



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Despliegue de una red MANET entre lanchas de instrucción

Grado en Ingeniería Mecánica

ALUMNO: Manuel Marín López

DIRECTOR: Rafael Asorey Cacheda

CURSO ACADÉMICO: 2014-2015

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Despliegue de una red MANET entre lanchas de instrucción

Grado en Ingeniería Mecánica
Intensificación en Tecnología Naval
Cuerpo General

Universida_{de}Vigo

RESUMEN

El presente Trabajo Fin de Grado (TFG) tiene como principal objetivo el despliegue de una red MANET (del inglés, *Mobile Ad-hoc Network*) entre las cuatro lanchas de instrucción de la Escuela Naval Militar. Asimismo, las lanchas de instrucción tendrán conexión con un nodo situado en tierra siempre y cuando estén dentro de la ría de Pontevedra, de manera que se pueda intercambiar información en tiempo real con los equipos instalados en la Escuela Naval.

Para ello, se expondrá el funcionamiento general de una red MANET, así como las diferencias de esta con las redes inalámbricas tradicionales, utilizadas para ámbitos domésticos. Seguidamente, se analizará cada una de las capas OSI dentro de una MANET. Será fundamental analizar los distintos algoritmos de encaminamiento que regirán la capa de red, pues en este nivel será donde más diferencias se pueden encontrar respecto a una red inalámbrica punto-multipunto convencional. En materia de seguridad, se tendrán en cuenta posibles vulnerabilidades las cuales son características de las redes MANET.

Finalmente, la instalación y adaptación de los equipos adquiridos será el pilar fundamental ya que son los medios que permiten la consecución del principal objetivo de este trabajo. Una vez en funcionamiento, se valorarán posibles aplicaciones que tengan cabida dentro de el escenario de trabajo, así como uno de los servicios principales a acometer en el despliegue de la red: La integración del usuario final dentro de la red MANET.

PALABRAS CLAVE

MANET, Red Mallada, *Ad-hoc*, encaminamiento, *wireless networking*, Wi-Fi, IEEE 802.11, OLSR.

AGRADECIMIENTOS

En primer lugar a mi padre que desde pequeño fue un referente a todos los temas relacionados con las nuevas tecnologías.

También quiero agradecer al director del presente trabajo fin de grado D. Rafael Asorey, por confiar desde el principio en la viabilidad del proyecto. Principalmente, contribuyendo a la adquisición del material necesario para las pruebas y la posibilidad de una instalación permanente en la Escuela Naval Militar.

Finalmente, y no por ello menos importante, a la Escuela Naval Militar por poner a mi disposición las lanchas de instrucción, ya que sin ellas no se podría a ver llevado a cabo las pruebas empíricas.

Índice

Índice de figuras	3
Índice de Tablas	4
1 Introducción y objetivos	5
1.1 Motivación	5
1.2 Objetivos	6
1.3 Redes inalámbricas	7
1.3.1 IEEE 802.11	7
1.3.2 Arquitectura	9
1.3.3 Ventajas y desventajas	10
1.4 Organización de la memoria	11
2 Estado del arte	12
2.1 Redes MANET (<i>Mobile Adhoc Network</i>)	12
2.1.1 Características generales	13
2.1.2 Capa física	14
2.1.3 Capa MAC (<i>Medium Access Control</i>)	15
2.1.4 Capa de red	15
2.1.5 Capa de transporte	17
2.1.6 Capa de aplicación	18
2.2 Encaminamiento en MANET: OLSR (<i>Optimized Link State Routing Protocol</i>)	18
2.2.1 Generalidades	18
2.2.2 Terminología	19
2.2.3 Mecanismo de inundación: MPR	20
2.2.4 Funcionamiento: Núcleo OLSR	21
2.2.5 Formato de los paquetes	23
2.2.6 Tipos de mensajes: HELLO, TC, MID	24
2.2.7 Tratamiento de los mensajes	27
2.2.8 Justificación de la elección del protocolo	28
2.3 Seguridad	28
2.3.1 Escenario	30
2.3.2 Ataques potenciales	31
2.3.3 Seguridad en MANET: mecanismos básicos	32

3 Despliegue de una red MANET	35
3.1 Generalidades.....	35
3.2 Equipos y material	37
3.2.1 Segmento embarcado.....	37
3.2.2 Segmento terrestre	40
3.3 Configuración y <i>software</i>	42
3.4 Acceso desde dispositivos cliente a bordo de buques.....	51
3.4.1 Configuración	51
4 Resultados	53
4.1 Realización de la 1ª Prueba.....	53
4.2 Realización de la 2ª Prueba.....	56
4.3 Datos obtenidos.....	58
5 Conclusiones y líneas futuras	61
5.1 Conclusiones extraídas.....	61
5.2 Líneas futuras	62
6 Bibliografía.....	63
Anexo I: Especificaciones de equipos	65

ÍNDICE DE FIGURAS

Figura 1-1 El alcance de un solo radio probablemente no dé cobertura a todo el sistema.....	8
Figura 1-2 Red en modo BSS.....	9
Figura 1-3 Red en modo IBSS	9
Figura 1-4 Diferencias entre IBSS y red mallada.....	10
Figura 2-1 Clasificación de redes inalámbricas multisalto [4].....	12
Figura 2-2 Enlaces de radio frecuencia establecidos en una red ad-hoc	13
Figura 2-3 Ilustración de la disminución de la tasa de datos en función del número de nodos	13
Figura 2-4 Protocolos de encaminamiento para redes Ad Hoc	16
Figura 2-5 Selección de nodos MPR.....	20
Figura 2-6 Escenario simplificado de detección de vecinos [14].....	22
Figura 2-8 Esquema de un mensaje HELLO. [13].....	24
Figura 2-9 Esquema de un mensaje TC. [13].....	26
Figura 2-10 Esquema del mensaje de seguridad en OLSR	33
Figura 3-1 Antena omnidireccional AOA-2415.....	37
Figura 3-2 Diagrama de radiación de la antena.....	38
Figura 3-3 Bullet M2.....	39
Figura 3-4 Sellamiento del cable CAT5	39
Figura 3-5 NanoStation M2.....	40
Figura 3-6 Diagrama de radiación de NanoStation M.....	41
Figura 3-7 Captura de pantalla del interfaz gráfico en la pestaña OLSR.....	45
Figura 3-8 TP-LINK WDR3500	51
Figura 4-1 Visión de nodo “TIERRA-1”	54
Figura 4-2 Situación y representación de sectores con obstáculos.....	55
Figura 4-3 Cobertura de los nodos. Escenario de prueba 1º.....	55
Figura 4-4 Disposición de nodos en tierra. 2º prueba	57
Figura 4-5 Cobertura de los nodos de tierra. Escenario de prueba 2º	57
Figura 4-6 Topología mostrada por el interfaz gráfico durante la 1ª prueba.....	58
Figura 4-7 Potencia Rx a bordo de “LANCHA-1”	59
Figura 4-8 Topología mostrada por el interfaz gráfico durante la 2ª prueba.....	60

ÍNDICE DE TABLAS

Tabla 3-1 Características generales L.I	35
Tabla 3-2 Especificaciones técnicas Bullet M2.....	38
Tabla 3-3 Especificaciones NanoStation M2	41
Tabla 3-4 Módulos necesarios en OLSR.....	45
Tabla 3-5 Especificaciones técnicas del AP	51
Tabla 4-1 Organización del material. 1ª prueba	54
Tabla 4-2 Organización del material. 2ª prueba	56
Tabla 6-1 Sensibilidades en recepción frente a Tasas de transmisión. BulletM2	65
Tabla 6-2 Sensibilidades en recepción frente a Tasas de transmisión. NanoStationM2	65

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Motivación

El avance vertiginoso de las tecnologías de la comunicación en el mundo civil se plantea como una fuente de ideas inmensa donde investigar para encontrar su correcta aplicación en la complicada disciplina de las comunicaciones militares.

Concretamente, desde que en el año 1911 el crucero Extremadura inaugurara las comunicaciones modernas en nuestra Armada, los enlaces inalámbricos desempeñan un papel fundamental en las comunicaciones navales.

La profunda inmersión en las tecnologías de comunicación no solo afecta a las labores cotidianas del mundo civil, sino que esta inmersión también se observa en la líneas de evolución de la tecnología militar. En el ámbito naval, cada vez es mayor la cantidad de información que un buque puede extraer de su zona de influencia, siendo necesario en la mayoría de los casos el envío de la información fuera del propio buque. Este traspaso de información puede ser, o bien hacia tierra firme con el fin de informar a la autoridad pertinente, o hacia otro buque al que le sea de utilidad esta información.

En base a la anterior premisa, son necesarios enlaces seguros de alta capacidad que permitan a los buques intercambiar esa gran cantidad de información para su posterior evaluación y toma de decisiones. En las comunicaciones militares es un factor de relevancia la disponibilidad de los sistemas, incluso en las condiciones más adversas. Por ello, un sistema de comunicaciones militares debe buscar la mayor independencia posible de infraestructuras externas a él. Un ejemplo de un sistema de comunicaciones muy extendido podría ser la telefonía móvil GSM donde la fiabilidad del enlace de voz no está únicamente supeditada al terminal móvil, sino también a toda la infraestructura desplegada por las compañías telefónicas. Es por ello que las comunicaciones navales buscan resistencia y redundancia en sus sistemas ya que si no se tuviera en cuenta, surgiría la pregunta de por qué nuestros buques siguen equipando sistemas HF para transmisión de voz y datos cuando las comunicaciones satelitales ofrecen unas capacidades muchísimo mayores. La respuesta es que las comunicaciones navales intentan, en la media de lo posible, depender lo menos posible de infraestructura de terceros para sus enlaces de voz y datos.

Por ello, en este trabajo fin de grado se van a utilizar enlaces autónomos capaces de transmitir tanto voz como datos utilizando el estándar de referencia en las comunicaciones entre sistemas: IP.

Más concretamente se hará referencia a una tecnología en auge en las comunicaciones inalámbricas aunque todavía sin estándares finales preparados para ser desplegados. Esta tecnología es conocida en el mundo de las telecomunicaciones como “*Wireless Mesh Networks*”, cuya traducción sería “Redes Inalámbricas Malladas”.

Las posibilidades que ofrece este tipo de redes radica en la posibilidad de poder mallar las conexiones entre los nodos que la compongan, de forma que una fuerza naval con todas sus unidades que se encuentren en alcance radio entre ellas, establezcan un enlace bidireccional. No hay un solo camino por el que deba viajar la información, si no que será el transmisor del buque quien de forma autónoma evalúe el mejor camino para llegar del buque A al buque B. Los posibles caminos por los que la información puede viajar son directamente proporcionales al número de buques (nodos) que el nodo A tenga en alcance radio. Puede darse el caso que el buque A y B no estuviesen en alcance radio debido, posiblemente, a que se encuentran fuera del horizonte respectivo de cada buque. En este caso, un buque intermedio podría retransmitir la información de manera automática.

Son numerosos los sistemas en la actualidad que implementan el mallado de enlaces en su redes de comunicaciones. Un ejemplo actual de considerable importancia son las redes de sensores, las cuales no necesitan un nodo central para gestionar el tráfico, sino que de manera autónoma cada nodo sabe cual es el nodo siguiente más adecuado al que debe retransmitir la información para que llegue a su destino. La diferencia más notable con las redes de sensores respecto a una red *MANET* es el carácter móvil de los nodos, pero el fundamento es el mismo.

Finalmente, no existe todavía un estándar certificado que trate toda la problemática de este tipo de redes. Por lo tanto, será importante para nuestro diseño e implementación real el estándar 802.11 en sus variantes b/g. Este estándar contempla conexiones punto a punto entre dispositivos, siendo este modo la base de partida para adaptarlo a una arquitectura de red punto-multipunto propia de las redes *MANET*.

1.2 Objetivos

El principal objetivo del presente TFG es el despliegue y configuración de una red mallada inalámbrica entre las lanchas de instrucción de la Escuela Naval Militar y una estación en tierra que extienda la red del Centro Universitario de la Defensa. Los nodos embarcados serán dotados de una interfaz de red y una antena omnidireccional de alta ganancia que transmitirá utilizando la banda ISM en el espectro de 2,4 Ghz. La estación de radio dispuesta en tierra será preferiblemente una antena sectorial que trabaje en la misma banda.

Para la consecución se utilizará *software* libre basado en Linux, que permite configurar el protocolo de encaminamiento el cual gestionará los enlaces *ad-hoc* entre todos los nodos que compongan la red. Dada la movilidad de los nodos en la red, el concepto de *Mesh Networking* puede ser concretado en un tipo de redes que reciben el nombre de *MANET* (del inglés *Mobile Ad-Hoc Networking*). El concepto *MANET* es el que mejor define la naturaleza del objetivo a conseguir en este trabajo, pues los nodos son móviles.

El principal servicio ofrecido en el despliegue de la red *MANET* es la conexión a Internet mediante una puerta de enlace en tierra. Esta puerta de enlace tendrá como principal rango de acción la parte

oeste de la ría de Pontevedra, siendo instalada en la mejor situación geográfica posible dentro del recinto de la Escuela Naval Militar.

