván Menes **DECANO FACULTAD INFORMÁTICA** **Y ELECTRÓNICA**	……	…….....
Ing. Pedro Infante **DIR. ESC.** **ING. ELECTRÓNICA** **TELECOMUNICACIONES Y REDES**	…….	…….....
Ing. Daniel Haro **DIRECTOR DE TESIS**	…….	…….....
Ing. Irene Tustón **MIEMBRO DE TESIS**	…….	…….....
Lcdo. Carlos Rodríguez **DIRECTOR CENTRO DOCUMENTACIÓN**	……	…….....

NOTA DE LA TESIS ESCRITA: …….

Yo, CARINA VALERIA ESCOBAR VALLEJO, soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis, y el patrimonio intelectual de la Tesis de Grado pertenece a la Escuela Superior Politécnica del Chimborazo.

_____

Carina Escobar Vallejo

ÍNDICE DE ABREVIATURAS

AES	Advanced Encryption Standard (Estándar de enciptación avanzada)
AODV	Ad hoc On-Demand Distance Vector
AOMDV	Ad hoc on-demand multipath distance vector routing
ARP	Address Resolution Protocol (Protocolo de resolución de direcciones)
CBR	Constant Bit Rate (Taza constante de bits)
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance (acceso múltiple por detección de portadora con evasión de colisiones)
DARPA	Defense Advanced Research Projects Agency (Agencia de Investigación de Proyectos Avanzados de Defensa)
DCF	Hybrid Coordination Function
DFS	Dynamic Frequency Selection (Selección de Frecuencia Dinámica)
DSDV	Destination-Sequenced Distance-Vector
DSE	Dependent Station Enablement (Activacion de estación dependiente)
DSR	Dynamic Source Routing
DSSS	direct sequence spread spectrum (Espectro Ensanchado por Secuencia Directa)
FTP	File Transfer Protocol (Protoclo de transferencia de archivos)
GNU	GNU is Not Unix (GNU No es Unix)
GUI	graphical user interface (interfaz gráfica de usuario)
HCCA	Enhanced Distributed Channel Access
HCF	Hybrid Coordination Function (Función de coordinación híbrida)
ICANN	Corporación de Internet para la Asignación de Nombres y Números

IEEE	Institute of Electrical and Electronics Engineers (Instituto de ingenieros eléctricos y electrónicos)
IETF	Internet Engineering Task Force (Grupo de Trabajo en Ingeniería de Internet)
IP	Internet Protocol (Protocolo de Internet)
ISM	Industrial, Scientific and Medical (Industrial, Científico y Médico)
ITU	Unión Internacional de Telecomunicaciones
LAN	Local Area Network (Red de Área Local)
LL	Link Layer (nivel de enlace)
MAC	Media Access Control (Control de Acceso al Medio)
MAN	Metropolitan Area Network (Red de Área Metropolitana)
MANET	Mobile AdHoc Network (Red AdHoc móvil)
MIMO	Multiple Input – Multiple Output (Múltiple Entrada - Múltiple salida)
NAM	Network animator
NS	Network Simulator
NS2	Network Simulator 2
OLSR	Optimized Link State Routing
OSI	Open System Interconnection (modelo de referencia de Interconexión de Sistemas Abiertos)
OSPF	Open Shortest Path First (Primero el camino abierto mas corto)
PCF	Point Coordinated Function (Función de Punto Coordinado)
PIC	Peripheral Interface Controller (controlador de interfaz periférico)
QoS	Quality of Service (Calidad de Servicio)
RED	Random Early Detection (Detección Randómica temprana)

RERR	Route Errors
RFC	Request For Comments
RIP	Routing Information Protocol (Protocolo de información de ruteo)
TC	Topology Control (Control de Topología)
Tcl	Tool Command Language (Lenguaje de herramientas de comando)
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión)
TPC	Transmitter Power Control (Control de Potencia de Transmición)
UCB	Unit Control Block (Bloque de control de unidad)
UDP	User Datagram Protocol (Protocolo de Datagramas del Usuario)
VANET	Vehicular Ad-Hoc Network (Red Ad-Hoc vehicular)
VoIP	Voz sobre Protocolo de Internet
WIFI	Wireless Fidelity (Fidelidad inalámbrica)
WIMAX	Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas)
WLAN	Wireless Local Area Network (Red de Área local inalámbrica)
WPA	Wi-Fi Protected Access (Acceso protegido de Wi-Fi)

ÍNDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCION

Las redes móviles ad-hoc (*mobile ad-hoc networks*, MANETs), son conjuntos de nodos móviles interconectados de manera inalámbrica. La característica fundamental que tienen es que son multi-salto, de forma que los nodos de la red enrutan el tráfico, haciendo de nodos intermediarios. Son redes de naturaleza muy dinámica, pensadas para establecerse rápidamente, donde los nodos pueden entrar, salir, o cambiar de posición en la red.

La comunicación inalámbrica con su gran desempeño y penetración en las redes de comunicaciones ha creado diferentes desafíos en cuanto a sus implementaciones y aplicaciones en múltiples ambientes. El concepto de movilidad para una red obliga a encontrar nuevas soluciones para las tareas principales de esta.

El presente trabajo revisa primero las características de gestión en las redes Ad-Hoc, el estudio se ejecutó mediante un cluster con varios equipos que trabajaban en modo Ad-Hoc haciendo que nuestra red funcione de esta manera, también la investigación esta apoyada en una programación de simulaciones en MobieEmu sobre Linux Ubuntu, creando escenarios los cuales fueron sometidos a distintas pruebas,

Uno de los puntos más estudiado son los protocolos de encaminamiento, ya que no todos nos ofrecen las mejores condicion. De los dos grandes grupos de protocolos reactivos y proactivos, se ha estudiado en este proyecto el más representativo de cada grupo. AODV (Ad-Hoc On-Demand Distance Vector) como representante de los protocolos reactivos y OLSR (Optimized Link State Routing) como representante de los proactivos.

Cada escenario estudiado representaba un estudio comparativo entre protocolos de enrutamiento en redes móviles AdHoc para mejorar el funcionamiento de las mismas.

El documento se compone de 5 capítulos. El primero de ellos consiste en el marco referencial el cual explica un poco los antecedentes del trabajo asi como también los objetivos del mismo. El capitulo 2 es una introducción a las redes Ad-Hoc en donde veremos las características y aplicaciones de las redes de este tipo. En el capítulo 3 se explica la metodología que será usada a lo largo del trabajo. El capítulo 4 muestran los resultados obtenidos en las pruebas realizadas. Y en el capítulo 5 encontramos las primeras pruebas realizadas con escenarios estáticos y posteriormente con el emulador de redes MobiEmu.

Como resultado se obtiene datos respecto a los paquetes recibidos, perdidos, reenviados que varían de acuerdo al escenario y a los principios básicos de cada protocolo, proporcionando de esta manera información sobre los puntos fuertes y debilidades de cada uno. Estas redes tienen características especiales, que hacen aparecer nuevos retos a la gestión de las mismas, los cuales son puertas a líneas de investigación.

CAPÍTULO I

MARCO REFERENCIAL

FORMULACION GENERAL DEL PROYECTO DE TESIS

1.1. ANTECEDENTES

IEEE 802.11s es un bosquejo de la enmienda IEEE 802.11 para establecimiento de una red del acoplamiento, la cual define cómo los dispositivos inalámbricos pueden interconectarse para crear redes ad hoc.

El estándar 802.11 es un sistema de IEEE que gobierna métodos inalámbricos de transmisión en una red. Son hoy de uso general en sus versiones 802.11a, 802.11b, y 802.11g que proporcionan conectividad inalámbrica en el hogar, la oficina y algunos establecimientos

comerciales. La utilización de una red inalámbrica provee movilidad y cobertura en acceso a la red, estas redes han tenido una amplia implementación dentro de las ciudades con diferentes tecnologías como wifi que es una solución trabajando con IP para dar una solución a las redes inalámbricas que utiliza ondas de radio en lugar de cables.

Las redes Ad Hoc tienen su inicio en los años 70, inicialmente desarrolladas por la agencia DARPA del departamento de defensa de los Estados Unidos. Una red Ad Hoc es una red inalámbrica descentralizada para casos en los que la red se sujeta en un escenario en el que los usuarios no pueden referirse a un punto central para acceder a la red, esto puede ser por factores geográficos o por la naturaleza misma de la red, en este tipo de red los puntos tienen la capacidad de enviar sus datos de forma dinámica en función de la conectividad de la red por ello no requiere de un punto central que gestione la conexión. El hecho de que este tipo de red sea descentraliza le provee ciertas características y aplicaciones en situaciones en las que no se puede confiar en un nodo central y se necesita una gran escalabilidad, así también son muy útiles en situaciones de emergencia en los que se requiere un rápido despliegue del sistema de comunicación. La movilidad dentro de una red inalámbrica es fundamental, pero en el caso de una red Ad Hoc, al hablar de movilidad, podemos hablar de a mayor escala manteniendo la comunicación entre los distintos puntos, así viene al caso el término MANET's, es decir, una red móvil Ad Hoc, ideada para que cada punto tenga movilidad en cualquier dirección de manera independiente, cambiando sus enlaces para adaptarse a la red de manera frecuente, de esta manera el enrutamiento para mantener los enlaces es fundamental.

Los beneficios que las redes Ad Hoc nos presentan, también vienen acompañados de problemas de gestión dentro de la red, los mismos que pueden ser solucionados en un tiempo relativamente corto una vez que se descubre la falla del sistema.

Es aquí donde radica la importancia de la Gestión de Redes la cual permite que partes diversas con propósitos comunes trabajen de manera articulada, evitando la duplicidad de acción, facilitando una mejor utilización de los recursos tanto técnicos como financieros

Además de estimular la complementariedad en función del propósito común, permitiendo que las fortalezas de cada parte se ponga a disposición del objetivo que se busca.

1.2. JUSTIFICACIÓN DEL PROYECTO DE TESIS

La necesidad de conocer la estructura de una red ad hoc móvil junto con las herramientas que permiten su funcionamiento nos lleva a analizar los diferentes problemas de gestión de red que se presentan en el uso constante de los mismos, así como también soluciones existentes para cada uno de estos casos, esto podremos lograr estudiando su comportamiento en un entorno estable para de esta manera poder establecer los parámetros que se deben considerar al momento de trabajar con una red de características únicas expuesta a múltiples conexiones variables y el constantes movimiento de los clientes de la red.

Las redes Ad Hoc móviles se han convertido en un tema muy popular para la investigación debido a su relación con la tecnología del momento como computadoras portátiles y el estándar 802.11/Wi-Fi, el establecimiento de una red inalámbrica llegó a su apogeo a mediados de los años 90. Muchos de los documentos científicos evalúan los protocolos y las capacidades que nos presentan estas redes para comprobar los grados de eficiencia que podemos encontrar al utilizarlas, estos varían de acuerdo a la movilidad dentro de un espacio limitado, todos estos factores son los que nos llevan a descubrir los principales problemas que experimentan este tipo de redes.

El presente proyecto de tesis busca hallar los principales problemas de gestión de red como el correcto funcionamiento día a día de las mismas y la planificación estratégica de su crecimiento entre otros muchos que experimentan las redes ad hoc móviles creando un escenario real y sometiendo la red creada a diferentes técnicas en diferentes escenarios posibles en los que una red de este tipo podría encontrarse, de esta manera lo que se busca es evaluar las distintas capacidades que posee y cómo funciona bajo distintas condiciones tratando de encontrar de esta manera su potencial y capacidades junto con sus falencias. Esto nos permitirá discernir y escoger la solución más optima como por ejemplo sistemas centralizados, gestión de inventario de hardware y software, monitorización entre muchas otras que nos ofrece la Gestión de Red para aplicarlos de la mejor manera y así poder trabajar en el entorno deseado.

De esta manera el estudio servirá a los estudiantes de la carrera de ingeniería en electrónica como un material de apoyo y complemento para asignaturas como redes inalámbricas aplicado en ambientes móviles con el fin de tener un conocimiento avanzado en este ámbito, ya que será un completo análisis de funcionamiento y aplicaciones dentro de este campo poco explotado en el país como lo son las redes inalámbricas ad hoc.

1.3. OBJETIVOS

1.3.1. OBJETIVOS GENERALES:

Evaluar los problemas de gestión de redes 802.11 s (Redes Manet/Mesh) y plantear diferentes soluciones para ellos.

1.3.2. OBJETIVOS ESPECÍFICOS:

- Implementar una red Manet/Mesh 802.11s y de esta manera conocer más sobre el funcionamiento y estructura de las mismas.
- Descubrir y evaluar los problemas que se encuentran con más frecuencia en las redes móviles, y aquellos que causen más daño en la estructura.
- Analizar las posibles soluciones que se pueden aplicar en los diferentes casos.
- Definir una política de Administración de Redes Manet/Mesh.

1.4. HIPÓTESIS

Con el estudio de los problemas de gestión de redes 802.11 s (redes Manet/mesh) se podrá plantear soluciones para encontrar las que mejor se adapten al ambiente propuesto.

1.5. RECURSOS NECESARIOS

1.5.1. EQUIPOS A UTILIZAR

CANTIDAD	NOMBRE
1	Impresora.
1	Clúster
1	Portátil

1.5.2. OTROS

CANTIDAD	NOMBRE
	Internet Libros

1.6. MÉTODOS Y TÉCNICAS

1.6.1. MÉTODO CIENTÍFICO-DEDUCTIVO

Para poder tener un conocimiento correcto de la lógica utilizada debemos tener una descripción de lo que ocurre como su correspondiente explicación del porqué ocurre. Las explicaciones del

porqué ocurre son importantes porque nos permiten hacer predicciones, que son un elemento crucial en nuestro proyecto.

Ya que el método científico implica una combinación de inducción y deducción que se retroalimentan es necesaria una fiabilidad de este conocimiento científico, y lo logramos sometiendo a pruebas una y otra vez las predicciones, que a su vez son interdependientes de predicciones de teorías en otras áreas y que también se ponen a prueba.

Todo será tratado como una función racional porque presupone ya una elaboración, un trabajo activo frente a la información recibida. De los datos recibidos vamos deduciendo otros y así, paso a paso, llegamos a la conclusión o al dato deseado

1.6.2. TÉCNICA DE LA OBSERVACIÓN

La técnica de observación es un procedimiento que dirige la atención hacia un hecho de la realidad, encontrando el sentido de lo observado realizando enlaces funcionales entre situaciones y acciones.

Además información escrita como:

- Textos
- Documentos
- Estándares
- Catálogos de Equipos de Medición
- Otros

CAPÍTULO II

MARCO TEÒRICO

2.1. INTRODUCCION A LAS REDES AD-HOC

2.1.1. TECNOLOGIAS INALAMBRICAS

Las tecnologías inalámbricas en los últimos años han tenido un desarrollo considerable debido a su concepto de movilidad en todos los campos, por ello su utilización en la vida cotidiana se ha visto incrementada gracias a la utilización de dispositivos móviles que explotan están tecnologías y para ello se han implementado estructuras de comunicación principalmente centralizadas para proveer un sistema de comunicación. En su gran mayoría las estructura centralizadas con tecnologías como Wi-Fi o Wi-Max brindan una solución al usuario al momento de proveer acceso

a la red, pero en el caso en el que no se pueda depender de una red centralizada sea por un problema geográfico en el que los nodos no puedan hacer referencia a un punto central o por necesidad de flexibilidad en los enlaces se recurre a una estructura descentralizada en la que la capacidad de comunicación no recaiga sobre un punto central.

Para proveer una comunicación descentralizada contamos con enlaces inalámbricos de igual a igual conocidos como “ad-hoc” en los cuales los nodos que desean comunicarse se enlazan entre sí, creando múltiples enlaces para alcanzar otros nodos, de esta manera, al no tener un punto central de referencia, la comunicación puede continuar entre los nodos que tengan la capacidad de comunicarse entre sí.

La naturaleza descentralizada de las redes ad hoc, hace de ellas las más adecuadas en aquellas situaciones en las que no puede confiarse en un nodo central y mejora su escalabilidad comparada con las redes inalámbricas tradicionales, desde el punto de vista teórico y práctico.

Por su aplicación pueden clasificarse como:

- Redes móviles ad hoc (MANETs)
- Redes inalámbricas mesh

Las redes ad hoc son también útiles en situaciones de emergencia, como desastres naturales o conflictos bélicos, al requerir muy poca configuración y permitir un despliegue rápido. El protocolo de encaminamiento dinámico permite que entren en funcionamiento en un tiempo muy reducido.

Al tener la capacidad de movilidad en una red inalámbrica contando con un estructura descentralizada ad-hoc hablamos de una “red móvil ad hoc” a sus siglas en inglés “MANET” que propone una solución al problema de dependencia de una red centralizada común, por lo tanto

una MANET es una red autónoma en la que los puntos se logran comunicar a través de múltiples saltos entre sí para alcanzar el punto deseado, permitiendo de esta manera una comunicación que no recae sobre un punto central, sino, a través de los mismos miembros de la red.

Este sistema nos presenta un concepto de adaptación de la red en un ambiente de movilidad constantemente variable, buscando una organización automática que responda a cambios en la infraestructura y esquema de la red ya que los puntos de este sistema nos son controlados por un ente externo, por ello, los nodos para converger en la red deben interactuar entre sí, de esta manera no es un solo punto el responsable de la comunicación sino que cada punto contribuirá a la conectividad de la red.

Al ser los nodos libres en la red se organizan entre ellos mismos, por ello son aptos para responder una manera rápida, espontánea y adaptable a los cambios continuos como en aplicaciones militares, operaciones de emergencia, dispositivos de red electrónicos personales, o sistemas de comunicación de alta movilidad como comunicaciones entre vehículos en una ciudad, como taxis o buses, también son aplicables en puntos de difícil acceso como zonas montañosas y áreas geográficas variables.

Las Redes Móviles ad-hoc fueron diseñadas para proveer comunicación y ser implementadas de una manera rápida y eficiente, en sitios carentes de una infraestructura de red. Pero para que esto sea posible se necesita contar con protocolos de enrutamiento específicos para esta estructura de red que lleven a cabo la tarea de organizar los enlaces, debido a que los protocolos tradicionales propios de redes centralizadas no se adaptan a este tipo de ambientes móviles.

2.1.2. AD HOC

Ad hoc es una locución latina que significa literalmente “para esto”. Generalmente se refiere a una solución elaborada específicamente para un problema o fin preciso y, por tanto, no es generalizable ni utilizable para otros propósitos. Se usa pues para referirse a algo que es adecuado sólo para un determinado fin.

Dentro del ámbito de las redes inalámbricas una red ad-hoc implica una estructura sin un nodo central sino varios nodos con iguales condiciones con una característica de auto organización que busca lograr la comunicación entre los entes de igual condición de la red. Por el propio concepto de red ad-hoc esta presenta ciertas dificultades en su funcionamiento a gran escala, ya que los nodos deberán gestionar las rutas para comunicarse entre ellos sin contar con un equipo que desempeñe el papel de enrutador para gestionar los enlaces, por ello, cada nodo actuara como un enrutador y decidirá como transmitir sus datos.

2.1.3. REDES INALAMBRICAS MESH

La comunicación inalámbrica es aquella en la que los emisores y receptores no se encuentran unidos por un medio de propagación físico como el cobre o la fibra óptica, sino que en su lugar se utiliza ondas electromagnéticas a través del espacio para propagar una señal, es decir el aire. Las redes inalámbricas Mesh, redes acopladas, o redes de malla inalámbricas de infraestructura, para definirlas de una forma sencilla, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura.

Básicamente son redes con topología de infraestructura pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los puntos de acceso están dentro del rango de cobertura de alguna tarjeta de red (TR) que directamente o indirectamente está dentro del rango de cobertura de un punto de acceso (PA).

La tecnología Mesh, siempre depende de otras tecnologías complementarias, para el establecimiento de backhaul debido a que los saltos entre nodos Mesh, provoca retardos que se van añadiendo uno tras otro, de forma que los servicios sensibles al retardo, como la telefonía IP, no sean viables.

Los expertos coinciden en que esta tecnología será la base sobre la que se sustenten los futuros sistemas de comunicación 4G, ya que permite ofrecer acceso inalámbrico en ciudades enteras sin contar con infraestructura previa alguna.

2.1.4. ESTANDARES Y SU RELEVANCIA

Para el correcto funcionamiento e implementación de redes inalámbricas se crearon estándares de la IEEE para las especificaciones de comunicación de los protocolos, para ello se utilizo el estándar 802.11 que define los dos niveles inferiores del modelo OSI para definir el funcionamiento de una WLAN, dentro de los que es 802.x se define el funcionamiento de redes área loca y metropolitana.

