FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

ANÁLISIS DE UNA RED MESH APLICADA A SISTEMAS AÉREOS NO TRIPULADOS

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieros en Redes y Telecomunicaciones

Profesor Guía

Ms. Milton Neptalí Román Cañizares

Autores

Pablo Andrés Alvear Sandoval

Natalia Verónica Tobar Pérez

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación

_____

Milton Neptalí Román Cañizares

Magister en Gerencia de Redes y Telecomunicaciones

CI: 0502163447

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____	_____
Pablo Andrés Alvear Sandoval	Natalia Verónica Tobar Pérez
CI: 1725124919	CI: 0401220314

DEDICATORIA

A Dios por darme la fuerza para continuar día a día, por ser prueba fehaciente de constancia, esperanza y amor.

A mi abuelita Zoila, por su entregado cariño.

A mi madre Martha por ese infinito amor y ternura.

A mi padre Víctor por enseñarme a luchar.

A mi hermano Byron por ser ejemplo de lucha y perseverancia

A mi hermana Aleida por compartir mi vida, por ser mi cómplice y mi amiga.

Natalia

AGRADECIMIENTO

A mis padres por todos los esfuerzos y sacrificios.

A mis amigos Mony, Oscar, Wendy, Andre, Santy, Pancho, con quienes compartí muchos momentos, gracias por su amistad dentro y fuera de las aulas.

A mis amigos Megasupply, por toda la ayuda brindada en esta época de estudio.

A Pablo Andrés, gracias por ser parte de este equipo, por tu paciencia, comprensión y cariño.

Natalia

DEDICATORIA

A mi madre Pilar y a mi abuelo Luis por enseñarme desde niño a ser perseverante y luchar por lo que quiero, así como por su apoyo constante y sus consejos a lo largo de toda mi vida estudiantil.

Pablo

AGRADECIMIENTO

A mis amigos, por sus palabras de ánimo y buena energía.

A los profesores que pudieron ayudarme con el desarrollo de mi trabajo de titulación.

A mis ex compañeros de trabajo por siempre colaborar conmigo y creer que podía lograrlo.

Pablo

RESUMEN

En el presente documento se analizan las redes mesh y su capacidad de interconectar Sistemas Aéreos no Tripulados.

Se identifican las características necesarias para la formación de la red mediante la investigación de proyectos e implementaciones previas para determinar parámetros analizables como el encaminamiento y cómo éste contribuye al funcionamiento de la red.

Se detalla el funcionamiento y clasificación de los protocolos de enrutamiento ad-hoc proactivos, reactivos e híbridos y cómo estos descubren y mantienen rutas hacia sus nodos vecinos.

Se identifican dos maneras de establecer una red mesh, la primera bajo el estándar el 802.11s que define componentes de la red, enrutamiento y seguridad. La segunda a través de redes MANET que se enfoca en protocolos de enrutamiento ad-hoc que permitan brindar movilidad a los nodos de la red.

De acuerdo al comportamiento de los protocolos de enrutamiento en proyectos de simulación más la teoría analizada, los protocolos proactivos demostraron menor retardo, pero mayor carga de control mientras que los reactivos presentaron menor carga de control, pero mayor retardo hasta encontrar una ruta. De esta manera se determinó que los protocolos proactivos son más eficientes en aplicaciones de tiempo real como voz o video.

Las redes analizadas emplearon microcomputadores con capacidad de instalar software basado en Linux para implementar los protocolos de enrutamiento.

ABSTRACT

This document analyzes a mesh network and its capability to interconnect Unmanned Aircraft Systems.

The necessary features to build the network are identified through research projects and previous implementations in order to determine parameters as routing and how it contributes to the network performance.

The operation of proactive, reactive and hybrid ad-hoc routing protocols and how they discover and maintain routes to its neighboring nodes are widely detailed.

It was found two ways to establish a mesh network, the first under the 802.11s standard that defines the network components, routing and security. The second one through MANET protocols that focuses on ad-hoc routing allowing mobility to network nodes.

According to the behavior of routing protocols in simulation projects and theory analyzed, proactive protocols show less delay but greater control load while the reactive protocols, lower load but more delay to find a route. Thus it was determined that proactive protocols are more efficient in real-time applications such as voice or video.

Analyzed networks used microcomputers capable of installing lightweight software based on Linux to implement routing protocol.

ÍNDICE

ÍNDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

El crecimiento de las redes inalámbricas en la actualidad permite una mejora en cuanto a movilidad, escalabilidad y uso de aplicaciones. Dentro de las redes inalámbricas se encuentran las redes mesh que son de tipo descentralizada, donde una estación no necesariamente debe comunicarse con un dispositivo central para gestionar la conexión, sino que también puede comunicarse directamente entre nodos o estaciones. Una ventaja de estas redes es la flexibilidad ante cambios y búsqueda de rutas además su implementación es económica en comparación a las redes tradicionales.

El desarrollo de los sistemas Aéreos no Tripulados tanto en el ámbito militar como civil ha significado nuevas áreas de investigación dentro de las cuales se incluye el desarrollo de comunicaciones y formación de redes entre estos dispositivos.

La combinación de redes mesh y Sistemas Aéreos no Tripulados son potencialmente útiles en situaciones donde la configuración de una red requiera el menor tiempo posible, un rápido despliegue ante situaciones de emergencia, toma de datos o simplemente establecer conexiones entre dispositivos donde no exista algún tipo de infraestructura fija.

El alcance de este trabajo plantea realizar un análisis técnico de varias tecnologías de red que usen conectividad tipo mesh; esto quiere decir redes compuestas de varios nodos interconectados unos a otros o a uno o más puntos de acceso de forma inalámbrica. Por lo tanto, se recopilará información con contenidos relacionados a estas redes, se investigará las características y las necesidades de funcionamiento, se analizará los protocolos de red existentes para sus aplicaciones, cómo se realiza la autoconfiguración de los nodos, facilidad de reconfiguración y métrica y así poder inferir, tomando en cuenta las ventajas de cada uno, cual es la mejor opción que permitirá solventar necesidades de comunicación aplicables a plataformas no tripuladas.

El objetivo general de esta investigación es realizar un análisis técnico de las redes mesh aplicadas a sistemas aéreos no tripulados (UAS).

Los objetivos específicos son:

- Identificar las características y requerimientos de red para los UAS basándose en escenarios de aplicación.
- Analizar los parámetros más relevantes que intervienen en el funcionamiento de una red mesh aplicada a los UAS con el fin de obtener plena funcionalidad.
- Determinar qué tipo de solución de red mesh es adecuada para los UAS.

La estructura del proyecto de tesis está determinada de la siguiente manera:

En el primer capítulo se explican los principales conceptos referentes a redes inalámbricas y Sistemas Aéreos no Tripulados para relacionarlo con el tema de investigación con la finalidad de enfocar y entender la composición del proyecto.

En el segundo capítulo se describe proyectos que hayan sido desarrollados y sirvan como base para comprender como está estructurada la red y los nodos en los UAS.

En el tercer capítulo se analiza la estructura de la red y sus características como protocolos de enrutamiento, formación y mantenimiento de rutas.

En el cuarto capítulo se presentan los componentes en hardware y software para la formación de una red mesh, se hace mención a simulaciones en las que se muestra el desempeño de algunos de los protocolos de enrutamiento analizados y de tal manera tener una referencia del comportamiento de la red.

Finalmente, en función del análisis de los componentes y escenarios de la red se determina qué tipo de red mesh puede ser aplicada para adaptarla a un Sistema Aéreo no Tripulado.

1. CAPÍTULO I MARCO TEÓRICO

En esta sección se muestran conceptos relacionados a redes inalámbricas y Sistemas Aéreos no Tripulados que son elementales para delimitar y comprender el enfoque de la investigación. Los conceptos descritos a continuación servirán de fundamento para el desarrollo del presente proyecto.

1.1 Redes Inalámbricas

Actualmente el uso de redes inalámbricas continúa incrementándose, debido a los diferentes beneficios que estas ofrecen, entre los que se puede destacar:

Las redes inalámbricas pueden aumentar su cobertura, facilitando el acceso para los usuarios en lugares donde una red cableada no puede llegar o la infraestructura del lugar no permite extender la red cableada.

Las redes inalámbricas tienen gran escalabilidad debido a que se puede tener múltiples configuraciones, esto ayuda al incremento del número de usuarios en la red.

Permiten movilidad a sus dispositivos dejando de lado la necesidad del cableado tradicional para acceder a recursos de la red.

1.1.1 Clasificación de las redes inalámbricas

Las redes inalámbricas se clasifican en diferentes tipos de acuerdo a los siguientes parámetros:

1.1.1.1 Por su cobertura

De acuerdo a su cobertura las redes inalámbricas de clasifican en: WPAN, WLAN, WMAN, WWAN, entre otras.

En la Figura 1 se muestra la clasificación de las principales redes inalámbricas de acuerdo a la cobertura.

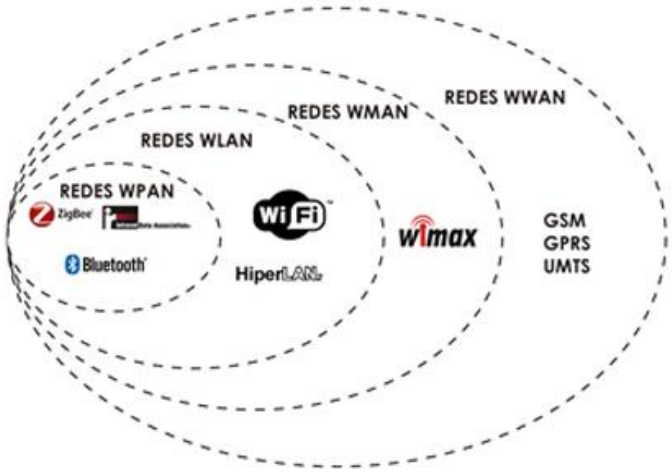


Figura 1. Clasificación de las redes inalámbricas por su cobertura
Tomado de: (Kioskea, 2014)

1.1.1.2 Por su topología

Desde el punto de vista de la topología, las redes inalámbricas se clasifican en: Estrella, árbol, anillo, malla completa y malla parcial. En la Figura 2 se muestra la clasificación de este tipo de redes.

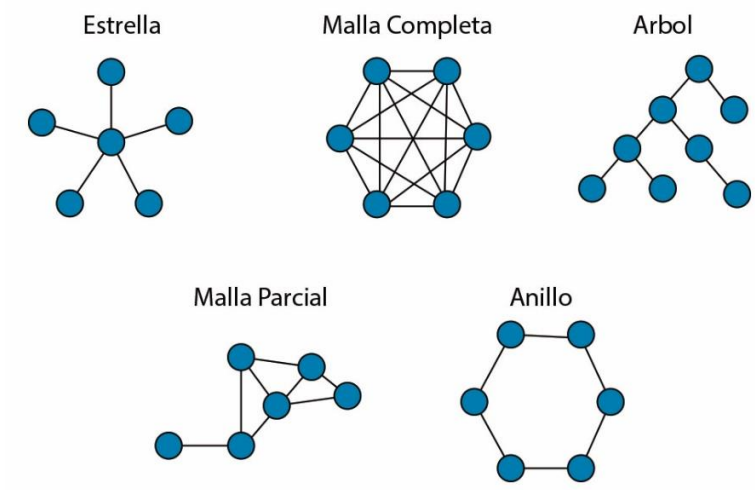


Figura 2. Clasificación de las redes inalámbricas por su topología

1.1.2 Tecnologías LAN inalámbricas

En 1997 se conformó la comisión IEEE 802.11 para la estandarización de las redes LAN inalámbricas y cuyo objetivo fue crear especificaciones para la capa física y enlace de datos; este estándar es también conocido como Wi-Fi o Wireless fidelity. A través de los años han existido mejoras al estándar permitiéndo tener mayor rendimiento, alcance y diferentes tipos de modulación.

A continuación, se muestra las variaciones del estándar IEEE 802.11 en cuanto a velocidad de transmisión y modulación.

1.1.2.1 IEEE 802.11a

Esta revisión fue aprobada en 1999, opera en la banda de 5GHz, tiene una velocidad máxima de 54Mbps, la modulación es OFDM (*Orthogonal Frequency-Division Multiplexing*). 802.11a tiene 12 canales no superpuestos, 8 para red inalámbrica y 4 para conexiones punto a punto. Este estándar no puede trabajar con equipos del estándar 802.11b.

1.1.2.2 IEEE 802.11b

IEEE 802.11b fue el primer estándar de LAN inalámbrica en ser ampliamente adoptado en muchos equipos, conocido como Wi-Fi. El estándar 802.11b fue ratificado por el IEEE en 1999. Trabaja en la frecuencia de 2,4 GHz, tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA.

1.1.2.3 IEEE 802.11g

Este estándar opera en la banda de 2,4 GHz, presenta compatibilidad con el estándar 802.11b, emplea dos tipos de modulación OFDM y DSSS, alcanza una velocidad teórica de hasta 54 Mbps. En ambientes indoor tiene un alcance de más de 30 m en interior y 300 en exterior.

1.1.2.4 IEEE 802.11n

Este estándar opera en la banda de 2,4 GHz y 5GHz presenta una mejora en sus canales con respecto a 802.11a/g que solo es de 20 MHz y en esta variante aumenta a 40 MHz.

Implementa sistema MIMO esto quiere decir múltiples entradas y múltiples salidas lo que permite al sistema configurar varios flujos de datos en el mismo canal, aumentando así la capacidad de transmisión de datos.

Trabaja con una modulación CCK, DSSS y OFDM y alcanza velocidades de hasta 300 Mbps. (Miller, 2008, pág. 22)

1.1.2.5 Comparación entre las características de estándares 802.11

En la tabla 1 se realiza una comparación del rendimiento, alcance y modulación de los estándares 802.11

Tabla 1. Resumen de algunas variantes del estándar 802.11 wi-fi.

RESUMEN DE ESTANDARES WI-FI				
Estandar	802.11a	802.11b	802.11g	802.11n
Velocidad	54 Mbps	11Mbps	54 Mbps	<100 Mbps
Banda de Frecuencia	5 GHz	2,4 GHz	2,4 GHz	2,4 y 5 GHz
Modulación	OFDM	DSSS	OFDM/DSSS	MIMO/OFDM
Rango	25m	35m	30m	100 m
Ancho de banda del canal	20 MHz	20 MHz	20 MHz	40 MHz

Tomado de: (Miller, 2008, pág. 27); (Poole, s.f)

1.1.3 Modos de operación de las redes LAN inalámbricas

1.1.3.1 Redes en infraestructura

En redes basadas en el estándar IEEE 802.11 el modo de infraestructura es conocido como Conjunto de Servicios Básicos o BSS.

En el modo de infraestructura existe un nodo central o estación base que realiza las funciones de coordinación. Los dispositivos del usuario se conectan de forma inalámbrica a un punto de acceso y este a su vez puede enlazarse a la red fija. A esta configuración entre el punto de acceso y los dispositivos del

usuario que se encuentran en su área de cobertura se los denomina Conjunto de Servicio Básico (BSS) o Basic Service Set. El identificador de cada BSS se llama BSSID y se compone de 48 bits, que en infraestructura se refiere a la dirección MAC.

En la Figura 3 se observa que se puede conectar varios BSS por medio de un enlace alámbrico o inalámbrico conocido como Sistema de Distribución (SD) con el propósito de transmitir información sobre los dispositivos, o en otros casos, datos emitidos por los dispositivos móviles y así conformar un Conjunto de servicio extendido (ESS).

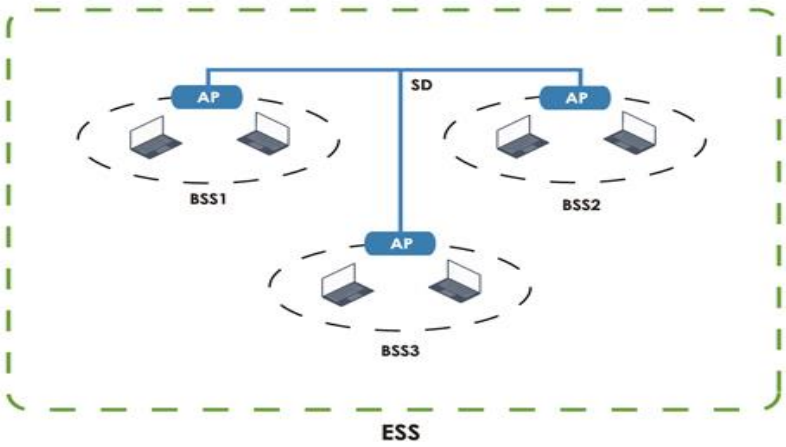


Figura 3. Red inalámbrica en modo infraestructura.
Tomado de: (Kioskea, 2014)

Un Identificador del conjunto de servicio extendido (ESSID) es la manera en que un ESS es identificado y lo realiza por medio de 32 caracteres alfanuméricos al que se lo refiere también como el nombre de la red o simplemente como SSID (López, s.f).

Cuando un nodo se desplaza entre algunas BSS dentro de un mismo ESS, el adaptador de la red del dispositivo varia su conexión a los puntos de acceso, dependiendo del nivel de señal recibido proveniente de los mismos; para el usuario todo este proceso también llamado itinerancia se lo realiza de forma transparente (Kioskea, 2014).

1.1.3.2 Redes en modo Ad-hoc

En redes bajo el estándar IEEE 802.11 el modo ad hoc es conocido como Conjunto de Servicios Básicos Independientes (IBSS).

Una red en modo ad hoc es una red que se configura sin necesidad de administración central alguna y sus nodos usan su interfaz inalámbrica para realizar la transmisión de datos. Debido a la configuración de los nodos de una red de esta clase, estos pueden realizar funciones de encaminamiento adicionales a las de envío y recepción o dicho de otra manera envían datos de otros nodos y establecen las aplicaciones del usuario.

Los dispositivos de la red deben configurar su adaptador inalámbrico en modo ad hoc, usar el mismo SSID de la red y conservar una distancia para mantener el enlace. En la Figura 4 se aprecia un ejemplo del conjunto de servicios básicos independientes.

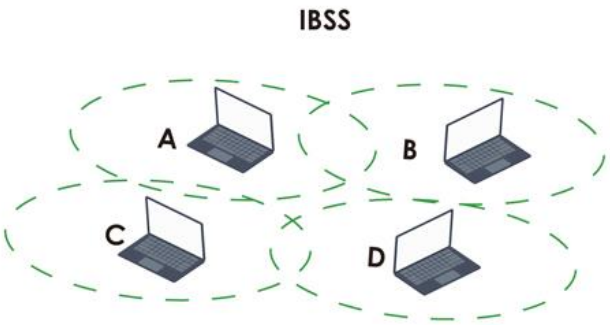


Figura 4. Red inalámbrica en modo Ad-hoc
Tomado de: (Kioskea, 2014)

1.1.4 Redes de malla inalámbrica

Las redes mesh o malla inalámbrica, reúnen a dos modos de operación de red, la primera es el modo ad-hoc y la segunda es el modo infraestructura. El diseño de estas redes toma en consideración el estándar 802.11 y generalmente son redes basadas en IP.

1.1.4.1 Características

Este tipo de red tiene la capacidad de auto organización y auto configuración de manera dinámica para proveer el enlace con los nodos.

Estas redes pueden ampliar su rango de cobertura, siempre y cuando estén dentro de la cobertura de otros nodos.

Permite la redirección del tráfico ya sea por un cambio en la estructura de la red o para evitar congestión.

1.1.4.2 Componentes de la Red

Routers mesh

El backbone de la red está conformado por los routers mesh y estos efectuarán las funciones de gateway y routing. Para realizar la conexión de los dispositivos que usen la misma tecnología su conexión será directa y si es distinta lo harán mediante una estación base.

Los routers mesh posibilitan la unión de dispositivos a su red estando directa o indirectamente conectados a la misma ya que pueden conectarse a otros dispositivos que estén dentro de la cobertura de una tarjeta de red.

Clientes Mesh

Dispositivos finales por los cuales se acceden a los servicios a través de otro cliente mesh, o por medio de la red de routers, de esta manera se logra ampliar la cobertura.

Pueden establecer una red sin la necesidad de conectarse directamente a un punto de acceso o un router mesh, este tipo de red tiene similitud a la red ad hoc, pero con capacidad de soportar dichas conexiones.

Todo este proceso de conexión y descubrimiento de sus nodos tiene que estar gestionado por un protocolo de red para redes de malla, el cual varía su complejidad en función de sus conexiones. En la Figura 5 se observa un esquema con los principales componentes de una red mesh.

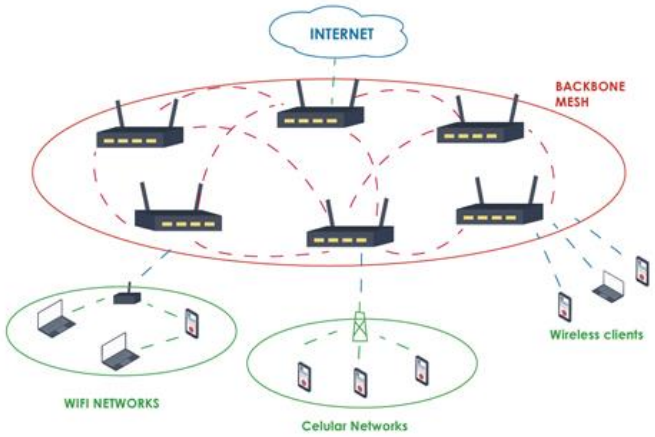


Figura 5. Componentes de una red mesh.

1.1.5 Redes MANET

Las redes MANET (Mobile Ad Hoc Network) son redes tipo Ad Hoc en las cuales un conjunto de nodos que se comunican entre sí mediante enlaces inalámbricos y que no tienen una infraestructura fija; otra característica en las MANET es la movilidad de los nodos que pueden abandonar o incorporarse a la red, en consecuencia, los parámetros como tasa de transmisión y retardo este tipo de red es variable.

Los nodos en la red MANET tienen la posibilidad de actuar como emisores, receptores o reenviadores, esta característica es muy importante ya que los caminos o rutas para llegar al destino pueden tener varios saltos (Chalmeta, 2009). En la Figura 6 se puede observar un esquema propio de una red MANET.

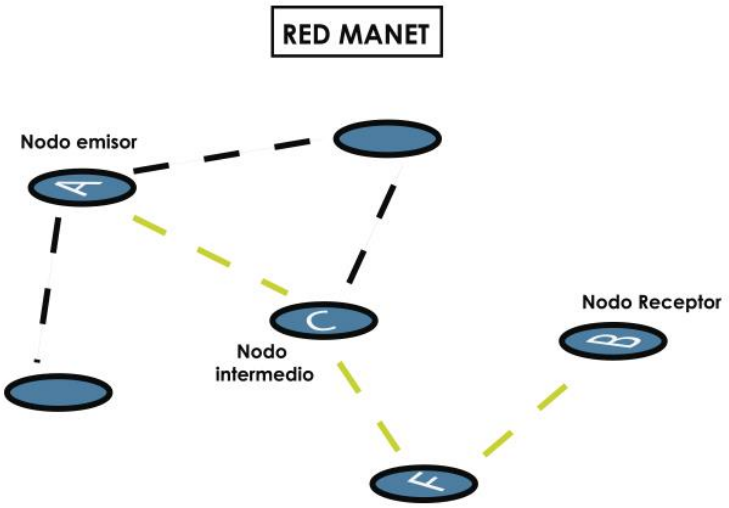


Figura 6. Red MANET.