Todos los equipos que se van a emplear en el despliegue de la red MANET serán sistemas embebidos basados en una arquitectura de *hardware* RISC [1] que cumplan con los requisitos reflejados en [2], necesarios para instalar en los nodos el sistema operativo *OpenWrt*. Esto supone un ahorro en lo que a material se refiere ya que esta tecnología añade placas miniPCI transmisoras de acuerdo a los esquemas de modulación y frecuencias a utilizar, pudiendo utilizar una misma placa madre, múltiples placas miniPCI transmisoras.

De manera paralela al objetivo principal se enuncian a continuación los siguientes objetivos secundarios:

- Introducción a las redes móviles *ad-hoc*.
- Protocolos de enrutamiento para redes *ad-hoc*.
- Protocolo OLSR (*Optimized Link State Routing*).
- Configuración e instalación del *hardware*.
- Realización de pruebas en la ría de Pontevedra.
- Exposición de resultados.
- Extensión de la red MANET a dispositivos cliente a bordo de la embarcación.
- Uso de red MANET para labores docentes.
- Posible instalación permanente.

1.3 Redes inalámbricas

1.3.1 IEEE 802.11

El principal estándar utilizado en este TFG es el estándar IEEE 802.11 en su revisión de 2012 [3]. A mediados de la década de 1990 comenzaron los primeros esfuerzos por parte del comité IEEE para idear un estándar válido para redes LAN inalámbricas. Una de sus mayores premisas a la hora de formalizar el estándar fue la de encontrar una banda libre del espectro que permitiese que la comunicación sin cables entre máquinas que no tuviera que estar supeditada a costosas licencias de transmisión. Los sistemas basados en el estándar que nos ocupa se caracterizan por operar en bandas sin licencia como las bandas ISM (Industriales, Científicas y Médicas, del inglés *Industrial, Scientific, and Medical*) siempre y cuando no superen la potencia de transmisión legislada en cada país. Debido a esto, el alcance del radioenlace puede variar en función de la materia legislativa de cada país (máxima PIRE), del tipo de antena y la tasa de datos, entre otros muchos factores.

- El IEEE 802.11 define, desde el punto de vista de la capa física, tres técnicas no interoperables entre sí: FHSS (*Frequency Hopping Spread Spectrum*) y DSSS (*Direct Sequence Spread Spectrum*), ambos son usados en la frecuencia de 2,4 GHz así como en su modalidad en la banda infrarroja. El estándar especifica, en primera instancia tres modos de funcionamiento:

- 802.11a : Utiliza la banda de los 5 GHz y fue el primero en utilizar OFDM (*Orthogonal Frequency Division Multiplexing*) en 1999.
- 802.11b: Trabaja en la banda de 2,4 GHz y debido a la implementación de técnicas DSSS en 1999 opera a una velocidad teórica de 11Mbps.
- 802.11g: Funciona en la misma banda que 802.11b y como su homólogo en los 5 GHz, en 2003 incluyó OFDM para soportar velocidades teóricas máximas de hasta 54 Mbps.

La alta demanda de los usuarios y el cada vez mayor flujo de datos requerido ha dado paso a la creación de otros estándares como 802.11n, capaz de soportar tasas de hasta 450 Mbps con la utilización de hasta cuatro antenas haciendo uso de la tecnología MIMO.

Actualmente, el estándar 802.11ac está en proceso de implantación para proporcionar una tasa de transferencia teórica de hasta 1 Gbps en de la banda de 5 GHz mediante la ampliación del ancho de banda y modulación de alta densidad (256QAM).

El medio de transmisión en las redes inalámbricas supone un problema añadido con el que el estándar tiene que hacer frente. El medio utilizado es de difusión por naturaleza, al contrario que los estándares de transmisión de datos por cable en los que cada transmisor tiene garantizado su porción del espectro. Para solucionar este problema, 802.11 utiliza CSMA (*Carrier Sense Multiple Access*). Aún así, este sistema plantea numerosos problemas, pues está supeditado al rango máximo de alcance del equipo radio, que no siempre es capaz de detectar a un tercer transmisor transmitiendo dentro de su alcance. Este caso es conocido como problema del “nodo oculto” y se tratará con más detalle en siguientes capítulos teniendo en cuenta la naturaleza la arquitectura de la red del presente TFG.

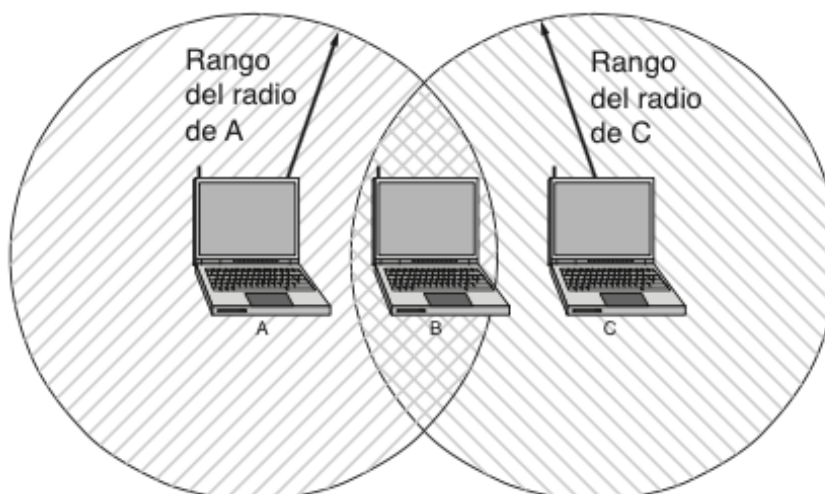


Figura 1-1 El alcance de un solo radio probablemente no dé cobertura a todo el sistema.

1.3.2 Arquitectura

Una red inalámbrica puede configurarse para funcionar en dos modos:

- **Modo BSS (*Basic Service Set*):** Es el utilizado normalmente. Es también denominado modo infraestructura. En este modo se conecta un número determinado de estaciones a un punto de acceso (AP, *Access Point*) normalmente realizando funciones de puerta de enlace y de encaminador del tráfico de la red sin cables. La figura 1-2 ilustra la arquitectura de este modo de funcionamiento.

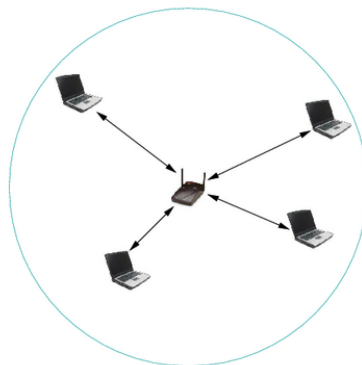


Figura 1-2 Red en modo BSS

- **Modo IBSS (*Independent Basic Service Set*):** Este modo es también conocido como *ad-hoc*. Está diseñado para facilitar las conexiones punto a punto sin la necesidad de un punto de acceso que encamine el tráfico. En la figura 1-3 se observa una representación gráfica de la disposición básica de los nodos en una red configurada en modo IBSS.

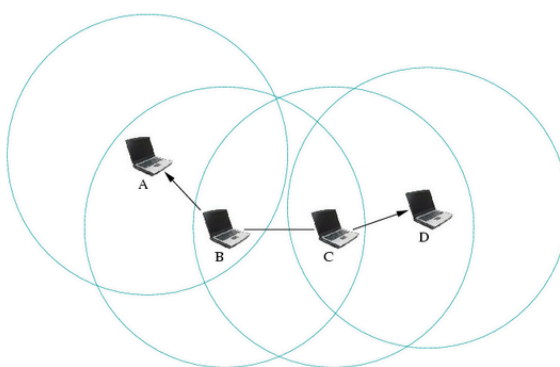


Figura 1-3 Red en modo IBSS

El modo IBSS contemplado en el estándar IEEE 802.11, también conocido como *IEEE Ad-hoc Mode*, representa el punto de partida que fundamenta las redes malladas. El término multisalto es el que diferencia a las redes malladas con el modo IBSS. Como se puede observar en la figura 1-4, en la

disposición superior de los nodos, la comunicación entre A y C sería imposible ya que las retransmisiones no están contempladas. Sin embargo, en la disposición de los nodos de la parte inferior de la figura 1-4 los nodos A y C sí se podrían comunicar pues se trata de una red mallada. Para que el multisalto pueda suceder en una red con enlaces *ad-hoc* es necesario un protocolo de encaminamiento.

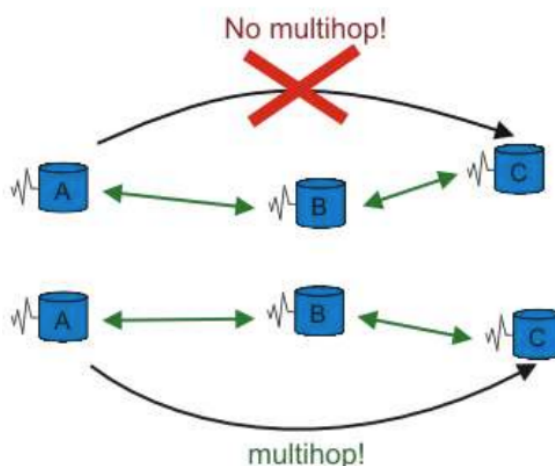


Figura 1-4 Diferencias entre IBSS y red mallada

1.3.3 Ventajas y desventajas

Una red inalámbrica presenta importantes ventajas respecto a su homóloga por cable:

- La principal ventaja es que en una red inalámbrica todos los terminales gozan de movilidad en tanto en cuanto su enlace inalámbrico le permita.
- Proporciona pasarelas de datos entre nodos que por su naturaleza resulta imposible la instalación de cables que los unan.
- El coste inmediato de una pequeña LAN que proporcione enlace a los terminales es menor que la infraestructura necesaria para instalar cableado entre todos los usuarios. Asimismo, la facilidad para incluir nuevos clientes es meramente superior en una red sin cables puesto que no es necesario dotar al establecimiento de una preinstalación en cuanto a cables se refiere.

Por otra parte, también hay que tener en cuenta las siguientes desventajas:

- La potencia de las señales es inversamente proporcional al cuadrado de la distancia del radioenlace, por lo que las máquinas de la red tienen un espacio de movimiento restringido supeditado directamente al estado del radioenlace.
- Debido a las limitaciones del medio, no es posible emitir y recibir al mismo tiempo. Hay una probabilidad no despreciable de colisión de mensajes. Estas colisiones provocan pérdidas añadidas que restan eficiencia a los estándares anteriormente mencionados.

- La seguridad es un tema complejo debido a que el medio de transmisión es por naturaleza de difusión, pudiéndose ver comprometidos los datos transmitidos por este medio. De hecho, cualquier receptor que se encuentre en alcance puede interceptar las transmisiones entre dos estaciones.
- Las tasas de transmisión son menores que las de un medio cableado, aunque numerosos estándares las están equiparando.

1.4 Organización de la memoria

El resto de la memoria se organiza en capítulos con la siguiente distribución:

- En el capítulo 2 se presenta un estado del arte de las tecnologías tratadas en el TFG. El estado del arte supone una puesta al día del desarrollo actual de la tecnología utilizada en el despliegue de la red MANET. Tiene un carácter comparativo con las redes inalámbricas Wi-Fi habituales, pues las redes malladas comparten una gran cantidad de rúbricas de funcionamiento heredadas de las redes Wi-Fi convencionales como, por ejemplo, los esquemas de modulación en la capa física utilizados en una red MANET. En la parte final se analizan varios algoritmos de encaminamiento para estas redes.
- En el capítulo 3 se describe la configuración de los equipos adquiridos y su puesta en marcha. En este capítulo se detallan los datos y experiencias acumuladas de las salidas a la mar en las que se han realizado pruebas con los equipos. También se trata todo lo relacionado con la extensión de la red MANET a los equipos cliente a bordo de la embarcación, así como las aplicaciones empleadas en la prueba y otras posibles que se consideran de especial utilidad para ser montadas sobre la red MANET ya en funcionamiento.
- En el capítulo 4 se exponen y analizan los resultados y prestaciones ofrecidas por la red MANET desplegada.
- En el último capítulo se presentan las conclusiones y líneas futuras. Básicamente serán recomendaciones y líneas de trabajo por las que seguir investigando para la mejora y el mejor aprovechamiento de los equipos adquiridos.
- En los anexos a esta memoria se proporciona información adicional de los fabricantes sobre los equipos de red.

2 ESTADO DEL ARTE

2.1 Redes MANET (*Mobile Adhoc Network*)

Las redes *ad-hoc* móviles consisten en un conjunto de nodos que se comunican mediante enlaces inalámbricos y que no tienen una infraestructura fija. Esto implica que no existe ningún tipo de control centralizado, proporcionando flexibilidad y eliminando la necesidad a los nodos de estar dentro de el alcance de un punto central. Este punto central es el llamado encaminador dentro de la terminología de las redes BSS, anteriormente tratadas. Dentro de las redes *ad-hoc* existen varios tipos [4]: las redes de sensores, las redes *mesh*, las redes vehiculares (VANET, *Vehicular Ad-Hoc Network*) y las redes móviles *ad-hoc* (MANET, *Mobile Ad-Hoc Network*). Este proyecto se centra en el último de los tipos mencionados, las MANETs.