En la figura II.2 podemos observar la evolución de los estándares al pasar los años, en la que cada protocolo ha brindado una solución diferente a las necesidades pertinentes de la red.

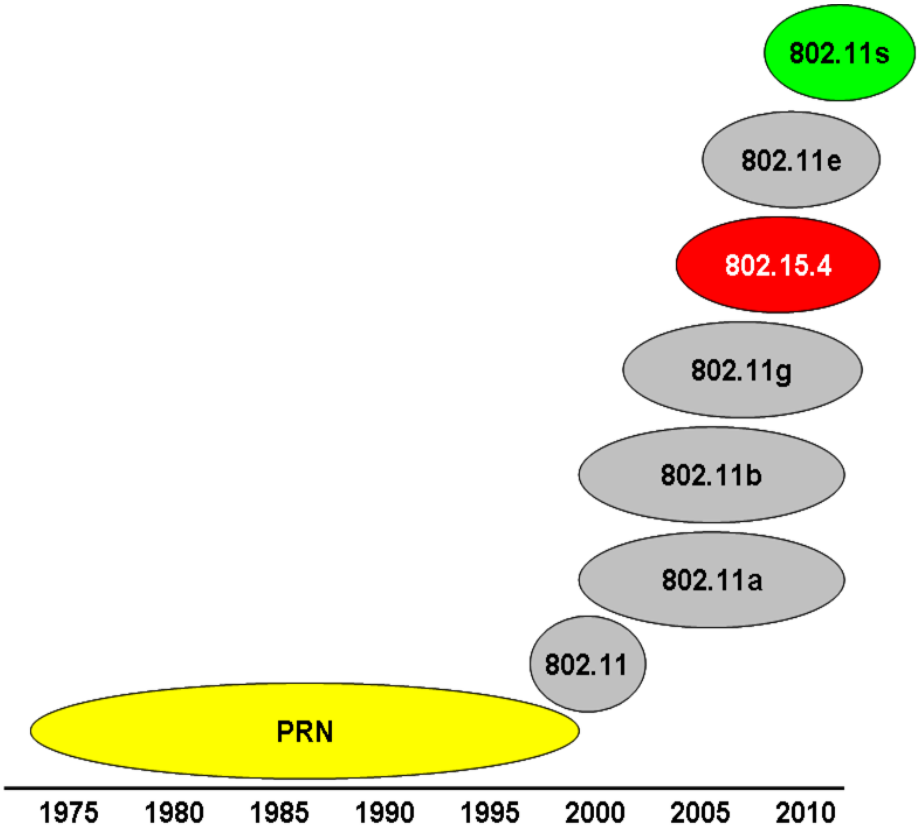

FIGURA II.1 ESTÁNDARES EN REDES INALÁMBRICAS 802.11

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 megabits por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR). IR sigue siendo parte del estándar, si bien no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

2.2. MANET'S

Las Manet's son sistemas autónomos constituidos por nodos móviles que se comunican a través de enlaces inalámbricos de múltiples saltos. En términos más sencillos esto quiere decir que una red móvil ad hoc permite que una red se pueda establecer sin la necesidad de una administración central o de infraestructura preestablecida, ya que la red se conforma sólo de usuarios móviles capaces de transmitir y recibir información entre sí.

Cada dispositivo en una MANET posee libertad para desplazarse independientemente en cualquier dirección, y eso permite que cambien dinámicamente las condiciones de enlace entre los dispositivos. Cada uno de ellos está desacoplado del tráfico y por lo tanto realiza misiones de router. Uno de los principales retos a la hora de construir MANET es lograr que sea posible equipar cada dispositivo para mantener continuamente la información necesaria para enrutar. Este tipo de redes puede operar de forma autónoma o ser conectada a Internet.

2.2.1. REDES AD HOC MÓVILES

MANET procede de las palabras "mobile ad hoc networks", algo como redes móviles entre iguales. No es exactamente lo mismo, pero como ejemplo podemos decir que el comportamiento de una MANET es similar al de una red P2P: los integrantes de la red reciben y envían información de forma descentralizada

Las Redes Móviles Ad-Hoc (MANET) fueron creadas para proporcionar comunicación y ser implementadas de una manera rápida y eficiente, en lugares carentes de una infraestructura de

red, puesto que son redes descentralizadas1. Sin embargo, para que esto sea posible se hace necesaria la introducción en la red de protocolos de enrutamiento específicos, debido a que los protocolos tradicionales propios de redes fijas no se adaptan a este tipo de ambientes móviles.

Puntos a considerar en una Manet:

- Enrutamiento
- Redes ad hoc móviles inalámbricas distribuidas de múltiples saltos
- Total movilidad de los nodos
- Topología dinámica sin estructura previa
- Administración distribuida
- Funcionan gracias a la cooperación entre nodos
- Se realiza enrutamiento en cada nodo (problema no solucionado)

2.2.2. TIPOS DE MANET's

Las MANET pueden ser clasificadas en MANET subordinadas o MANET autónomas en función de si están conectadas o no a una red externa.

- **Redes MANET autónomas**

Son redes que no están conectadas a ninguna otra red. Los nodos de la red se pueden identificar unívocamente a través de una dirección IP con la única premisa de que sea distinta a la de cualquier otro nodo de la red

- **Redes MANET subordinadas**

Son redes conectadas a una o más redes externas. Se obliga a usar un direccionamiento IP topológico correcto y enrutable globalmente. Un ejemplo típico de MANET subordinada es una MANET que es parte de Internet.

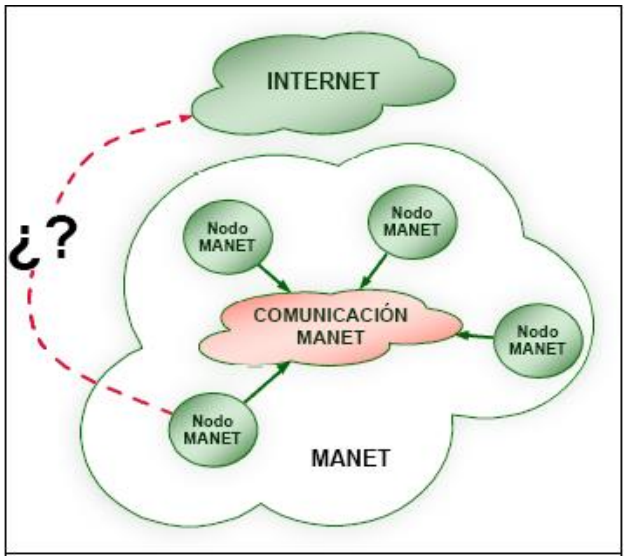

FIGURA II.2 ESPECTRO ELECTROMAGNÉTICO

2.2.3. INTRODUCCION A LOS PROTOCOLOS DE RUTEO

El encaminamiento de redes ad hoc es una tarea primordial. Al tener nodos independientes con la capacidad de gestionar sus enlaces debe buscarse alcanzar la conectividad de extremo a extremo, evitando los lazos y buscando la mejor ruta.

Tomando en cuenta la movilidad de una red inalámbrica esta tarea puede volverse muy compleja para los nodos, por ello la necesidad y variedad de protocolos de enrutamiento que tienen la tarea de gestionar los enlaces de la red a través de los mismos nodos que estarán en constante

movimiento en el tiempo de manera aleatoria lo que conlleva un cambio constante en las tablas de enrutamiento.

Los protocolos de ruteo comunes como OSPF o RIP no están diseñados para llevar a cabo estos cambios excesivos en las tablas de ruteo, ya que su eficiencia se debe a su comprensión de la red, pero cuando nos encontramos en una red ad hoc móvil, se requiere de protocolos diseñados con el fin de buscar la conexión de extremo a extremo buscando la mejor ruta del escenario móvil.

Las variaciones en la red darán como resultado que una ruta que se consideraba optima, en pocos segundos sea obsoleta, por ello se busca que el protocolo tenga una rápida capacidad de respuesta ante los cambios.

2.2.3.1. ALGORITMOS DE ENRUTAMIENTO

Como se observa al interior de una red de computadoras, para transferir información de un punto a otro se quiere de un protocolo que gestione la ruta entre los puntos. En el caso de la arquitectura TCP/IP, esta tarea está confiada a la capa de Internet, en la cual se implementan los denominados algoritmos de enrutamiento, responsables de la determinación del camino seguido por cada paquete hasta alcanzar al destinatario. Igualmente, la responsabilidad de la red de conexión de internet (internetworking) es delegada al protocolo IP. En Internet cada nodo es individualizado mediante una dirección IP, única en toda la red. Las direcciones IP se generan bajo la autoridad de la Internet Coorporation for Assigned Names and Numbers (ICANN), en base a las directivas impuestas por la RFC (Request for Comments) 2050, que se organizan en muchas clases jerárquicas.

En particular, en Internet, cada datagrama IP transmitido lleva al interno la dirección IP del servidor remitente y del receptor: es, pues, tarea de los enrutadores hacer llegar el paquete al terminal de destino. La operación de tramitación de cada paquete viene llevada a cabo consultando la llamada tabla de enrutamiento. Una tabla de enrutamiento puede verse como una lista en la cual, a cada dirección de destinatario, le corresponde una puerta de salida hacia la que se transmite las informaciones. Tal lista se construye y se actualiza mediante un algoritmo de enrutamiento que implica el uso de protocolos y algoritmos entre más enrutadores.

Existen diversas tipologías de algoritmo de enrutamiento; aquellas más usadas en las redes cableadas tradicionales son: Link State, Distance Vector, Source Routing, Random e Flooding.

- Con el Link State se asigna un costo a cada link o conexión. Cada nodo administra un mapa completo de la topología de la red. Periódicamente cada nodo manda en broadcast (difusión) el costo de los enlaces a los cuales está conectado, y los restantes actualizan el mapa de la red y la tabla de enrutamiento aplicando un algoritmo que tiene en cuenta el camino a menor costo.

- En el Distance Vector cada nodo conoce ya el costo de los enlaces a los que está conectado. Cada nodo comunica con su vecino a que otros nodos pueden alcanzar y a qué costo. Así cada nodo re calcula la propia tabla de enrutamiento siguiendo las informaciones que ha recibido, y usando un algoritmo que tiene en cuenta, por ejemplo, el camino a menor costo.
- Con el Source Routing, las decisiones pertinentes al router vienen tomadas de la fuente y los paquetes de información siguen un camino ya establecido.

- El direccionamiento Random es de tipo casual ya que la rama de salida del nodo, a menos que el servidor destinatario del paquete no esté directamente conectado al nodo en cuestión, viene elegida casualmente. De este modo, sin embargo, el algoritmo garantiza una utilización óptima de los recursos de la red, ya que goza de la simplicidad de implementación y gestión.

- Finalmente, en el Flooding sucede que cada paquete de información recibido viene transmitido y replicado sobre todos los enlaces salientes, a menos que la dirección de destino no sea un servidor directamente conectado al mismo nodo.

2.2.3.2. PROTOCOLOS DE RUTEO

Los protocolos de ruteo para las redes inalámbricas como podemos ver en la figura II.3 se clasifican en varias categorías dentro de las cuales tenemos protocolos estandarizados de propósitos generales y otros más específicos para cada necesidad de acuerdo a propósitos específicos, de manera general se pueden clasificar en tres categorías:

- Proactivos
- Reactivos
- Híbridos

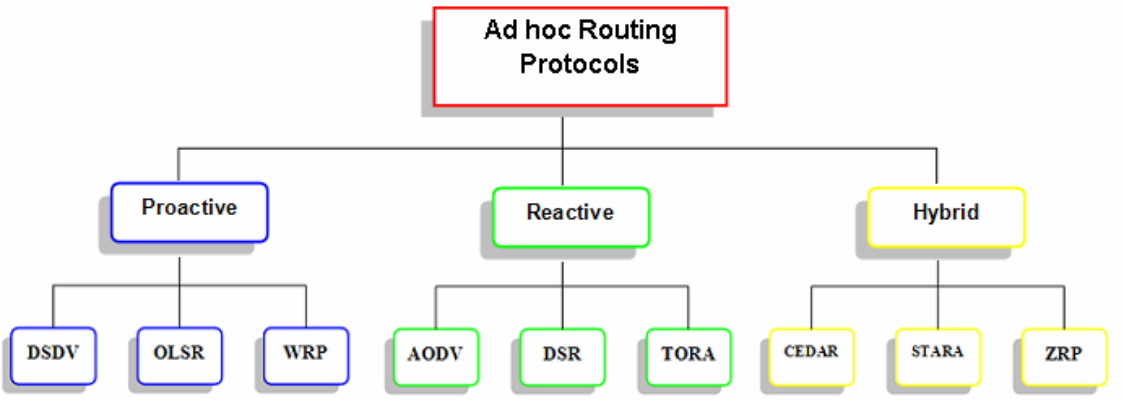

FIGURA II.3 PROTOCOLOS DE RUTEO PARA COMUNICACIÓN INALÁMBRICA

Aquellas de tipo proactivos mantienen constantemente actualizados la información de direccionamiento a través de intercambios de paquetes a intervalos temporales fijos. Esto permite tener un direccionamiento disponible a cada petición de enrutamiento, pero está la desventaja de producir tráfico de señalización incluso cuando no se transmite ningún paquete de datos; esto puede provocar sobrecarga en la red.

En los protocolos de tipo reactivos viene invocado un procedimiento para determinar el correcto direccionamiento sólo en el momento en el que el paquete deba efectivamente transmitirse. De este modo, se reduce el tráfico de señalización en detrimento de un aumento de los tiempos de entrega.

El tercer tipo de protocolos, híbridos, busca, como dice su nombre, de unir las ventajas de ambos protocolos precedentes, limitando la aplicación de algoritmos proactivos sólo a los nodos adyacentes del que quiere transmitir.

En el caso en el que se encuentren redes no dotadas de una infraestructura como por ejemplo, las redes ad-hoc, se hacen necesarios los algoritmos de enrutamiento adecuados en los que hay

que tener en cuenta la característica dinámica de tales sistemas (en las redes inalámbricas ad-hoc, los nodos podrían moverse modificando así la topología de la red). En este tipo de redes, cada nodo debe tener la capacidad de un router.

A continuación se describen algunos de los algoritmos de direccionamiento más usados en las redes inalámbricas ad-hoc:

AODV (Ad-hoc On Demand Vector),

AOMDV (Ad-hoc On Demand Multipath Distance Vector)

DSR (Dynamic Source Routing),

OLSR (Optimized Link State Routing

)

- **AODV (Ad-hoc On Demand Vector)**

El protocolo AODV es un protocolo de enrutamiento de tipo reactivos basado en el algoritmo Distance Vector.

Una característica fundamental del protocolo es que los nodos destino de un trayecto, antes de proporcionar información de direccionamiento, crean un número de secuencia de destino (destination sequence number), que proporciona a los nodos un instrumento para evaluar cuanto se ha actualizado un determinado recorrido evitando la formación de lazos (loop) en el camino de enrutamiento. Un terminal que deba elegir entre varios caminos hacia un cierto destino, elegirá aquel caracterizado por el número de secuencia mayor, correspondiente a una información de routing mas reciente.

Además, el protocolo soporta el enrutamiento multidifusión (multicast). Este protocolo usa mensajes particulares llamados RREQ (Route Request), RREP (Route Replies) y RERR (Route Errors) que son enviados y recibidos mediante el protocolo UDP.

Cuando un nodo quiere encontrar un camino hacia otro nodo de la red:

1) envía en broadcast un mensaje del tipo RREQ

2) atiende una respuesta del destinatario o, de otro nodo, que posee un camino de enrutamiento bastante reciente hacia aquel destino. Esta respuesta llegará con un mensaje de tipo RREP confirmando incluso que el camino buscado está disponible.

Por nodo que posea un camino de direccionamiento bastante reciente se entiende un nodo que conozca un trayecto asociado a un número de secuencia destino que sea de grande, al menos, como aquel contenido en el mensaje RREQ.

Además, los nodos de la red que forman parte de trayectos activos pueden transmitir periódicamente mensajes especiales de RREP, llamados mensajes “Hello”, a sus nodos más cercanos. La falta de mensajes “Hello” por parte de los nodos vecinos viene interpretada como pérdida de la conexión con ese nodo y hace que el nodo que debería haber recibido tal mensaje proceda a corregir su tabla de enrutamiento, eliminando aquel trayecto.

En la fase de extracción de la tabla de enrutamiento de una puerta de acceso a un nodo vecino, con motivo de que ya no es alcanzable, el nodo se preocupa de mandar un mensaje RERR a los nodos adyacentes que usaban el trayecto, informándoles del acontecimiento. Todo esto sucede

sin dificultad en cuanto a que cada nodo conserva una lista de los nodos cercanos que están activos en cualquier comunicación.

El procedimiento del mensaje RERR viene, por tanto, repetido por los nodos intermedios determinando así la actualización de las tablas de direccionamiento de todos los nodos de la red

.

- **AOMDV (Ad-hoc On Demand Multipath Distance Vector)**

AOMDV comparte muchas características en su funcionamiento básico con AODV . Se basa en el concepto de vector distancia y utiliza aproximación de salto en salto. Este protocolo a demás descubre rutas bajo demanda utilizando un procedimiento de descubrimiento de ruta.

La principal diferencia es el número de rutas encontradas para cada descubrimiento de ruta. En AOMDV la propagación de RREQ de la fuente hacia el destino establece múltiples caminos en reversa junto con los nodos intermedios al igual que el nodo destino

Varios RREPS atraviesan estos caminos de retorno utilizando varias rutas. AOMDV también provee nodos intermedios con caminos alternos, de esta manera se puede reducir la frecuencia de descubrimiento de rutas.

El núcleo de AOMDV busca asegurar que se descubran múltiples caminos libres de lazos, además de la eficiencia al encontrar rutas mediante inundación de la red. Este protocolo actualiza las reglas aplicadas localmente a un nodo, juega un papel fundamental al mantener la red libre de bucles.

AOMDV confía en la información de ruteo disponible bajo los lineamientos de AODV, en general no emplea ningún control de paquetes, de hecho el envió de RREPS y RERRS para descubrir múltiples rutas y mantenerlas, junto con campos extra en los campos de ruteo constituyen la única sobrecarga para el protocolo

- **DSR (Dynamic Source Routing)**

El protocolo DSR, de tipo reactivos, se caracteriza por el uso del Source Routing y del mecanismo de tipo “On Demand”. En tal sistema el source routing hace que los nodos fuente conozcan “paso a paso” (hop by hop) el camino que deben efectuar para alcanzar al destinatario. Esto se lleva a cabo gracias a una memoria de enrutamiento (route cache) que memoriza todos los caminos a efectuar.

Si el nodo que quiere enviar un paquete informativo pertenece a una red inalámbrica ad-hoc, se inicia un proceso de Routing Discovery. Tal proceso consiste en el envío, por parte del nodo, de mensajes RREQ en Flooding sobre la red, mensajes que todos los otros nodos receptores enviarán a su vez en Flooding. En cambio, en el caso en el que el nodo sea el nodo destinatario o son nodos que tienen, en la propia memoria de enrutamiento, un trayecto válido, responden al mensaje RREQ, transmitiendo al nodo solicitante un paquete RREP. Habitualmente, este último sigue un camino inverso respecto al del RREQ y mantendrá toda la información de direccionamiento que se memorizará desde el nodo solicitante.

Por último, si una conexión se interrumpe, vienen notificados una serie de paquetes RERR de modo que todos los nodos actualicen su memoria de direccionamiento y no usen más ese

enlace. El protocolo DSR hace un uso intenso de la memoria de direccionamiento y de la fuente de direccionamiento para evitar los lazos (loop).

- **OLSR (Optimized Link State Routing)**

El protocolo Optimized Link State Routing (OLSR) es un mecanismo estándar de enrutamiento pro-activo, que trabaja en forma distribuida para establecer las conexiones entre los nodos en una red inalámbrica ad hoc (mobile ad hoc networks, MANETs). Este protocolo fue diseñado en un principio por investigadores del Instituto Nacional francés de Investigación en Informática y Automática (INRIA, por sus siglas en francés), y ha sido posteriormente estandarizado por el Internet Engineering Task Force (IETF).

La diseminación directa de información por toda la red (flooding) es ineficiente y muy costosa en una red inalámbrica y móvil, debido a las limitaciones de ancho de banda y la escasa calidad del canal radio. Por ello, OLSR prové un mecanismo eficiente de diseminación de información basado en el esquema de los Multipoint Relays (MPR).

Bajo este esquema, en lugar de permitir que cada nodo retransmita cualquier mensaje que reciba (flooding clásico), todos los nodos de la red seleccionan entre sus vecinos un conjunto de multipoint relays (retransmisores), encargados de retransmitir los mensajes que envía el nodo en cuestión. Los demás vecinos del nodo no pueden retransmitir, lo que reduce el tráfico generado por una operación de flooding.