1.1.5.1 Funcionamiento

Emplean las frecuencias de las redes inalámbricas de área local en las bandas de 2,4GHz y 5 GHz, no se requieren permisos para operar en ella por lo que tienen más aplicaciones y por ende más susceptible a interferencias. Usan antenas omnidireccionales propias de este tipo de red inalámbrica lo que contribuye el enlace con nodos cercanos. Utiliza funciones de coordinación distribuida y protocolos de acceso aleatorio concretamente CSMA /CA para disminuir las colisiones y. En el enrutamiento es donde se destacan las MANET ya que emplean protocolos que se adapten a la movilidad y así poder mantener la ruta de comunicación entre los nodos.

Se ha determinado protocolos de enrutamiento clasificados de acuerdo a la forma como determinan las rutas:

- Protocolos reactivos
- Protocolos proactivos
- Protocolos híbridos

Estos protocolos serán analizados más adelante en el capítulo 3.

1.1.5.2 Aplicaciones

Debido a que no se requiere una infraestructura fija, este tipo de redes son sencillas en lo que a despliegue se refiere, son favorables con respecto a costo en comparación con las redes con infraestructura fija. Algunas de las aplicaciones son las siguientes:

Entornos militares

Como en muchos avances tecnológicos, las aplicaciones militares han sido pioneras, así mismo sucedió con las redes MANET. Uno de los primeros proyectos fue desarrollado por DARPA (Defense Advanced Research Projects Agency), el proyecto llamado PARNET permitía la comunicación directa entre usuarios móviles sobre grandes áreas geográficas. (Ruiz, 2008)

Situaciones de emergencia

En caso de desastres o situaciones de emergencia, si las redes normales han quedado inhabilitadas o se requiere un rápido despliegue de una red para transmitir información las redes MANET son una buena alternativa. El proyecto Workpad es impulsado por la Comisión Europea destinada a crear comunicaciones P2P en situaciones de emergencia, cada terminal se conecta a la MANET usando una red WiFi en modo Ad-Hoc.

Entornos civiles

En este tipo de entorno las aplicaciones son muy amplias, en entornos agrícolas, para compartir información en una sala de un congreso, una clase, etc. Otra aplicación se tiene en el ambiente vehicular, el proyecto eCall, creado por la Comisión Europea, su función principal es prestar ayuda inmediata a los conductores implicados en un accidente de tráfico en cualquier parte de la Unión Europea. (Los Santos, 2009)

1.1.6 Otros estándares aplicables a redes mesh

Adicionalmente a las redes mesh inalámbricas de área local se conocen otros estándares mediante los cuales se implementan redes mesh. A continuación, se describe brevemente algunas de estas.

1.1.6.1 Redes 802.15.4 zigbee

Zigbee es el nombre de una especificación con base en el estándar 802.15.4 que corresponden a las redes inalámbricas de área personal WPAN como ya se mencionó anteriormente y define los niveles físicos y enlace dentro del modelo OSI. Trabaja en la banda de 868MHz 915MHz y 2,4GHz

Zigbee permite comunicación mallada peer to peer, pero actualmente los routers zigbee no emiten balizas normales 802.15.4 por lo que se habla de redes intra WPAN y debido a esto su rango de acción solo se limita a ese tipo de red (ZigBee Alliance, 2012).

Existen 3 tipos de nodos en una red ZigBee:

- Coordinador: Es el dispositivo administra toda la red
- Routers: Los que realizan el encaminamiento de la información.
- Dispositivos finales o motes: son los nodos que recolectan información.

En la capa de red emplea direccionamiento de 16 bits para cada nodo de la red y se puede implementar protocolos como AODV (Ad-hoc On Demand Distance Vector) para el enrutamiento entre sus dispositivos. (Dignani, 2011)

Las ventajas de esta red son que los dispositivos tienen un bajo consumo de energía y son auto organizables, pero el área de cobertura es relativamente corta alrededor de 75 metros y su velocidad de transmisión llega a los 250 kbps.

1.1.6.2 Redes IEEE 802.16 WIMAX

Conocidas comúnmente como WIMAX, estas redes ofrecen coberturas de hasta 50 Km y velocidades transmisión de 30 a 75 Mbps.

El estándar IEEE 802.16 se lo divide en WIMAX Fijo y móvil. El primero denominado también 802.16d trabaja en las frecuencias de 2 y 11 GHz, posee una tasa de transmisión de hasta 75 Mbps y WIMAX móvil o 802.16e donde ya permite el uso de teléfonos móviles y servicios en alta velocidad. Trabaja en frecuencias de 2 y 6GHz y alcanza tasas de transmisión de hasta 30 Mbps (Andrade & Naranjo, 2011).

Tabla 2. Comparación de las características entre WIMAX fijo y móvil.

WIMAX Fijo y Móvil			
Tipo de estandar	**Frecuencia**	**Distancia**	**Velocidad**
802.16-2004 Wimax fijo	2-11 GHz (3.5 GHz en Europa)	10 km	75Mbps
802.16e Wimax Móvil	2 - 6 GHz	3.5 km	30Mbps

Tomado de: (Kioskea, 2014)

1.2 Enrutamiento

El enrutamiento consiste en seleccionar el mejor camino desde un nodo fuente hacia un nodo destino. Esta selección la realiza basándose en las tablas de enrutamiento que tienen información de las rutas sobre redes conectadas directamente y sobre redes remotas.

1.2.1 Clasificación

Para conocer sobre las redes remotas y poder enlazarse a las mismas se la puede hacer por dos maneras:

- Enrutamiento estático: Es la configuración manual de las rutas para saber cómo llegar hacia los dispositivos, no requiere mucho procesamiento.
- Enrutamiento dinámico: Por medio de protocolos que realizan la elección del mejor camino en base a ciertos criterios.

1.2.1.1 Enrutamiento Dinámico

Funciones del enrutamiento dinámico

Los protocolos de encaminamiento dinámicos envían información sobre su estado y la conexión hacia redes remotas, entre sus principales funciones está:

- **Descubrimiento de redes.**
  Para compartir datos acerca de las redes que conoce con otros enrutadores que se encuentren utilizando el mismo protocolo de

encaminamiento y así aprender automáticamente entre enrutadores y determinar el mejor camino en la red.

- **Mantenimiento de las tablas de enrutamiento.**
  Adicionalmente de decidir sobre la mejor ruta, también determinan nuevas rutas en caso de que la ruta inicial se vuelva inutilizable o si cambian su topología para que de esta manera no se requiera un cambio manual. Todo esto representa una gran ventaja sobre el enrutamiento de manera estática.

Protocolos de enrutamiento dinámico

Dentro de los protocolos de enrutamiento dinámico existen distintas estrategias para reunir información para su encaminamiento. A los protocolos de enrutamiento dinámico se los puede clasificar en protocolos de gateway interior y protocolos de gateway exterior que emplean los siguientes algoritmos.

- **Vector distancia**
  Envían un paquete de control a sus nodos vecinos y la información que conoce un enrutador sobre una red remota es la distancia para llegar a esa red, normalmente el número de saltos, tiene actualizaciones periódicas y la interfaz por la que se la va a alcanzar. Un ejemplo de estas redes son RIP (Routing Information Protocol) V1 y V2 e IGRP (Interior Gateway Routing Protocol).

- **Estado de enlace**
  Mediante el uso de este algoritmo se obtiene una visión completa de la red por medio de la difusión de la información de tablas enrutamiento hacia todos nodos de la red, a diferencia de los algoritmos de vector distancia, la actualización del estado de enlace se realiza solo cuando se produce un cambio en la topología. Un ejemplo de estas redes son OSPF (Open Shortest Path First) e IS-IS (Intermediate system to intermediate system).

- **Vector camino**

  Para intercambiar información de los sistemas autónomos y saber cómo llegar a estos, mediante que enrutadores y el número que se va a atravesar. Un ejemplo de estos es BGP (Border Gateway Protocol).

1.2.2 Métrica

Son varios parámetros de desempeño que emplea el protocolo para determinar cuál de todas las rutas hacia su destino es la más efectiva, con la selección de la ruta se busca disminuir el retardo y las pérdidas, así como aumentar el throughput etc (Cisco Systems, 2011, pág. 81).

Ejemplos de métricas en protocolos de enrutamiento IP:

- Conteo del número de saltos o routers que el paquete debe atravesar.
- Selección del camino mediante el ancho de banda más alto.
- El tráfico de una ruta determinada o también llamado carga.
- El tiempo que demora un paquete en cruzar una ruta.
- Probabilidad de falla de una ruta mediante el cálculo del conteo de fallos o errores anteriores.
- El costo que representa un valor para indicar preferencia por una ruta y puede ser una mezcla entre varias métricas.

1.3 Calidad de Servicio

La calidad de servicio en términos generales se puede resumir como la capacidad de la red para brindar un mejor o especial servicio para cierto grupo de usuarios y aplicaciones con perjuicio a otros usuarios y aplicaciones. (Cisco Systems, 2008)

Para aplicar calidad de servicio se puede hacer mediante dos maneras, la primera mediante aprovisionamiento de recursos y la segunda a través de la administración y métodos de gestión de estos. Estos dos métodos se los conoce como IntServ y DiffServ.

1.3.1 Modelos de calidad de servicio IntServ y DiffServ

En el modelo IntServ el ancho de banda es reservado y fue creado para un comportamiento predecible en red y sus aplicaciones. Se debe realizar una reserva de recursos previo al envío de datos y emplea el protocolo RSVP (Resources reSerVation Protocol) el cual está orientado a conexión y está encargado de la señalización lo cual implica mayor uso de recursos. Por otro lado, esta DiffServ con características más eficientes y escalables como la identificación del tráfico por clases.

1.3.2 Calidad de Servicio en Capa de Acceso

Como ya se había mencionado antes empleando el acceso al medio con evasión de colisiones CSMA /CA emplea tiempos aleatorios para volver a realizar una solicitud del canal en caso de que este no se encuentre disponible en ese momento generando así un retardo en él envió de las tramas, adicionalmente no existe una priorización del tráfico, es decir se emplea un método conocido como FIFO (First Imput y First Output) el cual el da el mismo tratamiento a todo tipo de tráfico. Es por esto que se plantea ciertas soluciones para brindar calidad de servicio enfocándose en sistemas distribuidos a nivel de capa enlace.

Una implementación de calidad de servicio en la capa de enlace se lo realiza mediante 802.11e que plantea un acceso al canal distribuido mejorado EDCA (Enhanced Distributed Channel Access) en el cual se optimiza y se configuran los espacios tiempos de espera entre las tramas de acuerdo al tipo de aplicación y se las clasifica en cuatro categorías de acceso que son las siguientes:

- Voz
- Video
- Best Effort
- Background

1.4 Seguridad

“La seguridad es una combinación de procesos, procedimientos y sistemas utilizados para garantizar los siguientes atributos o requerimientos: confidencialidad, autenticación, integridad, no repudio” (Rocabado, 2013). Adicional se debe tomar en cuenta los siguientes atributos: disponibilidad, supervivencia, privacidad, control de acceso y autorización.

1.4.1 Atributos de la seguridad

1.4.1.1 Confidencialidad

La función de la confidencialidad es ocuparse de conservar la clave de los datos intercambiados y asegurar que la información enviada no sea descubierta por usuarios no autorizados. El medio de transmisión en las redes inalámbricas ocasiona que todos los nodos que están en el rango de transmisión puedan conseguir los datos transmitidos, por esta razón es obligatorio evitar que nodos intermedios y no seguros tengan acceso al contenido de los paquetes que están siendo transmitidos.

1.4.1.2 Autenticación

La autenticación es una confirmación de que la comunicación entre las partes es legítima, los nodos deben mostrar su identidad para que se cumpla esto. Sin autenticación, un oponente podría ocultar un nodo y acceder a información clasificada o también obstaculizar el desempeño de la red.

1.4.1.3 Integridad

La integridad avala que los datos transferidos entre los nodos de la red sean aceptados por las entidades implicadas sin tener cambios por parte de terceros y lo que se ha aceptado sea lo que en un inicio se envió.

1.4.1.4 No repudio

El no repudio posibilita a cada parte de la comunicación demostrar que ha intervenido en la comunicación; una entidad no puede negar que un mensaje ha sido emitido por ella, si esta entidad lo emitió. En el no repudio de origen, el

emisor del mensaje no puede negar haberlo enviado. En el no repudio de destino, el receptor del mensaje no puede negar haberlo recibido.

1.4.1.5 Disponibilidad y Supervivencia

La disponibilidad representa conservar asequible los servicios de la red aun si existieran fallos maliciosos. La supervivencia es la suficiencia de la red para ordenar los servicios después de producirse un fallo malicioso.

1.4.1.6 Anonimato y Privacidad

El anonimato indica que toda información que pueda servir para reconocer el origen, el destino, la ruta de transmisión y el contenido de la información debe permanecer secreta.

1.4.1.7 Control de acceso y Autorización

El control de acceso posibilita limitar el acceso a los recursos de la red a entidades debidamente autorizadas. La autorización instaura normas que determina lo que cada nodo de la red tiene aprobado hacer.

1.4.2 Clasificación de los atacantes

La clasificación se muestra en dos grupos: atacantes externos y atacantes internos.

Los atacantes externos no son parte de la red o del grupo de nodos que se relacionan de forma autorizada. No tienen las claves criptográficas empleadas para asegurar la red y es más factible su detección. Estos atacantes normalmente causan atascos de tráfico o cambian la conducta de los nodos de la red.

Los atacantes internos consiguen el control de un nodo que forma parte de la red por adjudicación ilegal, esto les posibilita el acceso a claves criptográficas usadas para asegurar el funcionamiento de la red. Estos enemigos son de compleja localización, por lo que pueden causar grave daño a la red.

1.4.3 Clasificación general de los ataques

Los ataques a una red inalámbrica están clasificados en dos tipos: ataques activos y ataques pasivos.

Tabla 3. Tipos de ataque en redes inalámbricas

Ataques en redes Inalámbricas	
Pasivos	-(Eavesdropping) Escuchas no autorizadas. -Snooping. -Análisis y monitoreo de tráfico.
Activos	-(Jamming) Interferencia. -(Spoofing) Suplantación de identidad. -(Masquerade) Cambio de campos. del encabezado de protocolo. -(Modification) Modificación de mensajes. -(Fabrication) Fabricación de mensajes. -(Message Replay) Repetición de mensajes.

Tomado de: (Rocabado, 2013)

1.4.3.1 Ataques pasivos

Un ataque pasivo proporciona acceso a información que se desplaza por la red sin interrumpir las comunicaciones, no afecta directamente al sistema, más bien se ocupa de apropiarse de la información mediante escucha clandestina a las comunicaciones inalámbricas y el monitoreo del tráfico para identificar a los participantes de la red y los mensajes intercambiados.

1.4.3.2 Ataques activos

Un ataque activo implica una suspensión, alteración o elaboración de información, cambiando la actividad habitual de la red. .

1.4.4 Medidas de seguridad

Las características y debilidades de las redes mencionadas anteriormente hacen que el cumplimiento de los atributos de seguridad sea un problema difícil de afrontar.

De manera general, estas soluciones proponen la utilización de mecanismos preventivos para asegurar protocolos y aplicaciones, los cuales se centran en las siguientes cuestiones:

- La seguridad física de los nodos.
  La mayor parte de la seguridad de una red depende de la seguridad física de los nodos, debido a que un nodo malicioso es apto para introducir fallos de seguridad en toda la red.
- Soluciones extremo a extremo que demandan la combinación de las redes Ad hoc con una red de infraestructura.
- El incremento de mecanismos de criptografía para proveer servicios de seguridad como confidencialidad y autenticación, para esto es necesaria la gestión de las claves criptográficas.
- La implementación de extensiones de seguridad para los protocolos de encaminamiento disponible.

El estándar adoptado ampliamente para la implementación de seguridad en redes LAN inalámbricas se basa en el estándar 802.11i y se describe brevemente el funcionamiento a continuación.

1.4.4.1 Autenticación de acceso

Se estableció en 802.11i dos procedimientos para mejorar los procesos de autenticación y la encriptación. El funcionamiento para seguridad de una red inalámbrica mediante el sistema WPA2 (Wi-Fi Protected Access 2) personal y otra con autenticación 802.1x conocida como WPA2 Enterprise pudiendo ser implementado con un modo de operación distribuido es decir ad-hoc.

La autenticación tiene las siguientes fases:

Acuerdo sobre la política de seguridad

En esta fase los participantes deben acordar que política se va a usar, las políticas que pueden aceptar los puntos de acceso, se muestran en un mensaje Beacon o Probe Response, después sigue una autenticación abierta que siempre tiene éxito. La respuesta se incorpora en el Association Request la cual es aprobada por un Association Response por parte del punto de acceso.

La información de la política de seguridad que se envía incluye:

- Métodos de autenticación soportados (802.1x, PSK)
- Protocolos de seguridad para tráfico unicast.
- Protocolos de seguridad para tráfico multicast.

Autenticación 802.1x

Esta fase es la autenticación 802.1x basada en EAP (Extensive Authentication Protocol). Comienza con punto de acceso que solicita información de identidad al cliente, el cliente responde con el método de autenticación preferido. Se intercambian una serie de mensajes entre el cliente y el servidor de autenticación y se crea una clave maestra común. El servidor de autenticación envía un mensaje Radius Accept al punto de acceso, el cual tiene la información de MK (Master Key) y un mensaje EAP Success para el cliente.

Jerarquía y distribución de claves

El elemento más importante en la seguridad de la conexión son las claves secretas. Se avala la seguridad usando un conjunto de claves formadas según una jerarquía, cada clave tiene un periodo de vida.

Una vez que se logra la autenticación, se constituye un entorno de seguridad, se generan claves temporales de sesión, estas claves se renuevan regularmente hasta que se cierra el entorno de seguridad. El objetivo de esta fase es crear e intercambiar claves.

1.5 Sistemas aéreos no tripulados

1.5.1 Definición

Un UAV se define como una aeronave en la que no es necesaria la tripulación a bordo, estos vehículos pueden ser autónomos, piloteados remotamente o tener una combinación de ambos (Organización de Aviación Civil Internacional, 2011, pág. 7).

Por otro lado, los UAS término con el cual se denomina a los Sistemas Aéreos no Tripulados, que se consideran como una combinación de la estructura y

robótica de un Vehículo Aéreo No Tripulado más todos los sistemas de comunicación existentes.

En la Figura 7 se puede apreciar los modelos de UAS más comunes. Los dos primeros son de ala fija aplicados en ambientes militares y el tercero con varias hélices usado en entornos civiles donde hoy en día se los emplea para diversas aplicaciones. La mayoría de ellos llevan a bordo sensores y cámaras, proporcionando datos para otras aplicaciones o usados para el ajuste de parámetros de vuelo actuales.

Figura 7. Tipos de Sistemas Aéreos no Tripulados

1.5.2 Aplicaciones de los UAS

Existe un gran número de aplicaciones entre las cuales se destaca las siguientes.

- Teledetección.
- Vigilancia y exploración.
- Transporte.
- Búsqueda y rescate.
- Investigación científica.
- Ataques armados.
- Fotografía y video.

1.5.3 Reglamentación interna

En cuanto a la regulación en el país sobre el uso de estos dispositivos la Dirección General de Aviación Civil (DAC) emitió un comunicado sobre ciertos reglamentos de uso de estos dispositivos entre los cuales menciona:

No deberán realizar vuelos en espacios aéreos controlados, es decir, cerca de aeropuertos y bases aéreas militares dentro de una distancia de 9 Km.

Los dispositivos deberán volar a una altura máxima de 122 metros sobre el terreno.

Si los dispositivos tienen función de vuelo autónomo, el operador debe poder tomar el control de la aeronave en cualquier momento (Dirección General de Aviación Civil, 2015).

2. CAPÍTULO II REDES MESH APLICADAS A UAS

En este capítulo se abordará varios proyectos de comunicación mediante redes de tipo mesh empleando sistemas aéreos no tripulados para conocer cómo se interconectan entre estos dispositivos, extraer las características más importantes de estos proyectos y comprender el funcionamiento y formación de estas redes.

2.1 Proyecto SMAVNET ll

2.1.1 Descripción del proyecto

El proyecto SMAVNET ll surgió con el objetivo de desplegar una red wifi ad-hoc mediante el uso de pequeñas aeronaves no tripuladas para transmitir información entre estos dispositivos y de esta manera construir redes de comunicación inalámbricas para en un futuro emplearlas en situaciones de emergencia, coordinar equipos en tierra y dirigir rescates.

SMAVNET II fue desarrollado en la Escuela Politécnica Federal de Lausana en Suiza e involucra Sistemas de Comunicación móviles y cuenta con el apoyo del departamento federal de defensa suizo.

2.1.2 Características del Sistema

El UAS fue desarrollado por la empresa SenseFly y es un dispositivo de ala fija denominado ebee, cuenta con piloto automático, alcanza velocidades de 15.8 m/s y presenta autonomía de 50 minutos (SenseFly, 2015).

En caso de cambio de misión de vuelo esta puede ser modificada remotamente por su sistema de telemetría y control de enlace a una distancia de hasta 3 Km por medio de un modem wireless modelo n2420 de Microhard Systems. Al ebee fue adaptado un mini ordenador Overo de Gumstix Inc. En la Figura 8 se puede apreciar la composición del dispositivo.

El software incorporado en el mini ordenador está basado en Linux, posee una tarjeta USB wifi 802.11n que junto con el miniordenador forman la red entre los eBee. Como se puede observar en la Figura 9 se realizó una conexión entre el

ordenador y el ebee lo que permite acceder a componentes del dispositivo como energía e información del GPS.

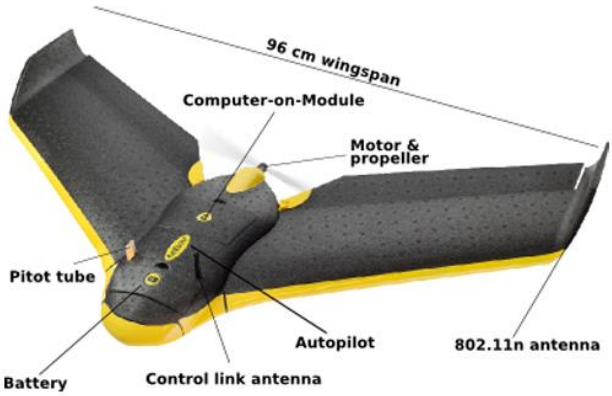


Figura 8. Componentes del eBee.
Tomado de: (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013)

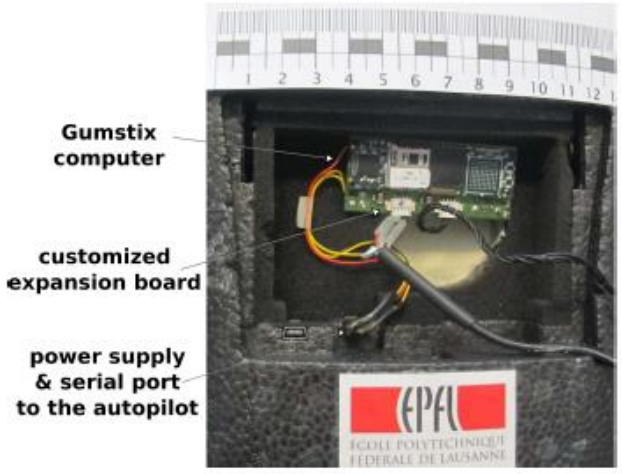


Figura 9. Hardware de comunicaciones del drone.
Tomado de: (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013)

2.1.3 Cobertura y movilidad

Para este proyecto trabajaron implementando redes MANET sobre Sistemas Aéreos no tripulados y se descartan proyectos en los que se emplea topologías

centralizadas como por ejemplo en estrella, debido esencialmente a que se restringe el radio de cobertura al nodo central y más bien se enfocan en redes en modo Ad-hoc con una topología de malla inalámbrica en forma parcial y que admite comunicación multisalto.