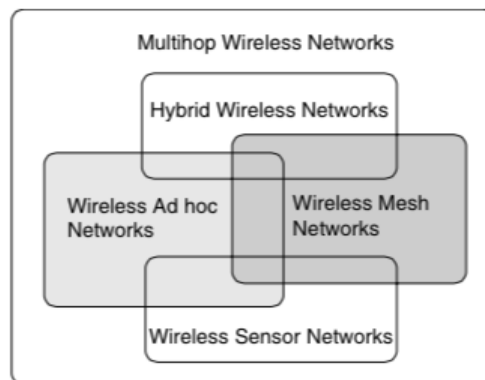


Figura 2-1 Clasificación de redes inalámbricas multisalto [4]

Las MANET permiten movilidad a los nodos. Esto conlleva que los enlaces entre nodos se puedan romper o crear dinámicamente y que haya nodos que se incorporen o abandonen la red en cualquier momento. Por lo tanto, la topología de red es altamente cambiante y aleatoria. Todos los nodos pueden actuar tanto como emisores, receptores y encaminadores de tráfico. Esto es necesario ya que los caminos a un destino pueden tener varios saltos. Aunque las MANET son un subgrupo dentro de las redes multisalto, la naturaleza cambiante de los dispositivos de la red plantea una dificultad más para encontrar el camino correcto de los paquetes de datos. Este último aspecto, aparte de otros, es de vital importancia para determinar el algoritmo de encaminamiento que mejor se adecúa a la características de la red.

2.1.1 Características generales

Las principales características de las redes malladas son las siguientes:

- La topología de la red es muy dinámica debido a que los parámetros externos que condicionan el coste de los caminos de retransmisión es muy cambiante. Si se utiliza como ejemplo de topología de una red inalámbrica la figura 2-2, se observa mejor la cantidad de factores en juego para establecer el camino de una máquina A a otra E.

‘A’ y ‘E’ se encuentran en alcance radio, pero debido a condiciones externas la tasa de datos que permite el enlace directo A-E es muy baja. Puede darse el caso que sea preferible aumentar el número de saltos entre nodos de manera que la tasa sea mayor teniendo en cuenta incluso la pérdida de rendimiento que supone retransmitir la información. El camino elegido en este ejemplo para comunicar a los dos nodos serían A-B-C-E.

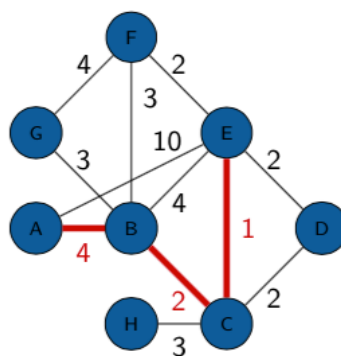


Figura 2-2 Enlaces de radio frecuencia establecidos en una red ad-hoc

La pérdida de eficiencia se debe a que todos los transceptores de radiofrecuencia trabajan en un mismo canal. En la práctica, supone una importante limitación en la capacidad total de la red. De manera teórica, esta limitación en la tasa de transferencia está asintóticamente limitada por $1/n \log n$, donde n es el número de nodos en la red [4]. Por lo tanto, si se incrementa el número de nodos en una red la capacidad decrece exponencialmente.

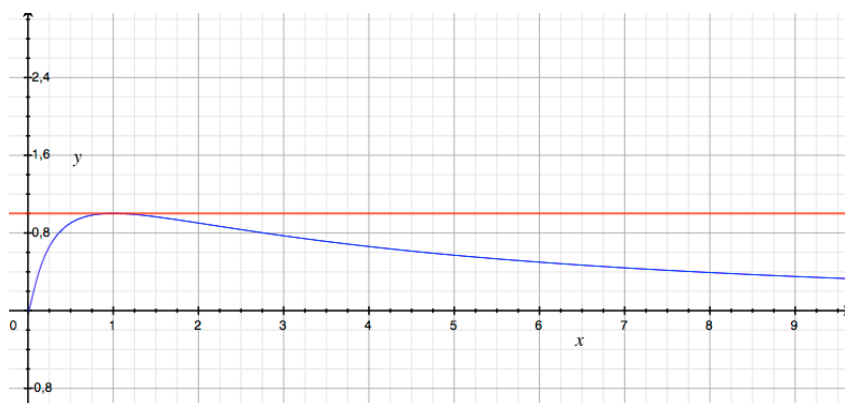


Figura 2-3 Ilustración de la disminución de la tasa de datos en función del número de nodos

- La movilidad física de los nodos es bastante superior en comparación a una red con infraestructura del tipo punto de acceso y estaciones (clientes). Este es el funcionamiento típico de las redes domésticas y que prestan servicio final de datos a sus clientes. Las MANET olvidan la existencia de la figura de un solo encaminador en la red, por lo que basta con verificar si la estación que tiene en alcance puede retransmitir los datos a la máquina correcta. De esta manera, los radios de alcance de todos los nodos se superponen, pudiéndose extender el alcance de la red automáticamente.
- Los escenarios de implantación suelen ser distintos. Mientras que una red con sus nodos fijos suele tener aplicaciones principalmente de comunicación en un entorno fijo con un despliegue planeado, las redes MANET posibilitan las comunicaciones tácticas entre nodos presentando un amplio abanico de posibilidades de implantación en entornos militares.
- Son redes de rápido despliegue, fácil mantenimiento, bajo coste, alta confiabilidad y escalabilidad. Las MANET, aparte de lo enunciado anteriormente, mejoran las capacidades de conectividad y resistencia en las comunicaciones inalámbricas. Debido a estas ventajas, las organizaciones internacionales de estandarización requieren activamente habilitar los estándares habituales para comunicaciones inalámbricas (por ejemplo, IEEE 802.11, IEEE 802.15, IEEE 802.16 y IEEE 802.20) para funcionar con un modo mallado nativo que complemente al modo infraestructura.

2.1.2 Capa física

En las redes MANET los nodos se comunican entre sí usando como medio de transmisión el espacio libre. Lo hacen a través de canales de radiofrecuencia (RF) o a través de rayos infrarrojos (IR). En la práctica, las redes basadas en rayos infrarrojos se usan muy poco y solo en aplicaciones muy concretas. Esto se debe a que los rayos infrarrojos tienen muchas desventajas respecto a las de radiofrecuencia. La principal es las altas pérdidas por propagación en el espacio libre.

Existen estándares del IEEE 802.11 que definen interfaces para los canales de RF en las bandas de 2,4 GHz y de 5 GHz. La banda de 2,4 GHz está más saturada ya que se utiliza para otro tipo de redes como Bluetooth y en dispositivos como hornos microondas y aparatos de radiocontrol. Además, en esta banda de frecuencias se permiten usos abiertos y experimentales, de manera que no hace falta tener licencias especiales para trabajar en ella, siempre que no se sobrepasen los niveles de potencia permitidos. Por lo tanto, las redes de RF que funcionan en esta banda sufren muchas más interferencias que las que funcionan en la banda de 5 GHz. Sin embargo, la ventaja que tiene la banda de 2,4 GHz respecto a la banda de 5 GHz es que las señales sufren muchas menos pérdidas de transmisión en el espacio libre.

En los canales de RF las señales se comportan de manera dispersa. Eso permite que se usen antenas omnidireccionales, las cuales son muy económicas y permiten que los dispositivos móviles se comuniquen con cualquier otro nodo que se encuentre lo suficientemente cerca en cualquier dirección. Esto es una gran ventaja pero genera otro inconveniente: dos nodos distintos pueden transmitir al mismo tiempo usando el mismo canal de RF. Por lo tanto, hace falta un protocolo MAC (*Medium Access Control*) que lo evite.

Al no poder transmitir libremente, aunque las velocidades de transmisión teóricas pueden alcanzar hasta los 54 Mbps en los estándares IEEE 802.11a y 802.11g (incluso más en los nuevos estándares IEEE 802.11), estas no se reflejan en la velocidad efectiva de transmisión vista desde las capas superiores de la red. Además, los mecanismos usados por la capa MAC para controlar el acceso a los canales de RF compartidos y maximizar su utilización, evitando colisiones, impiden que se logre una utilización del 100% de los recursos de la red. Existen posibles soluciones a este problema, pero pasan por usar antenas direccionales que no permiten que los nodos sean móviles, ya que al moverse, la antena dejaría de apuntar al siguiente nodo [5].

Como conclusión, podemos decir que el problema principal de la capa física de las redes MANET se debe al medio de transmisión utilizado. Además, las señales de RF al ser transmitidas por el espacio libre sufren atenuaciones debidas a distintos fenómenos como la absorción, la distorsión, el multitrayecto, etc. Por lo tanto, nos encontramos frente a un canal de transmisión dinámico y de carácter impredecible.

2.1.3 Capa MAC (Medium Access Control)

Existen dos familias principales de protocolos de control de acceso al medio (MAC): protocolos de acceso aleatorio y protocolos de acceso controlado. En los protocolos de acceso aleatorio los nodos compiten entre ellos para conseguir el canal de transmisión, mientras que en los de acceso controlado existe un mecanismo preestablecido para decidir cuál de los nodos puede acceder al medio en cada momento.

Debido a que las redes MANET no tienen infraestructura, utilizar protocolos de acceso al medio controlados no es una solución eficiente. Por lo tanto, las redes MANET utilizan protocolos MAC de acceso aleatorio. Concretamente, el protocolo estandarizado por el comité IEEE 802.11 es el CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) debido a su inherente flexibilidad y porque resuelve el problema de los terminales ocultos a través del sencillo mecanismo de paquetes de control RTS/CTS- DATA/ACK [6].

Para mejorar el comportamiento de CSMA/CA se incluyen varias propuestas como reducir el consumo de energía de los nodos móviles que permite que entren en un estado de bajo consumo cuando su demanda no supera unos umbrales, reducción dinámica de los radios de transmisión y diferentes esquemas de codificación y modulación de la señal [7].

2.1.4 Capa de red

El encaminamiento de la información es la función primaria de IP. En el encaminamiento IP tradicional los paquetes de datos se procesan y dirigen por encaminadores que retransmiten tráfico por rutas que se configuran con protocolos de encaminamiento. Máquinas con TCP/IP utilizan unas bases de datos (llamadas tablas IP) para conocer otras redes y máquinas IP. Cuando se envía un paquete, se consultan las tablas de encaminamiento para transmitir el paquete por el interfaz que contiene la mejor coincidencia para el destino requerido. Si ninguna opción coincide con el destino del paquete, se utiliza una ruta por defecto.

El encaminamiento tradicional mantiene la idea de que todos los equipos dentro de la misma subred siempre utilizan la misma ruta, lo cual significa que todas las máquinas de una subred están disponibles en un solo salto, típicamente a través de encaminadores o conmutadores. En redes multisalto no es el caso. En esta situación se redefine la idea de nodos disponibles mediante un solo salto. En redes MANET los nodos encaminan el tráfico retransmitiendo paquetes como si fueran encaminadores y actualizan sus tablas de encaminamiento en tiempo real

Las redes MANET son las que más se distinguen de las redes inalámbricas convencionales. A este nivel, los protocolos de encaminamiento se deben de adaptar rápidamente a los cambios de la topología de la red para poder mantener una ruta en todo momento para la comunicación de los nodos. Existe una gran variedad de protocolos para redes *ad-hoc*, se pueden clasificar en tres grupos en función del método que utilicen para determinar las rutas [8] [9]:

- Protocolos reactivos.
- Protocolos proactivos.
- Protocolos híbridos.

También existe un pequeño grupo que intenta dotar a estos protocolos de los mecanismos necesarios para proporcionar calidad de servicio (QoS) en las comunicaciones.