Hay varias formas de escoger los multipoint relays de un nodo, pero independientemente de la forma de elección, el conjunto de MPRs de un nodo debe verificar que son capaces de alcanzar

a todos los vecinos situados a una distancia de 2 saltos del nodo que los calcula (criterio de cobertura de MPR).

Una red enrutada con OLSR utiliza básicamente dos tipos de mensajes de control:

- Los mensajes HELLO son enviados periódicamente por cada nodo de la red a sus nodos vecinos, pero nunca son retransmitidos más allá del primer salto (1 hop) desde su emisor (alcance local). Estos mensajes contienen la lista de vecinos conocidos por el nodo emisor así como la identidad de los multipoint relays seleccionados por transmisor. Su intercambio permite a cada nodo de la red conocer los nodos situados a 1 y 2 saltos de distancia (es decir, aquellos a los que se puede hacer llegar un mensaje con una transmisión directa o con una transmisión y una retransmisión) y saber si ha sido seleccionado como MPR por alguno de sus vecinos.

- Los mensajes TC (Topology Control) son enviados periódicamente y de forma asíncrona. A través de ellos, los nodos informan al conjunto de la red acerca de su topología cercana. Al contrario que los HELLO, los mensajes TC son de alcance global y deben llegar a todos los nodos de la red. El conjunto de los mensajes TC recibidos por un nodo inalámbrico le permite reconstruir su base de datos topológica, computar el árbol de caminos mínimos (mediante el algoritmo de Dijkstra) y calcular así la tabla de enrutamiento hacia todas las posibles destinaciones. La diseminación de mensajes TC se hace de acuerdo con el mecanismo de flooding basado en MPR.

2.2.4. APLICACIONES PRÁCTICAS

- **Vanet**

Las VANET (Vehicular Ad-Hoc Network) son redes ad-hoc móviles capaces de comunicar información entre diversos vehículos colindantes y el sistema de tráfico.
El objetivo principal de estos sistemas es proporcionar un mejor conocimiento de las condiciones de las carreteras a los conductores para reducir así el número de accidentes y que la conducción sea más cómoda y fluida. Asimismo, estas redes permiten el acceso a contenidos multimedia e Internet, como la compartición de archivos entre diferentes vehículos.

Este tipo de redes, al ser una extensión de las redes ad-hoc móviles (MANET), supone los mismos desafíos aunque con diferencias sutiles.

- **Aplicaciones militares**

En caso de requerirse una red inalámbrica en la que no se puede depositar el funcionamiento de la red sobre un punto central como un punto de acceso inalámbrico, se requiere que cada nodo sea autosuficiente para comunicarse con los demás, al permitir que cada nodo actué como un enrutador se provee la capacidad de autosuficiencia, convirtiendo esta estructura descentralizada en una ventaja para aplicación militar en la que cada móvil, sea este un vehículo o persona, tiene la capacidad de comunicarse con la red siempre que esté al alcance de un nodo cercano que tenga capacidad de acceso a la red

- **Operaciones de emergencia**

En caso de necesitarse un red con la capacidad de desplegarse rápidamente sin tiempo para instalar un dispositivo central que brinde cobertura a la red o que no pueda cubrir la zona requerida por condiciones geográficas se vuelve una necesidad contar con una Manet que permita que cada nodo actué independientemente a demás de brindar conectividad entre nodos distantes

- **Otras aplicaciones**

Gracias a la característica de red descentralizada se pueden encontrar numerosas aplicaciones para una red con la capacidad de brindar independencia a los nodos en especial en casos que se requiera un despliegue rápido de la red o que geográficamente no sea posible o eficiente instalar un dispositivo central.

2.3. REDES MESH

Las redes inalámbricas Mesh (WMNs) es un subtipo de red Ad-Hoc en las que existe un backbone de nodos mallados entre sí, se puede definir como un tipo de red radical que marca la diferencia en relación con las tradicionales y centralizadas sistemas inalámbricos, tales como las redes celulares y las redes de área local (LAN).

Unas de las características de las redes Mesh es su inherente tolerancia a fallos cuando existe algún problema en la red, incluso cuando varios nodos fallan, la facilidad de implementación de este tipo de red, y una gran capacidad de ancho de banda.

Existen muchas formas de hacer redes malladas, de hecho las redes son una gran malla sobre la Internet pero no solo la malla corresponde a la capa física sino también la acompañan una serie de protocolos de comunicaciones que hacen factible el flujo de datos entre los nodos y clientes de una red.

Las Redes Inalámbricas Mesh Networks (WMNs) consisten en dos tipos de nodos los enrutadores y los clientes, donde los enrutadores tienen movilidad mínima y forman el "backbone"o dorsal de las WMNs. Estas redes pueden integrarse a otras como Internet, IEEE 802.11, IEEE 802.15, IEEE 802.16, etc. Los clientes pueden ser estáticos o móviles y pueden crear una red mallada entre ellos mismos o con los enrutadores. Estas redes solucionan las limitaciones y mejoran el rendimiento de las redes Ad-hoc.

Gracias a la posibilidad de conectarse a distintos puntos de acceso en lugar de a uno sólo se aumenta el ancho de banda que puede tener cada cliente, también resulta mucho más estable ya que puede seguir funcionando aunque caiga un nodo, en cambio en las redes habituales si cae un punto de acceso los usuarios de ese punto de acceso se quedan sin servicio. En la siguiente figura se puede observar una red mallada ejemplo en la que se pueden ver las distintas características que pueden tener estas redes.

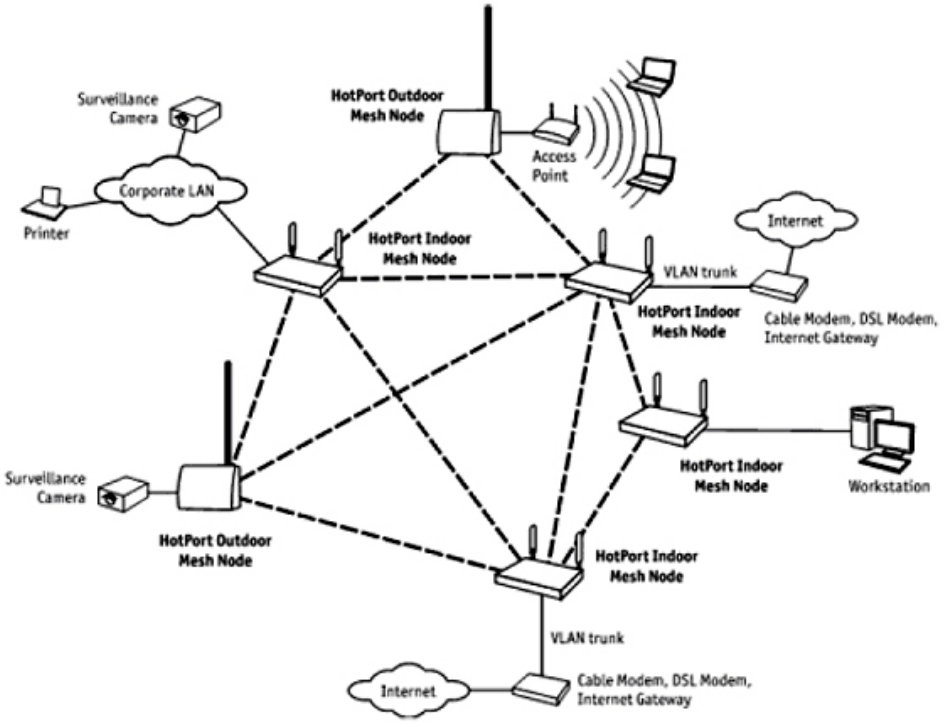

FIGURA II.4: EJEMPLO RED MALLADA INALÁMBRICA

Estas redes se organizan y se auto configuran automáticamente: entre los nodos de la red se establecen automáticamente los enlaces y mantiene la conectividad en malla entre ellos. Además, este proceso se realiza dinámicamente, permitiendo la aparición de nuevos nodos y la desaparición de nodos existentes. Estas características aportan grandes ventajas como robustez, fiabilidad y un mantenimiento fácil de redes. Para obtener una mejor flexibilidad de las redes malladas, los nodos están normalmente equipados con múltiples interfaces que pueden ser de diferentes tecnologías de acceso inalámbricas.

2.3.1. DESAFIÓS EN REDES MESH

Comúnmente las redes inalámbricas Ad Hoc y las redes Mesh se basan en un solo canal o en un solo interfaz de radio. Las redes Mesh con independencia de su sencillez y alta tolerancia a

fallos, se enfrentan a una limitación en cuanto a la capacidad de la red. Los recientes avances en redes Mesh se basan principalmente en un enfoque multiradio, factores como la ineficacia de los protocolos, las interferencias de fuentes externas, compartir el espectro electromagnético y su escasez reducen la capacidad que pueden alcanzar las redes inalámbricas para funcionar en base a sistemas monoradio.

Con el fin de mejorar la capacidad de las redes Mesh y poder cubrir cada vez más la alta demanda de tráfico planteado por las nuevas aplicaciones, las redes Mesh multiradio (MR-WMNs) están bajo intensa investigación, lo cual se cree que proveerá de ventajas tales como el aumento de la capacidad de la red, aunque no hay que dejar a un lado que este tipo de red se enfrenta a varios problemas y desafíos que se mencionan a continuación.

2.3.1.1. CAPACIDAD

La capacidad alcanzable por los nodos en una red Mesh se limita si utilizamos sistemas de un solo canal en comparación con sistemas multicanal. La tabla II.I muestra la variación del rendimiento en la capacidad de una red Mesh. Se puede apreciar que con más de un salto el rendimiento se degrada.

	1er salto	2do salto	3er salto	4to salto	5to salto	Más de 5 saltos
Rendimiento	1	0,47	0,32	0,23	0,15	0,14

Tabla II.I. Variación del rendimiento en función del número de saltos en una red Mesh

Aunque hay varios factores que contribuyen a la degradación del rendimiento, como características del protocolo MAC, la tasa alta de error presente en canales inalámbricos y

factores imprevisibles esto se conoce como el problema del nodo expuesto que contribuye a la degradación del rendimiento a lo largo de la ruta, hay que considerar que la degradación del rendimiento aumenta hasta llegar a los cinco saltos de ahí en adelante el rendimiento empieza a permanecer constante.

2.3.1.2. CONFIABILIDAD Y ROBUSTEZ

Una característica importante que motiva el uso de redes Mesh y sobre todo de las redes MR-WMNs se debe a que mejora la confiabilidad y la robustez de las comunicaciones.

La topología en malla proporciona una alta confiabilidad, en los sistemas de acceso inalámbrico los errores en el canal pueden ser muy elevados en comparación con las redes cableadas, por lo tanto se necesita una alta calidad de comunicación durante la transmisión cuando se utiliza un canal inalámbrico.

Esto es muy importante en una red Mesh que utiliza frecuencias sin licencia, para mejorar la confiabilidad de la comunicación se puede emplear la diversidad de frecuencia, mediante el uso de múltiples interfaces de radio, lo cual es difícil de lograr en sistemas monoradio. Mientras que en redes MR-WMNs puede lograr mayor tolerancia a fallos en la comunicación, ya sea por cambio de las radios, los canales, o mediante el uso de radios múltiples simultáneamente.

2.3.1.3. GESTION DE RECURSOS

La gestión de los recursos se refiere a la gestión eficiente de los recursos de la red como son: la energía, el ancho de banda, interfaces, etc. Por ejemplo, el balanceo de carga a través de múltiples interfaces podría ayudar a prevenir que cualquier canal en particular que esté muy

saturado pueda convertirse en un cuello de botella esto también podría ayudar para obtener una alta velocidad de transmisión de datos.

Una importante ventaja de utilizar un sistema multiradio en una red Mesh es la posibilidad de tener calidad de servicio a través de la diferenciación de servicio.

2.3.1.4. CLASIFICACION DE ARQUITECTURAS EN REDES MESH

Una red inalámbrica Mesh (WMNs) puede ser diseñada basadas en tres diferentes arquitecturas de red:

- Arquitectura plana
- Arquitectura jerárquica
- Arquitectura híbrida

2.3.1.4.1. ARQUITECTURA PLANA

En una red plana WMNs, la red está formada por los equipos cliente que actúan como hosts y routers. En este caso, todos los nodos están al mismo nivel. Los nodos de los clientes inalámbricos coordinan entre sí para proporcionar enrutamiento, configuración de la red, provisión de servicios, y algún otro tipo de solicitud. Esta arquitectura es la más parecida a una red Ad Hoc y es el caso más simple entre los tres tipos de arquitecturas WMNs.

La principal ventaja de esta arquitectura es su sencillez, y sus desventajas incluyen la falta de escalabilidad y limitaciones de recursos. Los principales problemas a resolver en el diseño de esta arquitectura WMNs son: esquema de direccionamiento, enrutamiento, servicios. En una red plana, el direccionamiento es uno de los problemas que llegan a impedir la estabilidad.

2.3.1.4.2. ARQUITECTURA JERÁRQUICA

En una arquitectura jerárquica, la red tiene múltiples niveles jerárquicos en la que los nodos del cliente forma el nivel más bajo dentro de la arquitectura. Estos nodos del cliente pueden comunicarse con la red que está formada por routers. En la mayoría de los casos, los nodos WMNs se dedican a forman un backbone de una red troncal WMNs. Esto significa que los nodos que forman el backbone no pueden originar o terminar el tráfico de datos como los nodos del cliente.

La responsabilidad de auto-organizar y mantener la red troncal está a cargo de los routers WMNs, algunos de los cuales pueden tener interfaz externa a Internet y a esos nodos se los llama nodos pasarela.

2.3.1.4.3. ARQUITECTURA HIBRIDA

Este es un caso especial de redes jerárquicas WMNs, donde la red WMNs utiliza otras redes inalámbricas para la comunicación. Por ejemplo, el uso de otras infraestructuras tales como las redes celulares, redes Wi-Max, o las redes satelitales.

2.4. SEGURIDAD

2.4.1. TECNOLOGÍAS EN SEGURIDAD

El potencial de una red WMNs no puede ser explotada sin considerar la seguridad**.** Las WMN se exponen a las mismas amenazas básicas comunes de las redes cableadas e inalámbricas: los mensajes pueden ser interceptados, modificados, duplicados, etc. Una red que posee recursos importantes, se podría acceder sin autorización.

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

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

Los Servicios de seguridad en el futuro serán mucho más restringidos buscando para el usuario privacidad y la confidencialidad del tráfico. La protección del tráfico de datos implica: la confidencialidad (cifrado), la autentificación de los socios de la comunicación, así como la protección de la integridad y de la autenticidad de mensajes intercambiados. La protección de la

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

Los datos pueden ser protegidos por diversas capas (capa de enlace, capa de red, capa de transporte y capa de aplicación): especialmente en sistemas inalámbricos, (IEEE 802.11 WLAN, Bluetooth, 802.16 WiMax), que incluye medios de proteger el enlace inalámbrico. Éstos utilizan diversos esquemas de encapsulación de tramas, diversos protocolos de autentificación, y diversos algoritmos criptográficos. Ya sea una llave compartida es configurada en los dispositivos WLAN (la llave precompartida PSK)

Las Redes de área local inalámbricas (WLAN) basada en IEEE 802.11i (WPA32, WPA2) soporta dos modos de seguridad: puede ser shared key (clave compartida) que es configurada en los dispositivos WLAN ([PSK = preshared key] claves pre-compartidas), que es de uso frecuente en las redes domesticas, los usuarios pueden ser autenticados con un servidor autentificador (servidor AAA). Para este propósito, se utiliza el protocolo extensible de autentificación (extensible authentication protocol) (EAP).

La autentificación real ocurre entre la estación móvil (MS) y el servidor AAA. Usando EAP como lo muestra la Figura 1.15. El EAP es transportado entre el MS y el punto de acceso (AP) que usan EAPOL (encapsulación EAP sobre LAN), y entre el AP y el servidor AAA por el protocolo

2.4.2. ESTANDARIZACIÓN DE MESH EEE 802.11s

Estas nuevas tecnologías se encuentran en proceso de estandarización por parte del IEEE para su aplicación directa en redes inalámbricas con tecnología 802.11. La norma que agrupará las actuales líneas de trabajo se define en **IEEE 802.11s**, cuyo primer borrador fue publicado en noviembre de 2006, y la versión final del mismo está prevista para finales de 200834

El grupo de trabajo que desarrolla dicho estándar (IEEE Task Group TGs) define la arquitectura de red y el protocolo necesarios a partir de las especificaciones del IEEE 802.11, con el objetivo de crear una topología de red auto-configurable que soporte la transmisión broadcast/multicast y unicast (topologías multihop o de varios saltos), todo ello manteniendo la latencia y la degradación del throughput dentro de unos márgenes tolerables para la transmisión de voz con requerimientos de tiempo real, y datos con requerimientos de anchos de banda elevados35.

A pesar de que fueron quince las primeras propuestas recibidas en junio de 2005, para septiembre de 2005 habían sido reducidas a cuatro. Hasta fecha reciente las dos principales propuestas que recibieron la mayoría de votos en las reuniones de julio, septiembre y noviembre de 2005 eran las siguientes:

2.5. GESTIÓN DE REDES

Las actuales redes de telecomunicación se caracterizan por un constante incremento del número, complejidad y heterogeneidad de los recursos que los componen. Los principales problemas relacionados con la expansión de las redes son la gestión de su correcto funcionamiento día a día y la planificación estratégica de su crecimiento. De hecho más se estima que más del 70 % del coste de una red corporativa se atribuye a su gestión y operación.

Por todo ello, la gestión de red integrada, como conjunto de actividades dedicadas al control y vigilancia de recursos de telecomunicación bajo el mismo sistema de gestión, se ha convertido en un aspecto de enorme importancia en el mundo de las telecomunicaciones.

La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlarlos recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable

El modelo de gestión ISO clasifica las tareas de los sistemas de gestión en cinco áreas funcionales. La tarea del encargado de gestionar una red empresarial será evaluar la plataforma de gestión a utilizar en cuanto a la medida en que dicha plataforma resuelva la problemática de gestión en cada una de estas áreas:

- Gestión de configuración.
- Gestión de rendimiento.
- Gestión de contabilidad.
- Gestión de fallos.
- Gestión de seguridad

2.5.1. GESTIÓN DE CONFIGURACIÓN

El objetivo de la gestión de configuración es obtener datos de la red y utilizarlos para incorporar, mantener y retirar los distintos componentes y recursos a integrar. Consiste en la realización de tres tareas fundamentales:

- Recolección automatizada de datos sobre el inventario y estado de la red, tales como versiones software y hardware de los distintos componentes.
- Cambio en la configuración de los recursos.
- Almacenamiento de los datos de configuración.

El proceso de gestión de configuración tiene como principal objetivo asegurar la integridad de los productos y servicios desarrollados.

Integridad del producto es:

- Saber exactamente lo que se ha entregado al cliente
- Saber el estado y contenido de las líneas base y elementos de configuración

Es una forma efectiva y eficiente de gestionar y comunicar los cambios en líneas base y elementos de configuración a lo largo del ciclo de vida.

A continuación se resaltan algunos beneficios de la implementación del proceso de gestión de configuración para la organización. Los siguientes puntos representan objetivos de negocio, por ejemplo: reducción de riesgos, mejora de la calidad y beneficios de coste en la entrega y soporte de productos.

- Asegurar la correcta configuración del software.
- Proporcionar la capacidad de controlar los cambios.
- Reducir los sobreesfuerzos causados por los problemas de integridad.
- Garantizar que todo el equipo trabaja sobre una misma línea base de productos.

2.5.2. GESTIÓN DE RENDIMIENTO

La gestión de prestaciones o del rendimiento tiene como objetivo principal el mantenimiento del nivel de servicio que la red ofrece a sus usuarios, asegurándose de que está operando de manera eficiente en todo momento. La gestión de prestaciones se basa en cuatro tareas:

- Recogida de datos o variables indicadoras de rendimiento, tales como el troughput de la red, los tiempos de respuesta o latencia, la utilización de la línea, etc.
- Análisis de los datos para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.
- Determinación de un sistema de procesado periódico de los datos de prestación de los distintos equipos, para su estudio continuado.

2.5.3. GESTIÓN DE CONTABILIZACIÓN

La gestión de contabilización consiste en actividades de recolección de información de contabilidad y su procesamiento para propósitos de cobranza y facturación. Actividades que establecen un límite contable para que un conjunto de costos se combinen con recursos múltiples y se utilicen en un contexto de servicio.