Los drones en este caso tienen una movilidad alta por lo que es necesario emplear protocolos que se adapten a esta característica y que al momento de transmitir información a través de varios saltos esta esté lo menos comprometida posible y que también exista buena comunicación con usuarios móviles en tierra.

Como los dispositivos en vuelo tienen un tiempo limitado, deben descender y reemplazar sus baterías, debido a esto es necesario que los algoritmos de comunicación permitan añadir y retirar nodos a la red para aumentar el tiempo de despliegue del sistema en general.

2.1.4 Enrutamiento de los dispositivos

La conexión a nivel de red de estos dispositivos la realizaron mediante OLSRD que es una implementación de código abierto del protocolo OLSR.

OLSR es un protocolo proactivo de enrutamiento por estado de enlace y para este proyecto, fueron modificados ciertos campos de los mensajes que emplea este protocolo para anunciar y difundir rutas hacia los demás nodos.

A esta versión modificada la llamaron POLSR (Predictive Optimized Link State Routing), que calcula la velocidad de cada dispositivo y la información es difundida entre cada par de nodos mediante la función de detección de vecinos es decir por medio de mensajes HELLO y mensajes TC de control de topología. Al ser estos campos modificados no son compatibles con su RFC y por ende todos los nodos de la red deben usar la misma versión del protocolo.

Los parámetros como altitud, latitud y longitud fueron obtenidos del GPS para calcular la velocidad entre los nodos. En la figura 10 se aprecia una comparación entre el formato del paquete de un mensaje HELLO tradicional y uno modificado.

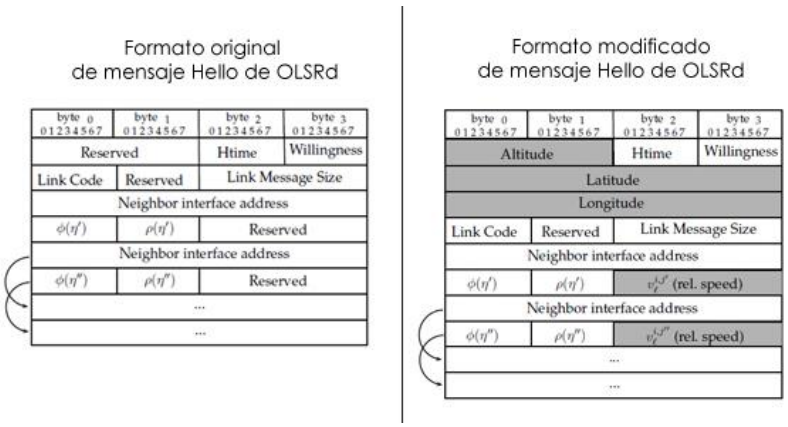


Figura 10. Formato de mensajes Hello y Hello modificado. Tomado de: (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013)

2.1.5 Experimentos

2.1.5.1 Evaluación de rendimiento del enlace.

En este experimento establecieron una red de 2 nodos compuesto por un nodo en el suelo y un UAS. El objetivo de este experimento fue hacer una medición de la cantidad de paquetes perdidos de acuerdo a la distancia variable que existe entre el emisor y el receptor en una transmisión en tiempo real. El UAS planeó entre dos checkpoints ubicados a 450 metros de distancia el uno del otro y colocados a una altura de 75 metros.

Se calculó la tasa de los datagramas perdidos dependiendo de su distancia mientras se realizaba una transmisión de video.

El Datagram Loss Rate (DLR) es la relación entre los datagramas perdidos del total de datagramas enviados y como se aprecia en la figura 11 con este valor se obtiene un promedio de DLR cada 20 metros en todo el trayecto. Hasta los 300 metros las pérdidas fueron mínimas, llegando a un 1% para los 450 metros.

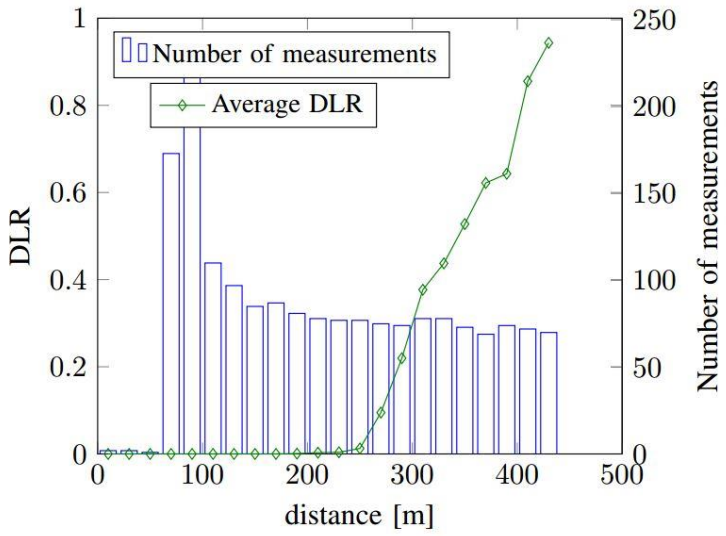


Figura 11. Medición de los datagramas perdidos en el trayecto. Tomado de: (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013)

Tomaron Hello Interval, es decir el periodo de emisión de mensajes Hello, similar al OLSR tradicional de 2 segundos que gracias a los parámetros obtenidos del GPS contribuye a la estimación la evolución de la calidad del enlace.

2.1.5.2 Evaluación de desempeño del enrutamiento

Para el segundo experimento de este proyecto emplearon 3 nodos, el nodo número 1 en la terraza de un edificio a 10 metros de altura, el número dos y tres son drones de origen y de retransmisión volando a 75 metros de altura. El drone número dos sigue una trayectoria recta de 600 metros partiendo del edificio. El drone número tres sigue una trayectoria circular de 30 metros de radio a 250 metros del nodo uno en el edificio. En la Figura 12 se puede apreciar cómo se desarrolló la prueba y en la figura 13 el resultado (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013).

Realizaron 10 vueltas empleando cada protocolo OLSR y POLSR para comprobar que el enrutamiento cambia de uno a dos saltos y viceversa y cuáles fueron las pérdidas a causa del cambio de ruta.

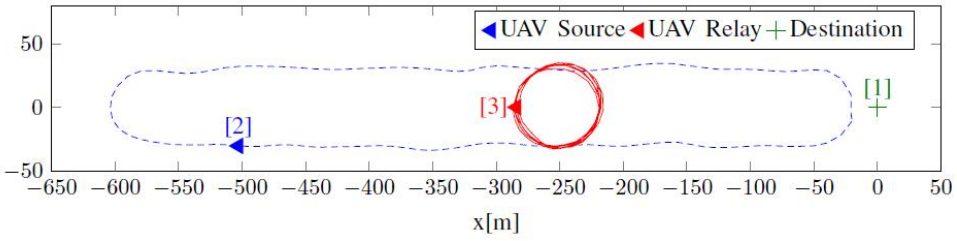


Figura 12. Evaluación del desempeño del enrutamiento.
Tomado de: (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013)

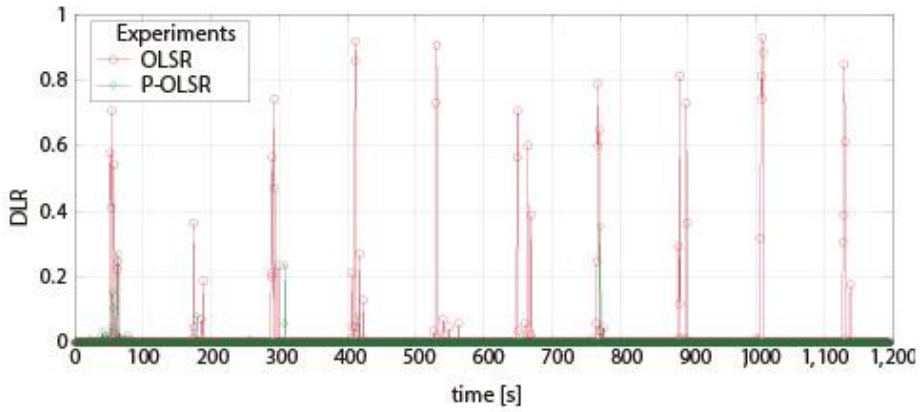


Figura 13. Comparación de la pérdida de paquetes con OLSR y P-OLSR.
Tomado de: (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013)

Como se observa en la figura anterior las pérdidas con P-OLSR fueron mínimas en los momentos en que cambia el enrutamiento de uno a dos saltos, llegando a un porcentaje de 0.2% en comparación a los picos de perdida experimentados con OLSR tradicional.

Después analizar el proyecto SMAVNET II se puede extraer:

- El Empleo de un sistema descentralizado de funcionamiento de una red ad-hoc compuesta por UAS y estación en tierra.

- El funcionamiento del protocolo de enrutamiento OLSR predictivo (Protocolo modificado) en una red Ad-hoc y compararlo con el protocolo

OLSR tradicional para demostrar que la modificación del protocolo tiene una mejor efectividad al momento de enrutar un paquete hacia el destino a través del nodo reenviador disminuyendo el tiempo que toma encontrar la nueva ruta generando de esta manera menos perdidas en la transmisión.

- La modificación del protocolo toma los valores de posición del UAS emisor y receptor, calcula la velocidad y distancia el uno del otro y en base a eso determina la elección de una nueva ruta antes de perder el enlace completamente.

2.2 Proyecto UAVNET

2.2.1 Descripción del proyecto

En este proyecto se describe el funcionamiento de una WMN (Wireless Mesh Network) adaptable y móvil utilizando Sistemas aéreos no tripulados (UAS). Incluye un concepto y un prototipo de aplicación de una WMN temporal con un despliegue autónomo, usando vehículos aéreos no tripulados con nodos mesh inalámbricos. La red de comunicaciones permite la conectividad entre las diferentes estaciones en tierra como laptops, Smartphones etc.

2.2.2 Características del sistema

Está compuesto por un UAS de cuatro hélices fabricado por Mikrokopter, un enrutador, un GPS y es alimentado por su batería que brinda energía por 30 minutos. En la Figura 14 se puede observar los componentes del UAS.

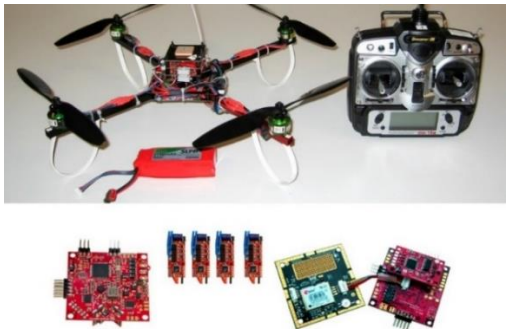


Figura 14. Componentes electrónicos del UAS.
Tomado de: (Morgenthaler, 2012).

Para el nodo mesh que se observa en la Figura 15 se observa un enrutador OM1P de Open Mesh y el software instalado es ADAM (Administration and Deployment of Ad-hoc Mesh networks) el cual está basado en software libre y permite trabajar con dos estándares 802.11g y 802.11s. La conexión con el UAS es mediante cable serial y también del UAS es de donde obtiene la energía. Esta conexión serial permite obtener varios parámetros como su longitud, latitud, altura y velocidad que son enviados a una aplicación de una estación receptora y así poder modificar estos parámetros.

Figura 15. Nodo mesh OM1P de Open Mesh.
Tomado de: (Morgenthaler, 2012).

2.2.3 Cobertura y movilidad

En este proyecto lograron extender el área de cobertura de una red LAN convencional para su aplicación en lugares donde existen distancias considerables entre el emisor y el receptor o la geografía es un obstáculo para

la comunicación, es por esto que, mediante el apoyo de uno o varios enrutadores inalámbricos adaptado a drones se busca solucionar estos inconvenientes.

Al existir degradación de la señal debido a la distancia entre emisor y receptor mientras más lejanos estén los dispositivos que conforman la red se requiere el uso de UAS adicionales para mantener una tasa de transmisión adecuada en función del tipo de aplicación a usar.

2.2.4 Experimentos

2.2.4.1 Escenarios de funcionamiento de la red

Tomaron en cuenta estos escenarios:

El primer escenario consiste en una red con 2 dispositivos en tierra y un UAS que actúa como enlace entre estos.

En un inicio el primer dispositivo en tierra es encontrado mediante el intercambio de mensajes ping entre este y el UAS para luego enviar su ubicación al UAS. El proceso se repite para encontrar al segundo dispositivo en tierra y ya teniendo la ubicación de ambos, el UAS calcula un punto medio entre los dos para determinar la posición final que tendrá para brindar cobertura a los dispositivos en tierra.

El segundo escenario está compuesto por 3 UAS que retransmiten la información de un dispositivo al otro. Para esto el primer UAS obtiene la posición del primer y segundo dispositivo en tierra y anuncia las posiciones al segundo UAS, el primer UAS se ubica a una distancia cercana al primer dispositivo en donde tenga la intensidad de la señal óptima configurada por el usuario. Posteriormente con la información del primer UAS, el segundo y tercer UAS toman posición formando una cadena hasta llegar al segundo dispositivo y establecer la conexión.

En la Figura 18 se representa estos dos escenarios, el primero con un UAS como nodo reenviador entre 2 puntos y el segundo escenario con 3 UAS formando un enlace entre los dispositivos en tierra.

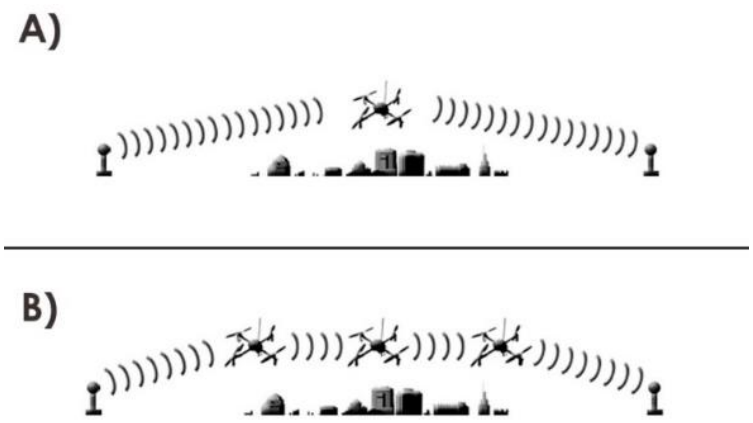


Figura 16. Escenarios de aplicación.
Tomado de: (Morgenthaler, 2012).

A) Con un drone reenviador.
B) Con tres UAS reenviadores.

Del primer escenario se destaca el empleo de algoritmos de búsqueda, en este proyecto el autor menciona la posibilidad de emplear una búsqueda automática o dirigida para encontrar otros dispositivos; así como también el posicionamiento en función de la intensidad de la señal mediante un parámetro configurado previamente. En el escenario siguiente se aprecia cómo se determina dicho valor.

2.2.4.2 Umbral óptimo de intensidad de señal

Tomaron en cuenta a dos nodos mesh mientras la distancia entre estos variaba, usaron la herramienta *netperf* para enviar mensajes TCP y UDP. La medición de la intensidad de la señal se la determinó con *iw la* herramienta para la configuración de interfaces wireless. A continuación, en la figura 19 la medición del rendimiento TCP.

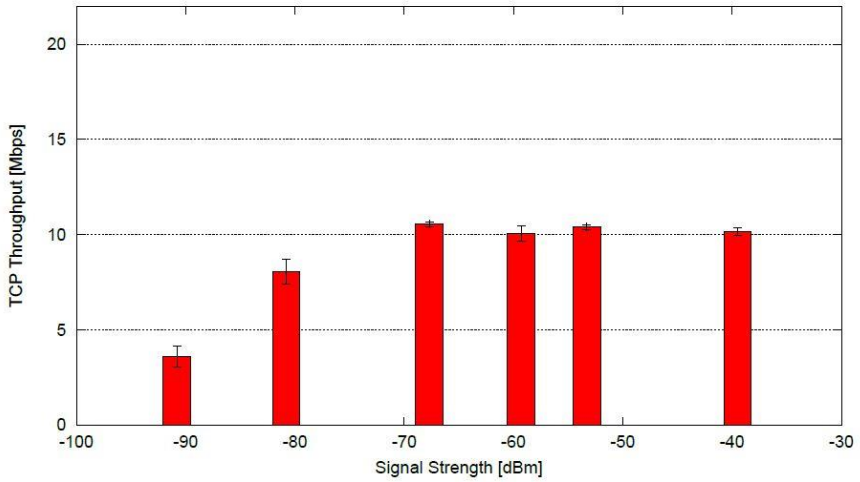


Figura 17. Rendimiento empleando TCP en función de la intensidad de señal.
Adaptado de: (Morgenthaler, 2012).

Los resultados del rendimiento en TCP arrojaron que para una intensidad de señal superior a -70 dBm el rendimiento del enlace llegaba a 10 Mbps e iba decreciendo a mayor distancia, mientras que el rendimiento con UDP como muestra la figura 20 es ligeramente superior alcanzado tasas de 16 a 17 Mbps en promedio.

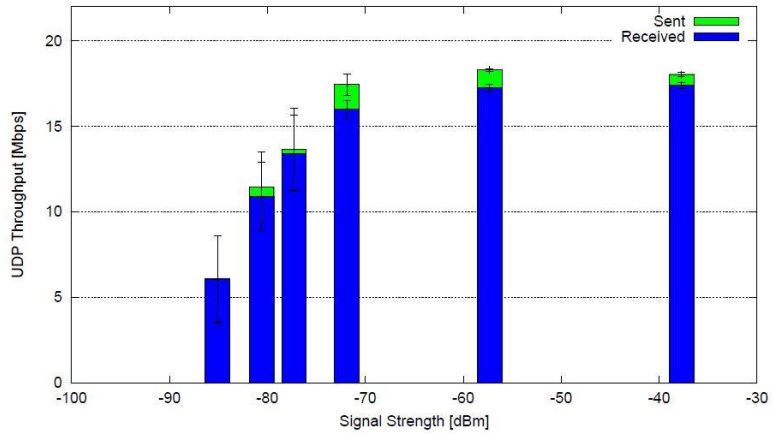


Figura 18. Rendimiento empleando UDP en función de la intensidad de señal.
Tomado de: (Morgenthaler, 2012).

Con los resultados de este segundo escenario se puede destacar los problemas que ocasiona la distancia entre los dispositivos. El problema en las conexiones TCP es que cuando hay distancias considerables o atenuaciones en el trayecto hay pérdida de paquetes por lo que el receptor no envía confirmación de haberlos recibido, se realizan retransmisiones y se reduce la ventana de transmisión, por ende, se reduce el rendimiento. Por otro lado, en conexiones con UDP al no ser orientado a conexión el rendimiento es algo superior, pero de igual manera existe perdida de paquetes.

2.2.4.3 Desempeño Multisalto

En esta prueba se utilizaron 4 nodos mesh con similares parámetros de la configuración anterior e intensidad de señal y se evaluó el rendimiento para un salto, 2 saltos y tres saltos. El esquema se observa a continuación en la figura 21.

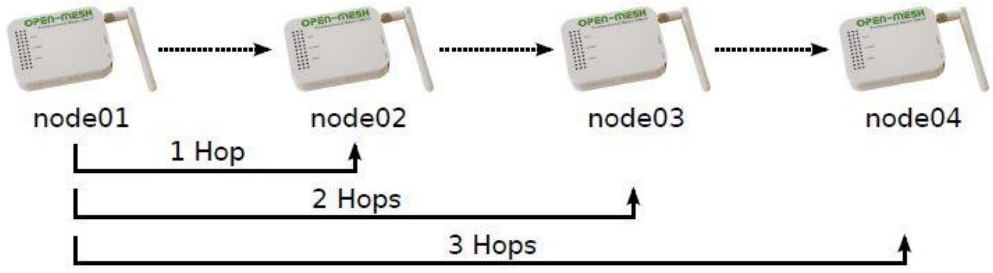


Figura 19. Esquema de envío multisalto.
Tomado de: (Morgenthaler, 2012).

En el primer salto el rendimiento tuvo tasas de transmisión similar al anterior experimento, pero al segundo y tercer salto se produce cierta disminución debido a que el enlace de radio emplea la misma frecuencia y el mismo canal para los 4 nodos disminuyendo el rendimiento promedio desde el emisor al receptor. Los resultados se muestran a continuación en la figura 22.

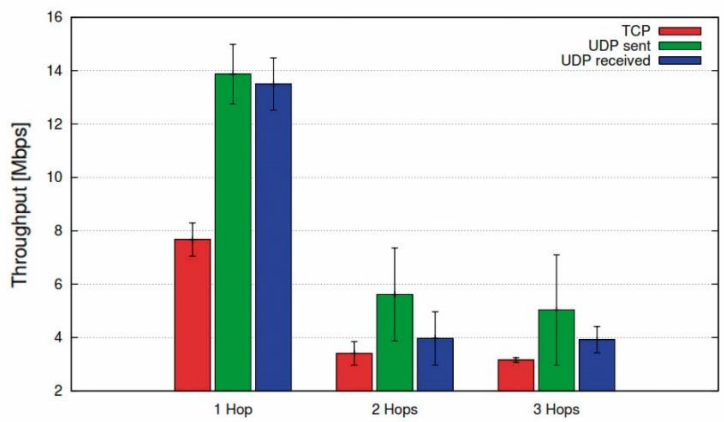


Figura 20. Rendimiento multisalto en red mesh.
Tomado de: (Morgenthaler, 2012).

Después analizar el proyecto UAVNET II se puede extraer:

- La importancia de establecer una distancia adecuada para llegar a una tasa de transmisión óptima donde se obtenga menores perdidas y mayor rendimiento en especial con transmisiones que son orientadas a conexión.

- El considerar el diseño de un enlace con el menor número de retransmisiones posibles porque al ser una red que trabaja en el mismo rango de frecuencias y el mismo canal de igual manera degrada el rendimiento.

- El emplear una tecnología 802.11s para formar la red entre los UAS, permite la creación de un sistema de distribución inalámbrico, diferenciación de dos segmentos de red, entre otros.

- El uso de algoritmos para determinar posiciones que deben adoptar los UAS con el fin de optimizar la cantidad de dispositivos en el aire y el desempeño de la red por los inconvenientes antes mencionados.

2.2.5 Enlace de los dispositivos

Para formar la red en este sistema se empleó dos configuraciones. Para el acceso inalámbrico de los dispositivos en tierra hacia los UAS mediante el estándar 802.11g, mientras que para el tráfico entre los nodos adaptados en los UAS es mediante 802.11s.

Los UAS poseen direcciones IP estáticas mientras que las direcciones de los dispositivos en tierra se les asignan direcciones dinámicamente mediante DHCP.

Los nodos de la malla se establecen como (MAP) Puntos de Acceso Mesh que son capaces de interconectar diferentes tipos de redes tanto a dispositivos clientes como la interconexión entre los nodos mesh.

En la Figura 16 se observa las configuraciones empleadas tanto para la conexión de los dispositivos hacia los UAS, así como entre los 2 UAS que forman la red mesh.