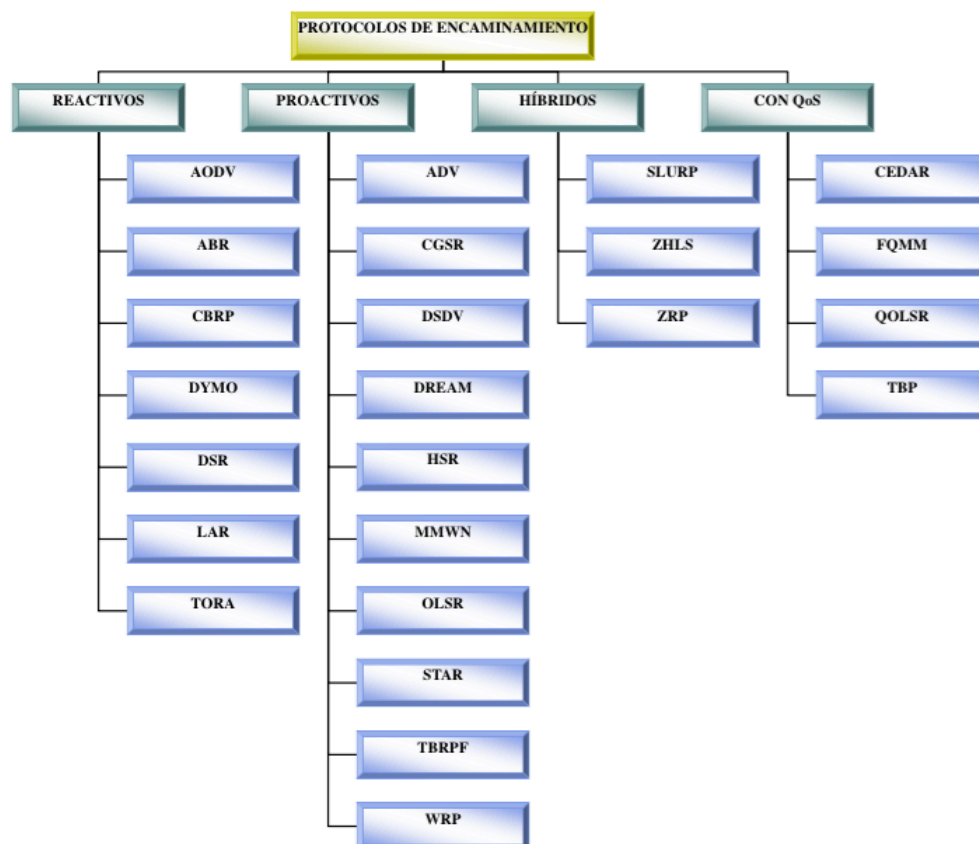


Figura 2-4 Protocolos de encaminamiento para redes Ad Hoc

2.1.4.1 Protocolos reactivos

Los protocolos de encaminamiento reactivos o bajo demanda son aquellos que solo hallan la ruta entre un nodo origen y un nodo destino bajo demanda del primero. Es decir, que solo cuando es necesario iniciar una transmisión se buscará una nueva ruta. Las ventajas de este tipo de protocolos es que no necesitan paquetes de control y señalización para mantener la topología de la red actualizada, optimizan el uso de baterías y reducen la saturación del espectro. Por el contrario, el tiempo de establecimiento de ruta es mayor porque una transmisión no comienza hasta que el mecanismo de descubrimiento de ruta concluye.

2.1.4.2 Protocolos proactivos

Los protocolos de encaminamiento proactivos intentan mantener las tablas de las rutas actualizadas constantemente. Eso significa que cada nodo debe mantener actualizada una tabla con todas las rutas hacia los otros nodos. La información que contienen las tablas debe actualizarse periódicamente y ante cualquier cambio de topología en la red. Esta actualización constante provoca que estos protocolos generen una gran cantidad de paquetes de señalización, que afectan al ancho de banda [10] y al consumo de energía, entre otras cosas. La ventaja principal que aportan es que el establecimiento de una nueva ruta precisa de un tiempo muy pequeño al tener todos los nodos las tablas de rutas actualizadas. Además, el consumo de recursos, aunque sea elevado, es bastante estable en el tiempo. El principal problema de estos protocolos ocurre con redes muy densas y nodos con movilidad alta, ya que en estos casos el consumo de recursos crece rápidamente y las tablas pueden llegar a ser demasiado grandes.

2.1.4.3 Protocolos con QoS

Este grupo de protocolos se basa en buscar rutas con los recursos suficientes para satisfacer los requerimientos de QoS establecidos. Su función no es otra que la de intentar garantizar la QoS de una comunicación dentro de una red MANET. Para ello, intentan que la comunicación extremo a extremo cumpla una serie de restricciones como el retardo, la variación del retardo, el ancho de banda mínimo necesario o una combinación de estos parámetros. Este objetivo es muy difícil de conseguir en las redes MANET debido a su naturaleza impredecible, así que es necesario encontrar un compromiso entre su modo de operación y los beneficios obtenidos. Además, no se puede garantizar que la QoS se mantenga estable, así que los protocolos deben adaptarse rápidamente en caso de que un camino se rompa o no garantice la QoS mínima.

2.1.5 Capa de transporte

La mayor dificultad encontrada en este nivel es el rendimiento de los protocolos de transporte para las MANET. Estas tienen una alta variación del RTT (*Round-Trip Time*), que depende del número de saltos en el camino. La pérdida y la colisión de paquetes, la asimetría de la red y los fallos en los enlaces contribuyen también a la degradación de la capa de transporte.

En las redes MANET se busca la máxima compatibilidad con los protocolos utilizados por Internet. Esto es porque el como objetivo final de las redes MANET es ofrecer acceso a Internet en

todo lugar y momento. Por lo tanto, las redes *ad-hoc* están basadas principalmente en la pila de protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*). Así, prácticamente todos los esfuerzos de investigación del MANET-WG (*MANET Working Group*) se dirigen al desarrollo de algoritmos de encaminamiento específicos para este tipo de redes, intentando que el resto de protocolos de la pila no se vean afectados. A pesar de ello, sí existen algunas propuestas con el fin de mejorar las prestaciones de los principales protocolos de transporte de Internet, TCP y UDP (*User Datagram Protocol*) [11] en entornos *ad-hoc*.

En [10] podemos ver una mejora de TCP para redes *ad-hoc*. Esta utiliza mecanismos de señalización implícita que permiten tener un TCP que no active, de manera equivocada, el mecanismo de control de congestión cuando se cae un camino entre el nodo fuente y el nodo destino debido a un fallo en un enlace. También existen propuestas de protocolos de transporte específicos para redes *ad-hoc*. Un ejemplo es TPA (*Transport Protocol for Ad-Hoc Networks*) [11]. El protocolo TPA incluye mecanismos que detectan cuando se pierde un enlace y se recupera la ruta [12]. Además, establece mecanismos de control de congestión distintos a los de TCP. Por otro lado, se han desarrollado otros protocolos de transporte para otras aplicaciones de tiempo real y distribución multimedia como SCTP (*Stream Control Transport Protocol*) y MRTP (*Multiflow Realtime Transport Protocol*). Estos protocolos tienen como característica principal que establecen múltiples flujos de datos entre dos nodos para una misma comunicación y funcionan junto a protocolos de encaminamiento multicamino.

2.1.6 Capa de aplicación

La aplicación más popular en ámbitos civiles es el servicio de acceso a Internet sobre todo en áreas residenciales o complejos de negocios. En general, las aplicaciones de transmisión de datos que no necesitan grandes anchos de banda ni tienen limitaciones de tiempo real funcionan bien *Best Effort* (ofrecer el mejor servicio posible a todo el mundo) [12].

2.2 Encaminamiento en MANET: OLSR (*Optimized Link State Routing Protocol*)

2.2.1 Generalidades

Desarrolladores: T. Clausen y P. Jacquet

Fecha de la primera versión: Noviembre 1998

Versión actual: RFC-3626, Octubre de 2003 [13]

OLSR es un protocolo de encaminamiento [13] para redes malladas basado en tablas proactivas de encaminamiento que utiliza un sistema de optimización llamado “retransmisión multipunto por inundación”. Este mecanismo consiste en elegir un conjunto de nodos vecinos que cubren el acceso de

nodos distantes a 2 saltos o más. T. Clausen y P. Jacquet lo desarrollaron para el proyecto *Hi-percom INRIA* en noviembre de 1998. A diferencia de otros protocolos como AODV, OLSR es un protocolo proactivo basado en la optimización del protocolo clásico *link state*.

Los protocolos proactivos tienen la ventaja de que mantienen las tablas de encaminamiento actualizadas en todo momento. Presentan la desventaja de que requieren una carga adicional en la red inalámbrica debido a la transmisión periódica de mensajes de control.

El intercambio de mensaje de control en una red mallada puede provocar congestión y suponer un grave problema en las comunicaciones. Para solucionarlo, OLSR utiliza los *Multi Point Relay* (MPR). Los MPR son nodos encargados de retransmitir paquetes *broadcast*. El número de MPR que retransmiten un paquete *broadcast* es siempre inferior al número total de nodos. Con esta técnica se aminoran considerablemente el coste de las inundaciones *broadcast*. Sin embargo, el protocolo sigue proporcionando caminos óptimos, pues dichos paquetes llegan a todos los nodos.

OLSR ha sido diseñado para redes móviles densas y extensas. Emplea técnicas multipunto de inundación para lograr un empleo óptimo de los recursos de la red inalámbrica. Cuanto más extensa es una red móvil, se obtienen mayores rendimientos en comparación al mecanismo clásico de inundación masiva de la red.

Es importante entender que OLSR no encamina tráfico, únicamente actualiza las tablas de encaminamiento. OLSR no es el único que lo hace, sino que toda la pila de protocolos de encaminamiento para MANET siguen el mismo patrón.

2.2.2 Terminología

Nodo: Un dispositivo capaz de encaminar tráfico de la manera especificada en [13].

Interfaz OLSR: Es un dispositivo de red partícipe de una red MANET OLSR.

Interfaz no OLSR: Hace referencia a cualquier dispositivo de red que no participe en las labores de encaminamiento de tráfico de la red MANET. Un nodo puede tener varios interfaces no OLSR aunque deben señalizarse convenientemente.

Nodo con un único interfaz OLSR: Es un nodo que simplemente realiza gestiones de encaminamiento de tráfico en la red MANET actuando, simplemente, como otro punto de retransmisión de la información.

Nodo con múltiples interfaces OLSR: Nodo con más de un interfaz integrado en la red MANET.

Dirección principal: Es la dirección del un nodo que utilizan los paquetes de control OLSR en el campo *originator address* de todos los mensajes emitidos por este nodo. Corresponde a la dirección de uno de los interfaces OLSR del nodo.

Nodo Vecino: Un nodo X es vecino de otro Y si el nodo Y se encuentra en alcance radio del nodo X.

Vecino a 2 saltos: Es un nodo en alcance radio de un vecino.

TTL (*Time To Live*): Es un atributo de un mensaje que le limita en el número de veces que se puede retransmitir.

Retransmisiones Multipunto (MPR): Es un nodo seleccionado por su vecino X para retransmitir todos los mensajes *broadcast* que recibe de X siempre y cuando el TTL sea mayor de una unidad.

Enlace: Hace referencia a una pareja de interfaces OLSR susceptibles a estar en alcance radio el uno del otro.

Enlace simétrico: Indica que los mensajes *HELLO* del nodo remoto han sido “oídos” por ambas partes. Hay comunicación bidireccional.

Enlace asimétrico: Indica que los mensajes *HELLO* del nodo remoto han sido “oídos”. Sin embargo, no está confirmado que este nodo haya sido capaz de recibir mensajes procedentes del nodo origen.

2.2.3 Mecanismo de inundación: MPR

Para la correcta comprensión del funcionamiento de este algoritmo, es necesario abordar el funcionamiento de uno de los pilares principales de los protocolos de encaminamiento *multicast*: los mecanismos de inundación.

El protocolo de encaminamiento OLSR está basado en un mecanismo de descubrimiento de nodos un tanto diferente a la inundación clásica. En la terminología utilizada, MPR (*Multipoint Relays*) es el sistema utilizado de forma que cada nodo selecciona un conjunto de nodos entre sus vecinos que se encuentre a un salto de distancia. La característica de estos nodos es que son capaces de llegar a todos los nodos que se encuentran a dos saltos de distancia y siendo el mínimo conjunto, es decir, evitando tener varios nodos que lleguen a los mismos vecinos innecesariamente. Estos serán los encargados de retransmitir los mensajes de control que envía el nodo en cuestión. Como se observa en la imagen 2.5, el nodo central ha seleccionado unos nodos llamados MPR, lo cual supone un aumento de la eficiencia en cuanto al mecanismo de descubrimiento de rutas, pues no todos los nodos pueden retransmitir los mensajes de control, sino solo los seleccionados como MPR.

La idea del empleo de retransmisiones multipunto (MPR) es minimizar la sobrecarga del espectro con mensajes de inundación (utilizados en algoritmos clásicos), evitando así la colisión de paquetes innecesariamente dentro del canal de radiofrecuencia utilizado.

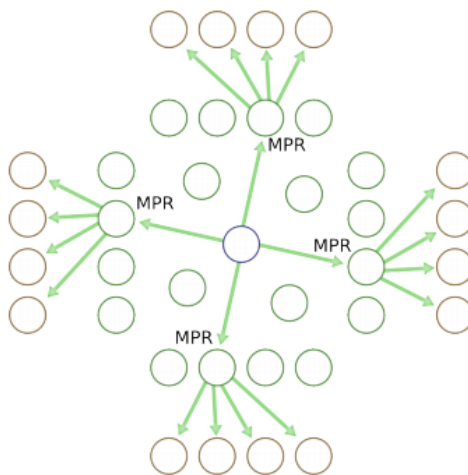


Figura 2-5 Selección de nodos MPR

2.2.4 Funcionamiento: Núcleo OLSR

La arquitectura del protocolo es modular, siendo necesario para su funcionamiento básico un “núcleo” central. De manera que funciones auxiliares que se añaden de forma posterior pueden complementarlo. Cada función auxiliar proporciona funcionalidades adicionales que pueden aplicarse según el escenario.

El propósito de la modularidad del protocolo es facilitar su comprensión y ofrecer una vía rápida de ampliación, aumentando las funciones específicas cuando estas se requieran.

El núcleo especifica el comportamiento de un nodo, equipado con un interfaz OLSR integrado en una MANET. Este incluye una especificación universal de los mensajes del protocolo OLSR y su transmisión a través de la red, así como estado del enlace, difusión de la topología y cálculo de rutas.