Tiene como misión la medida de parámetros de utilización de la red que permitan a su explotador preparar las correspondientes facturas a sus clientes. Entre las tareas que se deben realizar en esta área, están:

- Hacer seguimiento del uso de la red por departamentos e individualmente
- Facilitar la facturación basada en el uso
- Encontrar a los abusadores que usan más recursos de los que deberían usar

2.5.4. GESTIÓN DE FALLAS

La gestión de fallas es la encargada principal de Informa sobre errores en el dispositivo, e informar sobre el estado del dispositivo, tiene por objetivo fundamental la localización y recuperación de los problemas de la red. La gestión de problemas de red implica las siguientes tareas:

- Detectar, aislar, diagnosticar y corregir los problemas
- Reportar el estado a los usuarios finales y a la gerencia
- Seguir las tendencias relacionadas con los problemas

2.5.5. GESTIÓN DE SEGURIDAD

La gestión de seguridad es aquella que requiere la habilidad para supervisar y controlar la disponibilidad de facilidades de seguridad, y reportar amenazas y rupturas en la seguridad.
La misión de la gestión de seguridad es ofrecer mecanismos que faciliten el mantenimiento de políticas de seguridad (orientadas a la protección contra ataques de intrusos). Entre las funciones realizadas por los sistemas de gestión de seguridad, están:

- Mantener y distribuir la información de login (*usernames* y *passwords*)

- Generar, distribuir y almacenar las claves y certificados de encriptamiento y acceso
- Analizar las configuraciones de los enrutadores, suiches y servidores, para revisar la adecuación a las políticas y procedimientos de seguridad
- Recolectar, almacenar y examinar los registros de auditoría de seguridad

CAPITULO III

MARCO METODOLOGICO E HIPOTETICO

3.1. TECNICAS DE INVESTIGACION

Las técnicas de investigación que se encuentran dentro de nuestro marco metodológico, serán pruebas de análisis o test; los cuales son muy utilizados en este tipo de investigaciones ya que permiten una máxima precisión en el dato obtenido. Plantearemos un escenario físico, el cual esta basado en un cluster que se ha configurado bajo el sistema operativo Linux. Se trata de un conjunto de 5 ordenadores que se encuentran interconectados trabajando conjuntamente o bien por separado según se especifique en los diferentes escenarios trazados.

Una vez hemos podido comprobar el correcto funcionamiento en escenarios estáticos se pasa a estudiar el comportamiento de los mismos en escenarios dinámicos, por lo tanto se realizara análisis de simulaciones en el programa NS2 por medio de un emulador. Gracias a las pruebas

que se realizaran podremos ver cómo se comportan dos protocolos de diferente tipo ante diferentes escenarios y poder tener claras las diferencias de funcionamiento de los mismos.
Pasamos a realizar pruebas con escenarios dinámicos acercándonos más a la finalidad de este tipo de redes. Para ello no se ha utilizado ordenadores portátiles en campo abierto, sino que se ha utilizado el cluster antes mencionado. El cluster se puede utilizar para que todas las máquinas trabajen de forma conjunta o independientemente ayudándonos a dar una movilidad con un emulador de redes. Estas pruebas de laboratorio sirven para saber que resultados vamos a obtener antes de hacer una puesta en escena real, pero sin tener algunas consideraciones.

Las pruebas realizadas en nuestro estudio serán pruebas de rendimiento, tomaremos en cuenta las variables que se consideren más relevantes en análisis de eficiencia y consumo de energía de los protocolos en la red. Para dicho efecto se analizan los siguientes puntos:

- Cantidad de paquetes enviados, recibidos, desechados y reenviados a nivel de aplicación por nodo y total
- Cantidad de paquetes enviados, recibidos, desechados y reenviados a nivel de protocolo de ruteo por nodo y total
- Numero de nodos, velocidad de los nodos, tipo de tráfico, cobertura, número de conexiones

Los resultados se clasifican en tres grupos principales que son:

- Paquetes a nivel de aplicación
- Paquetes a nivel de protocolo

- Numero de Conexiones

Paquetes a nivel de aplicación

Se obtuvieron datos generando trafico CBR mediante una conexión UDP y trafico FTP mediante una conexión TCP

La generación de trafico FTP permite analizar la red mediante un protocolo orientado a la conexión, de esta manera se tiene un transporte más confiable de la información pero que genera mayor carga para la red, de esta manera antes de transportar la información se procede a crear una conexión entre los nodos lo que permite que una mayor parte de paquetes enviados lleguen a su destino.Este tráfico es el que en una red es generado por los usuarios para intercambiar información y dentro de este tenemos:

a) Paquetes enviados

Son los paquetes generados por el nodo emisor que es seleccionado de acuerdo a la cercanía o de forma aleatoria para crear un enlace de comunicación. Estos paquetes son de tipo FTP sobre una conexión TCP o de tipo CBR sobre una conexión UDP

En este caso tenemos por ejemplo un enlace entre el nodo 1 y 2 con paquetes de 512 bytes en un intervalo de 0,5 segundos y con un máximo de 10000 paquetes.

El número de paquetes enviados puede variar entre las distintas simulaciones y más aun en conexiones TCP dado que en este caso primero se establece el enlace para enviar los paquetes.

Aquí se puede observar un enlace sobre TCP con una ventana de 32 bits, y paquetes de 512 bytes.

b) Paquetes recibidos

Respecto a los paquetes recibidos estos son aquellos que lograron transmitirse exitosamente entre los nodos saltando en ciertos casos varios puntos para alcanzar su destino, de esta manera en el destino tendremos el paquete enviado por el emisor.

Cabe especificar que el número de paquetes recibidos es proporcional al número de paquetes enviados tomando en cuenta la diferencia con los paquetes que se desechan en la red.

c) Paquetes reenviados

Los paquetes reenviados son aquellos que para alcanzar su destino realizaron saltos a través de la red, de esta manera los nodos intermedios reenvían paquetes que en este caso se contabilizan como reenviados teniendo la misma estructura que un paquete emitido por el emisor de tipo FTP o UDP.

De este número de paquetes podemos concluir el número de saltos que utiliza cada conexión para enviar la información ya que mientras más paquetes se reenvíen significa que el número de saltos es mayor.

d) Paquetes desechados

Los paquetes desechados o caídos en la red son aquellos que por distintas razones como cambios en la topología de la red, destinos inalcanzables u otros no lograron llegar a su destino y en algún punto de la red fueron desechados.

Paquetes a nivel de protocolo de ruteo

Cada protocolo posee su técnica para encontrar las diferentes rutas de la red, por ello el trafico generado por el mismo es considerable en el desempeño de la red, por ello se analiza tanto los paquetes enviados y recibidos así como los reenviados y desechados, ligados directamente a la creación y mantenimiento de las tablas de ruteo

Este tráfico es generado por el protocolo de ruteo empleado para establecer las tablas de ruteo, de esta manera el numero de paquetes dependiendo de la topología de la red puede volverse una verdadera carga para el funcionamiento adecuado de los enlaces. Entre estos paquetes tenemos los siguientes:

a) Paquetes enviados

El número de paquetes enviados viene dado por las solicitudes de conocimiento de la red de los distintos nodos manejado de manera diferente por cada protocolo, estos paquetes en la mayoría de casos son de broadcast o a los nodos adyacentes para el intercambio de información

b) Paquetes recibidos

El número de paquetes recibidos es elevado en la mayoría de casos ya que al ser enviados mediante broadcast la cantidad de paquetes recibidos por los nodos se eleva consideradamente esto provoca por lo general tormentas de broadcast al inicializarse la red.

c) Paquetes reenviados

De igual manera el número de paquetes reenviados se debe a aquellos que atravesaron por distintos nodos para alcanzar su destino.

d) Paquetes desechados

Dado que el envío de paquetes por parte de los nodos que buscan establecer sus rutas tenemos varios paquetes de ruteo que no alcanzaron su destino sea por la topología o por problemas en el medio.

También utilizaremos una técnica de observación estructurada, la cual nos permitirá captar, apreciar y percibir la realidad que interese a nuestro trabajo, mediante diversas pruebas y guías de observación; al ser una observación de tipo estructurado podemos utilizar instrumentos que nos facilite la evaluación de los escenarios utilizando diferentes herramientas

3.2. MÈTODOS DE INVESTIGACION

Método Científico – Deductivo

Para poder tener un conocimiento correcto de la lógica utilizada debemos tener una descripción de lo que ocurre como su correspondiente explicación del porqué ocurre. Las explicaciones del porqué ocurre son importantes porque nos permiten hacer predicciones, que son un elemento crucial en nuestro proyecto.

Ya que el método científico implica una combinación de inducción y deducción que se retroalimentan es necesaria una fiabilidad de este conocimiento científico, y lo logramos sometiendo a prueba una y otra vez las predicciones, que a su vez son interdependientes de predicciones de teorías en otras áreas y que también se ponen a prueba.

Todo será tratado como una función racional porque presupone ya una elaboración, un trabajo activo frente a la información recibida. De los datos recibidos vamos deduciendo otros y así, paso a paso, llegamos a la conclusión o al dato deseado.

Se parte de la observación después de haber planteado nuestro escenario basado en redes Ad-Hoc, mediante un proceso deductivo podremos llegar una teoría que nos explique los principales problemas que se presentan en este tipo de redes en forma de hipótesis, con el análisis de estos resultados validaremos empíricamente las posibles soluciones que se recomendaran se den en cada caso. Este tipo de métodos es muy utilizado en estudios educativos o sociales que establecen una relación entre teoría, utopía y realidad.

Encontraremos las siguientes fases dentro de nuestro sistema de metodología: Planteamiento de problema, revisión bibliografía, formulación de hipótesis, recolección de datos, interpretaciones,

conclusiones, generalizaciones de resultados para aumentar el conocimiento teórico. Todos estos pasos nos llevaran a los resultados que comprobaran nuestro planteamiento.

3.3. INSTRUMENTOS

Como se menciono anteriormente a parte de la técnica de test o pruebas aplicadas en los escenarios planteados, también utilizaremos la técnica de observación; la cual nos permite usar varios instrumentos para una mejor apreciación de los resultados que vamos a obtener.

Un instrumento es un recurso del cual nos valemos para obtener información, los principales instrumentos que se emplean en las técnicas de observación son: los registros de rasgos, las escalas estimativas, los registros anecdóticos y las entrevistas. Dentro de nuestro proceso utilizaremos los registros de rasgos ya que deseamos obtener las características principales de las redes Ad-Hoc, y las escalas estimativas que nos ayudaran a profundizar las características encontradas. A continuación hablaremos un poco de cada uno de estos términos.

Registro de rasgos

A través de un registro de rasgos se pretende reunir el mayor número de datos posibles acerca del funcionamiento de este tipo de redes; se trata de tomar nota de cuáles rasgos son característica suya y cuáles no, aunque de algunos no podrá definirse con toda claridad.

Podríamos decir que el registro de rasgos es un reflejo del funcionamiento que proporcionará un panorama general del escenario, de donde podremos partir para planear la promoción individual de cada equipo. Es importante tener en cuenta que, por medio de este registro, se trata de saber

solamente si la red posee o no el rasgo señalado, pero no podremos saber el grado en que lo posee.

Escalas Estimativas

Las escalas estimativas concentran la atención sobre una característica determinado exclusivamente, pero lo matizan de tal manera que se pueda conocer en qué grado ese rasgo es poseído. Es muy útil en caso de que deseemos un estudio más detallado sobre determinadas características.

Como principal instrumento hemos utilizado un emulador que nos ayudara a comprender de mejor manera el funcionamiento de este tipo de redes, el mismo funcionara en base a las técnicas nombradas con anterioridad:

3.3.1. MOBIEMU

MobiEmu es una herramienta para emular redes móviles ad hoc conectando a la red máquinas fijas. Esta herramienta puede emular prácticamente cualquier escenario de movimiento sin la necesidad de mover los nodos físicamente.

MobiEmu es una plataforma de software para probar y analizar en vivo como se comportan en la red los protocolos. El software usa una red fija de n ordenadores configurados en linux para emular una red móvil ad hoc de n nodos. La topología de conectividad entre nodos es dinámica ya que los nodos se mueven siguiendo un patrón.

El software imita un banco de pruebas de una red ad hoc real de forma dinámica poniendo o quitando filtros de paquete. El objetivo es crear la misma dinámica de red para el escenario de

prueba, de modo que las pruebas y el análisis ad hoc se conecten a una red que fácilmente puede ser ajustada en un laboratorio. También se puede controlar distinto software para cada máquina del banco de pruebas. La entrada es una historia de posiciones y movimientos de cada nodo. Con la componente de interfaz de usuario, se puede ver con anticipación, controlar, y visualizar la red ad hoc en acción. El usuario puede tratar de conectar las redes al software o bien realizar las pruebas reales de los n nodos independientes y moviéndose libremente con el mismo patrón.

El banco de pruebas de red

Cada anfitrión del banco de pruebas es un ordenador que emula un nodo móvil de la red ad hoc. Esto une a todos los otros nodos con una red dedicada (la red del banco de pruebas). La red del banco de pruebas puede ser cualquier tipo de redes locales, como Ethernet rápida o 802.11 LAN inalámbrico. Aunque físicamente la red del banco de pruebas no sea unida (conectada), el sistema MobiEmu hará cumplir una topología parcialmente unida (conectada) en la capa de enlace de transmisión.

El sistema MobiEmu funciona en una arquitectura de master/esclavo. El maestro está fuera de la red y controla a todos los esclavos y sincroniza sus acciones: el maestro dicta cuando la topología de conectividad debería cambiarse y los esclavos hacen cumplir esos cambios.

La comunicación de maestro/esclavo está sobre un canal de control. El canal de control debería ser separado de la red de banco de pruebas. Un escenario puede ser visualizado por una interfaz gráfica. El escenario es una lista de posición y definiciones de movimiento para todos los nodos.

MobiEmu acepta dos tipos de formato: el formato de un simulador de redes llamado NS2, y un formato simplificado. El primer formato es el mismo formato de movilidad que es usado en el NS2 para conectar una red al simulador con la extensión CMU inalámbrica. Es decir cualquier escenario generado por el instrumento “setdest” del CMU puede ser usado para conducir la emulación.

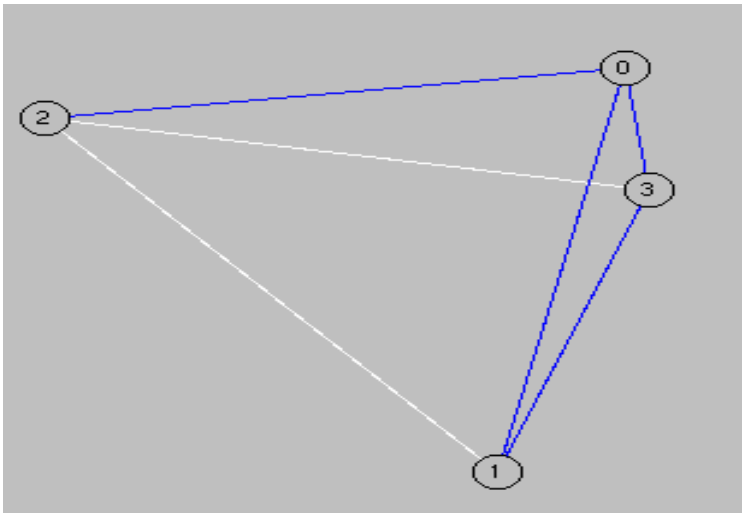

FIG. III.5 GUI DEL ESCENARIO MOBIEMU

Una vez que el escenario es cargado, se visualizará la red ad hoc sobre una interfaz gráfica, véase la figura III.1. Cada nodo se representa por un círculo con el número de nodo identificador. Si dos nodos están dentro del alcance de comunicación, les une una línea sólida azul. En caso contrario, estarán unidos por una línea gris. Durante la emulación, todos los nodos y eslabones se moverán según el argumento. Cada eslabón puede cambiar el color entre azul y gris cuando los dos nodos se mueven van rompiendo sus alcances. El usuario también puede decidir no mostrar cualquier tipo de eslabones para no cargar el escenario y ser más fácil de visualizar en el caso de tener muchos nodos.

En el sistema MobiEmu, los reguladores de esclavo son responsables de hacer cumplir la topología.

Filtrado de paquetes

El filtrado de paquetes es la técnica básica usada como criterio selectivo para dejar caer paquetes de red. Ya que el regulador de esclavo MobiEmu es puesto en práctica en Linux, se usan las “iptables” por facilidad de instalación. De la misma forma que se configuraron los escenarios para las primeras simulaciones estáticas, MobiEmu utilizará la misma técnica pero previamente configurado un patrón de movimiento. Los eslabones pueden ser puestos o quitados en cualquier momento con una orden. El esclavo MobiEmu usa esta interfaz para poner reglas con filtros y poner nodos fuera de su alcance.

Por ejemplo, si el nodo A está fuera del alcance del nodo B y el número MAC de A es 01:23:45:67:89:0a, MobiEmu pondrá la regla siguiente en B:

```
# iptables -t mangle -A PREROUTING -m mac --mac-source 01:23:45:67:89:0a -j DROP
```

Una vez se produce un movimiento y nuevamente pasa a tener alcance, el nodo B puede quitar la regla para permitir de nuevo comunicaciones entre estos nodos. Como vemos a continuación:

```
# iptables -t mangle -D PREROUTING -m mac --mac-source 01:23:45:67:89:0a -j DROP
```

3.4. VALIDACION DE RESULTADOS

En las tablas se presentan la operacionalización conceptual y metodológica de las variables, las mismas que se han identificado de acuerdo a la hipótesis, las mismas que nos ayudaran a:

- Operacionalización Metodológica

Variables	Categoría	Indicadores	Técnicas	Fuente de Verificación
V1. Independiente Problemas de Gestión	Compleja	I1. Capacidad de adaptación I2. Manejo de rutas I3. Manejo de Recursos	Observación Razonamiento Recopilación de información Análisis	Información bibliográfica (Libros, Internet, Tesis)

TABLA III.I: OPERACIONALIZACIÓN METODOLÓGICA DE LA VARIABLE INDEPENDIENTE

Variable	Categoría	Indicadores	Técnica	Fuente de Verificación
V2. Dependiente Rendimiento	Compleja	I4.Capacidad de envío I5.Capacidad de recepción I6. Paquetes perdidos	Pruebas Resultados Emulación Conclusiones	Emulación

TABLA III.II: OPERACIONALIZACIÓN METODOLÓGICA DE LA VARIABLE DEPENDIENTE RENDIMIENTO

3.4.1. DESCRIPCIÓN DE LAS VARIABLES Y SUS RESPECTIVOS INDICADORES

Para el estudio comparativo de protocolos de ruteo para redes móviles Ad-Hoc se determinaron varios indicadores que servirán de base para comparar las distintas capacidades de los mismos.

3.4.1.1. V1. VARIABLES INDEPENDIENTES: PROBLEMAS DE GESTIÓN

3.4.1.1.1. INDICADORES

I1. Capacidad de adaptación

Cuando la red presenta movilidad, se debe tomar en cuenta que se trabaja sobre una topología en constante cambio por debe ser capaz de adaptarse a los cambios constantes en sus tablas de ruteo.

Esto puede apreciarse en la cantidad de trafico capaz de manejar.

I2. Manejo de rutas

Al ser una red tipo mesh, se tiene múltiples caminos para la comunicación. El protocolo debe seleccionar un camino a seguir.

Esto se puede determinar en base al número de saltos que existe entre cada enlace al momento de seleccionar rutas.

I3. Ancho de banda

Al tener un manejo diferente de tráfico en la red, se puede constatar que existe una variación en el ancho de banda real que existe en cada caso. Este ancho de banda se expresa en Kbps o Mbps

3.4.1.2. V2. VARIABLE DEPENDIENTE: RENDIMIENTO

3.4.1.2.1. INDICADORES

I4.Capacidad de envío

Cada protocolo crea enlaces de diferente manera por ello solo envía la información si existe un enlace disponible.

De esta manera se contabiliza el número de paquetes que se lograron generar para el envío.

I5.Capacidad de recepción

Se refiere al número de paquetes que lograron llegar a su destino, de esta manera se los contabiliza al llegar al nodo receptor

I6. Paquetes perdidos

Por diferentes motivos como rutas inexistentes, colas, retrasos, etc. Los paquetes que no llegan a su destino se desechan o se caen en la red, de esta manera se los puede contabilizar.

3.4.2. POBLACION Y MUESTRA

Población

La población en este estudio está compuesta por todos los escenarios planteados para redes móviles Ad hoc y sus respectivos resultados.

Muestra

- Para el estudio de protocolos de enrutamiento para redes móviles AdHoc, la muestra estuvo constituido por los protocolos AODV, AOMDV, DSR, OLSR.
- Para determinar la capacidad de respuesta, la carga del protocolo las pruebas se las realizaron mediante la emulación de escenarios en MobiEmu en los cuales se implementara varios escenarios utilizando varios protocolos.