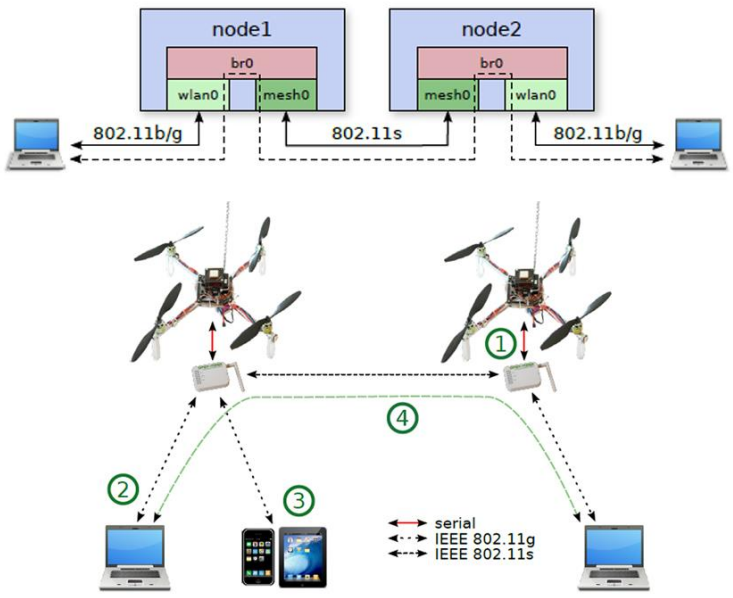


Figura 21. Configuración de una red mesh con UAS.
Tomado de: (Morgenthaler, 2012).

El software que emplearon es una distribución de Linux para redes mesh llamado ADAM que por ser un software liviano y porque desde la versión 2.6.26 del kernel Linux se incluyen nativamente los componentes necesarios para implementar un enlace mesh como se propone en el estándar 802.11s.

En la Figura 17 se observa la arquitectura de comunicación que consiste en la aplicación Uavcontroller desarrollada en lenguaje de programación C para gestionar los datos recibidos de los sensores o GPS de los UAS a través de la librería “libuavint” y que posteriormente serán enviados mediante sockets TCP y UDP de la librería “libuavext” hacia el siguiente nodo de la red mesh o al dispositivo final.

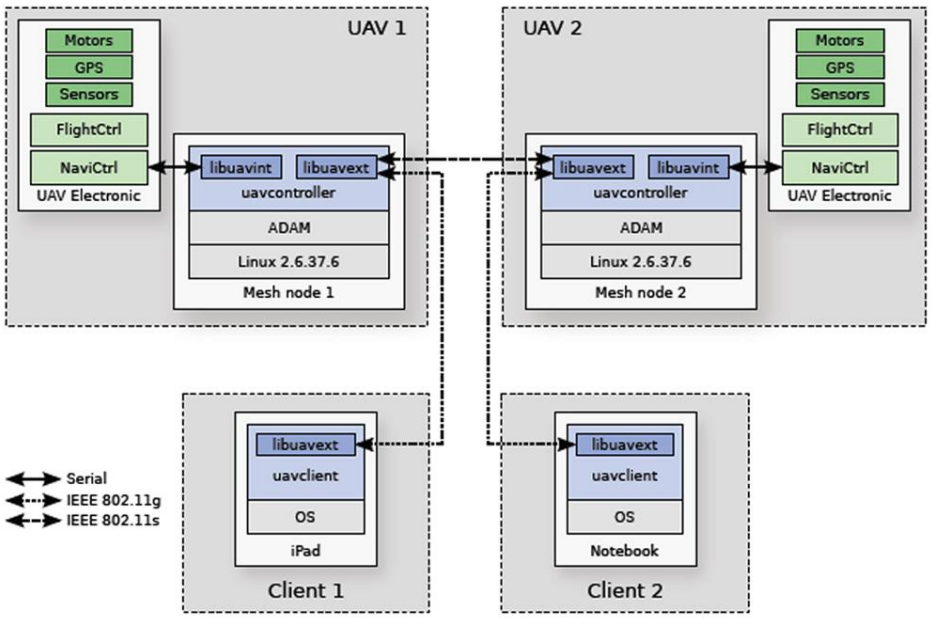


Figura 22. Arquitectura de la red UAVnet.
Tomado de: (Morgenthaler, 2012).

2.3 Proyecto AUGNET

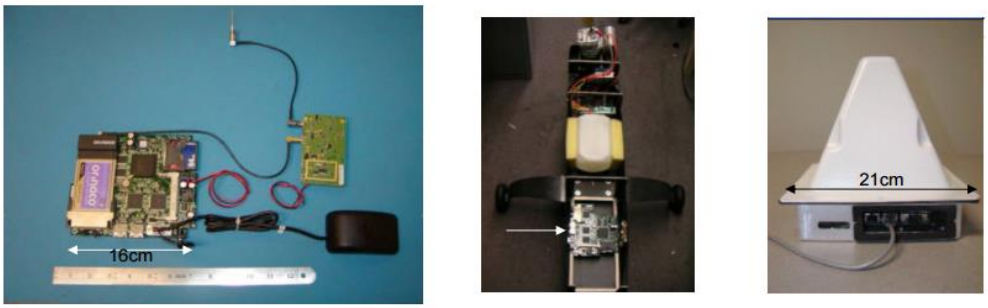
2.3.1 Descripción del proyecto

En este proyecto se implementó una red móvil ad-hoc mixta compuesta de nodos fijos en tierra, nodos móviles en tierra y un sistema aéreo no tripulado, el

proyecto fue desarrollado por estudiantes de la Universidad de Colorado en el año 2004 y en el cual se analizaron escenarios de conectividad entre nodos en tierra y aire.

2.3.2 Características del Sistema

El proyecto está compuesto por un Sistema Aéreo No Tripulado de ala fija construido en la misma Universidad y sobre el cual se adaptó, como se aprecia en la Figura 23, un micro computador Soekris, una tarjeta Orinoco Wireless 802.11b, un GPS y un amplificador de 1 W de salida. En lo que se refiere a software, se empleó una distribución basada en Linux llamada WISP-Distribution y DSR como protocolo de enrutamiento.



(A) (B) (C)

Figura 23. Componentes del sistema AUGNET
Tomado de: (Brown, y otros, 2004)
(A) Hardware (microcomputador, tarjeta Wireless, GPS)
(B) Dispositivo montado en el UAS
(C) Protección externa

2.3.3 Cobertura y movilidad

Las pruebas fueron realizadas en una extensión aproximada de 7Km^2 con nodos distribuidos de acuerdo a como se observa en la Figura 19, se colocaron dispositivos fijos, móviles y un UAS.

2.3.4 Enrutamiento de los dispositivos

Como se trata de un encaminamiento descentralizado se empleó el protocolo de enrutamiento DSR (Dynamic Source Routing) implementado en un sistema Linux tanto para los nodos en tierra como para el UAS. Como ya se mencionó, el dispositivo no tripulado cuenta con un microcomputador adaptado para funcionar como enrutador y sobre este configurar las características del protocolo de enrutamiento.

2.3.5 Experimentos

El banco de pruebas fue en Boulder Colorado en una extensión de 7 km^2 despejado sin obstáculos e interferencias ajenas al sistema. Realizaron 2 experimentos en los que evaluaron la latencia y el rendimiento.

En el primer experimento emplearon 5 nodos en tierra y 1 UAS.

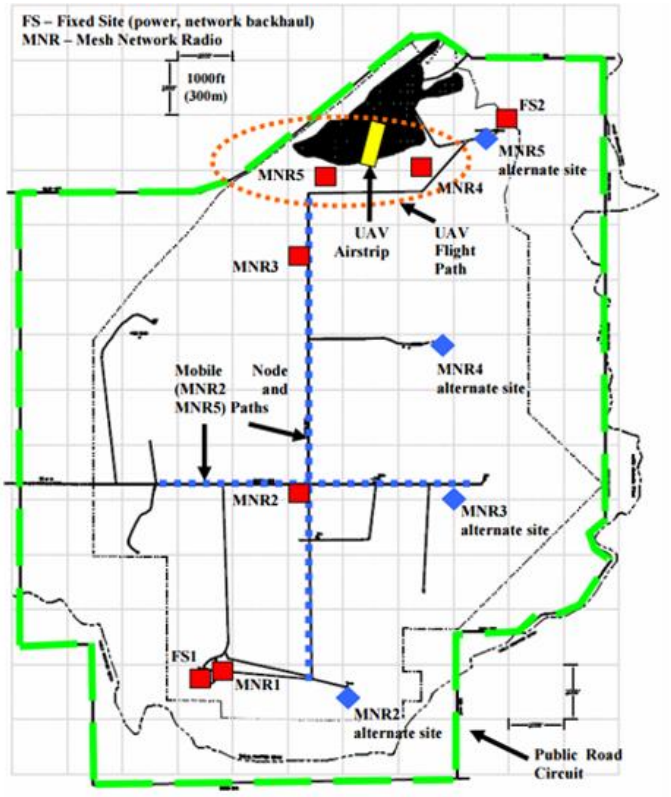


Figura 24. Área de pruebas de la red AUGnet.
Tomado de: (Brown, y otros, 2004)

2.3.5.1 Rendimiento

Los 5 nodos colocados empezaron a transmitir datos, primero sin la presencia del UAS entre todos los nodos. Después incluyeron al UAS con el fin de que el protocolo de enrutamiento pueda identificar una ruta más corta entre cada par de nodos para que de esta manera pueda mejorar el rendimiento.

Los resultados en la Figura 25 muestran una mejora en el rendimiento al emplear el UAS.

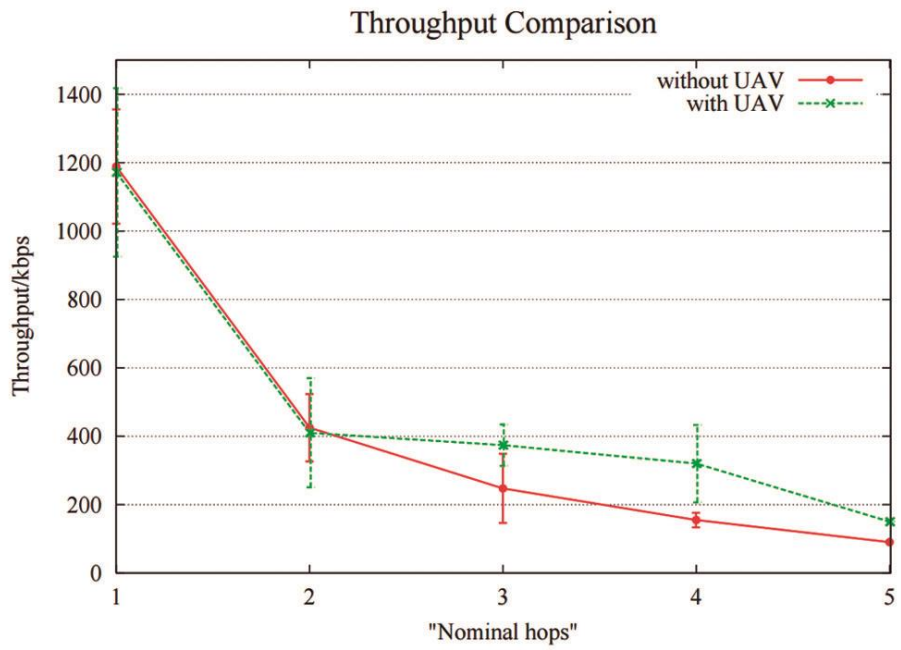


Figura 25. Rendimiento de acuerdo al número de saltos con y sin UAS. Tomado de: (Brown, y otros, 2004)

En este escenario analizaron el rendimiento, el cual va a depender de varios factores como la distancia, el número de saltos, si los nodos son fijos o móviles o emplean un UAS. La comunicación se establece entre origen y destino, ya sea de forma directa con un camino de un solo salto o por uno o más nodos de retransmisión indicando una ruta de saltos múltiples; aquí el protocolo DSR busca una ruta al destino cuando tiene datos que enviar. Por lo tanto, los nodos no desperdician el canal de transmisión tratando de establecer rutas que nunca

van a utilizar. Cuando el nodo origen necesita enviar un paquete a un destino, el protocolo inicia un proceso de petición de ruta entre todos los nodos para establecer la mejor ruta.

De lo señalado anteriormente se puede comprobar que el rendimiento entre emisor y receptor mejora con la ayuda de un UAS y hasta llega a duplicarse debido a que existe un menor número de saltos que en una comunicación solo con los nodos en tierra.

2.3.5.2 Latencia

En el segundo experimento evaluaron la latencia. Lo realizaron en dos grupos de dos nodos fijos adyacentes separados por dos nodos móviles (automóviles). Los dos nodos móviles tomaron trayectorias circulares en sentidos opuestos con el fin de interconectar a ellos mismo y a los dos grupos de nodos fijos. Después emplearon el UAS entre estos dos grupos y de igual manera evaluaron la latencia entre los nodos fijos, los nodos móviles y finalmente entre los nodos fijos y móviles como reenviadores. (Brown, y otros, 2004)

Los resultados pueden ser observados en la Figura 26.

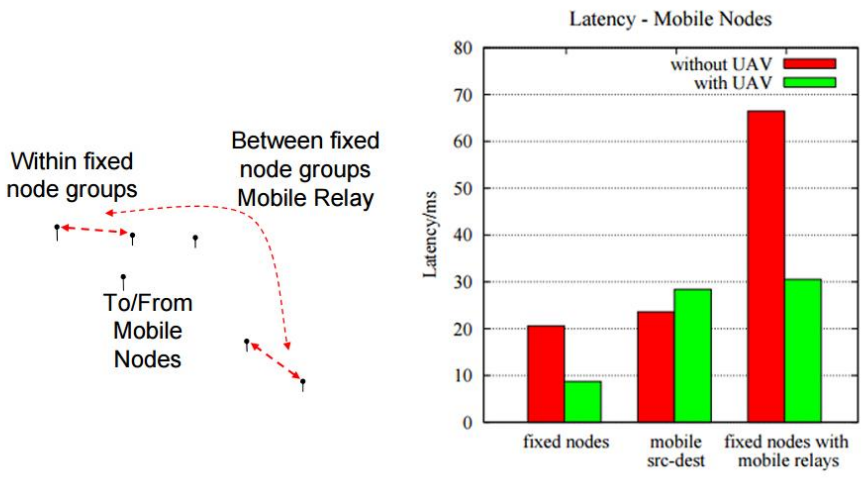


Figura 26. Medición de latencia entre nodos fijos móviles y UAS.
Tomado de: (Brown, y otros, 2004)

En este segundo experimento se analiza la latencia que es la suma de los retardos que se producen por la demora en la transmisión de los paquetes dentro de la red. Aquí se observa que la latencia entre nodos fijos es inferior al emplear el UAS, ya que el UAS puede servir para evitar los nodos móviles en tierra, el protocolo DSR escoge la mejor ruta y por lo tanto puede proporcionar un enlace más fiable para los nodos fijos.

Posteriormente cuando los nodos son móviles no existe mayor diferencia si se emplea o no el UAS teniendo en promedio entre 20 y 30 ms y finalmente cuando se evalua la latencia entre los nodos fijos con el UAS como reenviador es muy inferior en comparación a cuando se emplea los nodos móviles en tierra por la misma razón que el protocolo DSR escoge la mejor ruta y puede dar un mejor enlace con los nodos fijos.

Del proyecto AUGNET se puede extraer:

- Se usa una red Ad-hoc formada por nodos fijos en tierra, nodos móviles y un UAS.
- Se busca mejorar el desempeño de la red Ad-hoc, tanto en el rendimiento como en la latencia, esto se logra con el uso del UAS y el protocolo DSR.

2.4 Resumen de los proyectos

Al revisar estos casos de aplicación de redes mesh en Sistemas Aéreos no tripulados se puede establecer un esquema comparativo entre las características de su funcionamiento la cual se detalla en la tabla 4 a continuación.

Tabla 4. Comparación entre las características de los 3 proyectos.

Características de los proyectos								
Proyecto	Aplicación	Cobertura	Protocolos de Comunicación	Número de nodos	Altitud	Tipo de UAS	Autonomía UAS	Movilidad
SMAVNET II	Video UDP	250, 450 y 600 (m) origen a destino	802.11n POLSR	3	75 (m)	Ala fija	50 min	Alta
UAVNET	Mensajes TCP/UDP	Intensidad de señal -70dBm entre nodos	802.11g 802.11s	4	No especifica	Quadcopter	20 min	Media
AUGNET	Voz y datos	1000 a 2000 (m) entre cada nodo	802.11b DSR	6	No especifica	Ala fija	60 min	Baja

3. CAPÍTULO III ANÁLISIS DE LA RED

Después de describir el funcionamiento de varias redes mesh mediante algunos prototipos y escenarios se puede resaltar algunas características de su funcionamiento.

Tienen un despliegue rápido y el tiempo de funcionamiento es limitado, varía de acuerdo al tipo de UAS y si el enrutador toma energía directamente de este o si adapta baterías externas.

Al ser redes móviles, emplear el mismo rango de frecuencia 2,4 o 5 GHz y mismo canal para la emisión y recepción de señales produce algunos inconvenientes como la interferencia. Esta es una diferencia en relación a las redes mesh tradicionales en las que su backbone generalmente es estático y usa tecnologías multi radio.

Otros factores producto de la movilidad de los dispositivos son el rendimiento y latencia variable debido a la distancia, el número de nodos entre el emisor y el receptor.

En aplicaciones que empleen protocolos orientados a conexión como TCP los paquetes necesitan confirmación de mensajes por parte del receptor, al existir perdidas de paquetes o congestión tal confirmación no existe y esto obliga al renvió de estos paquetes disminuyendo la ventana de transmisión en consecuencia reduciendo la tasa de transmisión. En el caso del tráfico UDP que generalmente se emplean en aplicaciones en tiempo real como voz o video existen pérdidas de paquetes, pero no hay retransmisiones.

Un punto importante para la interconexión de los nodos UAS son los protocolos de enrutamiento a emplear. La mayoría de protocolos tradicionales fueron creados para esquemas de red en infraestructura. En los escenarios descritos en el capítulo anterior se emplean protocolos para redes ad-hoc como OLSR y DSR. Adicionalmente con el empleo de esquemas de tecnología para redes de malla como 802.11s se busca estandarizar la formación de estas redes.

A continuación, se describe el funcionamiento de las redes MANET y las redes mesh con el estándar 802.11s, así como el funcionamiento de los protocolos de enrutamiento especializados para este tipo de redes.

No se ha considerado otras tecnologías para la formación de redes de malla inalámbrica como Zigbee o WIMAX por características propias de su tecnología como cobertura, tasas de transmisión o por no disponer de documentación que sustente el uso sobre plataformas aéreas no tripuladas.

3.1 Redes Mesh 802.11s

En redes mesh convencionales cada fabricante tiene su implementación del sistema de distribución inalámbrico WDS (Wireless Distribution System) con el fin de interconectar a los distintos puntos de acceso de la red, pudiendo de esta manera reducir el funcionamiento del sistema a solo equipos del mismo fabricante. Con el desarrollo de la enmienda para redes mesh por el IEEE con la especificación 802.11s lo que se busca es:

- Estandarizar la formación de redes mesh para volverlas compatibles independientemente de la marca de dispositivos que estas empleen.
- Que la red mesh funcione de manera similar como funciona un conjunto de servicio extendido en redes cableadas.
- Tener una red con facilidad de autoconfiguración.
- El poder implementar protocolos de seguridad.

Así como existen los modos de operación infraestructura y ad-hoc, 802.11s específica el modo de operación mesh MBSS que considera únicamente al enlace entre dispositivos que tengan la capacidad de implementar esta configuración, creando una interfaz virtual para formar un sistema de distribución entre los dispositivos pertenecientes a la red.

El diseño e implementación de redes bajo este estándar significa una mejora en la movilidad en cuanto a los componentes y usuarios finales conservando una estructura, encaminamiento a nivel de capa enlace y convirtiéndola en una tecnología aplicable a Sistemas Aéreos No Tripulados.

3.1.1 Descubrimiento de nodos

El proceso de descubrimiento de nodos se lo realiza mediante un perfil de malla que son un grupo de parámetros que componen inicialmente la red mesh. El perfil de malla está formado por dos campos: el identificador de malla similar al SSID y el campo de configuración de malla que posee varios campos que definen características del nodo mesh en la red entre los cuales se puede mencionar:

- El protocolo de selección de camino.
- La métrica empleada para la selección del camino.
- Identificador del protocolo de control de congestión.
- Protocolo de autenticación entre nodos
- Elemento de formación de la mesh para informar cuantos pares conectados tiene la estación y si tiene conexión a otro tipo de redes.
- Capacidad de la red mesh para aceptar o no emparejamientos con nuevos nodos

3.1.2 Emparejamiento de nodos

Posteriormente que los MP se unen a la red proceden con el protocolo de emparejamiento con otros nodos vecinos. Este protocolo se encarga de controlar los nodos que se unen o se desconectan de la red.

El proceso inicia con un MP al enviar una trama (Peer Link Open) y el MP con el que se desea establecer el emparejamiento responde con un (Peer Link Confirm). El proceso se repite por cada nodo y se lo observa en la Figura 27.

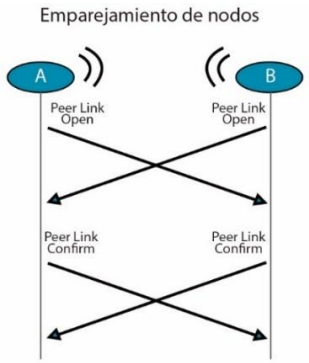


Figura 27. Proceso de emparejamiento de nodos.

3.1.3 Control de Acceso al Medio

Emplean el protocolo EDCA (Enhanced Distributed Channel Access) que a su vez es una variante de la función de coordinación distribuida. La ventaja de EDCA es la posibilidad de brindar calidad de servicio en la capa de enlace clasificando el tipo de tráfico en 4 categorías de acceso como voz, video, best effort y background al cual se le asignan distintos espacios de tiempo entre tramas dando prioridad a las tramas que tengan menor espacio de tiempo y que corresponderá al trafico prioritario.

3.1.4 Formato de la trama

A la trama 802.11 como se observa en la Figura 28 se incluye un campo adicional denominado de control de malla que se emplea para extender el número de direcciones que puede llevar una trama tradicional y para funciones del encaminamiento.

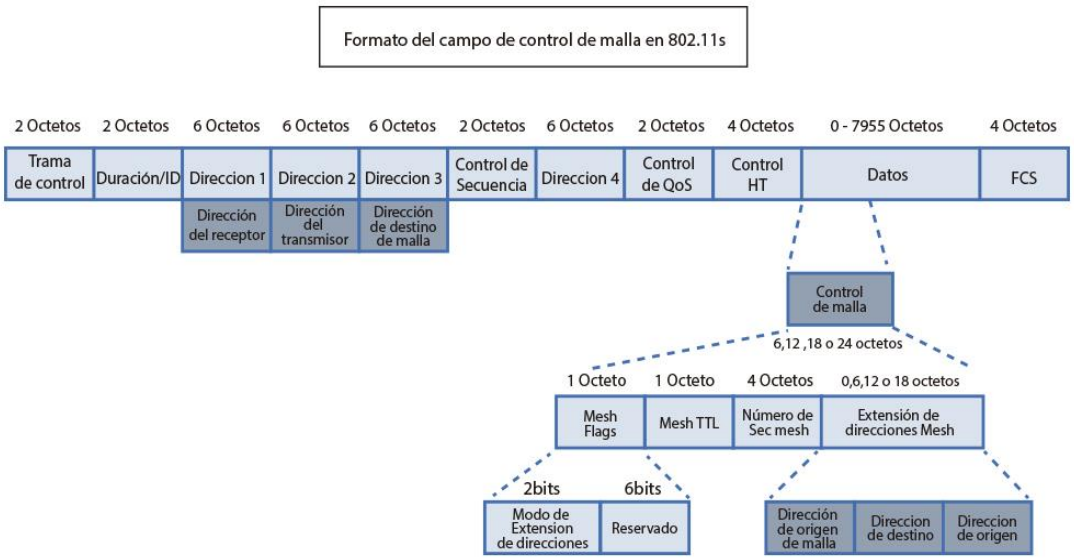


Figura 28. Formato de trama de 802.11s
Tomado de: (Hiertz, y otros, 2010)

Los cuatro campos dentro del control de malla son:

- **Mesh Flags** - Empleado para el control.
- **Mesh TTL** - Limita el número de saltos en el encaminamiento.
- **Mesh Número de secuencia** - Elimina tramas duplicadas debido al broadcast.
- **Extensión de direcciones mesh** – Hasta 3 direcciones MAC adicionales.