El núcleo se divide en las siguientes partes lógicas:

- **Formato de los paquetes y reenvío:**

Define las especificaciones del formato de los mensajes de los interfaces OLSR y optimiza los mecanismos de inundación. OLSR se comunica con un formato de paquete unificado para todos los datos relacionados con el protocolo. Estos paquetes son encapsulados dentro de datagramas UDP para su transmisión sobre la red en el puerto 698.

Cada paquete puede encapsular uno o más mensajes, teniendo un formato de cabecera común que permite a los nodos aceptar y retransmitir mensajes correctamente.

Los mensajes pueden transmitirse a toda la red, o bien a los nodos que se encuentren en alcance radio directo (un solo salto) utilizando el tipo de inundación especial tratado en la sección anterior: MPR.

Además, cualquier nodo puede examinar la cabecera del mensaje para obtener información acerca de la distancia (en términos de saltos) a la que se encuentra del originante del mensaje.

- **Estado de enlace:**

El estado del enlace se determina mediante las emisiones periódicas de mensajes “HELLO” a través de los interfaces. El objetivo es el establecimiento de un enlace entre los nodos vecinos.

- **Detección de enlaces y nodos vecinos:**

Dada una red con nodos dotados con un solo interfaz OLSR, un nodo puede deducir la disposición de los nodos vecinos únicamente con examinar el contenido de los paquetes “HELLO”.

En una red con nodos dotados de múltiples interfaces OLSR, es necesario información adicional para conocer correctamente las direcciones de los interfaces. Esta información adicional se adquiere mediante mensajes MID (*Multiple interface declaration*).

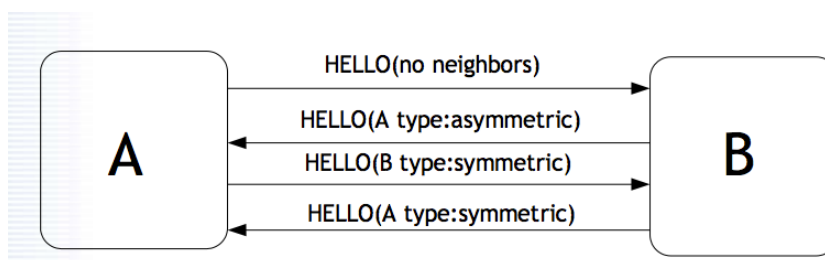


Figura 2-6 Escenario simplificado de detección de vecinos [14]

- **Selección y señalización MPR:**

El objetivo del proceso de selección MPR es el elegir un subconjunto de nodos vecinos a un solo salto de distancia. Ese subconjunto de nodos posibilita al originante del mensaje inicial conocer todos los nodos que se encuentren al menos a dos saltos de distancia. El conjunto de nodos seleccionados se calcula por cada interfaz de manera que satisfaga la condición anterior. La información necesaria para llevar a cabo este cálculo se extrae de los mensajes “HELLO”.

- **Difusión de los mensajes de control:**

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

- **Cálculo de la ruta:**

La tabla de encaminamiento para cada nodo se calcula a partir de la información extraída del estado del enlace entre cada nodo dada por el intercambio de mensajes periódico.

2.2.5 Formato de los paquetes

OLSR se comunica con un formato de paquete unificado en base a datos relacionados con el protocolo. El propósito es facilitar la extensibilidad del protocolo sin romper la compatibilidad con versiones anteriores. Esto también proporciona una manera fácil de transportar diferentes "tipos" de información en una sola transmisión. Cada paquete encapsula uno o más mensajes. Estos mensajes comparten un mismo formato de cabecera que les permite a los nodos aceptar y retransmitir correctamente mensajes de cualquier tipo.

El paquete básico de OLSR está dividido en tres partes:

- **Cabecera del paquete.**
- **Cabecera del mensaje.**
- **Datos del mensaje.**

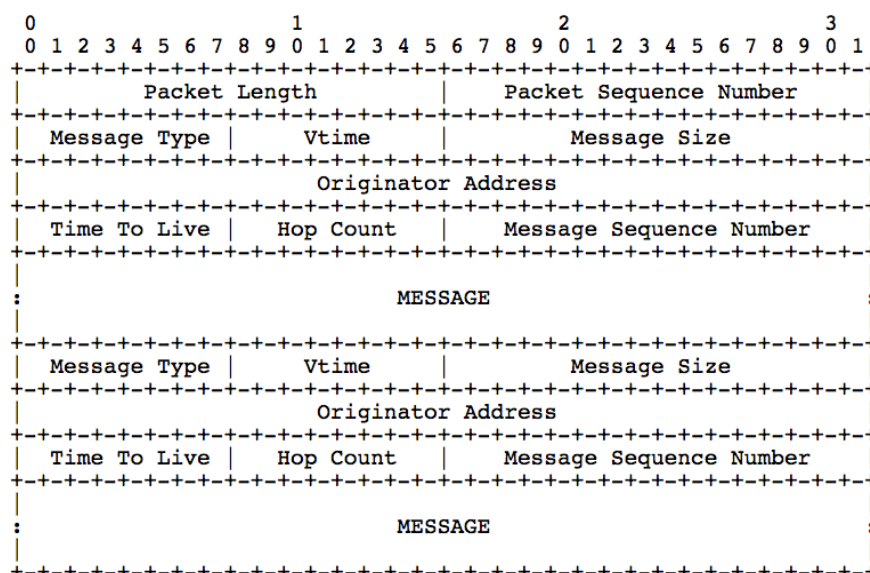


Figura 2-7 Esquema de un paquete OLSR

2.2.5.1 Cabecera del paquete

- *Packet Length*: El tamaño que tiene el paquete en *bytes*, incluyendo la cabecera.
- *Packet Sequence Number (PSN)*: Debe incrementarse en una unidad cada vez que se transmite un paquete OLSR. PSN se utiliza en OLSR con el propósito de descartar información antigua.

2.2.5.2 Cabecera del mensaje

- *Message Type*: Designador del tipo de mensaje que contiene. En OLSR existen cuatro tipos de mensajes: HELLO, TC, MID y HNA.

- *Vtime*: Indica durante cuánto tiempo después de la recepción del mensaje, la información que contiene debe ser válida.
- *Message Size*: El tamaño de la información del mensaje que viene justo después de esta cabecera.
- *Originator Address*: Es la dirección del nodo que creó el mensaje OLSR. Esta información puede ser distinta a la de la cabecera IP puesto si hay un nodo que haya hecho de intermediario desde el nodo origen hasta el destino.
- *Time To Live*: Un nodo emisor configura la validez de un mensaje en función a los saltos que vaya a dar. Es decir, *Time To Live* igual 1 equivale a un mensaje válido solo para el vecino más próximo.
- *Hop Count*: Número de saltos que ha realizado el paquete desde el nodo origen hasta el nodo que ha recibido el mensaje
- *Message Sequence Number*: Número de secuencia del mensaje. Debe ser único para cada uno de los mensajes que envíe el nodo fuente. Como el resto de número de secuencias que encontramos en los demás protocolos, se utiliza para conocer si el nodo ha recibido el mensaje y poder descartar los duplicados o anticuados.

2.2.6 Tipos de mensajes: HELLO, TC, MID

Los tipos de mensajes definidos por defecto en la funcionalidad del núcleo del protocolo son los siguientes:

2.2.6.1 Mensaje HELLO

Son los responsables del el estado del enlace, detección de nodos vecinos y señalización de las retransmisiones MPR. Este mensaje viajará dentro del apartado denominado anteriormente como MESSAGE.

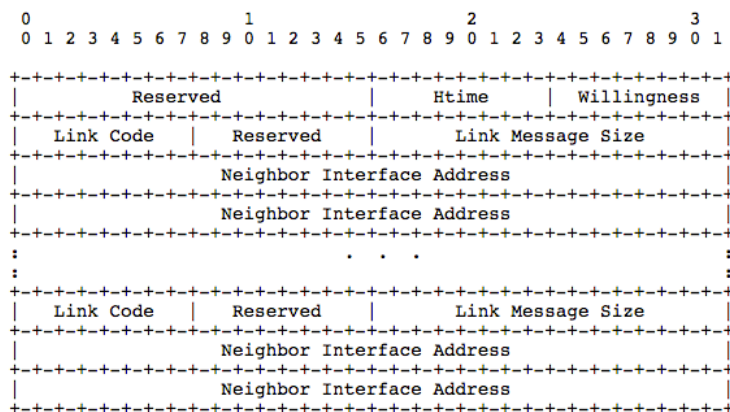


Figura 2-8 Esquema de un mensaje HELLO. [13]

No obstante un mensaje HELLO contiene otra pequeña cabecera con la siguiente información:

- *Htime*: Este campo especifica el intervalo de emisión usado para transmitir los mensajes HELLO por el nodo.
- *Willingness*: Este campo especifica la disponibilidad del nodo para llevar y retransmitir tráfico hacia otros nodos. Es útil para los nodos conocer la disposición a la hora de seleccionar sus MPR.

A la cabecera le sucede una lista de los vecinos organizados de la siguiente forma:

- *Link Code*: El tipo de conexión que mantiene actualmente con los vecinos que se especifican a continuación. Este campo realmente se divide en dos:
 1. El estado del enlace: Los valores que puede tener este campos son simétrico, asimétrico, no especificado o perdido.
 2. El tipo de vecino: Con valores muy parecidos a los anteriores, indica si los nodos son vecinos MPR y si tienen conexiones simétricas o asimétricas.
- *Link Message Size*: El tamaño de la lista de vecinos que viene posteriormente.
- *Neighbor Address*: La lista de direcciones de los vecinos que tienen el tipo de conexión determinado anteriormente. Mediante esta lista, cada nodo conoce sus vecinos al mismo tiempo que sus vecinos tienen conocimiento de todos los nodos que se encuentra a dos saltos de distancia.

Cada nodo genera dos tablas con la información obtenida de los paquetes HELLO. Una primera donde se encuentran todos sus nodos vecinos. Es decir, todos los nodos de los que recibe los paquetes HELLO. Junto a la dirección del nodo, se guarda además, el estado del enlace que mantiene con ellos. Los posibles valores que puede tomar este atributo son: MPR, bidireccional o unidireccional. El enlace se considera asimétrico cuando el nodo recibe paquetes HELLO pero no se encuentra incluido en ellos como vecino.

Con la información de la tabla anterior, más el conocimiento de los nodos que se encuentran a dos saltos y el vecino que los conecta se genera una segunda tabla. Para ello, se emplea un algoritmo de mínimos conjuntos, teniendo en cuenta la disponibilidad de los nodos, y se calcula cuáles son sus nodos MPR. Una vez realizados los cálculos, en esta segunda tabla se guardan los nodos de dos saltos y a través de qué nodo MPR se accede ellos. Por lo tanto, con los mensajes HELLO, se tiene un conocimiento completo de la red a una distancia de dos saltos. Aparte de la información de los nodos vecinos, los mensajes HELLO añaden cuáles han sido seleccionados por el nodo emisor para que sean sus MPR. Así, cuando se recibe un paquete HELLO, además de conocer la topología de la red de uno o más saltos, sabe si ha sido seleccionado por su vecino como MPR y por tanto está obligado a retransmitir los mensajes de control que reciba a partir de ese momento.

2.2.6.2 Mensajes TC (de control de la topología)

Este tipo de mensajes realizan la tarea de la difusión de la topología.

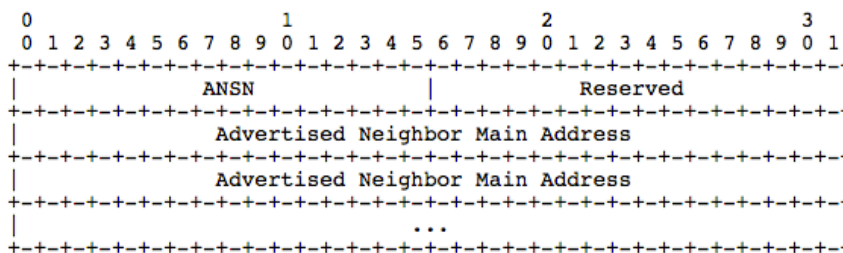


Figura 2-9 Esquema de un mensaje TC. [13]

Contiene los siguientes campos mostrados en la figura 2-9:

- *Advertised Neighbor Sequence Number (ANSN)*: Es un número de secuencia para conocer si la información transmitida es reciente o no.
- *Advertised Neighbor Main Address*: Refiere a una lista con las direcciones de los vecinos del nodo, de manera que, aparte de conocer de su presencia en las tablas de un nodo adyacente, también pueda referirse a ellos utilizando su dirección.

Un nodo envía el mensaje de la figura 2-9 utilizando el formato de paquete expuesto en el apartado 2.2.5 para declarar un conjunto de enlaces, los cuales deben incluir al menos los enlaces con todos sus nodos MPR. Merece la pena resaltar que los mensajes TC tienen el TTL máximo permitido con el fin de llegar a todos los nodos de la red. Se transmiten por *broadcast*, pero al ser un mensaje de control OLSR, solo lo reenvían los nodos MPR.