CAPITULO IV

ANALISIS Y RESULTADOS

4.1. RESULTADOS OBTENIDOS

Luego de haber realizado las pruebas mencionadas en el capitulo V, podemos mostrar los resultados obtenidos de acuerdo a cada uno de los escenarios planteados.

4.1.1. RESULTADOS ESCENARIOS

Escenario I

Las pruebas se realizan con los dos protocolos de encaminamiento iniciados entes de realizar el ping, para así poder ver cual de ellos tarda más en llegar del nodo S al nodo 4

		Número de saltos			
		1	2	3	4
AODV	min (ms)	0.198	0.407	0.673	0.925
	avg (ms)	0.328	0.572	0.832	1.081
	max (ms)	0.458	0.736	0.989	1.241
OLSR	min (ms)	0.109	0.239	0.490	0.741
	avg (ms)	0.346	0.424	0.614	0.867
	max (ms)	0.579	0.610	0.737	0.991

TABLA IV.I. RESULTADO DE TIEMPOS PARA LOS DIFERENTES NODOS

En la tabla IV.I podemos ver como va creciendo el retardo en función del número de nodos. Si nos fijamos en cada uno de los protocolos nos encontramos que para el caso del proactivo (OLSR) se obtienen unos tiempos más bajos. Esto se debe a que cuando se inicia el protocolo se intercambia rápidamente mensajes con el resto de nodos de la misma red para poder conocer la topología de red. Por eso cuando se hace el ping de 10 paquetes ya sabe donde se encuentra cada nodo. Al contrario que los protocolos reactivos que no conocen los caminos y primero deben descubrir la ubicación de cada nodo.

Escenario II

Una vez vistos los retardos que se introducen en función del número de saltos en el escenario hasta alcanzar a un nodo, pasamos a estudiar la pérdida de paquetes que se llega a tener cuando se produce una rotura de enlaces.

Después de realizar las pruebas con el comando traceroute podemos notar la diferencia entre el escenario que tiene la rotura con aquel que no tenia problemas de trafico En el protocolo AODV que fue el primero en ser utilizado, se realizara un ping de 100 paquetes desde la maquina S a la 3 y vemos que con el corte se produce la pérdida del 1%.

100 packets transmitted, 99 received, 1% packet loss, time 99041ms

Para el caso de OLSR se produce una pérdida de 7 de los 100 enviados. Cuando se produce el corte OLSR almacena los paquetes en un buffer y éste se congestiona a la espera de una nueva ruta; otros paquetes se pierden en el enlace caído.

En AODV la pérdida de de paquetes es del 1 % debido a que al producirse el corte reencamina antes por la nueva ruta (tal y como se demostrará en los escenarios siguientes

El escenario se crea a partir de las iptables y se forzará la rotura con ayuda de la misma herramienta. El envío de información será mediante un ping y para verificar el encaminamiento utilizamos el comando traceroute obteniendo los siguientes resultados..

Resultados AODV

Se le hace un traceroute a la ip del nodo 3 desde el nodo S antes de la rotura de enlace para ver que camino selecciona.

```
:~# traceroute 192.168.1.5
1 192.168.1.3 (192.168.1.3) 1.446 ms 0.167 ms 0.105 ms
2 192.168.1.5 (192.168.1.5) 1.735 ms 0.286 ms 0.239 ms
```

Una vez se fuerza la rotura del enlace con el siguiente comando:

```
# /sbin/iptables –t mangle –A PREROUTING –m mac –mac-source 00:0E:0C:5D:04:3E –j
DROP
```

Se verifica el nuevo encaminamiento:

:~# traceroute 192.168.1.5 Con la rotura del enlace

1 192.168.1.4 (192.168.1.3) 2.564 ms 0.161 ms 0.230 ms

2 192.168.1.6 (192.168.1.4) 0.365 ms 0.411 ms 0.490 ms

3 192.168.1.5 (192.168.1.5) 2.369 ms 0.550 ms 0.616 ms

Resultados OLSR.

Mismas pruebas realizadas para el protocolo OLSR. Vemos que el encaminamiento es el correcto.

ANTES DEL CORTE:

:~# traceroute 192.168.1.5

traceroute to 192.168.1.5 (192.168.1.5), 30 hops max, 38 byte packets

1 192.168.1.3 (192.168.1.3)

2 192.168.1.5 (192.168.1.5)

DESPUES DEL CORTE

:~# traceroute 192.168.1.5 Con la rotura del enlace

traceroute to 192.168.1.5 (192.168.1.5), 30 hops max, 38 byte packets

1 192.168.1.3 (192.168.1.3)

2 192.168.1.4 (192.168.1.4)

3 192.168.1.5 (192.168.1.5)

Nos encontramos con la diferencia del número de paquetes perdidos.

100 packets transmitted, 93 received, 7% packet loss, time 99039ms

Escenario III-a

Con el siguiente escenario se realizan pruebas para obtener unos valores concretos y así poder realizar una buena conclusión del funcionamiento.

Resultados AODV

Una vez montado el escenario se arranca el protocolo aodv (# aodvd –l –r 1 –i eth0) y vemos que éste rápidamente inicia el proceso de descubrimiento de ruta desde el nodo S al nodo 3. Se comprueba que al iniciar el envío de datos con la herramienta iperf no se pierden ningún paquete ya que los nodos S y 3 tienen visión directa entre ellos.

A continuación se muestra partes importantes del archivo aodvd.log generado por el nodo S.

Log del nodo S

10:56:11.154 hello_start: Starting to send HELLOs!

10:56:12.058 rt_table_insert: Inserting 192.168.1.5 (bucket 0) next

hop 192.168.1.5

10:56:12.059 nl_send_add_route_msg: Send ADD/UPDATE ROUTE to kernel:

192.168.1.5:192.168.1.5

10:56:12.059 rt_table_insert: New timer for 192.168.1.5, life=2100

10:56:12.059 hello_process: 192.168.1.5 new NEIGHBOR!

10:56:26.153 wait_on_reboot_timeout: Wait on reboot over!!

10:56:36.452 rt_table_insert: Inserting 192.168.1.3 (bucket 0) next hop 192.168.1.3

10:56:46.096 rreq_create: Assembled RREQ 192.168.1.5

10:56:46.096 log_pkt_fields: rreq->flags: rreq->hopcount=0 rreq->rreq_id=2

10:56:46.096 log_pkt_fields: rreq->dest_addr:192.168.1.5 rreq->dest_seqno=2

10:56:46.096 log_pkt_fields: rreq->orig_addr:192.168.1.2 rreq->orig_seqno=4

…

10:56:46.099 aodv_socket_process_packet: Received RREP

10:56:46.099 rrep_process: from 192.168.1.3 about 192.168.1.2->192.168.1.5

10:56:46.099 log_pkt_fields: rrep->flags: rrep->hcnt=2

10:56:46.099 log_pkt_fields: rrep->dest_addr:192.168.1.5 rrep->dest_seqno=3

10:56:46.099 log_pkt_fields: rrep->orig_addr:192.168.1.2 rrep->lifetime=1922

…

Como hemos podido observar en el aodvd.log, se ve en que momento los nodos que entran en la red van enviando mensajes HELLO para informar de su presencia. También se ve el proceso de descubrimiento de ruta con los mensajes de tipo RREQ y RREP que se están enviando y en que momento va insertando las nuevas rutas en su tabla de encaminamiento

Tabla de encaminamiento del nodo S

Time: 10:56:36.176 IP: 192.168.1.2, seqno: 1 entries/active: 1/1

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.77.9 192.168.1.5 1 VAL 1 2961 eth0

Time: 10:56:37.177 IP: 192.168.1.2, seqno: 1 entries/active: 2/2

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.1.3 192.168.1.3 1 VAL 1 1375 eth0

192.168.1.5 192.168.1.5 1 VAL 1 2960 eth0

En la tabla de encaminamiento se muestra la dirección destino a la que envía los paquetes de información (en este caso 192.168.1.5, que corresponde con el nodo 3). A todas las rutas se les va asignando un tiempo de vida para evitar calcular nuevamente su ubicación para cada envío de datos. En el caso de no utilizarse la ruta, el tiempo expiraría y se invalidaría automáticamente. En la tabla de encaminamiento también podemos ver el número de saltos que debe hacer cada paquete para alcanzar su destino (en este caso 1 salto, ya que es vecino). Vemos que al tener dos rutas en la tabla aparece en el estado de entradas activas 2 de 2. Vemos como el nodo S no conoce al nodo 2 debido a que no tiene cobertura con él y no es necesario para realizar su encaminamiento.

Cuando se fuerza la rotura del enlace directo entre el nodo S y 3, el protocolo debe iniciar un nuevo descubrimiento de ruta para alcanzar al destino.

Descubrimiento de Ruta para el nodo S

10:57:38.769 aodv_socket_process_packet: Received RERR

10:57:38.769 rerr_process: ip_src=192.168.1.3

10:57:38.769 log_pkt_fields: rerr->dest_count:1 rerr->flags=-

10:57:38.769 rerr_process: unreachable dest=192.168.1.5 seqno=10

10:57:38.769 rerr_process: removing rte 192.168.1.5 - WAS IN RERR!!

10:57:38.769 nl_send_del_route_msg:Send DELROUTE tokernel:192.168.1.5

10:57:38.769 rt_table_invalidate: 192.168.1.5 removed in 15000 msecs

10:57:38.769 rerr_process: Not sending RERR, no precursors or route in

RT_REPAIR

10:57:39.146 nl_callback: Got NOROUTE msg from kernel for 192.168.1.5

10:57:39.146 rreq_create: Assembled RREQ 192.168.1.5

10:57:39.146 log_pkt_fields: rreq->flags: rreq->hopcount=0 rreq-

>rreq_id=3

10:57:39.146 log_pkt_fields: rreq->dest_addr:192.168.1.5 rreq-

>dest_seqno=10

10:57:39.146 log_pkt_fields: rreq->orig_addr:192.168.1.2 rreq-

>orig_seqno=6

10:57:39.146 aodv_socket_send:AODV msg to 255.255.255.255 ttl=5size=24

10:57:39.146 rreq_route_discovery: Seeking 192.168.1.5 ttl=5

10:57:39.706 route_discovery_timeout: 192.168.1.5

…

Cuando se rompe una ruta se envía un mensaje de RERR para informar a los nodos de la invalidación de la misma y así poder ir actualizando sus tablas de encaminamiento.

Tabla de Ruta para el nodo S después de la rotura de enlace

Time: 10:56:44.181 IP: 192.168.1.2, seqno: 1 entries/active: 2/2

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.1.3 192.168.1.3 1 VAL 1 1566 eth0

192.168.1.5 192.168.1.5 1 VAL 1 2955 eth0

Time: 10:56:45.181 IP: 192.168.77.6, seqno: 2 entries/active: 2/1

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.1.3 192.168.1.3 1 VAL 1 2955 eth0

192.168.1.5 192.168.1.5 1 INV 2 14728 eth0

Time: 10:56:46.180 IP: 192.168.1.2, seqno: 4 entries/active: 2/2

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.1.3 192.168.1.3 1 VAL 1 2918 eth0

192.168.1.5 192.168.1.5 3 VAL 3 2955 eth0…

Al recibir el mensaje de RERR, el protocolo deja de utilizar la ruta directa a través de la cual veía al nodo destino a un salto y pasa a utilizar el otro camino posible realizando 3 saltos. Se ve como pone en estado INV (inválido) y como pasa de tener el contador de saltos de 1 a 3. Vemos ahora como el estado de rutas activas pasa a ser momentáneamente 1 de 2.

El tiempo que tarda en descubrir la nueva ruta es del orden de ms. Este valor no se puede apreciar bien en la tabla de enrutamiento (aodvd.rtlog) porque el mínimo intervalo de tiempo para refrescar los datos es de 1 s.

--- 192.168.1.5 ping statistics ---

100 packets transmitted, 98 received, 2% packet loss, time 99038ms

Podemos ver como se produce pérdida de paquetes cuando se rompe la ruta. El ping desde el nodo S al nodo 3.

Resultados OLSR

A diferencia de AODV se memoriza un solo archivo de texto en el que aparecen la tabla con los enlaces posibles, los vecinos y la topología de red vista desde cada nodo. Vemos que calcula correctamente la ubicación de cada nodo y sabe como llegar a cada uno de ellos.

Rutas del nodo S

--- 16:38:49.55 ----------LINKS

IP address hyst LQ lost total NLQ ETX

192.168.1.5 0.059 0.000 0 0 0.000 0.00

192.168.1.3 1.000 0.000 0 0 0.000 0.00

--- 16:38:49.55 ----------NEIGHBORS

IP address LQ NLQ SYM MPR MPRS will

192.168.1.3 0.000 0.000 YES YES YES 3

192.168.1.5 0.000 0.000 NO NO NO 3

--- 16:38:49.55 ----------TOPOLOGY

Source IP addr Dest IP addr LQ ILQ ETX

192.168.1.3 192.168.1.4 0.000 0.000 0.00

192.168.1.3 192.168.1.2 0.000 0.000 0.00

192.168.1.4 192.168.1.5 0.000 0.000 0.00

Se pasa a estudiar el caso de la figura IV.10 en la que se fuerza la rotura del enlace directo entre los nodos S y 3. A diferencia de AODV, no es necesario tener iniciado un envío de información entre los nodos S y 3 para que calcule una nueva ruta cuando se produce la rotura. Sin embargo si que se envían paquetes UDP del nodo S al nodo 3 para poder comparar después la pérdida de paquetes utilizando OLSR o bien AODV como protocolos de encaminamiento.

Rutas del nodo S después de la rotura de enlace

--- 16:38:54.66 ----------LINKS

IP address hyst LQ lost total NLQ ETX

192.168.1.3 1.000 0.000 0 0 0.000 0.00

--- 16:38:54.66 ----------NEIGHBORS

IP address LQ NLQ SYM MPR MPRS will

192.168.1.3 0.000 0.000 YES YES NO 3

--- 16:38:54.66 ----------TOPOLOGY

Source IP addr Dest IP addr LQ ILQ ETX

192.168.1.3 192.168.1.4 0.000 0.000 0.00

192.168.1.3 192.168.1.2 0.000 0.000 0.00

192.168.1.4 192.168.1.5 0.000 0.000 0.00

192.168.1.4 192.168.1.3 0.000 0.000 0.00

Cuando se anula la visión directa con el nodo 3 se encamina los paquetes hasta llegar al destino por la nueva ruta. Vemos como en la tabla ya desaparece como vecino el nodo 3 (ip: 192.168.1.5).

El tiempo que tarda desde que se da cuenta de la rotura hasta que reestablece su nueva ruta supera los 5s.

--- 192.168.1.5 ping statistics ---

100 packets transmitted, 94 received, 6% packet loss, time 99037ms

Con OLSR se produce una pérdida mayor de paquetes en comparación con AODV (6% frente a un 2%). OLSR tarda más tiempo en utilizar la nueva ruta y se produce una pérdida mayor mientras no utiliza la nueva ruta. AODV tiene que descubrir la nueva ruta cuando se produce el corte del enlace y consigue hacerlo en menos tiempo que OLSR, teniendo unas pérdidas menores

Escenario III-b

Una vez comprobado el buen funcionamiento de los protocolos encaminamiento, se pasa a estudiar sobre el escenario III-a con la incorporación de un nuevo nodo vecino y el restablecimiento del enlace roto entre los nodos S y 3.

Resultados AODV

Vemos como el protocolo detecta que el enlace con el nodo S se ha reestablecido y puede alcanzar al nodo 3 con un solo salto. El proceso comienza con el envío de un mensaje HELLO desde el nodo S al nodo 4 como veremos aodvd.log generado por el nodo S.

Descubrimiento de rutas para el nodo S

16:13:28.806 aodv_socket_process_packet: Received RREP
16:13:28.806 rrep_process: from 192.168.1.2 about 192.168.1.6-
>192.168.1.5
16:13:28.806 log_pkt_fields: rrep->flags: rrep->hcnt=3
16:13:28.806 log_pkt_fields: rrep->dest_addr:192.168.1.5 rrep-
>dest_seqno=7
16:13:28.806 log_pkt_fields: rrep->orig_addr:192.168.1.6 rrep-
>lifetime=5355
16:13:28.806 rt_table_insert: Inserting 192.168.1.5 (bucket 0) next
hop 192.168.1.2
16:13:28.806 nl_send_add_route_msg: Send ADD/UPDATE ROUTE to kernel:
192.168.1.5:192.168.1.2
16:13:28.806 rt_table_insert: New timer for 192.168.1.5, life=5355

16:13:35.482 route_expire_timeout: Route 192.168.1.5 DOWN, seqno=7

16:13:35.482 nl_send_del_route_msg:Send DELROUTE tokernel:192.168.1.5

16:13:35.482 rt_table_invalidate: 192.168.1.5 removed in 15000 msecs

Vemos como reconoce la nueva ruta y calcula el nuevo tiempo para alcanzar al nodo 4. También se le asigna un tiempo a la ruta anterior para que cuando esta expire se elimine de su tabla de encaminamiento.

Rutas de rutas del nodo 4

Time: 16:16:46.355 IP: 192.168.1.6, seqno: 5 entries/active: 2/2

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.1.5 192.168.1.2 4 VAL 12 155 eth0

192.168.1.2 192.168.1.2 1 VAL 1 1977 eth0

Time: 16:16:47.356 IP: 192.168.1.5, seqno: 5 entries/active: 2/1

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.1.5 192.168.1.2 4 INV 13 14155 eth0

192.168.1.2 192.168.1.2 1 VAL 1 2006 eth0

…

Vemos como la ruta pasa del estado VAL (válido) a estado INV (inválido).

Time: 16:16:58.378 IP: 192.168.1.5, seqno: 5 entries/active: 2/1

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.1.5 192.168.1.2 4 INV 13 3133 eth0

192.168.1.2 192.168.1.2 1 VAL 1 1258 eth0

Time: 16:16:59.379 IP: 192.168.1.6, seqno: 6 entries/active: 2/2

Destination Next hop HC St. Seqno Expire Flags Iface Precursors

192.168.1.5 192.168.1.2 2 VAL 13 4889 eth0

192.168.1.2 192.168.1.1 1 VAL 1 2448 eth0

Queda reflejado en la descripción anterior que la comunicación entre los nodos D y 3 necesitaba realizar 4 saltos y con la detección del nuevo enlace solo necesita hacer 2. El cálculo de la nueva ruta es del orden milisegundos, pero para que esta se vea reflejada en la tabla de encaminamiento tarda más de 13 segundos. La ruta más larga se conserva durante un determinado período de tiempo antes de ser invalidada. Por defecto en la configuración de parámetros de AODV es de 15000 ms.

Importante comentar que para que la ruta sea calculada es necesario que entre los nodos 4 y 3 haya una comunicación en todo momento. Esto es así porque el protocolo es reactivo y no calcula la ruta en caso de no tener que hacer uso de ella.

Resultados OLSR

Si sigue un buen funcionamiento, veremos como todos los nodos memorizan en su tabla la ruta más corta y podremos ver cuando tiempo tardan en hacerlo.

Pasamos a analizar el archivo de texto generado por el nodo 3 ya que es uno de los implicados en el envío de datos y nos aportará más información.

Ruta del nodo 3

--- 17:24:00.61 ----------LINKS

IP address hyst LQ lost total NLQ ETX

192.168.1.2 0.999 0.000 0 0 0.000 0.00

--- 17:24:00.61 ----------NEIGHBORS

IP address LQ NLQ SYM MPR MPRS will

192.168.1.2 0.000 0.000 YES YES NO 3

--- 17:24:00.61 ----------TOPOLOGY

Source IP addr Dest IP addr LQ ILQ ETX

192.168.1.2 192.168.1.3 0.000 0.000 0.00

192.168.1.2 192.168.1.6 0.000 0.000 0.00

192.168.1.3 192.168.1.4 0.000 0.000 0.00

192.168.1.3 192.168.1.2 0.000 0.000 0.00

192.168.1.4 192.168.1.5 0.000 0.000 0.00

192.168.1.2 192.168.1.3 0.000 0.000 0.00

Setting 192.168.1.6 as MPR

(ioctl)Deleting route with metric 4 to 192.168.1.5/255.255.255.255

via 192.168.1.2/eth0.

(ioctl)Adding route with metric 2 to 192.168.1.5/255.255.255.255 via

192.168.1.2/eth0.