3.1.5 Componentes de la red

El estándar define 3 tipos de nodos:

- **MP (Mesh Point):** Dispositivos que se encargan exclusivamente del encaminamiento.
- **MAP (Mesh Access Point):** Nodos con capacidad reenvió de tráfico agregado de otras estaciones 802.11
- **MPP (Mesh Portal):** Nodos para interconexión a otras redes.

En la Figura 29 se puede observar los principales componentes de la red mesh basada en el estándar 802.11S.

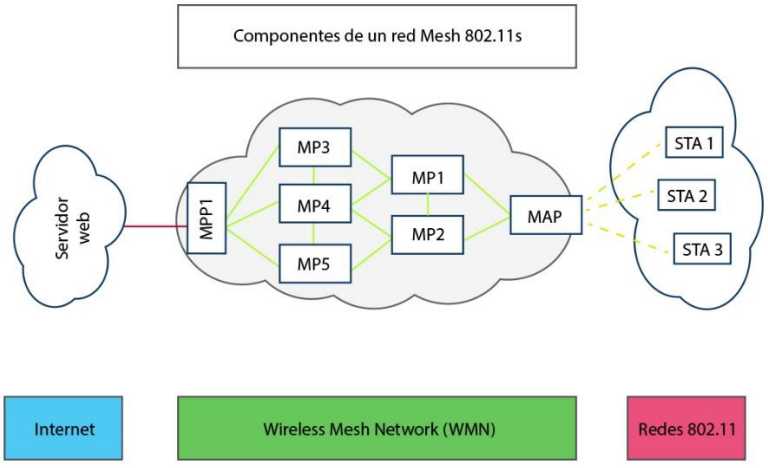


Figura 29. Componentes de una red 802.11s

3.1.6 Control de congestión

Presenta un mecanismo de control de congestión salto a salto en el que cada MP toma en cuenta el tráfico que ingresa y sale del nodo. Cuando la capacidad de procesamiento es incapaz de transmitir la cantidad de datos que recibe se produce congestión por lo que el MP debe informar a los nodos vecinos para limitar la tasa de transmisión a dicho MP.

Se determina el tamaño de la cola por la diferencia que existe entre paquetes enviados y recibidos a nivel MAC. Mediante la señalización se envía un mensaje “Neighborhood Congestion Announcement” para limitar el tráfico en base a criterios de EDCA a través de la diferenciación de servicios.

3.1.7 Encaminamiento en 802.11s

802.11s realiza el reenvío de paquetes para los MP’s, MAP’s y STA’s y es necesario que la cabecera MAC tenga al menos 4 direcciones. Las direcciones MAC origen y destino no sufren cambios a lo largo del trayecto mientras que las otras direcciones cambian con cada salto.

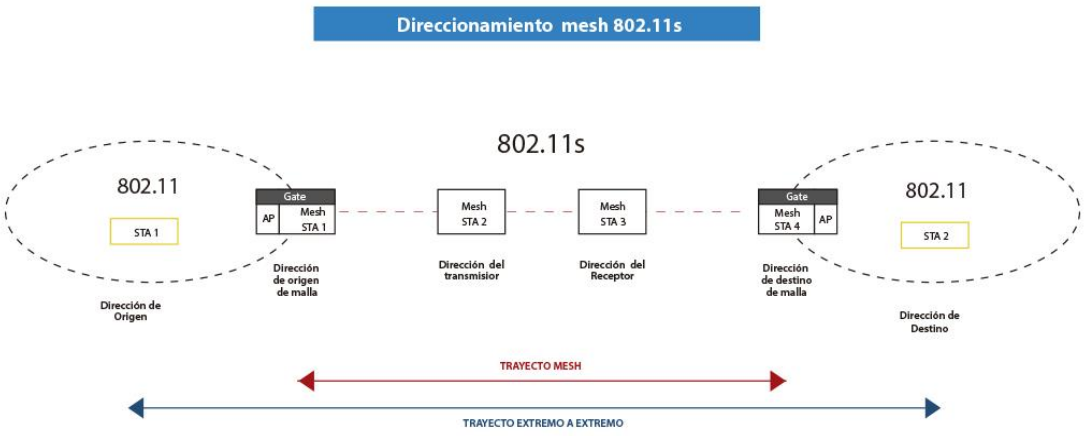


Figura 30. Direccionamiento mesh 802.11s

Se puede identificar los distintos tipos de nodos con el fin de realizar encaminamiento y diferenciar el trayecto de una red mesh de una red basada en 802.11 y comprender porque se añaden direcciones MAC en la trama para realizar este proceso. Un ejemplo de esto se puede apreciar en la Figura 30.

El estándar 802.11s propone un esquema de encaminamiento a nivel de capa enlace mediante el uso de su dirección MAC y emplea encaminamiento híbrido HWMP (Hybrid Wireless Mesh Protocol) es decir una combinación de encaminamiento proactivo y reactivo pero adaptados a la capa enlace y pudiendo actuar independientemente el uno del otro.

Para el encaminamiento reactivo emplea procedimientos similares a AODV como:

- **PREQ (Path Request):** Solicitud de camino.
- **PREP (Path Reply):** Respuesta de camino.
- **PERR (Path Error):** Error en el camino.

Tomando como ejemplo la figura anterior se puede describir este procedimiento.

La estación 1 necesita comunicarse con la estación 2, para esto quien inicia el descubrimiento de ruta con un PREQ es la estación mesh 1 que se denomina dirección de origen de malla que llevará adjunta la dirección de la estación 1, el primer receptor es la estación mesh 2 y luego la estación mesh 3 hasta llegar a la dirección de malla de destino en la estación mesh 4 quien finalmente responderá con un PREP hacia la estación mesh 1 y empezará la comunicación entre la estación 1 y 2.

Para el encaminamiento proactivo emplea una estructura de árbol donde se establece un nodo raíz que es el encargado de emitir mensajes PREQ proactivos para alcanzar a los demás nodos de la red. De la misma manera se actualiza la ruta para encontrar al nodo raíz mediante los números de secuencia. Este nodo seleccionado como raíz suele ser un MPP que como ya se mencionó conecta con otras redes. Otro método es mediante mensajes RRAN que tiene una función similar a los mensajes PREQ proactivos.

Airtime Cost Routing Metric

Esta métrica se plantea como la métrica de enrutamiento predeterminada en IEEE 802.11s. Evidencia la cantidad de recursos del canal consumidos para la transmisión de una trama sobre un enlace en particular.

La métrica “airtime” C_a para cada enlace se calcula como:

$$C_{a=}\left[O_{ca}+O_p+\frac{B_t}{r}\right]\frac{1}{1-e_{pt}} \qquad \text{(Ecuación 1)}$$

Donde Oca, O_p, y B_t son constantes cuyos valores dependen de la tecnología de transmisión utilizada. O_{ca} es la sobrecarga del acceso al canal, O_p es la sobrecarga de protocolo, y B_t es el número de bits en una trama de prueba (1024 bytes). Los parámetros r y e_{pt} son la velocidad en Mbit/s, y la tasa de error de trama (probabilidad de error) para las tramas de prueba de tamaño B_t, respectivamente (Espiga, 2012).

3.1.8 Seguridad

El esquema de seguridad emplea el modelo 802.11i que incluye las funciones de autenticación 802.1x, distribución de claves y encriptación. La diferencia a

una red centralizada radica que en las redes malladas los puntos de acceso deben tener funciones de autenticador y suplicante.

El estándar propone una solución distribuida conocida como Autenticación Simultánea de Iguales (SAE) en conjunto a una llave maestra Pairwise Master Key (PMK) empleada para generar una clave de encriptación de las tramas. De esta manera se consigue que cada par este asegurado independientemente.

El protocolo SAE como se observa en la Figura 31 inicia cuando se sabe de un vecino mediante el intercambio de balizas y consiste en el intercambio de dos mensajes uno de compromiso y otro de confirmación por cada nodo en la red mesh que inicie el protocolo.

Autenticación de SAE se realiza en la capa enlace del modelo OSI antes de la asociación y una estación puede aprovechar el hecho de que puede estar autenticándose en muchos puntos de acceso de forma simultánea

El intercambio de compromiso se emplea para obligar a cada parte a solo una estimación o adivinanza de contraseña lo que hace que se vuelva resistente a ataques de diccionario. El intercambio de confirmación es usado para probar que la estimación de la contraseña fue correcta.

La PMK se la puede obtener mediante SAE o empleando otro método de autenticación basado en 802.1x es decir un servidor. La autenticación mediante un servidor toma más tiempo en función de la complejidad de la red por lo que SAE presenta ventajas sobre este método.

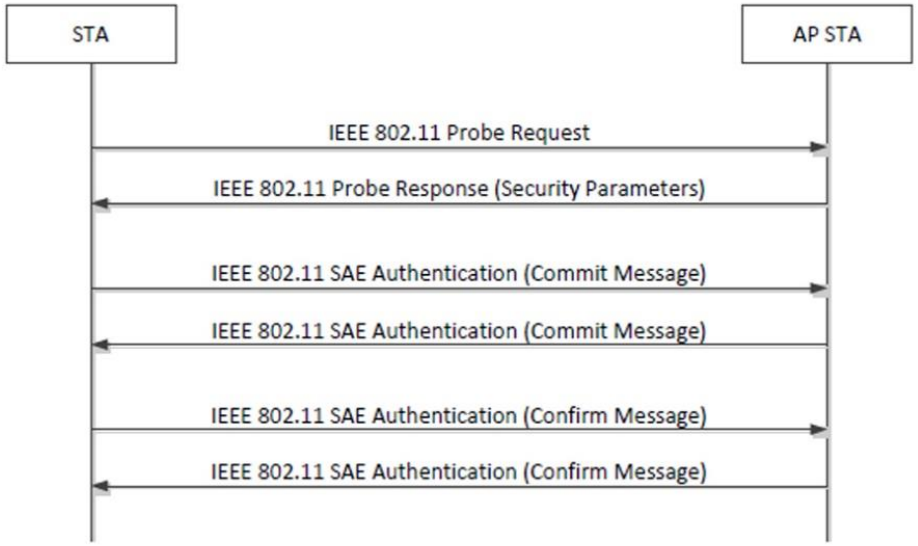


Figura 31. Proceso de Autenticación empleando SAE.
Tomado de: (IEEE Computer Society, 2012, pág. 87).

3.2 Redes MANET

Las redes netamente ad-hoc tienen la característica de ser redes descentralizadas y los nodos que forman los enlaces pueden cambiar continuamente su posición. Todos sus nodos están al mismo nivel pudiendo actuar como emisores, receptores o encaminadores y tomando en cuenta estas particularidades más el apoyo de protocolos de comunicación adecuados nacen las redes MANET donde la entidad que las norma y regula es el IETF (Internet Engineering Task Force).

El Grupo de Trabajo de Ingeniería de Internet IETF es quien creo el MANET Working Group cuyo propósito es estandarizar las funciones de los protocolos de enrutamiento en IP con características móviles.

3.2.1 Características de las redes MANET

- **Topología dinámica:** Nodos en constante movimiento los cuales deben adaptarse rápidamente a los cambios.

- **Variabilidad de rendimiento:** Al conformarse un enlace los nodos intermedios pueden estar congestionados por lo que el rendimiento puede cambiar entre cada par de nodos.

- **Consumo de energía:** Consumo de baterías para los nodos móviles que disminuyen el tiempo de uso de los nodos, un factor importante a tratar es de conseguir fuentes de energía más duraderas.

- **Funcionamiento distribuido:** sin elementos centrales para la gestión y control.

3.2.2 Enrutamiento

Uno de los puntos más importantes en las redes MANET son los protocolos de enrutamiento para determinar el camino a seguir de los paquetes hasta llegar a su destino. Para las redes MANET existen varios protocolos que llevan a cabo este proceso con el objetivo que la red se organice por si sola y de manera eficiente, adaptándose a la movilidad, estableciendo y manteniendo rutas entre los dispositivos, buscando que en las cabeceras de los paquetes de control se tenga la menor sobrecarga.

3.2.2.1 Clasificación de los protocolos de enrutamiento.

Existen clasificaciones de los protocolos de enrutamiento que muestran varios aspectos a considerar previos a la creación de un diseño entre los cuales se tiene:

Información del estado

Estos protocolos pueden clasificarse dependiendo de cuál sea la información conservada en los nodos y los receptores de la información, como ejemplo están:

- Protocolos de estado de enlace
- Protocolos de vector distancia.

Actualización

Los nodos necesitan actualizar y mantener su información con respecto al enrutamiento y de acuerdo a cuando se realiza esta actualización se clasifica en:

Actualización periódica

Los nodos difunden información de enrutamiento cada cierto tiempo, esto ayuda a que los nuevos nodos, así como los que están en movimiento aprendan el estado de la topología. Por un lado, las actualizaciones en periodos de tiempo muy cortos pueden generar un mayor uso del ancho de banda y en periodos muy largos es posible que la información no sea la más actual.

Actualización por evento

Dependiendo de la situación sea esta un nuevo enlace o el fallo de uno de estos, como respuesta a este tipo de eventos se envía un mensaje del tipo broadcast para informar a la red su nuevo estado.

Estructura

Desde este punto de vista se toma en cuenta los nodos y su función. En una red ad-hoc dependiendo de su protocolo se puede tener nodos en los que todos actúan de igual manera y otros en los que ciertos nodos la red que cumplen otras funciones.

- Uniforme: Todos los nodos están al mismo nivel envían y reciben mensajes de control
- No uniforme: Algunos nodos en específico cumplen funciones específicas en cuanto al enrutamiento como la selección de vecinos.

Descubrimiento de rutas

Esta clasificación es la más conocida y se la realiza de acuerdo a como se descubren las rutas en las redes MANET. Los protocolos de encaminamiento son empleados en distintos escenarios y se los clasifica de esta manera.

- Protocolos Proactivos
- Protocolos Reactivos
- Protocolos Híbridos

En la Figura 32 se puede observar cómo se clasifican los protocolos de enrutamiento que pueden ser empleados en las redes MANET.

Figura 32. Protocolos de enrutamiento en redes MANET

De acuerdo a la investigación realizada en base a estudios y proyectos implementados, la clasificación más usual de los protocolos de enrutamiento para redes MANET es en base a como los nodos descubren sus rutas. A continuación, se presenta esta clasificación con las características principales y el funcionamiento de los protocolos más importantes de cada uno dentro de esta clasificación.

3.2.2.2 Protocolos de enrutamiento Proactivos

Esta clase de protocolos establecen y actualizan todos los caminos posibles que existen en la red de forma constante mediante el intercambio de sus tablas para tener conocimiento de sus nodos y cuando estos realizan cambios en su topología. El encontrar rutas para la comunicación de sus nodos se hace de forma casi inmediata y no hay un significativo retardo, pero por otro lado existe una carga extra en la señalización y esto puede disminuir el rendimiento y el consumo de energía.

Los protocolos proactivos emplean algoritmos de estado del enlace o de vector distancia. Estos envían mediante broadcast la información de sus tablas y toman esta información para determinar la ruta más corta hacia otras estaciones.

Los protocolos proactivos más importantes son los siguientes:

- Destination-Sequenced Distance Vector (DSDV), 1994
- Hierarchical State Routing (HSR), 2000
- Optimised Link State Routing (OLSR), 2003
- B.A.T.M.A.N. Better Approach To Mobile Ad-hoc Networks. (2011)
- Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), 2004

A continuación, se realiza una descripción del funcionamiento de OLSR y BATMAN.

OLSR (Optimized Link-State Routing Protocol)

Funcionamiento

Protocolo que trabaja de forma distribuida y debido a las características que ofrecen los algoritmos de estado de enlace hacen que sus rutas sean utilizables de forma inmediata mediante el anuncio y difusión de su tabla de vecinos hacia todos los nodos de la red.

OLSR disminuye la cantidad de paquetes de control ya que estos no se envían a todos los vecinos sino solo a nodos seleccionados como reenviadores multipunto MPR (Multipoint Relay) para reducir la cantidad de retransmisores por broadcast.

OLSR conserva sus rutas para todos los destinos de la red y esto es muy útil cuando existen gran cantidad de nodos en la MANET que estén enviando información constantemente.

Es tolerante a perdidas eventuales de paquetes de control debido a que los nodos transmiten periódicamente mensajes de este tipo. Adicional a esto posee un reordenamiento de paquetes y cada mensaje tiene un número de secuencia

por lo que cada estación usa su información más reciente al momento de enrutar un paquete.

Los mensajes en OLSR emplean UDP en el puerto 698 y son los siguientes:

- Mensajes Hello
- Mensajes de Control de Topología (TC)
- Mensajes MID para múltiples interfaces

Descubrimiento de nodos vecinos

Todos los nodos de la red en OLSR envían mensajes por broadcast conocidos como mensajes Hello los cuales transmiten información de los nodos vecinos y el estado del canal hacia estos. Los mensajes Hello se envían periódicamente de acuerdo al tiempo asignado en el campo “HTime” que por defecto está configurado en 2 segundos.

Las tareas del mensaje Hello se las puede resumir en:

- Detección de vecinos
- Señalización para elección de MPR

En la Figura 33 se puede ver la composición de un mensaje Hello.

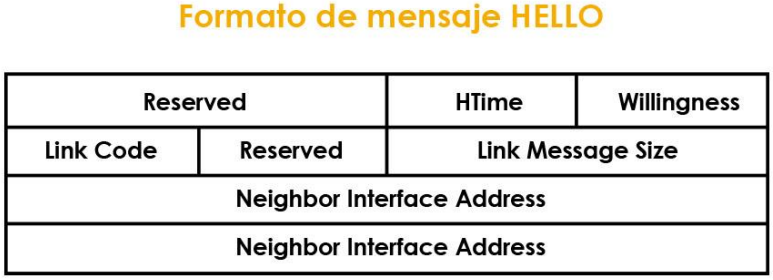


Figura 33. Formato de mensajes Hello.
Tomado de: (Clausen & Jacquet, 2003)

Selección de la ruta

Cada nodo de la red escoge un subconjunto dentro de sus nodos vecinos para retransmitir paquetes, estos nodos son llamados nodos MPR. Para la selección

de rutas sigue un criterio en el que debe asegurarse que todos los nodos que están a dos saltos de un nodo dado puedan alcanzarse con un número mínimo de MPR's. Cuanto más pequeño sea un conjunto de MPR's, menos sobrecarga de tráfico de control existirá por el protocolo de enrutamiento. En la Figura 34 se puede apreciar este concepto donde los nodos de color naranja tienen la función de Multipoint Relay.

Por otro lado, los nodos que no se establecen como MPR's recibirán paquetes de la misma manera, pero no los reenviarán y de esta manera cada nodo mantiene una tabla con nodos que han sido denominados MPR's.

Criterio para selección Multipoint Relay

Por medio de los mensajes Hello cada nodo conoce de sus vecinos a uno y dos saltos. Además, en los mensajes HELLO, el campo "Willingness" indica la predisposición del nodo para ser considerado como MPR. También en el campo "Link Code" se verifica si el enlace es unidireccional o bidireccional ya que un nodo unidireccional no podrá actuar de ninguna forma como reenviador.

Partiendo de estos datos, un nodo determina cuál de sus vecinos a un salto tiene mayor información nodos vecinos cercanos a estos, es decir a dos saltos. Aquel nodo que en su tabla de vecinos tenga enlace con un mayor número de nodos será elegido como un nodo MPR.

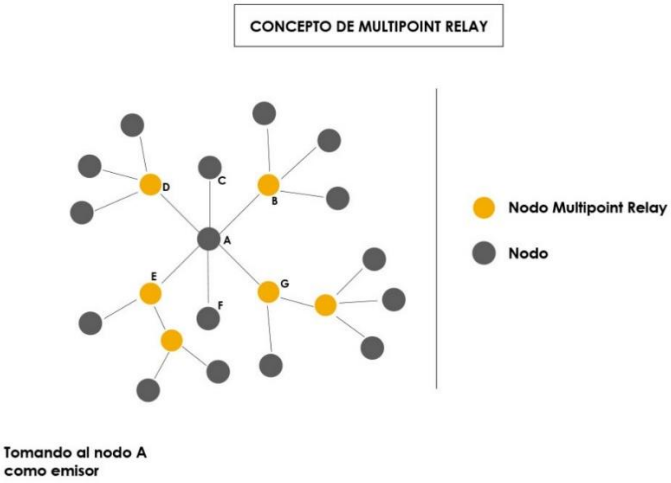


Figura 34. Concepto Multipoint Relay.

Actualización de las rutas

Por medio de los mensajes de control de topología TC cada nodo actualiza los enlaces con sus vecinos, así puede conocer los cambios que se producen en la topología de la red y mantener sus rutas actualizadas.

Un mensaje TC es enviado únicamente por un nodo MPR en la red para declarar el “MPR Selector” es decir los nodos que lo han escogido como reenviador. De igual manera este mensaje se adjunta un número de secuencia para tener información actualizada.

De esta manera ya se puede tener una tabla de enrutamiento hacia todos los nodos posibles en la red.

Mensajes HNA (Host Network Association)

Estos mensajes se generan para enviar información a los nodos de la red OLSR acerca de una puerta de enlace hacia otras redes como internet. Como se puede observar en la Figura 35 dentro del mensaje consta la dirección de red asociada y su máscara de red. (Clausen & Jacquet, 2003)

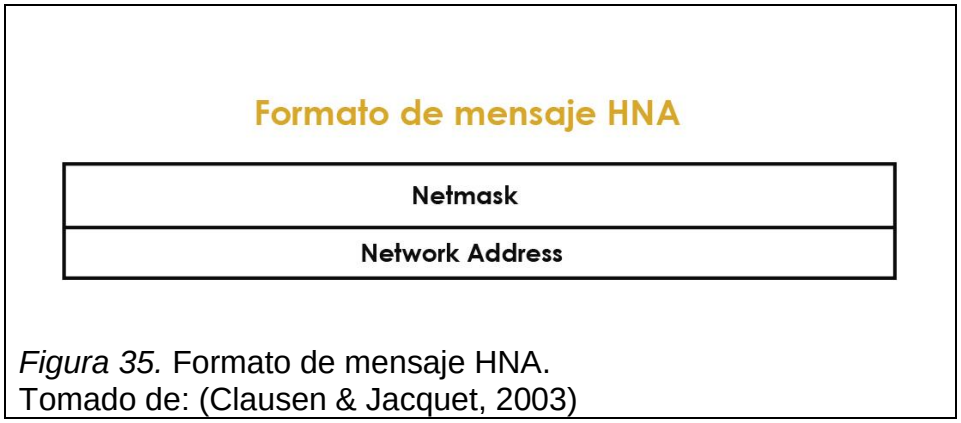


Figura 35. Formato de mensaje HNA.
Tomado de: (Clausen & Jacquet, 2003)

La forma de difusión del mensaje HNA es siguiendo el mismo proceso de broadcast que los mensajes anteriores en OLSR.