Cuando un nodo detecta la llegada de un mensaje de control OLSR, comprueba si el nodo vecino que le ha enviado el mensaje se encuentra en su lista de MPR. En caso afirmativo, vuelve a enviar el mensaje por *broadcast* de manera que todos sus enlaces MPR que no hayan recibido el mensaje vuelven a enviarlo de nuevo, extendiéndose el mensaje por la red sucesivamente.

Todos los nodos de la red envían de forma asíncrona un mensaje TC. Si cualquier nodo detecta que la red no ha sufrido ningún cambio puede omitir retransmitirlo. Con la información contenida en los mensajes TC, que al menos contienen la tabla de los MPR seleccionados por el nodo fuente, los nodos generan una tercera tabla denominada “de topología” con información concerniente a toda la red, al igual que tienen una con los vecinos (un salto de distancia) y otra con los nodos a dos saltos de distancia.

2.2.6.3 Mensajes MID

Declaran la presencia de nodos con múltiples interfaces. La correspondencia entre un interfaz OLSR y su dirección principal es trivial pues se retransmite en los mensajes vistos hasta el momento. En el caso de la existencia de nodos con múltiples interfaces es necesario la transmisión de mensajes MID que informen a la red de las direcciones de otros interfaces contenidas en el mismo nodo. En la

generación de un mensaje MID se incluye la lista direcciones pertenecientes a los interfaces asociados al interfaz principal OLSR.

2.2.6.4 Mensajes HNA

Se utilizan para declarar los interfaces no OLSR de la red. En su estructura son similares a los mensajes TC, aunque con la diferencia de que los mensajes TC pueden cancelar información previa, mientras que la información en los mensajes HNA solo se sustituye cuando expira.

2.2.7 Tratamiento de los mensajes

El procesamiento y el reenvío de los mensajes son dos acciones totalmente diferentes condicionadas por reglas distintas. El procesamiento hace referencia directamente al uso de la información contenida en los mensajes mientras que el reenvío está relacionado con la retransmisión del mismo mensaje a otro nodo de la red.

Los mensajes con cabeceras que sean “conocidas” no deben retransmitirse de manera arbitraria por el algoritmo. El reenvío (y la configuración de la cabecera correspondiente en el mensaje a retransmitir) es responsabilidad del algoritmo, especificando qué hacer con ese mensaje y si debe ser o no retransmitido. Esto permite que un tipo de mensaje previamente formateado pueda ser modificado durante el tránsito, por ejemplo, para reflejar la ruta que ha tomado ese paquete a los demás nodos.

También se contempla la derivación del mecanismo de inundación MPR si por cualquier motivo se requiere la inundación clásica para el correcto funcionamiento de la red. Es posible extender el protocolo mediante la introducción de mensajes adicionales que amplíen las posibilidades de la red definiendo un conjunto de mensajes formateados, que todas las implementaciones de OLSR deben reconocer. La única premisa necesaria es que siempre se mantenga la compatibilidad con antiguas versiones del protocolo. Otros tipos de mensajes pueden incluir otras funcionalidades como el ahorro de energía de los nodos, encaminamiento *multicast*, soporte para enlaces unidireccionales dentro de la red y configuración automática de direcciones, entre otros.

La detección de enlaces alimenta la información referente a los enlaces locales. En [13], este concepto se conoce como *Link Set*. Asimismo, tiene en cuenta las direcciones de los interfaces OLSR y la habilidad para intercambiar paquetes con ellos.

El mecanismo fundamental para la verificación de la detección de enlace, es el intercambio periódico de mensajes *HELLO*.

La base de datos de enlaces locales se rellena en base a los nodos vecinos. Por lo que *Link Sensing* se define como el proceso de difundir en la red la base de datos anteriormente enunciada.

Cada nodo debe detectar el enlace en sí mismo y su nodo vecino. Puede darse el caso de que estos enlaces sean unidireccionales debido a vicisitudes de la propagación radio por lo que, consecuentemente, todos los enlaces tienen que verificarse en ambas direcciones para ser válidos.

Para lograr la detección de enlace, cada nodo vecino tiene un estado asociado: “simétrico” o “asimétrico”. Simétrico indica que el enlace ha sido verificado bidireccionalmente. Es decir, es posible intercambiar información en ambas direcciones.

2.2.8 Justificación de la elección del protocolo

Los algoritmos que rigen las pautas de actuación de un protocolo de encaminamiento para MANET son numerosos. Para la correcta elección del protocolo es necesario tener en cuenta algunos aspectos referentes al escenario de aplicación de la red, así como los requisitos y recursos disponibles.

Aunque en el capítulo siguiente se expone en su totalidad la instalación y configuración de la red inalámbrica, objeto principal de este trabajo, se enumeran a continuación los aspectos a tener en cuenta más importantes:

- Número de nodos.
- Tiempo de establecimiento de la ruta.
- Latencia.
- Consumo eléctrico de los nodos.
- Modularidad.
- Capacidad de ampliación.

En primer lugar, el número de nodos del que está dotada la red inalámbrica no es un parámetro del cual pueda depender la elección de uno u otro. Si se atienden al estado del arte anteriormente citado, los protocolos de encaminamiento desarrollados actualmente están diseñados para un número de nodos de un orden bastante mayor que el de la red que nos ocupa.

En segundo lugar, el consumo de energía de los equipos de radiocomunicación en un barco no es significativo. La planta eléctrica de un buque está dimensionada en unos valores adecuados para proporcionar energía eléctrica del orden de Kilovatios.

Con lo anteriormente citado, la preferencia de este sistema de comunicación es la eficacia en la transmisión de datos.

OLSR es un protocolo de encaminamiento proactivo que da preferencia al establecimiento de conexiones optimizando la rapidez y eficiencia en las comunicaciones. En este sentido, la implementación del sistema de inundación MPR (definido en secciones anteriores) proporciona un medio óptimo de mantener actualizadas las tablas de encaminamiento en todo momento, minimizando el tiempo de espera necesario para establecer una conexión inicial.

Asimismo, la flexibilidad que proporciona el código libre para conseguir una buena adaptación al escenario de aplicación es un factor clave para la elección del mismo. Su arquitectura por módulos, además, permite implementar y adaptar nuevas funcionalidades a las características iniciales.

2.3 Seguridad

Un sistema seguro puede definirse [4] como el que hace la función concebida por sus diseñadores y no muestra ningún comportamiento inesperado, incluso cuando un atacante intenta hacer que el sistema realice una función no concebida para ello.

Una definición de seguridad sería incompleta sin especificar contra quién o qué se quieren proteger los sistemas. La seguridad absoluta es imposible de obtener ya que se debe implementar un balance de costes y beneficios.

Cuando se habla acerca de seguridad en las redes de comunicaciones, hay diferentes áreas de aplicación. Se pueden definir las áreas en función de su ataque o su efecto.

- **Confidencialidad:** Los datos deben solo revelarse a personal autorizado.
- **Integridad:** Los datos no puede modificarse sin detectarse.
- **Autenticación:** Se debe garantizar que el originante del mensaje es quién dice ser.
- **Control de acceso:** Únicamente las acciones previamente autorizadas pueden llevarse a cabo.
- **Disponibilidad:** Seguridad a la hora de llevar a cabo acciones permitidas.

La protección de la comunicación entre nodos implica confidencialidad (técnicas de cifrado), autenticación de los nodos participantes, así como la protección de la integridad y autenticidad de los mensajes intercambiados. La protección de la integridad no solo se refiere a la integridad de un simple mensaje, sino a la coherencia en la entrega de ellos. Tan importante es la información de un solo mensaje como que sucesivos mensajes lleguen al destinatario en el orden en el que han sido generados.

Aunque una red inalámbrica es más versátil que una cableada, esta es muchísimo más vulnerable a ataques. En un red cableada, un intruso debe tener acceso a una máquina que sea componente de la red o bien, físicamente tener acceso al medio conductor por el que viaja la información. Una red inalámbrica es, teóricamente, mucho más fácil de penetrar puesto que cualquier usuario malicioso que esté en alcance radio puede monitorizar el tráfico que fluye a través del medio. A día de hoy, con el desarrollo de antenas de alta ganancia, el rango de acción de un usuario malicioso que esté dispuesto a monitorizar tráfico es extremadamente grande, por lo que la seguridad es un problema que nunca está totalmente resuelto.

Las comunicaciones se protegen en diferentes capas (capa física, capa de enlace, capa de red, capa de transporte y capa de aplicación). En los sistemas inalámbricos es de vital importancia la seguridad en la capa física ya que el medio utilizado para transmitir los datos es común a más usuarios. Estos usan diferente esquemas de encapsulación de los datos, diferentes métodos de autenticación y diferentes algoritmos de cifrado.

Tan importante es la técnica de cifrado utilizada como el sistema de difusión de claves. Es por ello que las redes inalámbricas de área local basadas en IEEE 802.11i [15] (*Wi-Fi Protected Acces: WPA, WPA2*) soportan, principalmente, dos formas de compartir claves. El primer modo y más extendido en entornos domésticos hace referencia a la utilización de una clave previamente distribuida a todos los usuarios(PSK, *PreShared Key*). El segundo modo se basa en la utilización de un servidor de autenticación, que se encarga de la distribución de claves previa comprobación de la identidad del usuario y se enfoca a entornos con mayor números de usuarios.

Puede inducir a error pensar que introduciendo seguridad en la capa física, las capas superiores están blindadas en cuanto a un ataque se refiere. Esto no es así en redes de infraestructura y tampoco en redes *ad-hoc*. El caso es crítico en el caso de todos los mensajes de señalización encargados de difundir la topología de la red. Un usuario mal intencionado podría identificar los paquetes cifrados pertenecientes a la señalización, pues estos, normalmente son periódicos y tienen un tamaño de paquete definido. Si este usuario volviese a inyectar esos paquetes en otro momento, o realizara peticiones masivas de envío de esos paquetes podría verse comprometida la integridad de la red.

Numerosos problemas surgen a la hora de hacer totalmente seguras la redes malladas basadas en enlaces *ad-hoc*. El multisalto es indispensable para que las redes malladas extiendan la cobertura de las actuales redes inalámbricas y que puedan proporcionar comunicación fuera del alcance radio de dos nodos consecutivos. Sin embargo, también retrasa la detección y el tratamiento de los ataques. Si se analizan las características y comparándolas con otras tecnologías en materia de redes de dispositivos, las dificultades se deben a las comunicaciones sin cables basadas en numerosos enlaces entre los nodos en alcance y a la constante transmisión de mensajes que contienen atributos como el estado de enlace entre nodos vecinos y la topología existente en cada momento, entre otros.

2.3.1 Escenario

Las medidas de seguridad apropiadas dependen en gran medida del escenario en el cual la red inalámbrica se use. El análisis de los problemas, posibles amenazas y el desarrollo de una arquitectura de seguridad es solo posible acotando el dominio de funcionamiento de la red. Se pueden considerar numerosos ámbitos de aplicación: un entorno militar donde los flujos de tráfico son confidenciales, una red mallada personal donde todos los nodos pertenecen al mismo control administrativo o una red mallada donde los nodos son siempre los mismos y se conocen entre sí.

Es necesario definir el rol que cada nodo de la red desempeña. Se puede distinguir los siguientes:

- **Nodo mallado:** Normalmente dotado de dos interfaces de red. Uno de cable y otro inalámbrico, siendo este último el encargado de realizar las tareas de encaminamiento del tráfico propios de una red mallada.
- **Nodo mallado de usuario:** Terminal de usuario configurado correctamente para actuar como otro nodo más de la red mallada. No hay otras máquinas detrás de este nodo.
- **Nodo final de usuario:** Terminal configurado para funcionar en modo infraestructura. La topología de la red mallada le es irrelevante.

Asimismo se pueden diferenciar dos tipos de escenarios fundamentales en los que se deberá tener presente los requisitos de seguridad necesarios para cada uno:

- **Dominio Administrativo Único:**

Desde la perspectiva de la seguridad, es el caso más simple de una red mallada inalámbrica, donde todos los nodos pertenecen al mismo dominio. El objetivo de la seguridad se resume en “mantener los intrusos fuera”. Esto requiere credenciales criptográficas que permitan a los nodos mallados autenticarse con los otros nodos que pertenecen a su mismo dominio, siendo el caso más simple la utilización de una clave precompartida (como en una red doméstica inalámbrica). Para una

configuración de un conjunto de nodos mayor en número, un sistema más viable es la configuración de un sistema de certificados criptográficos que validen los nodos adyacentes.

- **Extensión de una red basada en infraestructura:**

Una red mallada puede configurarse como una extensión de una red de infraestructura, cableada o no. Los nodos se operan como si de un dominio único se tratara (caso anterior). Es decir, los nodos finales utilizan la infraestructura mallada únicamente como pasarela de acceso a una puerta de enlace que proporciona servicios como el acceso a Internet. En este caso, la seguridad tiene dos vertientes de aplicación: la primera es hacer segura la red mallada frente a intrusos y el segundo es la seguridad propia que cada terminal tiene con respecto a los otros nodos de la red mallada cuando se establecen flujos de datos con la red de infraestructura.

En función de las relaciones de confianzas establecidas entre los nodos de la red mallada, el tráfico de usuario puede protegerse salto a salto dentro de la red mallada o bien establecerse un túnel cifrado de datos hacia la puerta de enlace localizada en la red de infraestructura.