--- 17:24:13.46 ---------- LINKS

IP address hyst LQ lost total NLQ ETX

192.168.1.2 1.000 0.000 0 0 0.000 0.00

--- 17:24:13.46 ---------- NEIGHBORS

IP address LQ NLQ SYM MPR MPRS will

192.168.1.2 0.000 0.000 YES YES NO 3

--- 17:24:13.46 ---------- TOPOLOGY

Source IP addr Dest IP addr LQ ILQ ETX

192.168.1.2 192.168.1.5 0.000 0.000 0.00

192.168.1.2 192.168.1.3 0.000 0.000 0.00

192.168.1.2 192.168.1.6 0.000 0.000 0.00

192.168.1.3 192.168.1.4 0.000 0.000 0.00

192.168.1.3 192.168.1.2 0.000 0.000 0.00

192.168.1.4 192.168.1.5 0.000 0.000 0.00

192.168.1.4 192.168.1.3 0.000 0.000 0.00

4.1.2. RESULTADOS EMULACIÓN

Emulación

La emulación es un proceso complementario mediante el cual podemos tener datos más exactos de los parámetros estudiados, ya que a diferencia de un simulador, que sólo trata de reproducir el comportamiento del programa, un emulador trata de modelar de forma precisa el dispositivo de manera que este funcione como si estuviese siendo usado en el aparato original. A continuación se muestran los resultados de las pruebas antes mencionadas.

Resultados Obtenidos

En estos gráficos está representado el número de paquetes y el instante de tiempo en segundos (s). Las gráficas resultantes están de forma acumulativa, es decir, es el resultado de sumar el número total de paquetes hasta el momento de la medida.

Se representa el número de paquetes que se envían en total, sin tener en cuenta si estos alcanzan su destino o si se pierden por el camino (Véase Fig.IV.1).

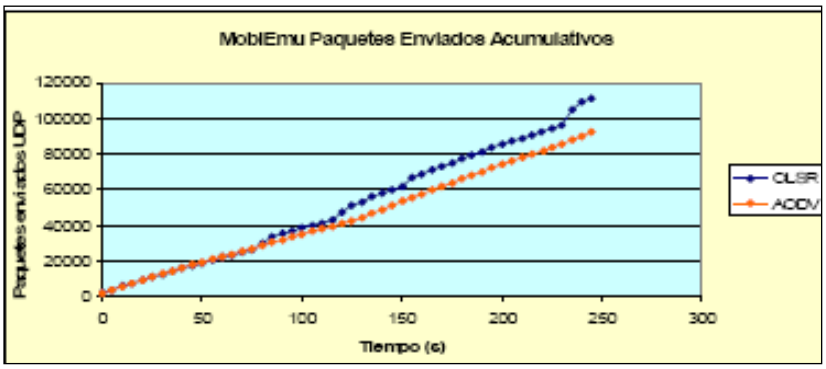

FIG. IV.6 TOTAL PAQUETES ENVIADOS EN LA SIMULACIÓN REALIZADA CON MOBIEMU

Como ya se ha comentado anteriormente, las gráficas representan la media de los paquetes enviados desde los distintos nodos configurados como clientes al servidor. En la gráfica de la figura IV.1 se muestra el resultado de ambos protocolos. Se observa que OLSR inyecta a la red más paquetes que AODV, pero no debemos realizar prejuicios por adelantado porque no se sabe por el momento si estos paquetes llegan a alcanzar a su destino. El hecho que AODV inyecte menos paquetes se debe a que cuando se rompe un enlace, recibe un

RERR y baja la tasa de envío hasta que no descubre una nueva ruta válida.

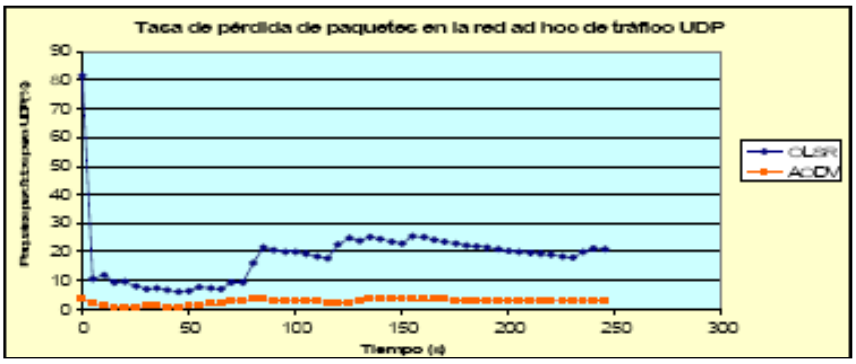

FIG. IV.7 TASA DE PÉRDIDA DE PAQUETES EN LA RED AD HOC DE TRÁFICO UDP EN LA SIMULACIÓN REALIZADA CON MOBIEMU

En la gráfica de la figura IV.2 se representa el número de paquetes que se pierden en porcentaje con respecto al número de paquetes enviados cuando se producen cortes. Las pérdidas en el caso de OLSR oscilan en torno al 20% y en el caso de AODV no alcanzan un 5%. Claramente OLSR pierde muchos más paquetes cuando congestiona el buffer y no encuentra una nueva ruta para enviar los paquetes; la razón es que OLSR tarda más en recalcular las rutas cuando un enlace está roto. Esto es muy perjudicial para las aplicaciones en tiempo real (voz, video, etc.) ya que la pérdida de muchos paquetes puede resultar crítica.

Vista esta gráfica, nos damos cuanta que OLSR inyecta mucho más paquetes que AODV en la red, pero sin embargo muchos de ellos no acaban de alcanzar a su destino.

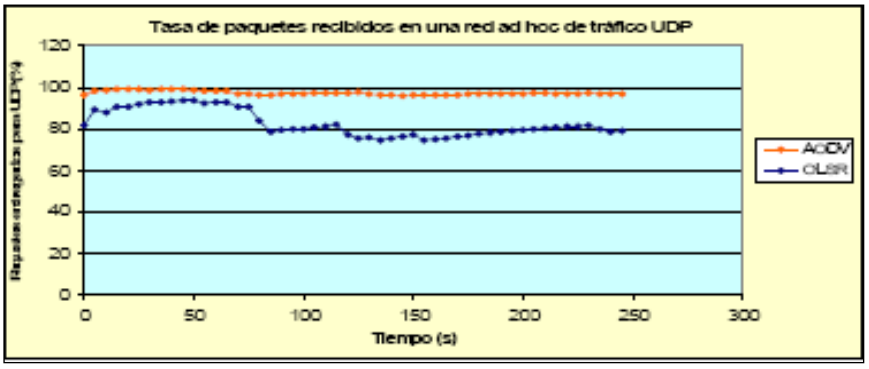

FIG. IV.8 PAQUETES QUE SE RECIBEN CORRECTAMENTE EN LA SIMULACIÓN REALIZADA CON MOBIEMU

La figura IV.3 representa el porcentaje de paquetes entregados al destino con respecto de los enviados. Gracias a la figura IV.3 y una vez vista las dos anteriores podemos sacar conclusiones en la comparativa de ambos protocolos. Como resultado tenemos que AODV entrega casi un 100% de los paquetes enviados y OLSR pasa de entregar un 90% a un 80% producido por los retardos en reencaminar nuevos paquetes cuando se rompen enlaces debido a la movilidad de la red ad hoc.

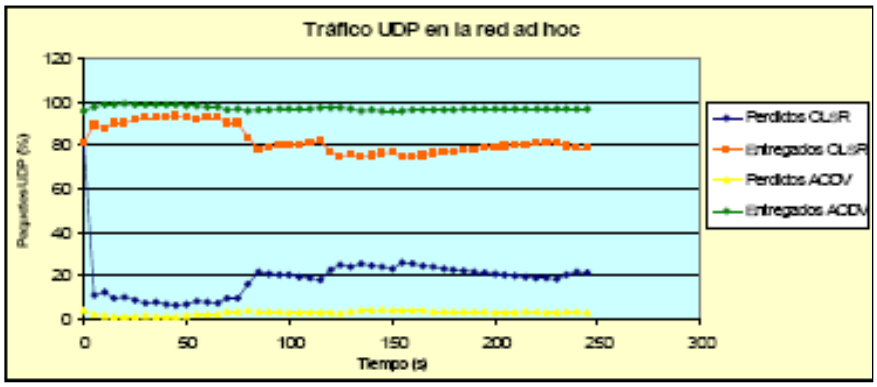

FIG. IV.9 MOBIEMU ANÁLISIS DE LOS PROTOCOLOS EN LA SIMULACIÓN REALIZADA CON MOBIEMU

Como resumen de las dos primeras gráficas y conclusión de las pruebas realizadas con MobiEmu tenemos lo que observamos en la figura IV.4. OLSR envía mucho más paquetes pero como contrapartida pierde también muchos más. Por el contrario con el protocolo AODV vemos que se envían menos paquetes al destino pero terminan por entregar muchos más al no tener tantas pérdidas.

FIG. IV.10 RESULTADOS DE ANCHO DE BANDA EN FUNCIÓN DEL TIEMPO EN LA SIMULACIÓN REALIZADA CON MOBIEMU

Como resultado del ancho de banda total obtenido al final de todas las simulaciones vemos que AODV consume más ancho de banda debido a que no pierde tantos paquetes de los que envía y entrega más paquetes al destino.

En cambio OLSR envía más paquetes pero al perder muchos de ellos deja de consumir tanto ancho de banda.

4.2. RESULTADOS RELEVANTES

Como se a mencionado con anterioridad, los resultados se evaluaran en tres grupos principales que son:

- Paquetes a nivel de aplicación
- Paquetes a nivel de protocolo
- Numero de Conexiones

Con cada uno de estos grupos se han planteado varios escenarios, para tener resultados mas precisos, así como también se a tomado un protocolo por cada grupo de acuerdo a su clasificación, en el caso de los protocolos reactivos se a tomado el AODV y en el de los proactivos el OLSR.

A partir de este planteamiento, podemos decir que los puntos relevantes que se han encontrado son:

- La aparición de redes ad-hoc y redes mesh conlleva un incremento de complejidad en las redes, que impacta en la gestión, de forma que aparecen nuevos problemas, como

son la configuración en un entorno heterogéneo y dinámico, la minimización de los recursos utilizados en la gestión, la escalabilidad, la adaptabilidad a cambios, la gestión en redes en localizaciones aisladas, y el *troubleshooting*.

A pesar de estos problemas, la actividad investigadora, aunque existe, no es muy grande, habiendo unos pocos trabajos de investigación en los últimos años en las distintas líneas mencionadas.

- El dinamismo de una red ad-hoc es un problema inherente a la misma, y que debe solucionar el protocolo de encaminamiento utilizado, ya que el tráfico crítico en una red es el tráfico de datos.

- El tráfico de gestión siempre debe tener menos prioridad que el de datos, por lo que no parece tener mucho sentido diseñar sistemas de gestión que utilicen sus propios protocolos de encaminamiento con el fin de solucionar un problema de dinamismo.

4.3. EVALUACION DE PROBLEMAS

Las características particulares de las redes ad-hoc y mesh hacen que la gestión de estas redes presenten distintos problemas o retos, que dejan abiertas puertas a la investigación:

- Configuración de los equipos, dada la heterogeneidad, dinamismo, sensibilidad a ruidos e interferencias
- Necesidad de minimizar los recursos utilizados por el tráfico de gestión-Escalabilidad, dado que las redes ad-hoc en el futuro podrían tener millones de nodos

- Adaptabilidad a cambios
- En algunos casos, cuando se utilizan redes mesh en localizaciones aisladas, la forma de acceder a ellas (radioenlace o WIMAX) supone un problema añadido
- Troubleshooting, dada la complejidad y posibles puntos de fallos de estas redes.

4.4. EVALUACION DE SOLUCIONES

A partir de los problemas mencionados, han aparecido varias ideas de soluciones o posibles campos de investigación futura:

Configuración

La puesta en marcha requiere la configuración de múltiples parámetros. Aunque se puede configurar un router por la interfaz web provista por el *firmware*, algunos parámetros, como el SSID o el canal, afectan a toda la red, y un cambio en uno puede tener efectos instantáneos en todos los routers de la red.

Se propone una herramienta (MAYA) diseñada para la gestión y la configuración de redes mesh, la cual requiere tener conectividad con cualquiera de los nodos mesh y genera muy poco tráfico.

Para la heterogeneidad y el alto número de nodos se propone un método de configuración definiendo una ontología para chequear sus posibles problemas y simular nuevas configuraciones para toda la red, de forma que puedan detectarse problemas.

También es importante la capacidad de autoconfiguración, en el sentido de que estas redes son mucho más dinámicas que las redes LAN /WLAN convencionales, donde los nodos pueden entrar o salir, o variar de posición de manera mucho más dinámica. Los protocolos de autoconfiguración usados habitualmente necesitan mejorarse, tanto para responder eficientemente a los nuevos cambios, como para no absorver los recursos de la red.

Se propone a la vez un método de descarga automática de servicios y protocolos por los nodos mesh, antes determinadas condiciones de contexto. Es por tanto un avance en donde no sólo se provisionan parámetros, sino que incluso se actualiza el software necesario, en función del contexto.

Minimización de recursos utilizados

Un problema importante de las redes mesh es que generalmente, los recursos (capacidad de procesamiento, ancho de banda, alimentación) son escasos. Es fundamental por lo tanto, minimizar los recursos utilizados por el tráfico de gestión.
Se propone que en lugar de gestionar todos los nodos durante todo el tiempo, se gestionen un subconjunto de ellos, elegidos por probabilidad. Así se ahorra ancho de banda.

Escalabilidad

Los actuales estándares no permiten muchos nodos, pero es de suponer que en el futuro, podrían darse redes ad-hoc de millones de nodos. Por lo tanto, es crítica la capacidad de gestionar la configuración en redes tan grandes.

En general, muchas de las propuestas de gestión de este tipo de nodos son descentralizadas o distribuidas.

Adaptabilidad a cambios

Algunas propuestan tratan de conseguir la adaptabilidad de la red a cambios utilizando P*olicy based network management* (PBNM) aplicando políticas las cuales básicamente son reglas con una condición de triller, que siguen el comportamiento "*Si* condición *entonces* acción".
En este sentido hay varias propuestas, como por ejemplo de gestión de la topología, gestión de nodos con mal funcionamiento o *autogestión* de nodos, reconfigurando parámetros de conectividad en función del contexto.

Localizaciones aisladas

Otro punto interesante a tener en cuenta es que una topología común para el uso de redes mesh es en localizaciones aisladas, para lo cual se necesita llegar a la localización mediante un radioenlace, o un acceso WIMAX.

Troubleshooting

Una vez detectado un problema mediante el sistema de gestión, éste debe solucionarse. El proceso de encontrar y solucionar un problema se denomina *troubleshooting*. El *troubleshooting* en redes ad-hoc presenta desafíos con respecto a las redes cableadas y a las redes *gíreles* tradicionales, debido principalmente a la variabilidad de la topología y heterogeneidad de la red.

Se propone un sistema mediante el que se reproduce la red en un simulador, y se reproducen en éste las condiciones de fallo, procesando los resultados para obtener las causas más probables del mismo.

Hay que destacar como nota interesante que varias propuestas utilizan la teoría de redes sociales a la gestión de redes mesh, calculando los nodos más interesantes de la red y teniéndolos en cuenta.

4.5. POLITICAS DE GESTION REDES AD-HOC

Luego de haber realizado las pruebas mencionadas, es un objetivo importante de este trabajo de investigación sugerir unas políticas de gestión para un mejor uso de las redes Ad-Hoc., se han tomado 5 puntos relevantes que deben ser revisados antes de diseñar una red Ad-hoc.

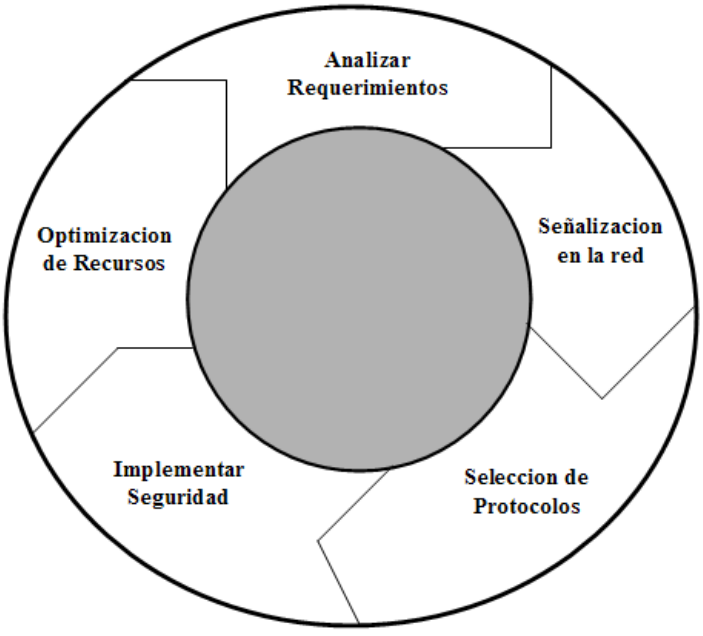

FIG. IV.11. FASES EN POLÍTICAS DE GESTIÓN REDES AD-HOC

FASE 1

ANALIZAR REQUERIMIENTOS

- Se debe analizar las metas a cumplir con el diseño de la red y el campo que se desea alcanzar
- Analizar de igual manera los pros y contras con las metas planteadas
- Caracterizar la red existente
- Caracterizar el trafico de la red

FASE 2

SEÑALIZACION DE LA RED

- Diseñar una topología de la red
- Diseñar modelos de direccionamiento y nombres
- Desarrollar estrategias para el mantenimiento de la red

FASE 3

SELECCIÓN DE PROTOCOLOS

- Seleccionar protocolos de conmutación y enrutamiento que se adapten de la mejor manera a los desafíos planteados, de esta manera los resultados serán los óptimos.
- Seleccionar tecnologías y dispositivos para las redes de cada nivel que se encuentren dentro de nuestro diseño.

- Seleccionar tecnologías y dispositivos para la red corporativa o red principal de nuestro sistema.

FASE 4

IMPLEMENTAR SEGURIDAD

- Identificar los recursos y bienes en la red para de esta manera analizar los riesgos de seguridad que existen.
- Las propuestas de seguridad se centran en aspectos concretos del problema a solucionar, se puede proponer una arquitectura distribuida y cooperativa para la detección de intrusiones que utiliza un modelo de detección de anomalías.
- Se debe dejar claro lo que se desea de los usuarios mediante políticas de uso, que deben ser diseñadas por un equipo de desarrollo de políticas de seguridad.
- El empleo de técnicas de detección dependerá siempre de las características de la aplicación y del escenario concreto sobre el que dicha aplicación se ejecuta

FASE 5

OPTIMIZACION DE RECURSOS

- Probar el diseño de la red con varias pruebas de trafico de red.
- Realizar un plan de contingencias el cual podremos implementar en caso de desastre de esta manera nuestra red aumenta su nivel de seguridad.

- Llevar un control permanente de los cambios que sufren nuestra red a lo largo de su vida, asi como también como se encuentran definida la información por parte de cada entidad.
- Documentar el diseño de la red de la manera mas clara y precisa.