Tabla 5. Resumen OLSR.

Resumen	
Protocolo:	OLSR
Tipo:	Proactivo
Conocimiento de topología:	Total
Capa:	Red
RFC:	3626

BATMAN (Better Approach To Mobile Ad-Hoc Networking)

Funcionamiento.

El protocolo BATMAN Conserva la información de los nodos de la red mallada de forma proactiva que son accesibles a un solo salto. La técnica que emplea BATMAN es determinar para cada destino de la red mallada un único salto vecino que pueda ser usado como el mejor gateway para comunicarse con el nodo destino.

“Aprender cuál es el mejor salto siguiente para cada destino es todo lo que el algoritmo BATMAN se preocupa. No hay necesidad de averiguar o calcular la ruta completa, lo que hace posible una aplicación muy rápida y eficiente.” (Neumann, Aichle, & Wunderlich, 2008)

Además, realiza un análisis estadístico por medio de la detección de los paquetes perdidos y la velocidad de propagación para tomar decisiones de enrutamiento y no necesita saber del estado o la información de topología de otros nodos.

Descubrimiento de rutas

Los mensajes de BATMAN emplean UDP en el puerto 4305 y se describen a continuación.

Mensajes OGM (Originator Messages)

Son mensajes que emplea un nodo con el protocolo BATMAN de forma periódica para dar a conocer su existencia a los otros nodos de la red. Estos mensajes también son empleados para determinar la calidad de una ruta. En la Figura 36 se puede observar los principales componentes del mensaje OGM.

Figura 36. Formato del mensaje OGM.
Tomado de: (Neumann, Aichle, & Wunderlich, 2008)

Un mensaje OGM está compuesto por:

- Ip origen
- TTL (Tiempo de vida)
- Número de secuencia
- Gatewayflags para anunciar que el nodo tiene acceso a internet.
- Flag para indicar si el enlace es vecino Directo o no.
- Flag para indicar si el enlace es Unidireccional o no

Al momento de reenviar los paquetes OGM por redifusión los paquetes OGM deben realizar un cambio indicando si un nodo es vecino o no y también su campo TTL debe decrecer en 1 (Neumann, Aichle, & Wunderlich, 2008).

B.A.T.M.A.N no realiza corrección de errores, pero emplea información de la perdida de sus paquetes para tomar mejores decisiones en sus rutas.

En la Figura 37 se puede observar cómo trabaja este protocolo inundando toda la red para determinar el mejor Gateway en cada nodo.

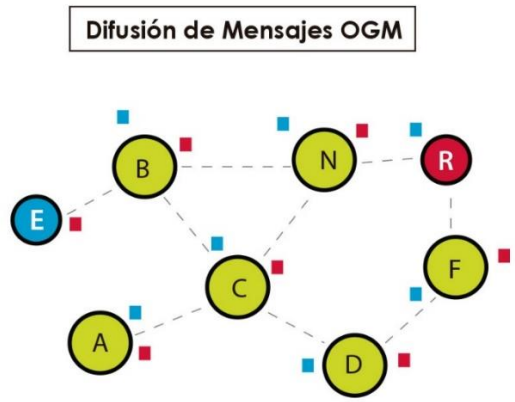


Figura 37. Difusión de OGM's para selección de Gateway en B.A.T.M.A.N.

Los números de secuencia de los nodos en BATMAN son almacenados en una de ventana deslizante hasta que son considerados fuera de rango. Este procedimiento que se encuentra representado en la Figura 38 se lo realiza con el objetivo de tener una métrica para saber la cantidad y calidad de los enlaces.

Figura 38. Ventana deslizante en BATMAN.
Tomado de: (Neumann, Aichle, & Wunderlich, 2008)

La ventana se irá actualizando de acuerdo a como llegan los OGM a cada nodo y verificando si la información es la más actual en base a su número de secuencia.

Tabla 6. Resumen protocolo B.A.T.M.A.N.

Resumen	
Protocolo:	BATMAN
Tipo:	Proactivo
Conocimiento de topología:	Parcial
Capa:	Red, enlace
Estado:	Draft

3.2.2.3 Protocolos de enrutamiento Reactivos

En estos protocolos también conocidos como bajo demanda se realiza una petición de ruta por parte del emisor. Se mejora el uso de recursos ya que no se envían paquetes que no sean necesarios, inicialmente se realiza un descubrimiento de la ruta y se espera una respuesta previa al envió de información al destino, esto puede significar una desventaja desde el punto de vista del tiempo, pero por otro lado se reduce la carga de mensajes de control y optimiza el uso de las baterías.

Los más destacables son los siguientes:

- Ad Hoc On Demand Distance Vector Routing (AODV), 2003
- Dynamic MANET On demand (DYMO), 2005
- Dynamic Source Routing (DSR), 2004
- Temporally Ordered Routing Algorithm (TORA), 2001

A continuación, se realiza una descripción del funcionamiento de DSR y AODV

DSR (Dynamic Source Routing)

Este protocolo es del tipo reactivo y por ende solo busca una ruta cuando esta es necesaria. Fue creado específicamente para redes MANET cuyas características son móviles multisalto.

Este protocolo tiene dos funciones principales:

Descubrimiento de ruta

En un inicio el proceso de descubrimiento de ruta busca en la memoria cache de cada nodo para determinar si dispone de una ruta para el destino requerido. Si en la búsqueda encuentra la ruta lo que realiza es simplemente añadir a la cabecera la ruta con el número de saltos que debe seguir para llegar al destino.

Por el contrario de no encontrar una ruta en su memoria cache el protocolo inicia un Route Discovery y así encontrar un camino al nodo destino.

Inicialmente envía un mensaje de broadcast del tipo RREQ a todos los nodos dentro del alcance del nodo emisor. Los paquetes RREQ como se observa en la Figura 39 tienen un identificador del nodo fuente y del nodo destino y un id único en cada mensaje RREQ. Los nodos intermedios realizan un forward con los datos anteriores acumulándolos hasta la llegada a su destino.

Figura 39. Formato de mensaje RREQ en DSR.
Tomado de: (D. Jhonson; Y. Hu; D. Maltz, 2007)

En el momento que un nodo recibe un mensaje RREQ realiza otra búsqueda en su cache y compara si ya ha recibido el mensaje del mismo origen, destino

e id lo descarta. Luego si el nodo en cuestión tiene alguna ruta al destino responde un mensaje de respuesta Route Reply (RREP) si no es así continua el broadcast.

Al encontrar el nodo destino el mensaje RREP (Figura 40) con el que se va a responder almacena todos los identificadores previos del RREQ para construir un camino de regreso al nodo origen. Los mensajes del emisor seguirán difundiéndose hasta que su campo TTL llegue a 0.

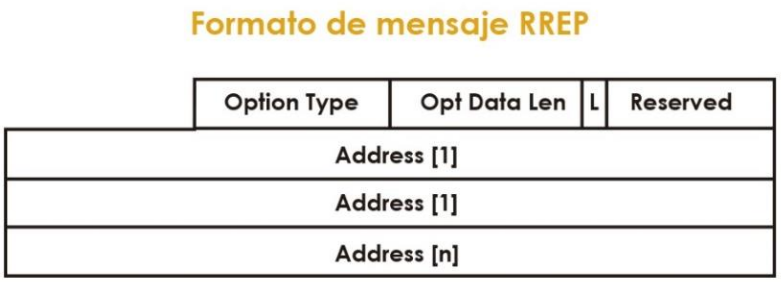


Figura 40. Formato de mensaje RREP en DSR.
Tomado de: (D. Jhonson; Y. Hu; D. Maltz, 2007)

Mantenimiento de rutas

Al momento de encontrarse con un error en la transmisión de paquetes debido a que se ha perdido el enlace el nodo, el nodo que ya no encuentra su siguiente salto envía un mensaje RERR hasta llegar al nodo origen para eliminar esa ruta de su cache. El mensaje RERR tiene el formato ilustrado en la Figura 41. Finalmente, proceso se vuelve a repetir para buscar una nueva ruta solo que esta vez se añade el mensaje de error para evitar que los nodos que aun conserven en su cache una ruta al nodo inexistente ofrezcan una ruta como válida para ese destino.

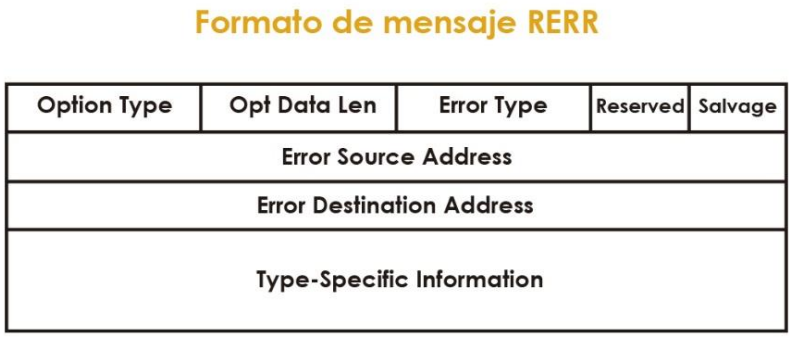


Figura 41. Formato de mensaje RERR en DSR.
Tomado de: (D. Jhonson; Y. Hu; D. Maltz, 2007)

Con el fin de disminuir la congestión de la red en el momento de generar los mensajes de error RERR, se creó un método llamado Packet Salvaging para evitar la pérdida de paquetes, por ejemplo, si un nodo intermedio se da cuenta que el enlace con el siguiente salto está roto, busca en su cache si dispone de una ruta alterna y si existe lo que realiza es una redirección del paquete, sino regresa hasta el nodo emisor buscando no dar por perdido el paquete.

Este proceso es transparente para el usuario y es una opción muy viable para optimizar el tráfico existente en la red. (D. Jhonson; Y. Hu; D. Maltz, 2007)

En la Figura 42 se ilustra el funcionamiento del protocolo DSR.

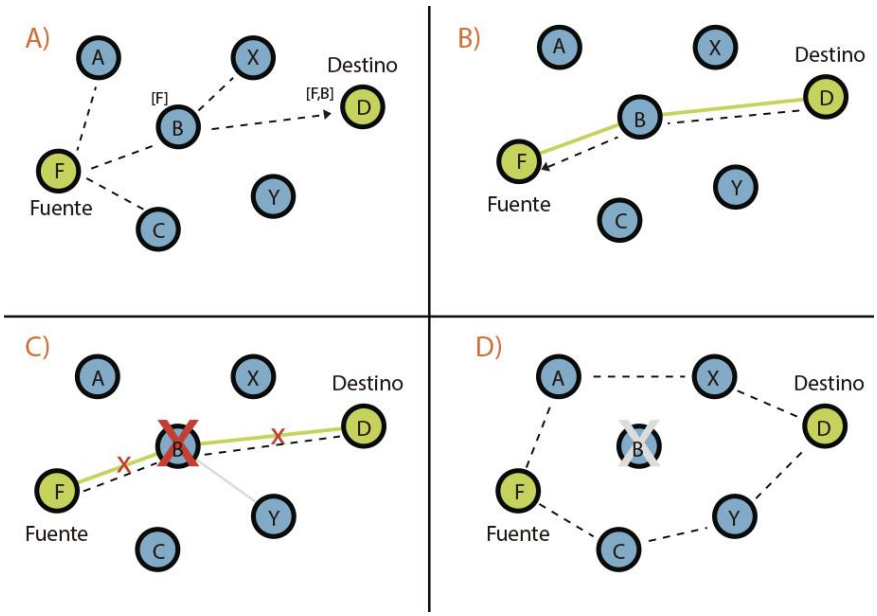


Figura 42. Funcionamiento del protocolo DSR.

A) Descubrimiento de ruta desde el nodo fuente si no la tiene en su cache.
B) Se ha encontrado la ruta más corta y se establece el camino de regreso.
C) Se pierde el enlace entre un nodo fuente y destino. El nodo que no encuentra el siguiente salto envía mensajes de error hasta llegar a la fuente.
D) La búsqueda de ruta inicia nuevamente.

Tabla 7. Resumen del protocolo DSR.

Resumen	
Protocolo	DSR
Tipo:	Reactivo
Conocimiento de topología:	Parcial
Capa:	Red
RFC:	4728

AODV (Ad hoc On Demand Vector Distance)

El protocolo de enrutamiento AODV (Ad hoc On-demand Distance Vector) trabaja bajo demanda o de forma reactiva y está basado en vector distancia. Solo se realiza el descubrimiento de rutas cuando algún nodo lo necesita. Cada

nodo posee una tabla de encaminamiento con la información de la ruta y no será necesario que los paquetes transporten datos de la ruta a seguir esto contribuye a la optimización en ancho de banda y energía.

La tabla de encaminamiento tiene un tiempo de vida para cada entrada, de forma que si este tiempo expira busca una nueva ruta para el destino que tuviera asociado.

De igual manera la tabla posee un número de secuencia para determinar la información más actual. Los tipos de mensajes en AODV son enviados por el puerto 654 empleando UDP y son:

- Mensajes RREQ
- Mensajes RREP
- Mensajes RERR

Descubrimiento de ruta

Los mensajes de petición de ruta o RREQ (Route Request) son utilizados por los nodos para el descubrimiento de ruta cuando desean comunicarse con otro nodo e inundan la red con un mensaje RREQ. Durante un tiempo, el nodo guardará el identificador del mensaje y la dirección origen del mismo para evitar procesarlo si le llega de vuelta. El formato del mensaje RREQ se lo aprecia en la Figura 43 donde se especifica entre otras cosas la dirección IP origen del mensaje, la dirección IP de destino, el conteo de saltos y un número de identificación del mensaje.

A diferencia de DSR, AODV no almacena la ruta completa que deben seguir los paquetes, sino que en sus mensajes de enrutamiento solo toma en cuenta el origen y el destino por lo que en redes extensas tiene una mejor adaptación.

Figura 43. Formato de mensaje RREQ en AODV
Tomado de: (Perkins, Belding-Royer, & Das, 2003)

Los mensajes de respuesta de ruta o RREP (Route Reply) se envían como respuesta de un RREQ, si el nodo es el destino. El camino hacia la fuente ya no será por broadcast sino unicast siguiendo un camino inverso hasta llegar al nodo que emitió la solicitud de ruta.

Si la información está actualizada se detectará gracias a los números de secuencia. Adicionalmente posee el campo “lifetime” que es el tiempo en milisegundos que el nodo receptor del RREP considera como una ruta como válida. El formato del mensaje RREP se lo aprecia en la Figura 44.

Figura 44. Formato de mensaje RREP en AODV
Tomado de: (Perkins, Belding-Royer, & Das, 2003)

Mensajes RERR

Los mensajes RERR (Route Error) se utilizan para notificar que no se puede alcanzar un destino determinado. El formato de un mensaje RERR puede observarse en la Figura 45.

Figura 45. Formato de mensaje RERR en AODV.
Tomado de: (Perkins, Belding-Royer, & Das, 2003)

Se produce este error cuando se pierde conectividad con el nodo vecino en una ruta que está en funcionamiento o cuando se debe enviar un paquete para cuando no se conoce ninguna ruta activa. (Perkins, Belding-Royer, & Das, 2003)

Tabla 8. Resumen Protocolo AODV.

Resumen	
Protocolo	AODV
Tipo:	Reactivo
Conocimiento de topología:	Parcial
Capa:	Red
RFC:	3561

3.2.2.4 Protocolos de enrutamiento Híbridos

Estos protocolos o esquemas de enrutamiento combinan las características de los protocolos proactivos y reactivos aprovechando las ventajas de cada uno.

Estos protocolos pueden establecerse en redes de tamaño medio a grande o para interconectar con otras redes.

Dentro estos protocolos se pueden mencionar los siguientes:

- Scalable Location Update Routing Protocol (SLURP), 2004
- Zone-based Hierarchical Link State (ZHLS), 1999
- Zone Routing Protocol (ZRP), 2002
- Hybrid Wireless Mesh Protocol (HWMP), 2006

A continuación, se realiza una descripción del funcionamiento del protocolo ZRP.

Protocolo ZRP

Es un framework de enrutamiento híbrido aplicable a redes móviles ad-hoc que combina protocolos proactivos y reactivos para optimizar el desempeño de la red y la búsqueda de rutas. El principio de funcionamiento se basa en dos mecanismos. El primero en la selección del radio de zona de enrutamiento y el segundo en un concepto llamado Bordercasting para extender la búsqueda hacia otras zonas

Descubrimiento de nodos vecinos

La tarea se la divide en dos componentes el primero conocido IARP (Protocolo de Ruteo Intra zonas) y el segundo IERP (Protocolo de Ruteo Inter zonas).

En el primero se emplean protocolos proactivos donde todos los nodos actualizan sus tablas de encaminamiento constantemente para saber las rutas hacia estos y con el limitante de que solo se tendrá conocimiento de los nodos que estén dentro de la zona de enrutamiento. El concepto del radio de zona de enrutamiento es simplemente para establecer hasta donde se mantiene una búsqueda proactiva.

En la Figura 46 se muestra el formato del paquete en ZRP empleando IARP para el descubrimiento de nodos vecinos, el formato es similar al de un protocolo proactivo pero añadido el campo de radio de zona.

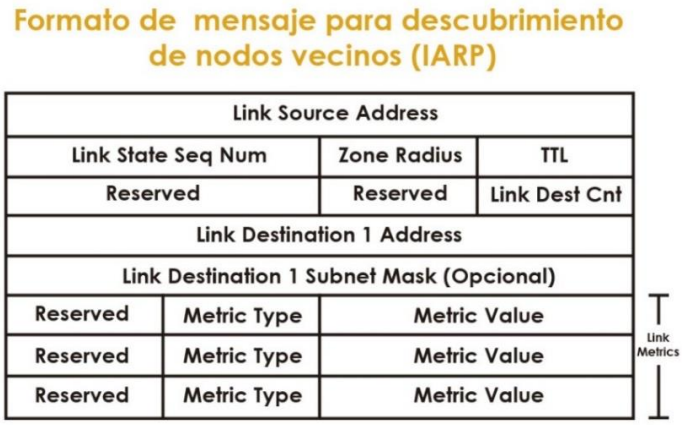


Figura 46. Formato del paquete de descubrimiento de vecinos en IARP. Tomado de: (Haas, Pearlman, & Samar, 2002)

A continuación, en la Figura 47 se muestra el concepto de radio de zona tomando como referencia el nodo A como emisor y un radio equivalente a 2 y en la Figura 48 se observa cómo se establece la zona de cobertura IARP donde se aplican protocolos proactivos.

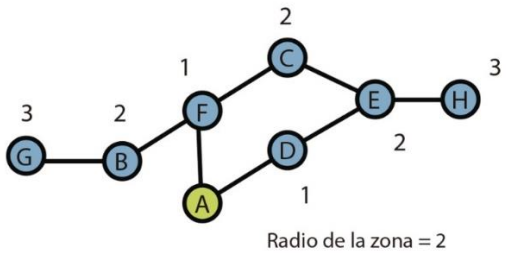


Figura 47. Establecimiento de radio de zona.

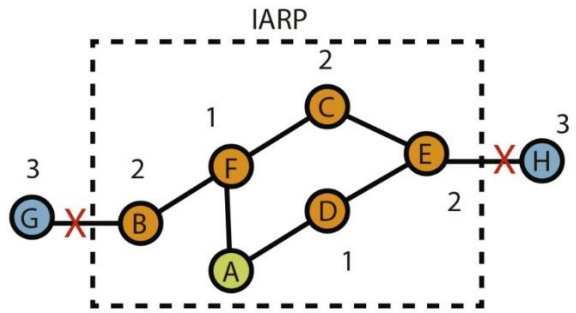


Figura 48. Concepto IARP con un radio de zona = 2

El segundo componente del protocolo es IERP en el que se aplica un enrutamiento de forma reactiva, donde se utiliza el servicio de distribución de mensajes también conocido como BRP Bordercast Resolution Protocol.

Con este servicio puedo obtener los parámetros de la consulta y la métrica para que sean tomados por IERP y así enviar consultas hacia nodos no cubiertos por las zonas anteriormente mencionadas.

El IERP comienza a funcionar cuando ninguna ruta es alcanzable localmente al momento que un nodo envía un paquete de datos. Los nodos de borde o periféricos determinados por el máximo número del radio de la zona son los que empiezan la búsqueda de nuevas rutas.

El proceso se repetirá tantas veces sea necesario hasta encontrar el nodo destino desde donde el cual se construye un camino inverso hacia el nodo fuente.

En la Figura 49 se observa el formato de los protocolos reactivos que incluyen campos como el tipo de mensaje si es Route Request o Route Reply, el número de secuencia y la dirección del origen del mensaje, así como las direcciones acumuladas en toda la ruta.

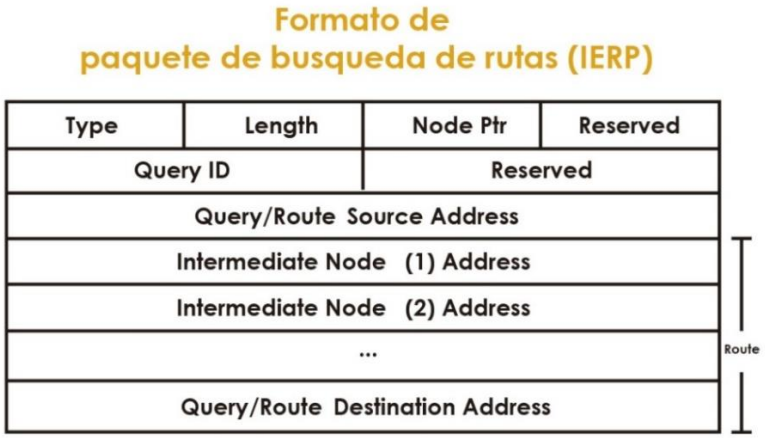


Figura 49. Formato del paquete de búsqueda de rutas en IERP. Tomado de: (Haas, Pearlman, & Samar, 2002)

El funcionamiento de IERP se lo puede apreciar claramente en la Figura 50 a continuación.

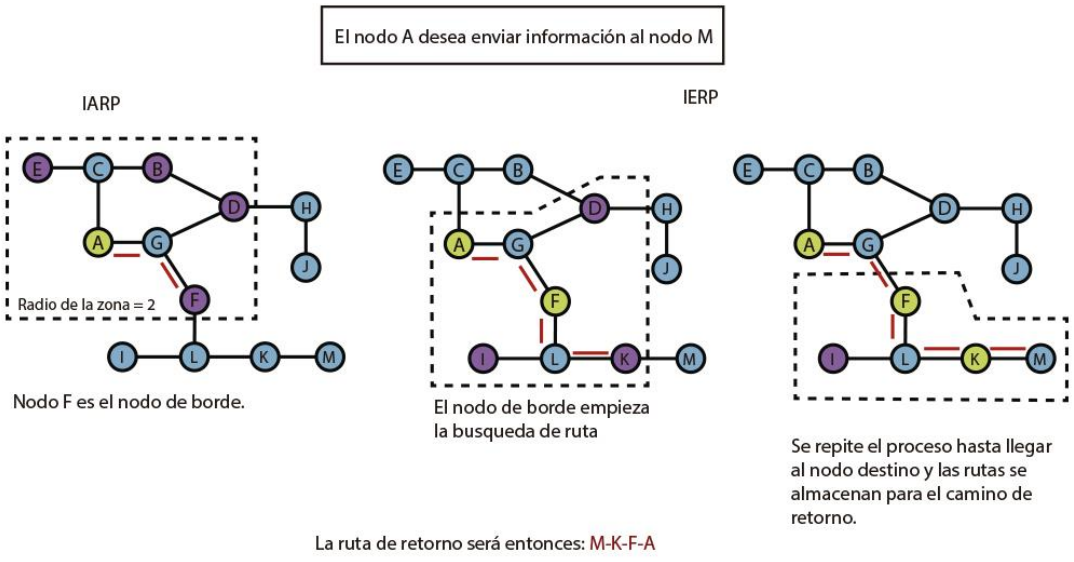


Figura 50. Ejemplo del funcionamiento de IERP en ZRP.