2.3.2 Ataques potenciales

Hay dos fuentes de amenaza en las redes malladas. El primero, son los atacantes externos que pueden perturbar o inyectar información errónea. El segundo, hacer frente a ataques de nodos internos pues no son tan fáciles de prevenir como los externos.

Se puede distinguir ataques pasivos y activos. Los pasivos pretenden el robo de información escuchando lo que se trasmite por el medio inalámbrico. Los activos pretenden la transmisión de paquetes falsos que engañen a los demás nodos, haciéndose pasar por otro nodo más de la red.

Los ataques no solo pueden tener como objetivo la capa de enlace del sistema, sino que también pueden abarcar otras capas de la red. En la capa física, un posible atacante puede perturbar las transmisiones o destruir el *hardware* de un nodo específico. En la capa MAC (capa de acceso al medio), un atacante puede enviar paquetes masivos de control, interrumpiendo las comunicaciones. A continuación se resumen distintos tipos de ataques que han demostrado tener cierta efectividad en redes basadas en enlaces *ad-hoc*:

- **Suplantación de la identidad:** Es un ataque en el que un adversario intenta suplantar la identidad de un nodo legítimo de la red. Si este atacante tiene éxito en el ataque, recibe los mensajes que el nodo suplantado debería recibir.
- **Nodo sumidero:** Un nodo malicioso “convence” a sus vecinos de que es el siguiente salto lógico por el que debe ir la información.
- **Nodo egoísta:** Un nodo obtiene más recursos de red de los que le corresponden al no cumplir con los protocolos de la red o mediante la manipulación de su interfaz inalámbrica.

- **Denegación de servicio e inundación:** Los ataques de denegación de servicio usan la inundación para llevar a los nodos a un estado de sobrecarga. Los ataques más avanzados de denegación de servicio están basados en la manipulación inteligente de los mensajes.

2.3.3 Seguridad en MANET: mecanismos básicos

En general, para conseguir seguridad en los mecanismos de encaminamiento de tráfico es necesario preocuparse de aspectos de la seguridad como la integridad o la disponibilidad del servicio. Por lo tanto, hay que considerar cómo un nodo debe generar y verificar una firma digital que establezca confianza entre los mensajes de control intercambiados entre los nodos. En este aspecto, la criptografía se podría dejar a un lado ya que requiere más carga de computación en los nodos y la confidencialidad en los mensajes de control intercambiados no es necesaria. Esto no es así siempre, puesto que en escenarios militares la información referente al encaminamiento son también parámetros tácticos de suma relevancia para el enemigo.

En redes MANET se tienen en cuenta varias cuestiones. Algunas, son problemas que especialmente afectan a la redes inalámbricas mientras que otros son aplicables también a las redes cableadas.

OLSR es un protocolo de encaminamiento proactivo que periódicamente difunde información acerca de la topología de la red. Si la red MANET no estuviese desprotegida totalmente, la topología se revelaría a cualquier usuario que escuche los mensajes de control. En situaciones donde la topología de la red sea confidencial se debe utilizar técnicas como el intercambio de mensajes de control de tráfico cifrados para evitar que nodos no autorizados lean estos mensajes.

En las redes MANET basadas en OLSR, cada nodo inyecta a la red información topológica mediante la transmisión de mensajes HELLO y, en el caso de algunos nodos, mensajes TC. Si por cualquier razón, un nodo inyecta de manera malintencionada tráfico de control erróneo, la integridad de la red se vería comprometida. A continuación, se exponen ejemplos de situaciones que pueden ocurrir debido a la falta de integridad:

1. Un nodo genera mensajes TC anunciando enlaces a nodos que no son vecinos.
2. Un nodo genera mensajes TC pretendiendo ser otro nodo.
3. Un nodo genera mensajes HELLO anunciando nodos que no son vecinos.
4. Un nodo genera mensajes HELLO pretendiendo ser otro todo.
5. Un nodo reenvía mensajes que han sido alterados previamente.
6. Un nodo se niega a reenviar los mensajes de control de OLSR.
7. Un nodo reenvía una topología antigua de otro nodo.

Una contramedida utilizada en las situaciones 2, 4 y 5 es la autenticación por parte del nodo originante de los mensajes de control. Para los casos 1 y 3 se deber autenticar los enlaces individuales anunciados en los mensajes de control. Sin embargo, para prevenir que los nodos repitan información antigua, es necesario un atributo temporal que permita identificar los paquetes anticuados.

La solución final más factible es finalizar todos los paquetes OLSR con un mensaje firmado. El contenido del mensaje se puede observar en la figura 2-9.

MAE [17] podría aplicarse a OLSR de manera que todos los mecanismos disponibles en OLSR pudieran incluirse de manera segura.

El módulo de seguridad disponible en OLSR actúa de la siguiente manera:

- Protección de los paquetes: A nivel de cada paquete de información, se comprueba salto a salto la todo el paquete. La firma anexa al paquete la calcula el nodo originante y la verificada el siguiente nodo que recibe la información. Para el cálculo de esta firma se tienen en cuenta atributos como *TTL* o *Hop Count*, que se añade al paquete de control. El algoritmo utilizado para generar la clave es SHA-1, partiendo de una clave precompartida previamente difundida a todos los integrantes de la red.
- Protección de los mensajes: En este nivel se utilizan claves simétricas y asimétricas [20] de la siguiente manera: los nodos autentican los mensajes con una clave pública, llevando a cabo una reautenticación cuando su topología cambia. Durante la autenticación, los nodos comparten dos claves simétricas. Una llamada *circle key*, utilizada solo entre nodos vecinos, y otra llamada *adhoc key*, utilizada en la totalidad de la red. Los nodos renuevan periódicamente ambas claves y se distribuye una nueva clave después de cifrarse con la antigua. Por este motivo, la nueva *adhoc key* se incluye en los mensajes TC.

3 DESPLIEGUE DE UNA RED MANET

3.1 Generalidades

Las lanchas de instrucción son uno de los principales medios de adiestramiento que la Escuela Naval Militar (ENM) pone a disposición de los alumnos para complementar su formación. La ENM dispone actualmente de cuatro lanchas monocasco de fibra de vidrio, fabricadas por la empresa nacional RODMAN, que son la plataforma sobre la que se instalan los equipos radio de la MANET.

Sus principales características, son las siguientes:

Eslora total.	20,50 m
Eslora del casco	20,00 m
Manga del casco	4,90 m.
Puntal	2,56 m.
Calado aproximado en rosca	0,90 m.
Capacidad de combustible	5000 l
Capacidad de agua	500 l
Potencia máxima en servicio de prácticos	2 x 715 CV
Propulsión	Eje/Hélices
Velocidad máxima 23 nudos.	23 kt
Velocidad de crucero 15 nudos.	15 kt
Desplazamiento en rosca	29,5 ton
Tripulación prevista	16 pax

Tabla 3-1 Características generales L.I

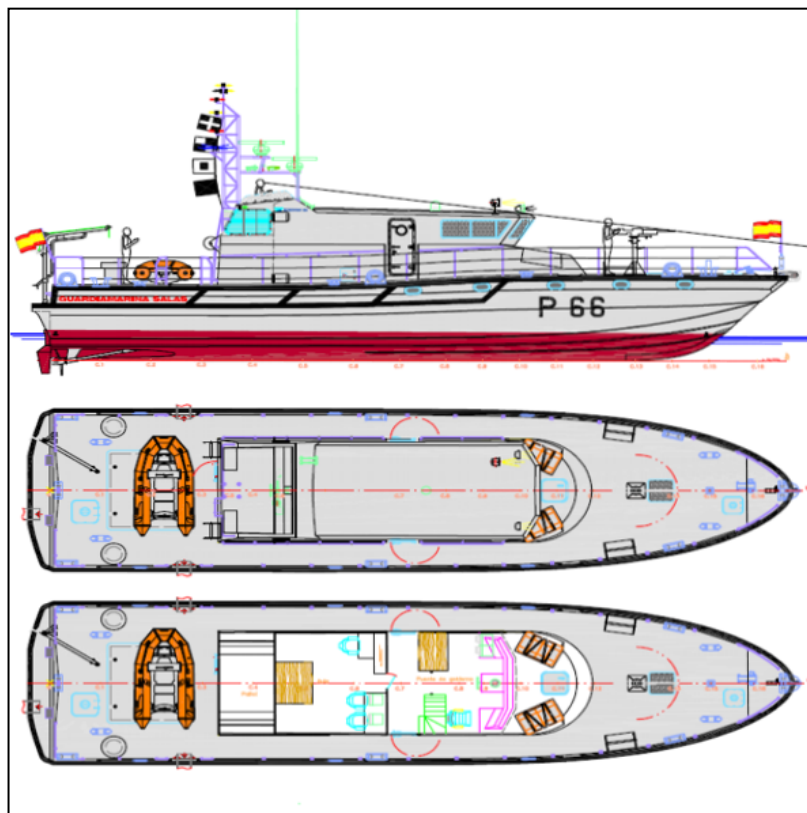


Figura 3-1 Alzado y planta de las lanchas de instrucción

Estas embarcaciones están dotadas de equipos de comunicaciones que satisfacen las necesidades básicas en cuanto a las comunicaciones por fonía analógicas. En su mayor parte, estos equipos están ubicados dentro de las bandas de VHF (bandas de uso civil y militar) y UHF (banda militar), aprovechando este último el amplio espectro disponible para aplicaciones militares de radiofrecuencia. Sobre la banda de UHF, tiene lugar la mayor parte de las comunicaciones tácticas a bordo de las lanchas de instrucción. Hasta ahora, toda la información táctica se transmite mediante voz utilizando procedimientos reglamentados en manuales de ámbito militar. No existe ningún equipo que permita intercambiar datos tácticos utilizando esquemas de modulación digital.

La mayoría de buques de la Armada disponen de equipos de transmisión de datos de radiodifusión HF, enlaces tácticos LOS (*Line of Sight*) y NLOS (*Non Line of Sight*) y enlace satélite con soporte del protocolo TCP/IP, ventajoso dada su facilidad de interacción con otras máquinas.

Dado el propósito docente de estas embarcaciones y su limitada capacidad de almacenamiento de víveres y de combustible, el tiempo de permanencia en la mar la distancia a costa están limitados. Es por ello que adaptar un sistema de comunicación satélite como en los buques de la Armada resulta poco provechoso para la aplicación requerida y económicamente inviable.

En ese sentido, un enlace LOS mediante microondas de arquitectura punto-multipunto, que utilice estándares extendidos, es una solución adecuada para el propósito requerido. Un enlace de datos inalámbrico basado en el estándar 802.11 que permita la comunicación directa (un solo salto) hasta los límites de la ría de Pontevedra aportaría infinidad de aplicaciones posibles en el ámbito docente.

Además, explicado el concepto de red MANET, se deduce rápidamente que ese alcance puede escalarse siempre y cuando la disposición espacial de los nodos sea la debida.

3.2 Equipos y material

En esta sección, se presenta el material disponible para el despliegue de la red MANET. Consta de un segmento embarcado y otro terrestre que sirve de puerta de enlace a Internet.

3.2.1 Segmento embarcado

ANTENA OMNIDIRECCIONAL AOA-2415 15dBi

Es una antena omnidireccional de exteriores fabricada por *Alfa Networks* con un revestimiento de fibra de vidrio y una base de aluminio que permite el anclaje a cualquier tubo cilíndrico de no más de 10 cm de diámetro. La frecuencia de funcionamiento dada por el fabricante es de 2,4 GHz a 2,5 GHz, ofreciendo una relación de onda estacionaria máxima de 1,3. La elevada longitud del monopolo vertical en relación a la longitud de onda con la que trabaja provoca como parámetro a resaltar, un haz de radiación vertical muy estrecho. Este último parámetro es el principal motivante para la elección de esta antena en concreto ya que al tratarse de una antena cuyo patrón de radiación en el plano horizontal es de 360°. Si se requiere una antena de alta ganancia hay que sacrificar irremediabilmente la apertura del lóbulo de radiación en el plano vertical.