Las redes Ad-hoc se encuentran en constante movimiento, lo que nos indica que nuestra red va a tener continuos cambios. Cada una de las fases mencionadas anteriormente, forman un ciclo que debe repetirse constantemente para que las políticas mencionadas nos ayuden a una verdadera optimización

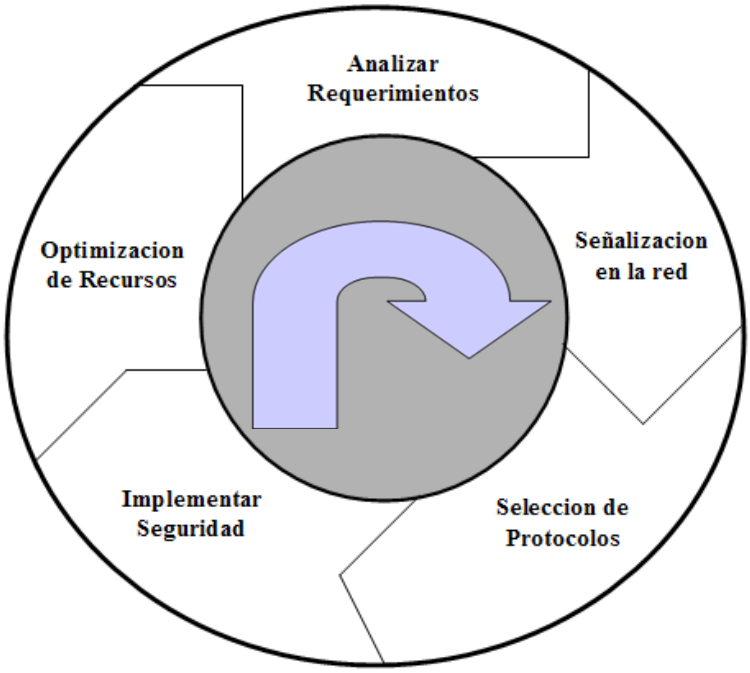

FIG. IV. 12. CICLO DE POLÍTICAS DE GESTIÓN REDES AD-HOC

CAPITULO V

MARCO PROPOSITIVO

5.1. AMBIENTES DE IMPLEMENTACION

El ambiente de la red ad hoc Manet Mesh que se utilizara se estructuró de la siguiente manera, tal como se observa en la figura V.1:

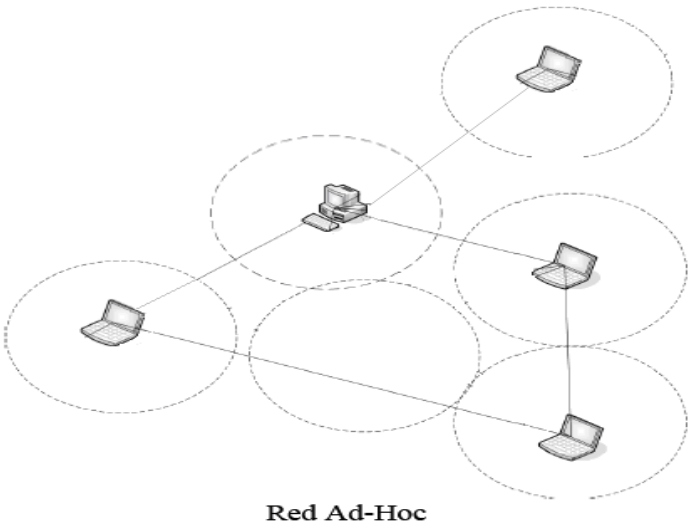

FIGURA V.13 ESTRUCTURA DE IMPLEMENTACIÓN

Una red Ad-Hoc conforma una malla, pero se necesita enrutamiento para entender a los vecinos, entonces hay que agregar protocolos. Existen una gran cantidad de protocolos de encaminamiento para las redes Ad Hoc, los cuales pueden ser revisados con mayor detenimiento en el capítulo 2. Como ya lo mencionamos estos protocolos se pueden dividir entres grandes grupos en función del método que utilizan para determinar las rutas

- Protocolos reactivos
- Protocolos proactivos
- Protocolos híbridos

Protocolos reactivos

Los protocolos de encaminamiento reactivo o bajo demanda son aquellos en los cuales se hallan las rutas entre un nodo origen y un nodo destino bajo demanda de la fuente. Es decir, que sólo cuando sea necesario iniciar una transmisión se buscará una ruta para realizarla.

Una vez establecida la ruta, los nodos que participen en la transmisión se encargarán de su mantenimiento. Las ventajas de este tipo de protocolos es que no necesitan demasiada señalización, lo cual reduce el *overhead* y optimiza el uso de las baterías, al contrario de lo que sucede con los protocolos proactivos. Sin embargo, el tiempo de establecimiento de las rutas es mayor, ya que cuando se necesita la ruta se inicia el mecanismo de descubrimiento de ruta y hasta que éste no termina no se puede iniciar la transmisión.

Hay una gran cantidad de protocolos de encaminamiento reactivos, las diferencias entre ellos se encuentran en la implementación del mecanismo de descubrimiento de ruta y en las optimizaciones del mismo. Los protocolos reactivos más importantes son los siguientes:

- Ad Hoc On Demand Distance Vector Routing (AODV), 2003
- Associativity-Based Routing (ABR), 1996
- Cluster-Based Routing Protocol (CBRP), 1999
- Dynamic MANET On demand (DYMO), 2005
- Dynamic Source Routing (DSR), 2004
- Location-Aided Routing (LAR), 1998
- Temporally Ordered Routing Algorithm (TORA), 2001

De ellos los protocolos AODV y DSR han sido presentados como RFC (*Request for Coments*) experimentales, mientras que del resto se han presentado como *Draft* por el IETF (*Internet Engineering Task Force*) los protocolos ABR, CBRP, DYMO y TORA. Aunque el DYMO está siendo considerado por el MANET-WG para convertirse en RFC.

Protocolos proactivos

Los protocolos de encaminamiento proactivos intentan mantener tablas de las rutas actualizadas constantemente. Eso significa que cada nodo debe mantener actualizada una tabla con todas las rutas hacia los otros nodos. La información que contienen las tablas debe actualizarse periódicamente y ante cualquier cambio de la tipología de red.

Esta actualización constante provoca que estos protocolos generen una gran cantidad de paquetes de señalización (*overhead*) lo cual afecta a la utilización del ancho de banda, el *throughput* y el consumo de energía entre otras cosas. La ventaja principal que aportan estos protocolos es que el establecimiento de una nueva ruta para iniciar una transmisión precisa de un tiempo muy pequeño al tener todos los nodos las tablas de rutas actualizadas. Además, el *overhead* aunque sea elevado también es bastante estable en el tiempo. El principal problema con el que se encuentran estos protocolos es cuando las redes son muy densas y los nodos tienen una movilidad alta ya que en estos casos el *overhead* crece muy rápidamente y las tablas pueden llegar a ser demasiado grandes.

Los distintos protocolos de encaminamiento proactivos de distinguen entre ellos por el número de tablas, la información que contienen las tablas y en como se actualizan éstas. Los protocolos proactivos más destacables son los siguientes:

- Adaptative Distance Vector (ADV), 2000
- Cluster Gateway Switch Routing (CGSR), 1999
- Destination-Sequenced Distance Vector (DSDV), 1994
- Distance Routing Effect Algorithm for Mobility (DREAM), 1998
- Hierarchical State Routing (HSR), 2000
- Multimedia support in Mobile Wireless Networks (MMWN), 1998
- Optimised Link State Routing (OLSR), 2003
- Source-Tree Adaptaive Routing (STAR), 1999
- Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), 2004
- Wireless Routing Protocol (WRP), 1996

De los cuales, los protocolos OLSR y TBRPF han sido presentados como RFC experimentales, mientras que del resto se han presentado como *Draft* por el IETF los protocolos ADV, CGSR, HSR y STAR.

Protocolos híbridos

Este grupo de protocolos híbridos se basan en combinar las características de los dos grupos anteriores para intentar aprovechar las ventajas de ambos.

En general su funcionamiento se basa en agrupar los nodos en grupos o zonas, de esta manera cuando necesitan descubrir rutas hacia otro nodo de su zona utilizan un encaminamiento proactivo y para descubrir rutas en nodos lejanos utilizan un encaminamiento reactivo.

Dentro de este grupo de protocolos existen algunos ejemplos como los siguientes:

- Scalable Location Update Routing Protocol (SLURP), 2004
- Zone-based Hierarchical Link State (ZHLS), 1999

Estudio y análisis de prestaciones de redes móviles Ad Hoc mediante simulaciones NS-2 para validar modelos analíticos.

- Zone Routing Protocol (ZRP), 2002

De estos tres protocolos sólo se ha presentado como *Draft* por el IETF el protocolo ZRP.

5.2. IMPLEMENTACION DEL ESCENARIO ESCOGIDO

El escenario establecido para implementar constara de un “cluster”, que se ha configurado bajo el sistema operativo Linux. Se trata de un conjunto de ordenadores que se encuentran interconectados trabajando conjuntamente o bien por separado según se especifique, en este caso actuaran como 5 equipos móviles y actuaran como nodos Ad-hoc, la configuración en el cluster se realizara según los programas y escenarios de análisis escogidos.

Nuestro escenario se presentara de la siguiente manera:

SunS:

Dirección MAC: 00:0E:0C:5C:F8:38

Dirección IP: 192.168.1.2

Sun1:

Dirección MAC: 00:0E:0C:5D:04:4B

Dirección IP: 192.168.1.3

Sun2:

Dirección MAC: 00:0E:0C:5C:F9:98

Dirección IP: 192.168.1.4

Sun3:

Dirección MAC: 00:0E:0C:5C:F9:BC

Dirección IP: 192.168.1.5

Sun4:

Dirección MAC: 00:0E:0C:5C:F9:B8

Dirección IP: 192.168.1.6

5.3. VARIABLES DE ANALISIS

Las redes Ad-hoc poseen protocolos de QoS que se basan en buscar rutas con los recursos suficientes para satisfacer los requerimientos establecidos. Su función no es otra que la de intentar garantizar la comunicación dentro de una red MANET. Para ello deben intentar que la comunicación extremo a extremo cumpla una serie de restricciones como: el retardo, la variación del retardo, el ancho de banda mínimo necesario o una combinación de estos parámetros.

Esta misión es muy difícil de conseguir en las redes MANET debido al *overhead* introducido, así que tienen que intentar encontrar un compromiso entre el *overhead* introducido y los beneficios obtenidos.

También deben combatir contra la dificultad de mantener información precisa sobre el estado de los enlaces debido a la naturaleza móvil de los nodos. Además, durante la comunicación la QoS tampoco se puede garantizar que se mantenga estable sino más bien todo lo contrario, así que los protocolos deben buscar rápidamente una nueva ruta en caso de romperse un enlace.

Existen algunos protocolos dentro de este grupo, algunos de los más conocidos son los siguientes:

- Core-Extraction Distributed Ad hoc Routing (CEDAR), 1999
- Flexible QoS Model for MANET (FQMM), 2000
- QoS Optimized Link State Rounting (QOLSR), 2006
- Ticket-based Probing (TBP), 1999

De ellos sólo el QOLSR ha sido presentado como *Draft* por el IETF.

5.4. PRUEBAS REALIZADAS

En este proyecto se estudia a fondo el funcionamiento de las redes ad hoc con el fin de conocer el comportamiento de las mismas en diferentes escenarios y con dos protocolos de encaminamiento.

De esta manera comprobaremos los principales problemas de tráfico que se presentan lo que nos llevara a concluir los resultados en su Gestión de Red. Como mencionamos anteriormente se realizaran pruebas en escenarios físicos y simulados para tener

5.4.1. HERRAMIENTAS UTILIZADAS

Para realizar todas las pruebas se han utilizado 5 equipos con sistema operativo Linux que se encuentran formando parte de un equipo dentro de un cluster, para los escenarios que describiremos posteriormente se han utilizado algunas herramientas para obtener datos de conocimiento de rutas, y de manejo de recursos en la red; dentro de cada escenario se utilizara un estudio con 2 tipos, un protocolo por cada tipo dentro de su clasificación.

Protocolos Utilizados

- **Reactivo: AODV**

Se ha seleccionado el protocolo AODV-UU, la versión utilizada es la última hasta el momento (AODV-UU 0.9.1).

Características:

- Funciona bien sobre el kernel 2.4.x o superior
- Cumple el estándar RFC3561.
- Soporta múltiples interfaces de red

Esta implementación nos facilita el estudio guardando unos archivos de texto en los que queda reflejado todos los movimientos de paquetes para cada nodo.

- **Proactivo: OLSR**

La implementación más conocida y probada de este software es la olsrd-0.4.9. Implementación creada por Andreas Tønnesen de la University Graduate Center.

Características:

- Funciona bien sobre el kernel 2.4.x o superior
- Cumple las especificaciones de RFC 3626 .

Este software nos va mostrando por pantalla todos los movimientos de paquetes que realiza cada nodo, con la opción de guardarlo en archivos de texto.

IPERF

Iperf es una herramienta diseñada para medir el rendimiento del ancho de banda vía TCP y UDP. Con iperf podemos saber cuantos mensajes de información se están perdiendo, cuando se producen cortes en los diferentes escenarios estudiados, etc.

Para cada simulación se configura un nodo como servidor y el resto como clientes. De esta forma todos los nodos se estarán enviando mensajes de información entre ellos.
Se pueden hacer diversas mediciones con Iperf, todo depende de los parámetros que utilicemos. Esta herramienta muestra en que instante de tiempo se producen las pérdidas de paquetes, lo que ha resultado útil para valorar cual de los dos protocolos se comporta mejor en estas situaciones.

Algunas de sus características son:

TCP

- Medida del ancho de banda.
- Reporta el tamaño de MSS/MTU.
- Soporte para ventana de TCP vía socket buffers.
- Conexiones múltiples simultáneas.

UDP

- El cliente puede crear flujos UDP y especificar su tamaño.
- Medida de pérdida de paquetes.
- Soporta Multicast.
- Conexiones múltiples simultáneas.

Opciones que se han utilizado:

- -f [bkmBKM] Especifica las unidades con las que desplegará el resultado
  b bits / s B Bytes / s
  k kilobits / s K KiloBytes / s
  m megabits / s m MegaBytes / s
- -i <segundos> Especifica un intervalo de tiempo en segundos en el cual volverá a hacer la medición
- -u Utiliza UDP en vez de TCP
- -t <segundos> Tiempo que dura la transmisión
- -c <host> Para configurar al cliente conectándose al host

ETHEREAL

El analizador de protocolos Ethereal se ha utilizado para controlar todo el intercambio de paquetes entre las distintas máquinas. Esta herramienta captura todos los paquetes que entran y

salen de la tarjeta de red. Así nos facilita el poder ver en que momento y que tipo de paquete se están intercambiando las máquinas.

IPTABLES

Las iptables se han utilizado para configurar los primeros escenarios. Al tratarse de pruebas de laboratorio y con escenarios estáticos dentro de la misma interfaz de red, no se contemplan problemas de cobertura. Todos pueden tener conexión con todos los nodos y por ello se va a simular distancias con la configuración de los firewalls.

Es importante tener en cuenta que se realiza un filtrado a nivel MAC para el aislamiento a nivel de la capa de enlace. A tener en cuenta que si se realiza un filtrado por IP sencillamente no funcionaría el encaminamiento.

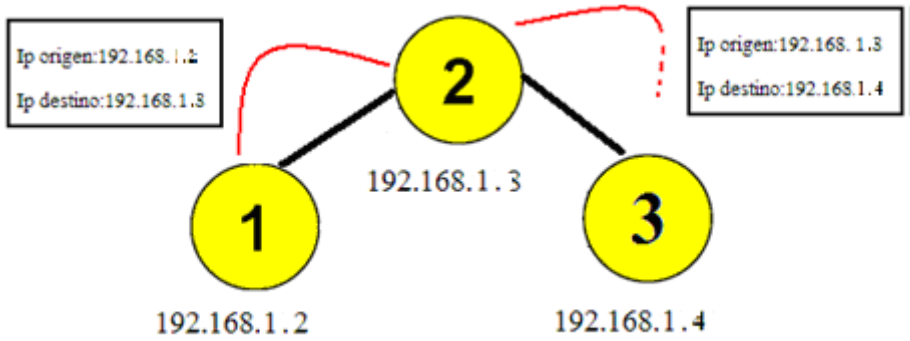

FIG. V.14 EJEMPLO DE FILTRADO IP

En la figura V.3 se hace un filtrado IP entre el nodo 1 y 3. Si se envía un mensaje al nodo 3 desde el nodo 1, nunca llegará a su destino aunque pase por el nodo 2. Esto sucede porque el mensaje de información contiene la dirección IP del nodo origen.

Una vez instalado el paquete de la iptables necesario, deberemos utilizar los siguientes comandos:

/sbin/iptables –t mangle –F PREROUTING

Borra todas las reglas que se hayan configurado previamente.

/sbin/iptables –t mangle –A PREROUTING –m mac –mac-source
00:00:00:00:00:00
–j DROP

Crea una regla para no tener una visión con el nodo de la MAC indicada.

/sbin/iptables –t mangle –D PREROUTING –m mac –mac-source
00:00:00:00:00:00
–j DROP

Elimina la regla que previamente se ha creado para volver a tener visión con el nodo de la MAC indicada.

5.4.2. PRUEBAS

Escenario I

El primer escenario se utiliza para ver los retardos producidos por la necesidad de realizar un mayor número de saltos. Consiste en un escenario con una configuración lineal en el que los nodos de la red solo tienen cobertura con sus nodos vecinos, tal como se muestra en la figura V.3.

Por lo que el nodo S solo tiene cobertura con el nodo 1, el nodo 1 con el nodo S y 2, etc. La otra herramienta necesaria ha sido la utilización del siguiente comando:

ping 192.168.77.1 –c 10 _ ping de 10 paquetes al nodo 1

Con el comando ping se envía del nodo S al resto de nodos paquetes para ver los retardos. Una vez realizada esta operación y repetida 10 veces, se hace una media de los resultados.

En el caso de AODV para cada primer ping de los 10 totales el nodo fuente (nodo S) necesitará iniciar un proceso de descubrimiento de ruta y para enviar los 9 restantes consultará las tablas de encaminamiento. En el caso de OLSR ya conoce la topología de red antes de iniciar el envío.

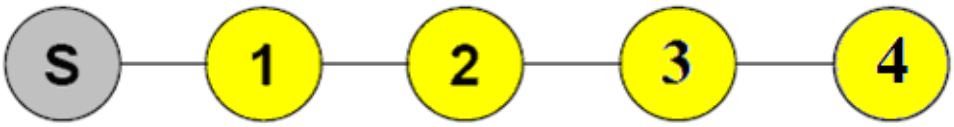

FIG. V.15 ESCENARIO LINEAL CON 5 NODOS

Hay que recordar que el protocolo (AODV) no conocen la topología de la red y cuando quieren enviar información deben descubrir primero donde están esos nodos.

Se da un caso para el primer salto en el que encontramos los tiempos más bajos para AODV, debido a que todos los nodos conocen a sus vecinos porque se intercambian mensajes de HELLO y no necesitan descubrirlos.

Escenario II

Se creara un nuevo escenario que nos dará la posibilidad de escoger entre dos caminos para alcanzar a un mismo destino. Cuando se inicie un envío de información entre los nodos S y 3 (Véase Fig.V.4) el protocolo deberá encaminar por la ruta más corta para hacer un uso eficiente. Cuando haya comenzado a encaminar los paquetes por el enlace entre 1- 3 se forzará una rotura del mismo.

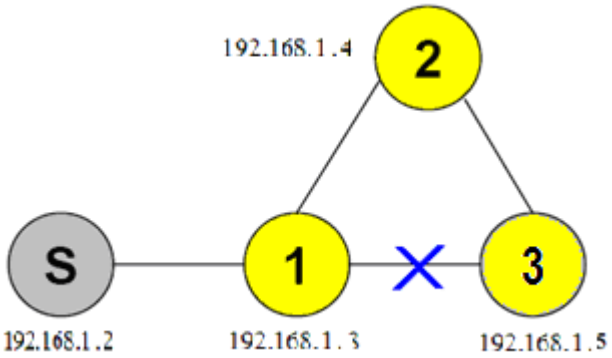

FIG. V.16 ESCENARIO II CON ROTURA DE ENLACE 1 Y 3.

Cuando se produce esta rotura, debe encaminar los paquetes por la otra posible ruta para no perder la comunicación. Se pasará a ver cual de los protocolos cambia antes de ruta al detectar el error.

Escenario III-a

En este escenario se fuerza una rotura de enlace para obligar a utilizar otras rutas y se añade un nuevo nodo para ver como esta se comporta. De esta forma se pude calcular los tiempos de descubrimientos de rutas y de detección de nuevos vecinos.

Para analizar a fondo estos nuevos escenarios, se pasa a mirar los archivos que genera cada uno de los protocolos.

Para crear el escenario de la figura V.5 y darle la movilidad se utiliza la herramienta de las iptables. Todos los comandos utilizados se irán comentando para no perder detalle de las pruebas realizadas.

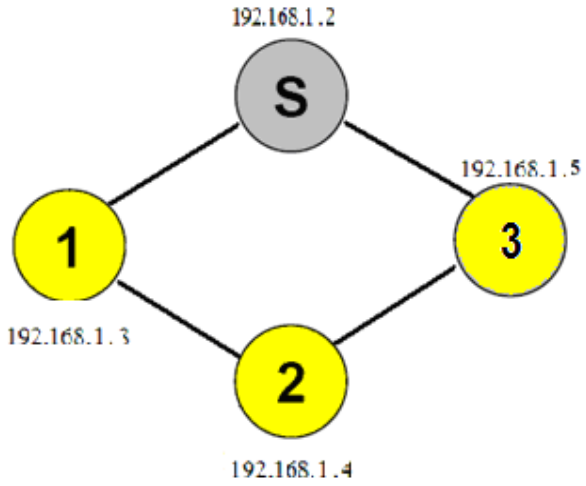

FIG. V.17 ESCENARIO III-A. TOPOLOGÍA CIRCULAR

A continuación se muestra el comando que se ha utilizado para realizar el filtrado desde el nodo S para anular la cobertura con el nodo 2.

```
# /sbin/iptables –t mangle –F PREROUTING
# /sbin/iptables –t mangle –A PREROUTING –m mac –mac-source 00:0E:0C:5C:F8:28 –j
DROP
```

Una vez realizado el filtrado MAC se utiliza la herramienta de iperf para enviar información entre la fuente (nodo S) y el destino (nodo 3). El nodo configurado como cliente (nodo S) hace peticiones al nodo configurado como servidor (nodo 3).