Mantenimiento de rutas

Los mecanismos de mantenimiento de rutas no son tratados en el borrador de este protocolo ya que dependen del tipo de protocolo proactivo y reactivo empleados que son los que se encargaran del mantenimiento de rutas como tal. (Haas, Pearlman, & Samar, 2002)

3.2.2.5 Comparativa de protocolos

En base a los protocolos analizados anteriormente se elaboró la siguiente tabla comparándolo sus principales características.

Tabla 9. Características de los protocolos aplicables a redes mesh analizadas en este capítulo.

CARACTERISTICAS DE LOS PROTOCOLOS APLICABLES A REDES MESH						
Protocolo	**OLSR**	**B.A.T.M.A.N**	**AODV**	**DSR**	**HWMP**	**ZRP**
Tipo	Proactivo	Proactivo	Reactivo	Reactivo	Hibrido	Hibrido
Información de estado	Estado de enlace	Vector Distancia	Vector Distancia	Vector Distancia	Vector Distancia	VD/EE
Modo de transmisión	Broadcast	Broadcast	Broadcast/ Unicast	Broadcast/ Unicast	Broadcast/ Unicast	Broadcast/ Unicast
Actualización	Periódica	Periódica	Eventos	Eventos	Eventos	Periódica/ Eventos
Troughtput	Disminuye por la movilidad	Disminuye por la movilidad	Disminuye por la movilidad	Disminuye por la movilidad	Disminuye por la movilidad	Disminuye por la movilidad
Implementación	Linux, Android, NS-3	Linux, Android, NS-3	Linux, Mathlab, C++	Linux NS-3	Linux	NS-2, Linux

3.2.2.6 Métricas de enrutamiento.

El protocolo de enrutamiento debe hallar una ruta cuyo costo sea mínimo entre el nodo origen y el nodo destino. Este costo se fija a través de la métrica de enrutamiento y es sobre esta métrica que el algoritmo de enrutamiento decide la ruta. Según las diferentes métricas el concepto del costo varía. Ejemplo: si se usa la cantidad de saltos como una métrica, entonces el costo entre el origen y el destino es el número de saltos entre estos dos nodos.

Algunos de los objetivos de los algoritmos de enrutamiento y de sus métricas son los siguientes:

- Minimizar el retardo: Aquí se escoge la ruta en la que los datos se entregan con un retardo mínimo. Si no se toman en cuenta el retardo de encolamiento, la capacidad del enlace, la interferencia y solo se considera minimizar el retardo esto equivale a disminuir la cantidad de saltos.
- Maximizar la probabilidad de entrega de los datos: Esto se considera para aplicaciones que no son en tiempo real, aquí lo más importante es tener una baja tasa de pérdida de datos en la ruta, incluso puede haber un mayor retardo.
- Maximizar el throughput del camino: Aquí lo importante es escoger una ruta de inicio a fin, que tenga enlaces de alta capacidad. El objetivo es maximizar el flujo de datos en toda la red, o minimizar las interferencias.
- Balanceo del tráfico: se debe asegurar que ningún enlace o nodo se use de forma desigual.

Las métricas propuestas para las redes MANET son las siguientes:

Cantidad de saltos (Hop-Count)

Es la métrica más sencilla, porque solo requiere conocer si existe un enlace o no. No entrega información favorable sobre un enlace, como pérdida de paquetes o calidad del enlace. Los protocolos que se basan en esta métrica toman en cuenta un único parámetro, la mínima cantidad de saltos en cada ruta. El propósito es que con menos saltos en la ruta, menor retardo y menor consumo de los recursos de la red. En la mayor parte de los casos esta métrica no es adecuada para que un protocolo de enrutamiento logre un buen cumplimiento, debido a que no se puede asumir para las MANET que los enlaces estén libres de errores.

Round Trip Time (RTT) por Salto

El per-hop RTT (tiempo de ida y vuelta por salto) se mide al enviar paquetes de pruebas unicast entre nodos vecinos y evaluar el tiempo que toma en enviar y recibir la respuesta. Se envía un paquete de prueba cada 500 ms, al aceptarlo

cada vecino contesta de inmediato. El aviso de recibo tiene un “time-stamp” para que el RTT pueda ser calculado.

De esta se manera se consigue evidenciar la predisposición del enlace, ya que solo una muestra no puede evidenciar la condición actual del enlace. El RTT estimado, o sea, el SRTT, se establece como el costo del enlace. Entonces, un protocolo de enrutamiento elige la ruta cuya suma de los RTT, de todos los enlaces que componen la ruta, es menor.

ETX (Expected Transmission Count)

Es una de las métricas creadas para redes MANET y que han sido empleadas en casos prácticos. El objetivo de ETX es encontrar rutas con alto rendimiento tomando en cuenta las relaciones de pérdida de paquetes de los enlaces. No está basada en el número de saltos y puede emplearse en varios protocolos.

Lo que se busca es el número de transmisiones y retransmisiones necesarias para enviar un paquete en un enlace. Se debe tomar en cuenta el cálculo de la probabilidad de éxito de que un mensaje enviado llegue a su destinatario y viceversa, LQ y NLQ representan esta probabilidad del emisor y receptor.

Partiendo de esto se puede obtener el conteo de transmisión esperada mediante la fórmula.

$$ETX = \frac{1}{(LQxNLQ)} \qquad \text{(Ecuación 2)}$$

Para protocolos como OLSR se toman en cuenta los 10 últimos paquetes para realizar esta medición de ETX.

Un problema que ETX no toma en cuenta es la capacidad de transmisión de cada enlace ya que si un enlace tiene un valor inferior de ETX este tendrá prioridad incluso si los de mayor valor de ETX tienen mayor capacidad de transmisión (Coya, Ledesma, & Baluja, 2014).

3.2.3 Comparación de características entre redes 802.11s y redes MANET.

Tabla 10. Comparación tecnologías de red mesh 802.11s y MANET

Comparación Mesh 802.11s y MANET		
	802.11s	**MANET**
Modelo de Comunicación	Monocanal	Monocanal
Modo de operación	MBSS	IBSS
Direccionamiento	Jerarquico	Plano
Encaminamiento	Capa enlace de OSI	Capa red de OSI
Implementación	Linux	Depende del protocolo de encaminamiento

4. CAPÍTULO IV RESULTADOS

En este capítulo se describen los elementos en hardware y software adaptados a UAS para formar una red mesh, se hace referencia a simulaciones en complemento a la teoría para tener conocimiento del comportamiento de los protocolos de enrutamiento en varios escenarios de aplicación y de esta manera establecer una posible solución para la formación de una red que sea aplicable a un Sistema Aéreo no Tripulado.

4.1 Tecnologías de red mesh

En los tres casos de aplicación descritos en el capítulo 2 las tecnologías inalámbricas empleadas se basan en el estándar 802.11.

Además, se identificó dos tipos de configuraciones con la que se puede formar una red aplicable a UAS, Redes MANET y redes MESH 802.11s

Como se aprecia en la Figura 51 por un lado las redes MANET se enfocan en los protocolos de enrutamiento descentralizados mientras que 802.11s propone un esquema estructurado para la formación de redes mesh.

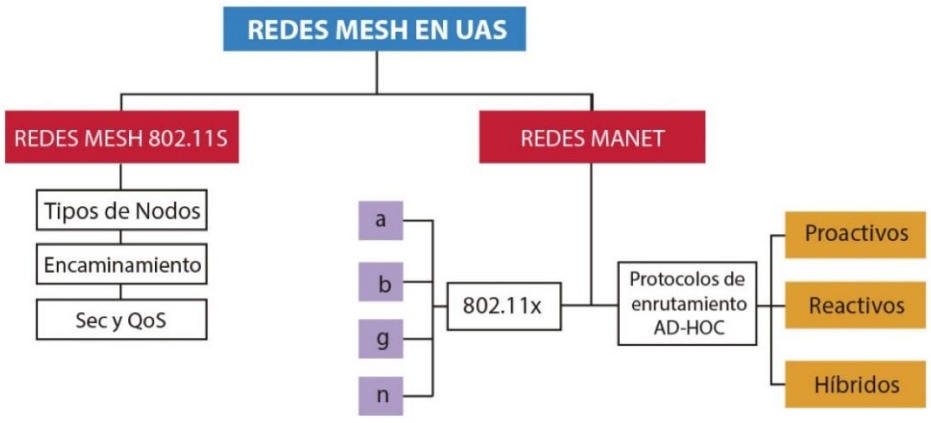


Figura 51. Tecnologías para establecer una red mesh aplicada a UAS.

4.2 Componentes de un nodo mesh

Los componentes de red que se adaptan a un UAS independientemente de su clase, es decir ala fija o hélices en primera instancia requieren de cierto nivel energía para adaptar nuevos componentes a su funcionamiento, esta puede ser tomada o bien del UAS o mediante baterías adicionales. Dependiendo de la aplicación pueden ser necesarias conexiones adicionales ya sea para la toma de datos como GPS o sensores.

Los elementos que forman un nodo de red mesh a manera general pueden ser observados en la Figura 52.

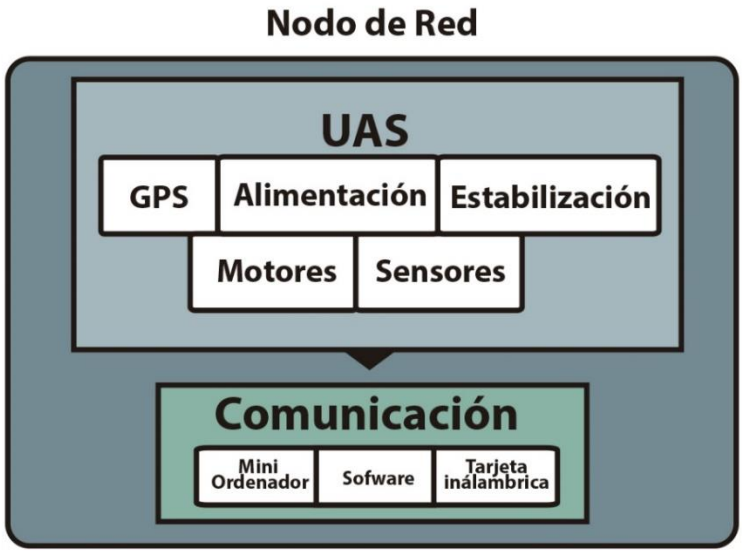


Figura 52. Componentes de un nodo de red mesh en un UAS.

4.3 Sistema de comunicación para la formación de la red.

4.3.1 Hardware

Los dispositivos adaptados en los UAS son microcomputadores y tarjetas inalámbricas wifi que cumplen con las características para la instalación del software a utilizar.

Entre los dispositivos empleados están:

- Overo de Gumstix.
- Single Board Computer de Soekris.
- Router OMP1 de Open Mesh.
- Raspberry PI model B de Raspberry.

4.3.2 Software

Desde el punto de vista de software los proyectos incluidos en esta investigación trabajan sobre software libre con varias distribuciones que permitan implementar los protocolos de enrutamiento y en las tarjetas de red inalámbrica el controlador adecuado para establecer una configuración en modo Ad-hoc o mesh 802.11s.

Para revisar la compatibilidad de los controladores de las tarjetas de red usb se lo puede hacer este enlace http://wireless.kernel.org/en/users/Drivers.

Como parámetro adicional, para la implementación de redes basadas en 802.11s se debe comprobar que la versión del kernel (nucleo) sea superior a la 2.6.26 ya que desde esa versión se incluyen soporte para 802.11s.

Algunos de los sistemas operativos mencionados y encontrados a lo largo de la investigación fueron los siguientes.

- Arch Linux
- Ubuntu
- WISP-Distribution
- ADAM
- Byzantium

4.4 Desempeño de la red en varios escenarios

Tomando en cuenta los proyectos del capítulo dos, y complementando con ejemplos de simulación, se describen los siguientes escenarios en los que se evalúan comportamiento de la red con distintos protocolos de enrutamiento.

4.4.1 Caso 1: Transmisión en tiempo real

(Sing-Borrajo, 2014, pág. 7) Evaluó el desempeño de Voz sobre Ip en redes MANET empleando un modelo de movilidad aleatorio, protocolos de encaminamiento proactivos como OLSR y DSDV y reactivos como AODV en el simulador de redes NS-3. Tomando en cuenta parámetros como movilidad, perdida de paquetes, retardo, aumento del número de nodos e interrupciones de comunicación se comprobó que el Protocolo OLSR presenta un mejor desempeño para este tipo de aplicación.

De la simulación se determinó que a partir de los 4 saltos en AODV el retardo fue superior a los 300 ms mientras que en OLSR se mantuvo constante durante los 8 nodos de prueba llegando a un máximo de 50 ms (ver anexo 1).

En la misma prueba con 8 nodos se observa que a partir de los 3 y 4 nodos se observan perdidas de paquetes en todos los protocolos de enrutamiento. OLSR presenta un menor porcentaje de perdidas llegando al 15% (ver anexo 2).

El retardo promedio fue superior cuando las conexiones en simultáneo en la red llegaron a 15. El resultado fue común para los 3 protocolos analizados (ver anexo 3).

4.4.2 Caso 2: Adaptabilidad a cambios de Topología

En el Proyecto SMAVNET II (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013) se realiza también una simulación sobre EMANE (Extendable Mobile Ad-hoc Network Emulator) en la que se emplea Predictive-OLSR con 32 nodos para mejorar el desempeño del enrutamiento, en la transmisión de datos en tiempo real, se compara BABEL, OLSR y POLSR. Los resultados obtenidos muestran que OLSR Predictivo se adapta mejor a los cambios de topología de una red MANET frente a los otros dos protocolos teniendo tasas de pérdidas de paquetes inferiores al 1% al momento de variar el enrutamiento (ver anexo 4).

4.4.3 Caso 3: Transmisión en tiempo real

(Mohapatra & Kanungo, 2012)**.** Las simulaciones realizadas en esta publicación se llevan a cabo en una red ad hoc móvil, variando tres parámetros: el número de nodos, tiempo de pausa de los nodos y el área de la red. Los protocolos que

se usan son: AODV, DSR y OLSR. Estas pruebas se realizan en el simulador de redes NS2.

Como resultado de estas simulaciones se tiene que en términos de carga de mensajes de control y número de nodos; DSR tiene una menor cantidad de mensajes de control respecto a los protocolos AODV y OLSR cuando se emplea 50 nodos. El protocolo OLSR tiene mayor cantidad de mensajes de control hasta los 25 nodos, después de esto es similar a AODV, debido a los mensajes de broadcast hasta encontrar el destino (ver anexo 5).

En términos de retardo extremo a extremo todos los protocolos presentan tiempos similares y van desde 0.0100 hasta 0.0250 ms la variación no es muy significativa (ver anexo 6).

En lo que respecta al análisis del tamaño de la red, el área geográfica varía en 200 m^2, 400 m^2, 600 m^2, 800 m^2 y 1000 m^2, manteniendo el número de nodos en 30. DSR tiene mejor desempeño en términos de carga de mensajes de control, esta es muy baja en comparación a AODV y OLSR (ver anexo 7).

También se observa que el retardo de extremo a extremo aumenta gradualmente para todos los protocolos a medida que aumenta el tamaño de la red. OLSR sin embargo llegó a tener un menor retardo llegando a 1 segundo en 1000 m^2 mientras que con DSR alcanza un pico superior a los 2 segundos (ver anexo 8)

El rendimiento para todos los protocolos disminuye gradualmente conforme aumenta el área de la red, teniendo un valor inicial de 4000 kbps llegando a un rango de 1600 a 1000 kbps. Esto puede deberse a las características de la capa física y enlace propias de la red (ver anexo 8).

4.4.4 Caso 4: Transmisión de datos.

(Al-Ani, 2011, pág. 4) Realiza un estudio comparativo entre protocolos de enrutamiento ad-hoc como OLSR AODV y DSR, con un servidor FTP fijo, se empleó 25 nodos móviles en un área de 1500 metros por 1500 metros mediante el simulador de redes OPNET, todos los nodos emulan sesiones ftp funcionando al mismo tiempo y la tasa de transmisión fue establecida en 5.5

Mbps. Se evaluó parámetros como retardo y el rendimiento, los resultados fue que OLSR presento un mejor rendimiento promedio de alrededor de 135 kbps. En AODV los primeros 8 minutos presentó un rendimiento igual a 0 kbps luego alcanzó 23,8 kbps que no se mantuvieron constantes. En DSR ocurrió una situación similar los primeros 7 minutos el rendimiento fue igual a 0 kbps para después alcanzar un pico de 11,4 kbps que de igual manera no se mantuvo constante en el tiempo de simulación (ver anexo 9).

Los resultados de las pruebas de retardo muestran que OLSR tiene el menor tiempo con 0.000330 segundos que se mantienen constantes en todo el tiempo de prueba seguido por AODV con 0,000608 segundos y luego DSR con 0, 001909 segundos (ver anexo 10).

Tabla 11. Resumen de los escenarios de red

RESUMEN DE ESCENARIOS DE RED				
	Caso 1	Caso 2	Caso 3	Caso 4
Aplicación	Voz	UDP	UDP	FTP
Protocolos	OLSR, DSR DSDV, AODV	BABEL, OLSR POLSR	AODV, OLSR DSR	AODV, OLSR DSR
Simulador	NS-3	EMANE	NS-2	OPNET
Nodos	2 - 9	32	25 -50	25
Parámetros Analizados	Pérdida de paquetes, retardo y variación del número de nodos	Pérdida de paquetes	Número de nodos mensajes de control retardo	Retardo y rendimiento
Área de cobertura	800x100 m	1200x1500 m	200, 400, 600 800 y 1000 m^2	1500x1500 m

5. CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Las redes mesh aplicadas a Sistemas Aéreos no Tripulados proponen un esquema diferente al de las redes inalámbricas centralizadas. Después de haber analizado los componentes que intervienen en la formación de la red se ha podido identificar a las redes mesh basadas en el estándar 802.11s y redes MANET como tecnologías más adecuadas para ser aplicadas en sistemas aéreos no tripulados. Mesh 802.11s tiene un esquema definido y estandarizado para enlazar y enrutar dispositivos, mientras que para la red MANET, se basa en los estudios que puede aportar el MANET WORKING GROUP con respecto a protocolos de enrutamiento para redes Ad-hoc.

Los dos tipos de redes analizadas al ser móviles presentan cambios en la distribución, en la distancia y el número de nodos, por tanto los inconvenientes que enfrentan estas redes son la interferencia, latencia y la variabilidad del rendimiento. En consecuencia, estas redes cambiantes deben estar gestionadas por protocolos de enrutamiento que se adapten a este tipo de comportamiento.

Independientemente del UAS que forme parte del nodo de red mesh, un factor importante es la elección del protocolo de enrutamiento. Se identificó varios protocolos para redes mesh de tipo proactivo, reactivo e híbrido y estos contribuyen al buen funcionamiento de aplicaciones que deseen implementarse.

El protocolo proactivo OLSR presenta un mejor desempeño en cuanto al retardo extremo a extremo frente a los protocolos reactivos de los entornos analizados lo cual lo vuelve apto para todo tipo de transmisión en especial aplicaciones en tiempo real como video o VoIP. Existen mejoras como P-OLSR que contribuyen a un mejor desempeño del enrutamiento reduciendo el tiempo

que toma el volver a encaminar un paquete en situaciones en las que existe alta movilidad.

Los protocolos reactivos como AODV o DSR por sus características de descubrimiento de rutas presentan ciertas desventajas como retardo hasta establecer un camino entre emisor y receptor, de la misma forma de existir pérdida de enlace a causa de una red de nodos con alta movilidad los protocolos reactivos inician nuevas peticiones de rutas lo que hace que estos protocolos no sean del todo óptimos ante esta característica.

Para el mantenimiento de rutas OLSR presenta más eficiencia ante la movilidad, pero genera mayor cantidad de paquetes de control. Si lo que se desea es reducir estos paquetes, BATMAN se presenta como una buena opción y al no mantener rutas hacia todos los destinos sino solo al siguiente salto lo vuelve un protocolo más ligero en comparación a OLSR.

Existen soluciones en hardware como los miniordenadores mencionados que permiten adaptar tarjetas de red inalámbricas y con la capacidad de almacenamiento necesaria para implementar el software que en todos los proyectos analizados están basados en software libre y sobre este se implementan los protocolos utilizados en redes mesh.

5.2 RECOMENDACIONES

Un tema que debe ser analizado en futuras investigaciones son las frecuencias, canales y potencia de transmisión debido a las interferencias en la red, por ser un rango de frecuencias de uso libre y los inconvenientes del sistema en sí, como la distancia y cantidad de nodos que pueden degradar el rendimiento general de la red y afectan a las aplicaciones.

En lo que se refiere a componentes para formar la red que son adaptados al Sistema Aéreo no Tripulado se debe tener en cuenta aspectos como compatibilidad de software y modos de operación de tarjetas de red inalámbricas y otros factores como el consumo de energía ya que de esto dependerá el tiempo de vida del nodo de la red.

Para crear un diseño en este tipo de red se debería partir del análisis de la aplicación y servicio que se quiera brindar, ya que de esto dependerá la tasa de transmisión promedio necesaria y el enrutamiento a ser usado además si es necesaria la conexión con otro tipo de redes, etc.

REFERENCIAS

Al-Ani, R. (2011). Simulation and performance analysis evaluation for variant MANET routing protocols. *International Journal of Advancements in Computing Technology*(1), 12.

Andrade, J., & Naranjo, S. (2011). *Análisis del comportamiento de la tecnología Wimax (IEEE 802.16) y Wimax Moblie (IEEE 802.16E) con tráafico de voz y datos en varios escenarios, usando el simulador NS-2.* Recuperado el 10 de Noviembre de 2015, de http://bibdigital.epn.edu.ec/bitstream/15000/4268/1/CD-3898.pdf

Brown, T., Argrow, B., Dixon, C., Doshi, S., Thekkekunnel, R., Thekkekunnel, G., & Henkel, D. (2004). *Ad Hoc UAV Ground Network (AUGNet).* Recuperado el 19 de Febrero de 2016, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.8768&rep=rep1&type=pdf

Chalmeta, J. (2009). *Estudio y análisis de prestaciones de redes móviles Ad Hoc mediante simulaciones NS-2 para validar modelos analíticos.* Recuperado el 16 de Febrero de 2016, de http://upcommons.upc.edu/bitstream/handle/2099.1/8374/PFC_Jordi_Chalmeta.pdf?sequence=1

Cisco Systems. (2008). *QoS on Wireless LAN Controllers and Lightweight APs Configuration Example.* Recuperado el 16 de Noviembre de 2015, de http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/81831-qos-wlc-lap.html

Cisco Systems. (2011). *Conceptos y protocolos de enrutamiento Versión 4.0.* Juárez, Mexico: PEARSON EDUCACIÓN DE MÉXICO.

Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR).* Recuperado el 3 de Febrero de 2016, de https://www.ietf.org/rfc/rfc3626.txt

Coya, L., Ledesma, T., & Baluja, W. (2014). *Protocolos de enrutamiento aplicables a las MANET.* Recuperado el 16 de Febrerro de 2016, de http://revistatelematica.cujae.edu.cu/index.php/tele/article/view/170/159

D. Jhonson; Y. Hu; D. Maltz. (2007). *The dynamic source routing protocol (DSR) for mobile Ad Hoc networks for IPv4.* Recuperado el 13 de enero de 2016, de https://tools.ietf.org/html/rfc4728

Dignani, J. P. (2011). *Análisis del Protocolo Zigbee.* Recuperado el 7 de Noviembre de 2015, de http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Dignanni_Jorge_Pablo.pdf

Dirección General de Aviación Civil. (2015). *Resolución No 251/2015.* Recuperado el 12 de Noviembre de 2015, de http://www.aviacioncivil.gob.ec/wp-content/uploads/downloads/2015/09/Resol.-251-2015-Normas-Operacion-Drones.pdf

Espiga, A. (2012). *Selección de portal en redes inalámbricas malladas utilizando aprendizaje estadístico.* Recuperado el 10 de Septiembre de 2015, de http://premat.fing.edu.uy/ingenieriamatematica/archivos/tesis_alejandro_espiga.PDF

Haas, Z., Pearlman, M., & Samar, P. (2002). *The zone routing protocol (ZRP) for Ad hoc networks.* Recuperado el 2 de Febrero de 2016, de https://tools.ietf.org/html/draft-ietf-manet-zone-zrp-04

Hiertz, G., Denteneer, D., Max, S., Taori, R., Cardona, J., Berlemann, L., & Walke, B. (2010). *IEEE 802.11s: The WLAN mesh standard.* Recuperado el 15 de Febrero de 2016, de http://cozybit.com/wordpress/wp-content/uploads/2010/03/ieee-80211s-the-wlan-mesh-standard.pdf

IEEE Computer Society. (2012). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* New York, EEUU: The Institute of Electrical and Electronics Engineers, Inc.

Kioskea. (2014). *Modos de funcionamiento Wifi (802.11 o Wi-Fi).* Recuperado el 4 de Octubre de 2015, de http://es.ccm.net/contents/791-modos-de-funcionamiento-wifi-802-11-o-wi-fi#infrastructure

Kioskea. (2014). *Redes inalámbricas.* Recuperado el 4 de Septiembre de 2015, de http://es.ccm.net/contents/818-redes-inalambricas

Kioskea. (2014). *WiMAX - 802.16 - Interoperabilidad mundial para acceso por micro.* Recuperado el 25 de Septiembre de 2015, de http://es.ccm.net/contents/795-wimax-802-16-interoperabilidad-mundial-para-acceso-por-micro

López, F. (s.f). *El estándar IEEE 802.11.* Recuperado el 8 de Octubre de 2015, de http://datateca.unad.edu.co/contenidos/301120/2014_II_LECCION_EVALUATIVA1.pdf

Los Santos, A. (2009). *Aplicación de las Redes de Sensores en el entorno vehicular.* Recuperado el 13 de Septiembre de 2015, de http://www.albertolsa.com/wp-content/uploads/2010/04/rsi-aplicacion-de-las-redes-de-sensores-en-el-entorno-vehicular-alberto-los-santos.pdf

Miller, M. (2008). *Redes inalambricas con windows vista.* Madrid, España: Anaya Multimedia.

Mohapatra, S., & Kanungo, P. (2012). *Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 simulator.* Recuperado el 30 de Enero de 2016, de http://www.sciencedirect.com/science/article/pii/S1877705812008454

Morgenthaler, S. (2012). *UAVNET: A prototype of a highly adaptative and mobile wireless mesh network using unmanned aerial vehicles (UAVS).*

Recuperado el 15 de Diciembre de 2015, de http://rvs.unibe.ch/research/pub_files/Mo12.pdf

Neumann, A., Aichle, C., & Wunderlich, S. (2008). *Better approach to mobile Ad-hoc networking (B.A.T.M.A.N.).* Recuperado el 18 de Febrero de 2016, de https://tools.ietf.org/html/draft-wunderlich-openmesh-manet-routing-00

Organización de Aviación Civil Internacional. (2011). *Sistemas de aeronaves no tripuladas (UAS).* Quebec, Canadá: OACI.

Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing.* Recuperado el 7 de Enero de 2016, de https://www.ietf.org/rfc/rfc3561.txt

Poole, I. (s.f). *IEEE 802.11 Wi-Fi Standards*. Recuperado el 12 de Noviembre de 2015, de http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php

Rocabado, S. (2013). *Caso de estudio de comunicaciones seguras sobre redes móviles ad hoc.* Recuperado el 14 de Enero de 2016, de http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Rocabado_Moreno_Sergio.pdf

Rossati, S., Kruzelecki, K., Traynard, L., & Rimoldi, B. (2013). *Speed-Aware Routing for UAV Ad-Hoc Networks.* Recuperado el 04 de Febrero de 2016, de http://arxiv.org/pdf/1307.6350.pdf

Ruiz, J. (2008). *Configuraciòn DHCP en redes MANET subordinadas.* Recuperado el 18 de Noviembre de 2015, de http://eprints.ucm.es/10066/1/Jos%C3%A9_Ignacio_Ruiz_N%C3%BA%C3%B1ez.pdf

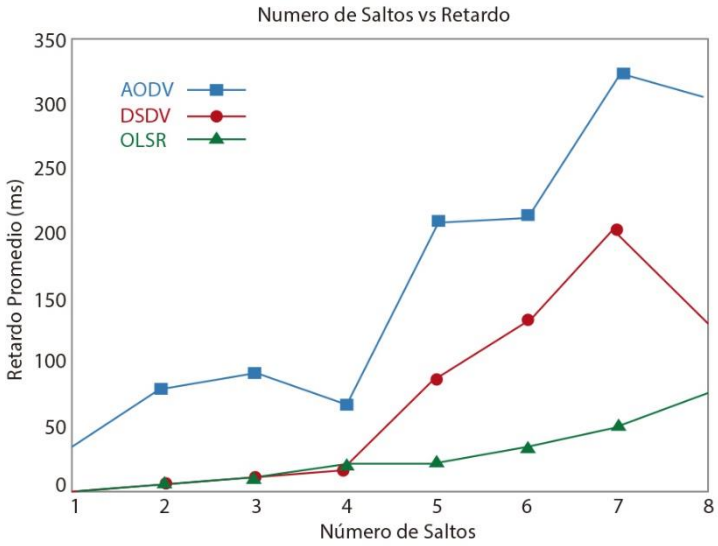
SenseFly. (2015). *eBee*. Recuperado el 12 de Diciembre de 2015, de www.sensefly.com/drones/ebee.html

Sing-Borrajo, P. (2014). Evaluación de desempeño de VoIP en redes MANET. *Revista de la división de ingenierias y arquitectura de la Universidad Santo Tomas*(1), 16.

ZigBee Alliance. (2012). *Zigbee Specification*. Recuperado el 6 de Noviembre de 2015, de http://www.zigbee.org/non-menu-pages/zigbee-pro-download/

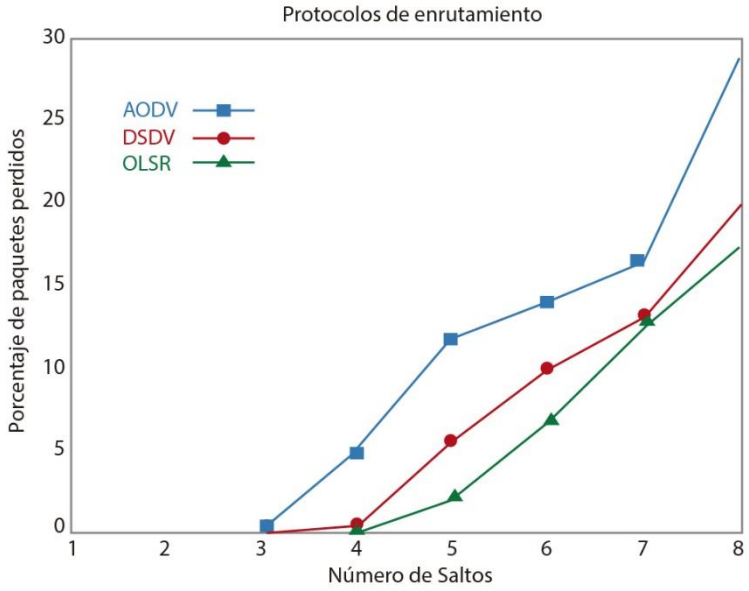
ANEXOS

Anexo 1: Variación del retardo de acuerdo al número de saltos.



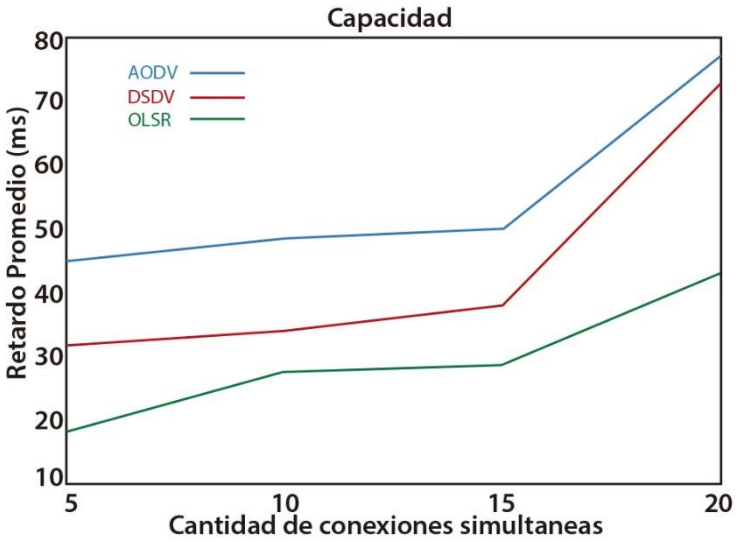
Tomado de: (Sing-Borrajo, 2014, pág. 11)

Anexo 2: Porcentaje de paquetes perdidos en función del número de saltos



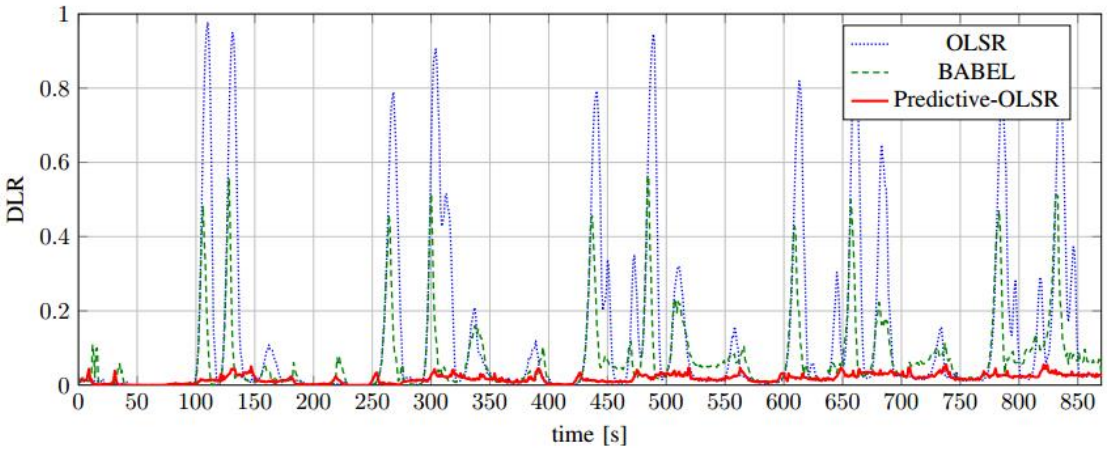
Tomado de: (Sing-Borrajo, 2014, pág. 12)

Anexo 3: Evaluación del retardo promedio de acuerdo al número de conexiones simultaneas



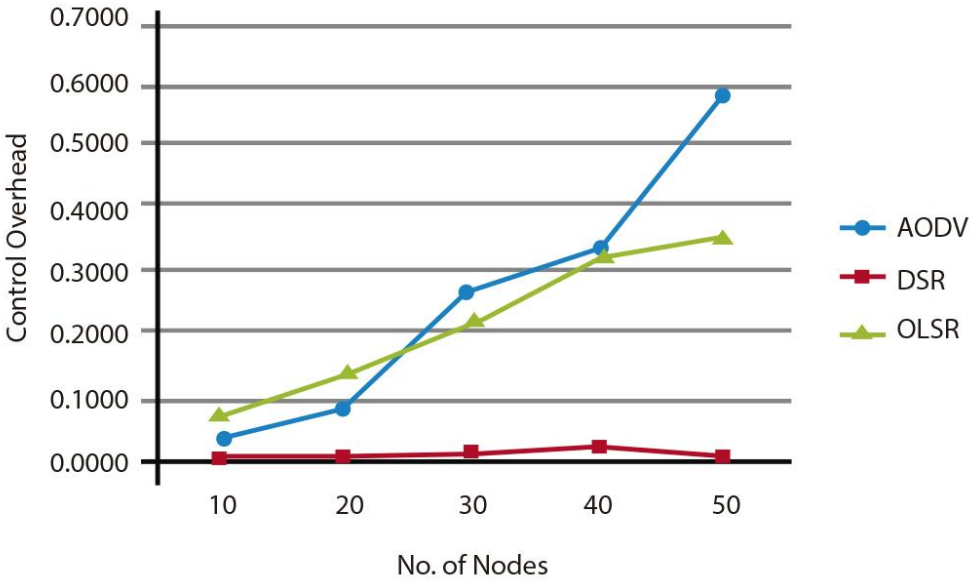
Tomado de: (Sing-Borrajo, 2014, pág. 13)

Anexo 4: Tasa de pérdida de paquetes para cada protocolo en un tiempo determinado



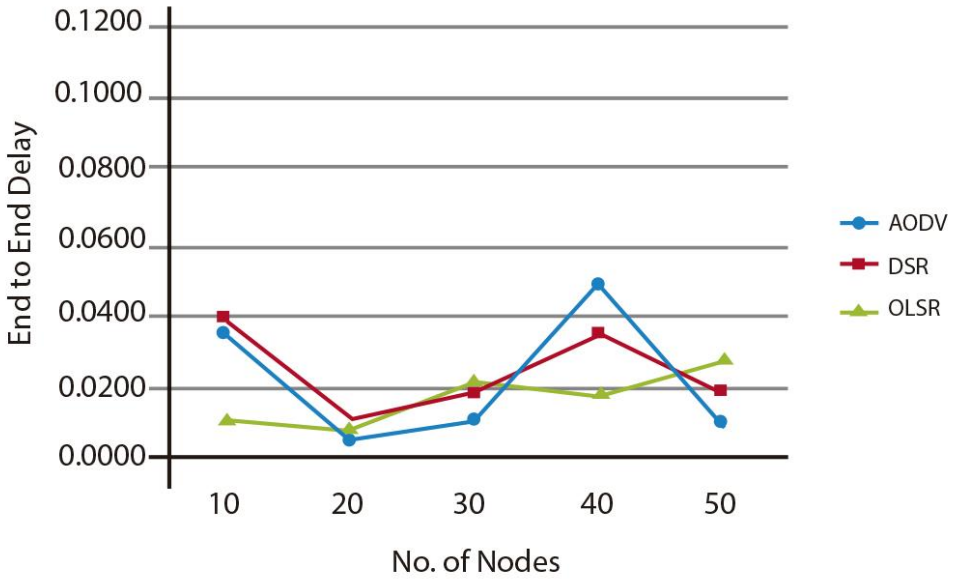
Tomado de: (Rossati, Kruzelecki, Traynard, & Rimoldi, 2013)

Anexo 5: Cantidad de paquetes de control de acuerdo al número de nodos



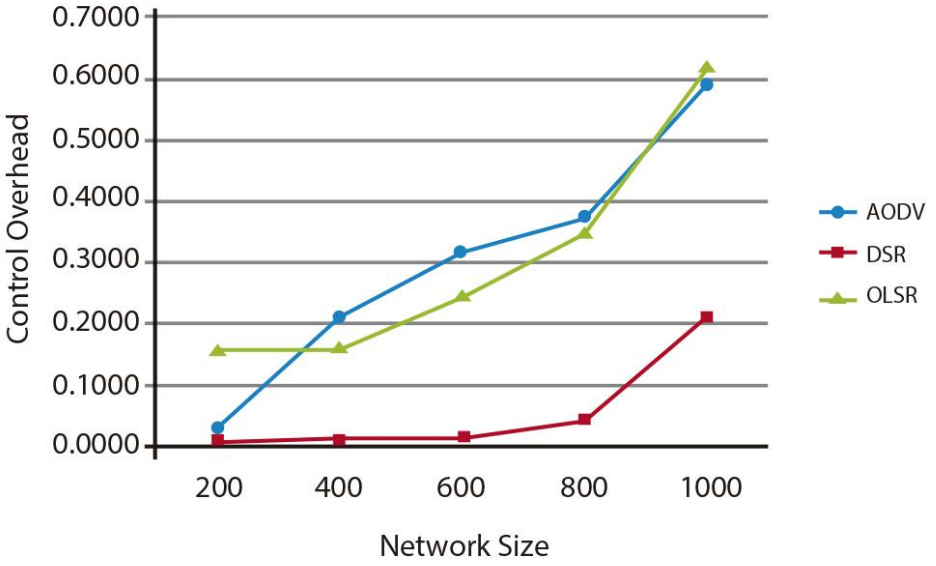
Tomado de: (Mohapatra & Kanungo, 2012)

Anexo 6: Retardo Extremo – Extremo de acuerdo al número de nodos



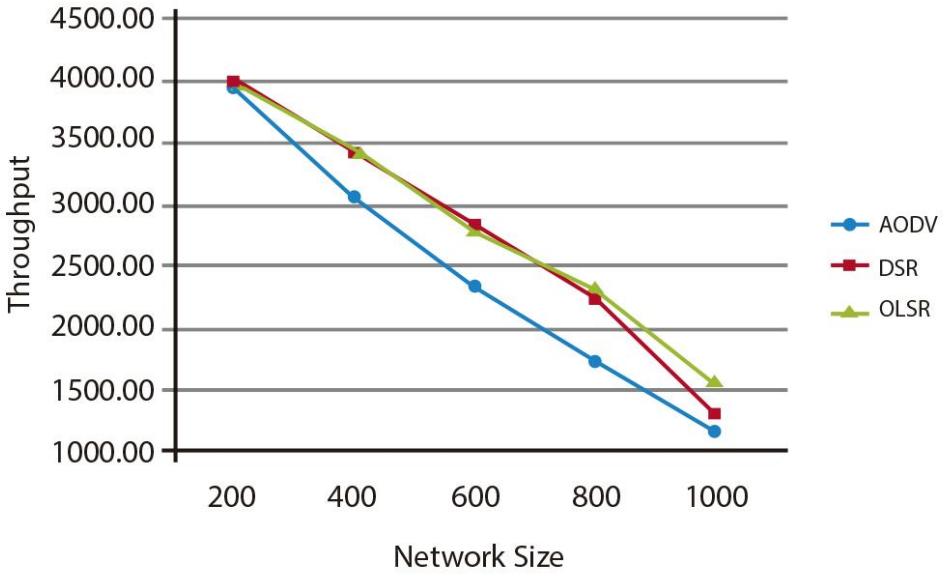
Tomado de: (Mohapatra & Kanungo, 2012)

Anexo 7: Mensajes de control en función del área en m^2 de la red.



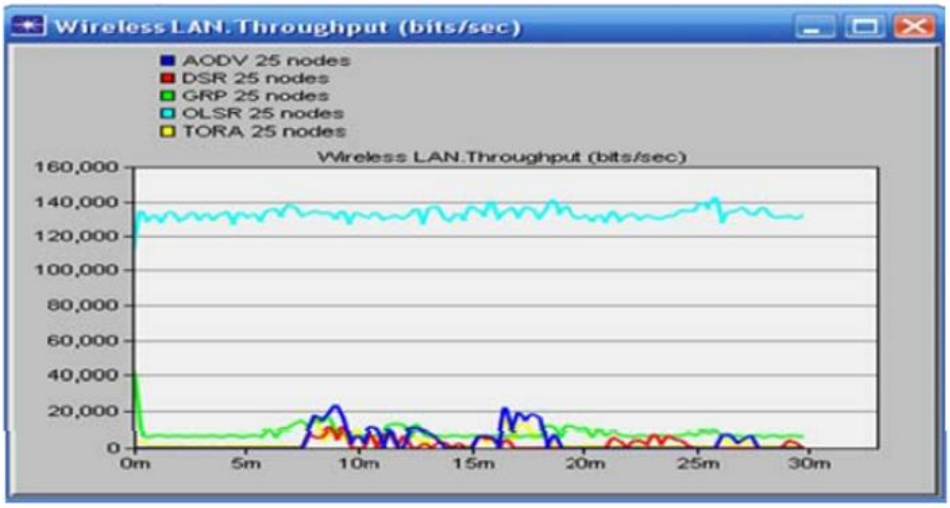
Tomado de: (Mohapatra & Kanungo, 2012)

Anexo 8: Rendimiento en función del área en m^2 de la red.



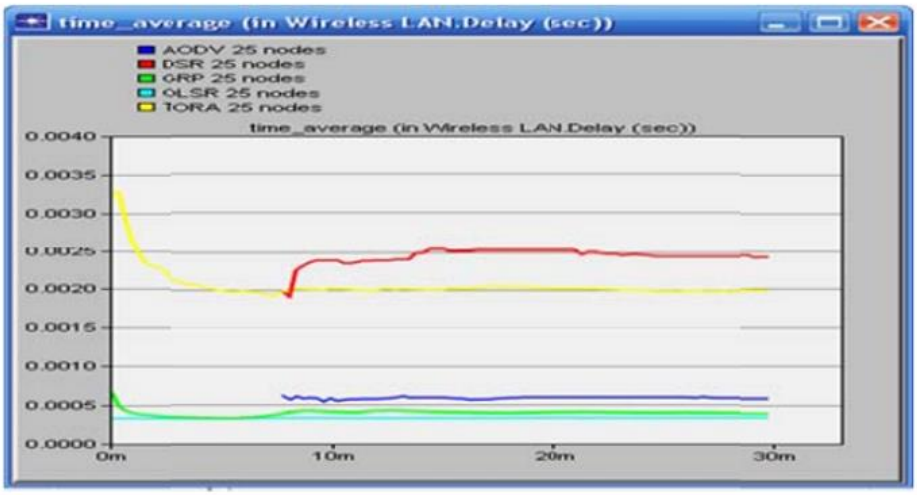
Tomado de: (Mohapatra & Kanungo, 2012)

Anexo 9: Evaluación del rendimiento durante treinta minutos con varios protocolos de enrutamiento.



Tomado de: (Al-Ani, 2011, pág. 5)

Anexo 10: Evaluación del retardo promedio durante treinta minutos con varios protocolos de enrutamiento.



Tomado de: (Al-Ani, 2011, pág. 5)