:~# iperf –s –u _Desde el nodo configurado como Servidor (nodo 3)

:~# iperf -c 192.168.1.2 -u -i 1 -r -t 100 Desde el nodo configurado como cliente (nodo S)

Con la herramienta iperf se está enviando información entre los nodos S y 3 de tipo UDP. Como es de esperar los dos protocolos de encaminamiento seleccionaran el camino más corto para el envío de datos. Para este escenario se forzará la rotura del enlace entre el nodo S y 3 (Véase figura V.6) en el que los protocolos tendrán que utilizar el la ruta alternativa para continuar con la comunicación.

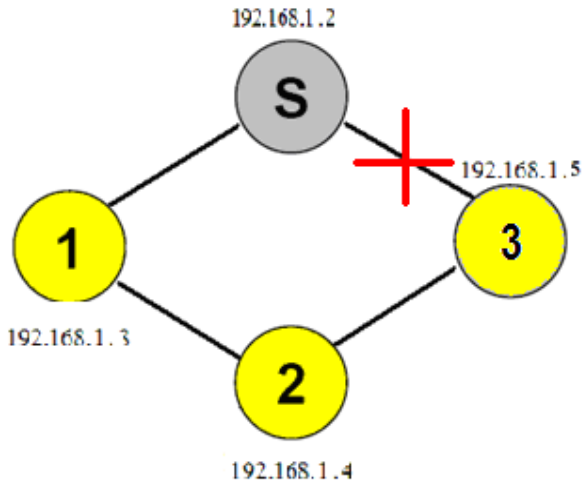

FIG. V.18 ANILLA CIRCULAR CON CORTE

En los siguientes apartados se verá como funcionan los protocolos con ayuda de los archivos que ellos mismos generan y se realiza la comparativa entre ambos.

Escenario III-b

El escenario de la figura V.5 dará lugar al escenario de la figura V.7. Con esta nueva configuración de escenario, se forzará un envío de información entre los nodos 3 y 4. Los mensajes del nodo 4 al nodo 3 (que se acaba de incorporar a la red) pasaran por todos los nodos de la red hasta alcanzar su destino. Cuando se reestablece el enlace directo entre los nodos S y 4, se estará dando la posibilidad de utilizar una ruta más corta para continuar la comunicación. Veremos como se comporta cada protocolo ante la posibilidad de hacer un uso eficiente utilizando el camino más corto.

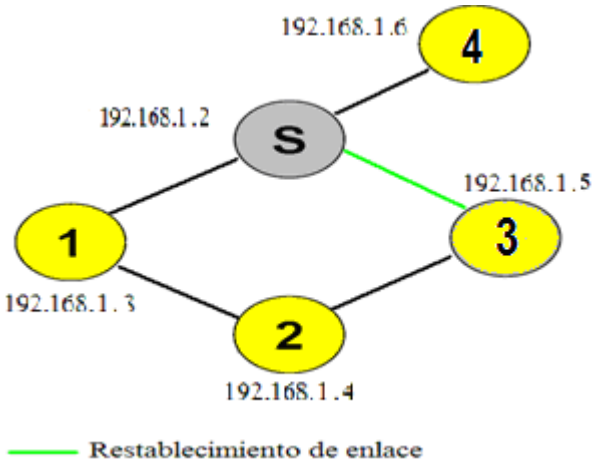

FIG. V.19 NUEVO NODO Y RESTABLECIMIENTO DE RUTA.

Se hace un envío de información del nodo D hacia el nodo 3 para forzar a los protocolos a calcular la ruta de la forma más rápida. De los archivos generados por ambos protocolos se sacarán los tiempos que utiliza cada uno de ellos.

Con los siguientes comandos se reestablece la ruta previamente anulada:

Nodo S

```
# /sbin/iptables –t mangle –D PREROUTING –m mac –mac-source 00:0E:0C:5C:F8:9C –j
DROP
```

Nodo 3

```
# /sbin/iptables –t mangle –D PREROUTING –m mac –mac-source 00:0E:0C:5C:F9:6C –j
DROP
```

5.5. EMULACION MOBIEMU

Gracias a las pruebas anteriores ya hemos podido ver como se comportan los protocolos ante diferentes escenarios y poder tener claras las diferencias de funcionamiento de los mismos.
Pasamos a realizar pruebas con escenarios dinámicos acercándonos más a la finalidad de este tipo de redes. Para ello no se ha utilizado ordenadores portátiles en campo abierto, sino que simularemos un escenario con el emulador de redes. Estas pruebas de laboratorio sirven para saber que resultados vamos a obtener antes de hacer una puesta en escena real, pero sin tener algunas consideraciones.

Escenarios

Para realizar las comparativas entre los dos protocolos dentro del emulador, se ha definido 5 escenarios diferentes. Estos escenarios se han creado con la herramienta “setdest”. Estos escenarios se crean de forma aleatoria para que no se de el caso que favorezcan a uno de los protocolos.

Cada uno de ellos se crea de 8 nodos y con diferentes dimensiones. La instrucción utilizada para generar los escenarios es la siguiente:

./setdest -v <1> -n <nodes> -p <pause time> -M <max speed> -t <simulation time> -x <max X> -y <max Y>

Una vez definidos todos los parámetros de los escenarios se debe retocar la cabecera para que quede como uno de los ejemplos que se muestra a continuación:

nodes: 8, pause: 5.00, max speed: 5.00 max x = 450.00, max y: 600.00

Hemos configurado una red con 8 nodos que se mueven en un área de 450x600 metros. Cada nodo escoge un destino al azar y se mueve hacia él con una velocidad máxima de 5 metros por segundo; cuando ya ha alcanzado el destino realiza una pausa de 5 s, selecciona otro destino y repite el proceso.

Configurado todo como se indica ya podemos pasar a cargar los escenarios en todos y cada uno de los nodos que van a formar parte del banco de pruebas. Una vez creados los escenarios se pasa al estudio de cada uno de ellos de forma independiente, analizando el número de paquetes que se pierde para cada uno de los protocolos después de los cortes que se van produciendo. De todos estos resultados se hace la media para ver las diferencias.

Para entender mejor como se han creado los escenarios llevados a estudio ir al anexo, donde se podrá encontrará el manual de uso de la herramienta y una parte de los escenarios utilizados en las pruebas.

Se ha seleccionado una secuencia de movimiento para ayudarnos a entender cómo se van posicionando los diferentes nodos en diferentes instantes de tiempo. En estas dos capturas de

pantalla se ve como los nodos están totalmente ubicados en diferentes posiciones para diferentes instantes de tiempo.

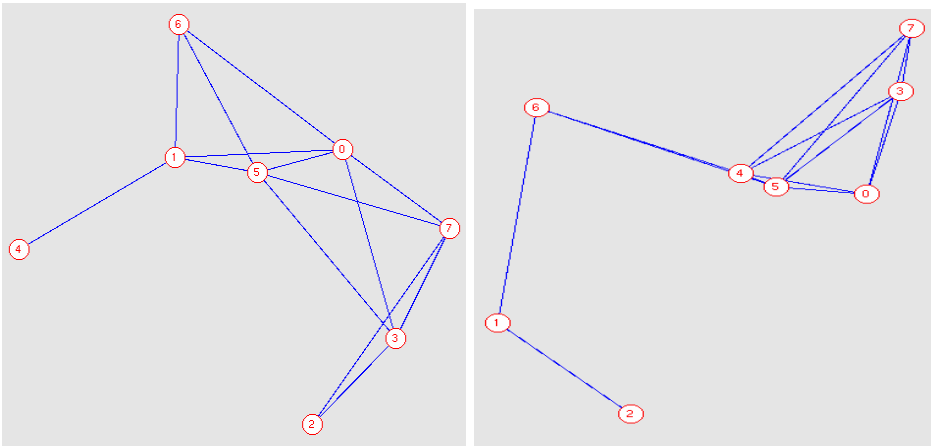

FIG. V.20 ESCENARIO 5 NODOS MOBIEMU

En la figura V.8 se muestran dos capturas en la que podemos ver la aplicación MobiEmu funcionando. Se puede ver como los nodos van cambiando de posición y van rompiendo los enlaces constantemente. Las líneas de color azul muestran los enlaces entre los nodos, los que no tiene alcance no se les representa una línea de otro color. Cada ordenador representa uno de los nodos, a los que se le asigna un número para identificarlos.

Inicio de MobiEmu

Se ha utilizado la versión 1.2 – de Junio del 2002, creada por Yongguang Zhang. Para poder arrancar la aplicación correctamente, debemos instalarla previamente en todas las máquinas. Como ya se ha comentado anteriormente una de ellas es la que actúa como master y el resto como esclavos. El master no aparecerá como nodo en el escenario, sino que se encargará de ordenar a los escenarios seguir el patrón de movimiento. Los escenarios de las simulaciones

deberán ubicarse dentro del directorio “slave” para los esclavos y dentro del directorio “master” para el maestro.

Para cada nodo del escenario deberemos asignar un ordenador con el número de nodo identificador. Esto se hace con el siguiente comando:

/home/mobiemu-1.2/slave# ./emulc X

X♉número de nodo

Una vez hecho esto para cada ordenador ya podemos arrancar el master con el comando:

/home/mobiemu-1.2/master# ./emul

Y la aplicación se encuentra en funcionamiento

CONCLUSIONES

- La movilidad en una red crea una nueva ramificación en el concepto de enrutamiento de redes, de esta manera se exploran puntos que no se consideraron al crear redes regulares, por ello, en base a los estándares ya desarrollados para redes cableadas se busca dar solución a los infinitos retos que pueden presentarse gracias a la movilidad.

- La aparición de redes ad-hoc y redes mesh conlleva un incremento de complejidad en las redes, que impacta en la gestión, de forma que aparecen nuevos problemas, como son la configuración en un entorno heterogéneo y dinámico, la minimización de los recursos utilizados en la gestión, la escalabilidad, la adaptabilidad a cambios, la gestión en redes en localizaciones aisladas, y el *troubleshooting.*

- Para el desarrollo de un proyecto el punto más importante que se debe tener en cuenta es identificar claramente las necesidades de los sectores en los cuales vamos a desarrollar dicho proyecto; con el fin de conocer sus necesidades en cuanto a comunicaciones se refiere y establecer un conjunto de actividades que presenten la mejor solución.

- Una de las características de las redes Mesh radica en su gran tolerancia a fallos cuando existe algún problema en la red. Por ejemplo si uno o más nodos salen de servicio, el protocolo de enrutamiento pueden re direccionar el flujo de información o otros nodos de la red

- Como cualquier tecnología, hay asuntos y limitaciones en las redes Mesh, la mayoría basadas en escalabilidad y las dificultades de garantizar calidad de servicio. Son tópicos que no se resuelven completamente pero se siguen haciendo estudios para resolver estos problemas.

- La simulación como herramienta de investigación y desarrollo permite explorar una realidad dentro de parámetros determinados llegando explotar las capacidades de una tecnología, de esta manera, se consigue determinar alcances, funcionamiento, capacidades y posibles soluciones a nuevos retos.

- Para un mejor uso de las redes Ad-Hoc, se a sugerido unas políticas de gestión., basadas en 5 puntos relevantes que deben ser revisados antes de diseñar una red Ad-hoc. Analizar requerimientos, señalización en la red, selección de protocolos, implementar seguridad y optimización de recursos.

RECOMENDACIONES

- Para estudiar distintas tecnologías se debe conocer de antemano su funcionamiento así como la razón de su existencia, ya que cada solución viene dada gracias a la existencia de una necesidad, por ello se recomienda entender el fin que busca cada a solución de manera que los análisis sean objetivos

- Es importante para tener una vista más amplia respecto a los sucesos dados en una simulación que se analicen situaciones reales de funcionamiento así como un análisis que permita explotar la red en sus máxima capacidad

- Es de gran importancia, implementar Políticas de Seguridad, debido a que la tecnología Mesh permite que un equipo inalámbrico pueda tener acceso a la red sin mayor problema lo que hace necesario políticas de configuración de los equipos, políticas de acceso remoto, políticas de contraseñas, etc. Que son necesarios para reducir en la medida de lo posible el ingreso a la red de usuarios no deseados

- Se debe tener en cuenta las Políticas de gestión planteadas en este trabajo en el momento de diseñar la red que deseamos, de esta manera se lograra una mayor optimización. Cabe recalcar que las políticas al igual que la red Ad-hoc sufrirá cambios de acuerdo al ambiente en el que se implementara.

RESUMEN

La evaluación y planteamiento de soluciones a los problemas de gestión de redes 802.11s (Redes Manet/Mesh se realizo con el fin de descubrir y evaluar los problemas que se encuentran con mas frecuencia en las redes móviles y aquellos que causen mas daño en la estructura de las mismas y de esta manera definir una política administrativa para este tipo de redes Manet/Mesh.

La metodología utilizada en este trabajo fue Deductiva, iniciando con el planteamiento de varios escenarios dentro de un clúster lo cual ayudo a la recolección de datos informativos sobre el funcionamiento de este tipo de redes, completando este proceso de recaudación de datos con una simulación en el programa llamado MobieEmu el cual nos presento una amplia forma de ver el funcionamiento de las redes Ad-Hoc en una manera que nuestro escenario por ser pequeño no lo permitió, deduciendo de esta forma que el campo de las redes Ad-Hoc cuenta con vatios problemas de los cuales ninguno a sido profundamente investigados.

Los resultados numéricos nos indican que el incremento de complejidad en las redes incrementan los problemas proporcional al crecimiento de la red siendo el mas frecuente en este tipo de redes la adaptabilidad a cambios debido a la distancia que abarca y a los constantes cambios que presenta.

Se concluyo que como cualquier tecnología, hay asuntos y limitaciones en las redes Mesh, la mayoría basadas en adaptabilidad y las escalabilidad en la calidad de servicio. Son tópicos que no se resuelven completamente pero se siguen haciendo estudios para resolver estos problemas.

Para un mejor uso de las redes Ad-Hoc, se a sugerido unas políticas de gestión., basadas en 5 puntos relevantes que deben ser revisados antes de diseñar una red Ad-hoc. Analizar requerimientos, señalización en la red, selección de protocolos, implementar seguridad y optimización de recursos.

SUMMARY

The evaluation and proposing solutions to the problems of network management 802.11s Networks (Manet / Mesh was conducted to identify and assess problems that are found more often in mobile networks and those that cause more damage in the structure of the same and thus define an administrative policy for this type of network Manet / Mesh.

The methodology used in this work was Deductive, starting with the approach of various scenarios within a cluster which helped data collection information on the operation of such networks, completing the process of collecting data with a simulation in the program called MobieEmu which we present a comprehensive way to see the performance of ad hoc networks in a way that our scenario to be small not allow it, thus deducing that the field of ad hoc networks has problems watts none of which has been deeply investigated.

The numerical results indicate that the increase in network complexity increases proportional to the growth problems of the network being the most frequent in this type of network adaptability to change due to the distance covered and the constant changes presented. It was concluded that like any technology, there are issues and limitations in mesh networks, mostly based on adaptability and scalability in the quality of service. Are topics that are not resolved completely but still doing studies to solve these problems.

To make best use of ad hoc networks are suggested to management policies., Based on 5 important points that must be reviewed before designing an ad-hoc network. Analyze requirements, network signaling, screening protocols, implementing security and resource optimization.

BIBLIOGRAFÍA

LIBROS

1. CHAI, K. Toh. Ad Hoc Mobile Wireless Networks: protocols and systems. Cambridge: Prentice Hall, 2002. 336 p.

2. OZAN, K. Tonguz and GIANLUIGI, Ferrari. Ad Hoc Wireless Networks: a communication theoretic perspective. New York: John Wiley and Sons, 2006. 330 p.

3. D. MANZANO, J. C. Cano, C. T. Calafate, P. Manzoni, "MAYA: A Tool For Wireless Mesh Networks

4. MANAGEMENT", 2007 IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, Octubre 2008.

BIBLIOGRAFÍA INTERNET

1. Estándares en redes

   http://standards.ieee.org/getieee802/802.11.html

   2012-01-12

2. Estándares en redes inalámbricas

   http://standards.ieee.org/inalámbricas/

   2011-11-27

3. Enrutamientos en redes móviles

   www.redhucyt.oas.org/webesp/PRESENTATIONS/.../Routing.pp

   2011-07-09

4. Movilidad en redes IP

   eav.upb.edu.co/banco/files/03INTRODUCCION

   2010-02-02

5. Protocolos en redes móviles

   http://www.arqhys.com/construccion/protocolos-introduccion.html

   2012-03-02

6. Redes AdHoc

   http://es.wikipedia.org/wiki/Ad_hoc

   2011-09-10

7. Redes móviles

http://www.hiperlan2.com/

2012-02-11

8. Simulación de redes

http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F08+-+Capitulo+3.pdf

2012-01-14

9. Wireless LAN

http://www.eveliux.com/mx/estandares-wlan.php

2011-12-10

ANEXOS

PROGRAMACION MOBIEMU 8 NODOS

```
#nodes: 8, pause: 10.00,max speed: 20.00 max x = 450.00, max y: 500.00
$node_(0) set X_ 335.398243126188
$node_(0) set Y_ 414.665312331725
$node_(0) set Z_ 0.000000000000
$node_(1) set X_ 384.037099901987
$node_(1) set Y_ 273.192582611008
$node_(1) set Z_ 0.000000000000
$node_(2) set X_ 86.364448690742
$node_(2) set Y_ 150.190630634234
$node_(2) set Z_ 0.000000000000
$node_(3) set X_ 110.955508746846
$node_(3) set Y_ 172.551882427836
$node_(3) set Z_ 0.000000000000
$node_(4) set X_ 314.500875390643
$node_(4) set Y_ 271.224713631612
$node_(4) set Z_ 0.000000000000
$node_(5) set X_ 271.170508443254
$node_(5) set Y_ 322.729231004529
$node_(5) set Z_ 0.000000000000
$node_(6) set X_ 323.638477459737
$node_(6) set Y_ 113.511874831857
$node_(6) set Z_ 0.000000000000
$node_(7) set X_ 98.386969956218
$node_(7) set Y_ 466.022724852135
$node_(7) set Z_ 0.000000000000
$god_ set-dist 0 1 1
$god_ set-dist 0 2 3
$god_ set-dist 0 3 2
$god_ set-dist 0 4 1
$god_ set-dist 0 5 1
$god_ set-dist 0 6 2
$god_ set-dist 0 7 1
$god_ set-dist 1 2 2
$god_ set-dist 1 3 2
$god_ set-dist 1 4 1
$god_ set-dist 1 5 1
191.803359634964 9.188490591758"
$ns_ at 10.000000000000 "$node_(4) setdest 37.241600581038
335.216837638314 19.465386576206"
$ns_ at 10.000000000000 "$node_(5) setdest 143.228572325675
278.016505955587 4.401339743165"
$ns_ at 10.000000000000 "$node_(6) setdest 61.733694244318
401.136451735250 13.904559861903"
$ns_ at 10.000000000000 "$node_(7) setdest 375.679413529885
127.586322496169 7.161465438452"
$ns_ at 10.278059894323 "$god_ set-dist 0 2 2"
$ns_ at 10.278059894323 "$god_ set-dist 2 5 1"
…
$ns_ at 206.648669612153 "$god_ set-dist 1 4 3"
$ns_ at 206.648669612153 "$god_ set-dist 1 7 3"
$ns_ at 207.079629138479 "$node_(6) setdest 439.356631072280
490.381868080343 0.000000000000"
```

```
$ns_ at 207.699301124613 "$god_ set-dist 1 4 2"
$ns_ at 207.699301124613 "$god_ set-dist 4 5 1"
$ns_ at 209.714051715975 "$node_(1) setdest 45.635316041798
25.771810058629 0.000000000000"
$ns_ at 211.400879369172 "$node_(3) setdest 206.808717471131
327.406145539246 18.892265406808"
$ns_ at 490.631954733165 "$node_(7) setdest 311.002585778138
283.295288198958 0.000000000000"
$ns_ at 490.791880352024 "$god_ set-dist 0 6 2"
$ns_ at 496.261608862692 "$node_(0) setdest 300.446760385047
0.270249917221 0.000000000000"
$ns_ at 496.358744258319 "$god_ set-dist 4 5 1"
$ns_ at 498.137184150146 "$god_ set-dist 0 3 2"
$ns_ at 498.137184150146 "$god_ set-dist 1 3 1"
# Destination Unreachables: 34
# Route Changes: 393
# Link Changes: 223
# Node | Route Changes | Link Changes
#    0 |            96 |           60
#    1 |            99 |           52
#    2 |           113 |           54
#    3 |            91 |           52
#    4 |           106 |           68
#    5 |           109 |           62
```