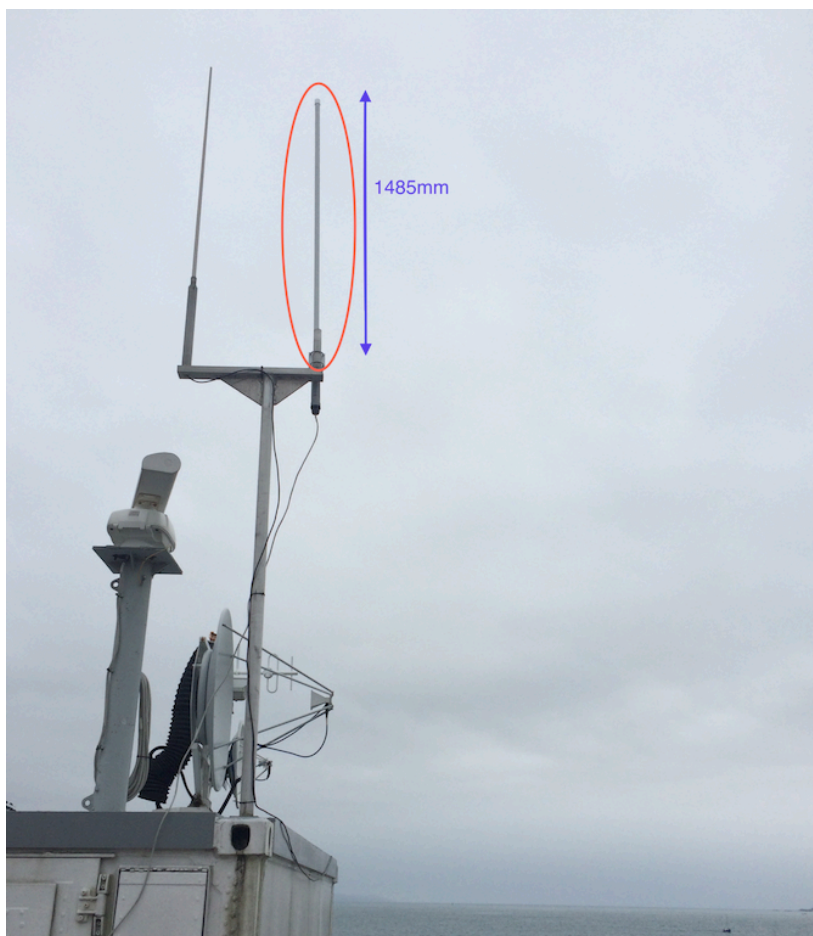


Figura 3-1 Antena omnidireccional AOA-2415

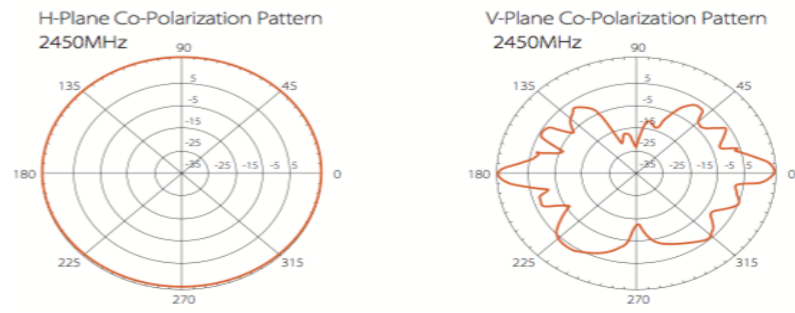


Figura 3-2 Diagrama de radiación de la antena

En la figura 3-1 se observa la antena instalada provisionalmente con una visión casi total de la ría de Pontevedra. El conector disponible en la parte inferior es un tipo N macho, ampliamente utilizado para suministrar alimentación de baja potencia. Asimismo, la impedancia de trabajo de la antena es 50 ohmios, que coincide con la impedancia del transmisor y evita utilizar dispositivos adaptadores de impedancia que supongan pérdidas.

El patrón de radiación es una de las variables que más se tuvo en cuenta a la hora de valorar qué antena elegir para los enlaces inalámbricos entre las lanchas. La estrechez de su lóbulo principal de radiación vertical, de nueve grados, la convierte en una solución viable de cara a equipar los buques con antenas punto-multipunto. Una antena omnidireccional es la solución más económica para el propósito requerido, de tal manera que también se evaluaron otras alternativas como un array de antenas sectoriales. Esta alternativa supondría la utilización de algoritmos de gestión de la transmisión, esquemas de multiplexado espaciales que eviten la producción de ruido en la antena vecina que estaría cubriendo el sector adyacente, así como un encarecimiento sustancial en el presupuesto de adquisición de equipos.

BULLET M2 TITANIUM

Procesador	Atheros MIPS 24KC, 400MHz
Memoria	32MB SDRAM, 8MB Flash
Interfaces de red	1 X 10/100 BASE-TX (Cat. 5, RJ-45)
Conector RF	Hembra tipo-N integrado
Tamaño	15.2 x 3.7 x 3.1 cm (Long x anchura x diámetro)
Peso	0.18kg
Alimentación	PoE; >24V
Interfaz de red	1 x10/100 BASE-TX (CAT5, RJ-45)
Humedad de operación	5% a 95%
Potencia de salida	27dBm

Tabla 3-2 Especificaciones técnicas Bullet M2

Es un transmisor de radiofrecuencia para exteriores situado en la banda ISM de 2,4 GHz. Está fabricado por *Ubiquiti Networks* y dotado con un conector N, igual que el de la antena. Este concepto se denomina *Zero Variable Deployment*, que hace referencia a la ventaja que ofrece despreocuparse de cables coaxiales. En este tipo de transmisores radio, los cables coaxiales desaparecen. El transmisor va directamente conectado al conector N de la antena. Esta característica es fundamental para el éxito del despliegue de la red, pues permite eliminar pérdidas adicionales que se producirían con el empleo de cables coaxiales y conectores de adaptación.

Dispone de un interfaz de red *ethernet* que, aparte de extender la red inalámbrica a cualquier otra máquina, también es el medio de alimentación del transmisor mediante PoE (*Power over Ethernet*). Esto representa una amplia ventaja en la instalación de cada uno de los transmisores de manera que solo es necesario un cable CAT5 para extender la red MANET y para alimentar el hardware. Tal y como se observa en la figura 3-3, la antena está enroscada mediante conectores N al transmisor inalámbrico y este a su vez se alimenta con un cable CAT5.

El transmisor en su totalidad está homologado para el funcionamiento en exteriores, siendo la cavidad inferior la mostrada en la figura 3-4. Esta se utiliza para conectar el cable de alimentación y está protegida por un conjunto de dobles juntas de goma y abrazadera sobre el aislante del cable para que el conjunto quede estanco.



Figura 3-3 Bullet M2



Figura 3-4 Sellamiento del cable CAT5

En la tabla 3-2, se observan las principales características del transmisor. Una de las características importantes a destacar es el procesador. La arquitectura MIPS del procesador junto con la memoria RAM de 32 Mb y sus 8 Mb de memoria flash lo convierten en un sistema embebido capaz de ejecutar sistemas operativos basados en Linux. Esto lo hace un sistema autónomo y tremendamente versátil que no necesita ninguna otra máquina de apoyo. Asimismo, todos los transmisores están equipados con un inyector PoE original que proporciona la tensión necesaria al cable CAT5.

El sistema de transmisión junto con la antena omnidireccional de 15 dBi conforman los nodos a bordo de las lanchas de instrucción.

3.2.2 Segmento terrestre

El segmento terrestre es el nodo de unión de los buques en la mar, con la red de infraestructura en tierra. Teniendo en cuenta la posición geográfica de la ENM respecto a la ría de Pontevedra y su topografía, el tipo de antena decidida para dar cobertura es de tipo sectorial. A continuación se exponen sus principales características y los motivos para su elección.

NANOStationM2

Es un sistema embebido, que sigue el mismo concepto que su homologo Bullet M2 tratado anteriormente. La principal diferencia radica en la incorporación de una antena sectorial en el sistema. Su alta integración de componentes lo hace un equipo extremadamente versátil para instalar en un punto geográfico en el que solamente se requiere una toma de alimentación a la red eléctrica.

En las figuras 3-5 y 3-6 se puede observar respectivamente el aspecto exterior del equipo así como el diagrama de radiación de la antena.



Figura 3-5 NanoStation M2

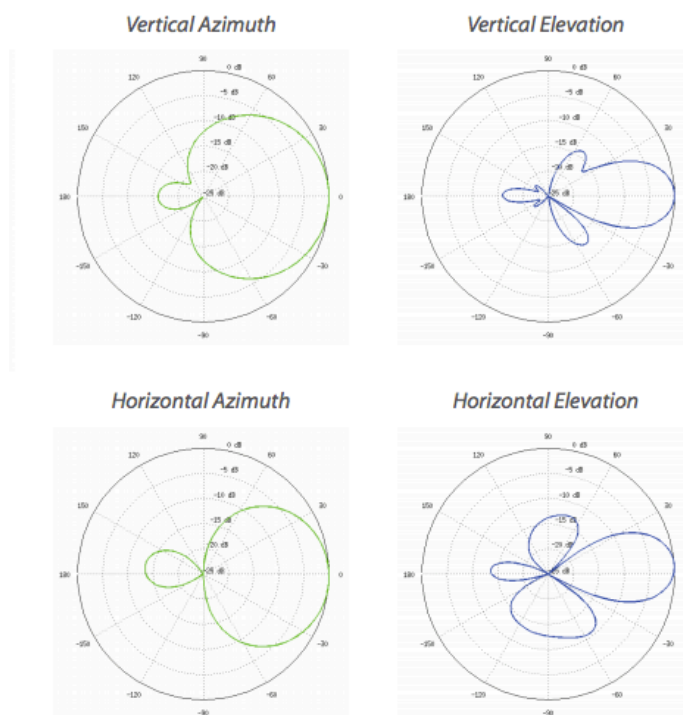


Figura 3-6 Diagrama de radiación de NanoStation M

Procesador	Atheros MIPS 24KC, 400MHz
Memoria	32MB SDRAM, 8MB Flash
Interfaces de red	2 X 10/100 BASE-TX (CAT5, RJ-45) Ethernet
Conector RF	Hembra tipo-N integrado
Tamaño	294 x 31 x 80 mm (Long x anchura x Prof.)
Peso	0.4kg
Alimentación	PoE; >24V. 0.5A
Polarización	Dual Lineal
Temperatura de operación	-40C° a 80C°
Humedad de operación	5% a 95%
Impactos y vibración	ETSI300-019-1.4
Consumo máximo	8 W
Ganancia antena	11 dBi
Potencia de salida	28 dBm

Tabla 3-3 Especificaciones NanoStation M2

3.3 Configuración y *software*

Una vez presentados los equipos de los que se dispone para el despliegue de la red se procede a exponer la configuración de los nodos y el proceso seguido para lograr su funcionamiento.

Son cuatro los nodos a configurar en lo que concierne el segmento embarcado. Para la mejor comprensión de la configuración de cada uno de los nodos se diferencian dos tipos de configuraciones. Una general, común y necesaria a todos los nodos para funcionar, y otra particular. La configuración particular trata aspectos relacionados con el rol que cada nodo desempeña dentro de la red MANET, así como valores identificativos de cada nodo en la red. A lo largo de este capítulo, se resaltan en **amarillo** los valores pertenecientes a la configuración particular.

La configuración particular engloba todo lo referente a los parámetros identificativos de cada nodo en la red MANET. En este sentido, se establecen diferencias entre los nodos embarcados y el nodo en tierra. Dentro de los nodos en tierra, pueden existir también diferencias. Puede darse de la existencia de dos nodos en tierra en el caso de que la mejor situación geográfica para el nodo dedicado a servir cobertura a las embarcaciones no disponga de conexión a Internet. En este caso, se instalaría otro nodo NanoStation M2, integrado también en la red MANET en alcance radio con el nodo con mejor situación geográfica para retransmitir la señal a los nodos embarcados.

Como punto de partida común a todos los nodos presentados, ya sean del segmento terrestre o embarcado, todos traen instalado de fábrica el sistema operativo característico del fabricante llamado “AirOs”. Este sistema operativo se caracteriza por una gran facilidad de manejo para el usuario con bajos conocimientos de redes inalámbricas. Ofrece un interfaz gráfico que de forma nativa permite realizar enlaces punto-punto y punto-multipunto en distintos modos. Entre todos los modos disponibles en el sistema operativo de fábrica destaca WDS (*Wireless Distribution System*). Este modo es el más parecido a lo que podría ser una red mallada, pues los nodos actúan como repetidores de forma nativa. El problema radica en que WDS está ideado para entornos estáticos de manera que el encaminamiento no sufra cambios debidos al movimiento de los nodos.

La realidad es que para la configuración de los transmisores como nodos de una red MANET es necesario prescindir del sistema operativo instalado de fábrica. Este es el primer paso a llevar a cabo en la configuración general.

El sistema operativo elegido para la realización es OpenWrt en su versión 12.09, denominado *Barrier Breaker*. Es un sistema operativo especialmente utilizado en dispositivos embebidos que van a realizar gestiones de encaminamiento de tráfico. OpenWrt se configura mediante un interfaz de línea de comandos o mediante un interfaz *web* conocido como “LuCI”. El principal motivo de elección de este sistema operativo es su excepcional versatilidad y capacidad de ampliación debido a su amplio soporte técnico disponible en línea, así como la disponibilidad de mas de 3500 paquetes de *software* que le añaden la posibilidad de realizar otras tareas aparte de la principal de encaminar el tráfico en los modos contemplados en el estándar IEEE802.11. OpenWrt usa licencia de *software* libre, una gran ventaja para adaptar sus funcionalidades al escenario de implantación de la red.

El ordenador utilizado para la configuración de los nodos utiliza el sistema operativo MAC OS X en su versión 10.10.1. Para muchos pasos de configuración se utiliza el terminal de este sistema operativo.

Durante la configuración general de los nodos se han seguido los siguientes pasos:

1. Para dar formato a la partición en la cual previamente viene instalado de fábrica el sistema operativo (SO) AirOS es necesario disponer de la correcta versión compilada de OpenWrt [21]. Para ello, en la página *web* oficial se puede encontrar una tabla de *hardware* compatible. Esta es una guía que permite encontrar la versión de SO adecuada para la arquitectura de procesador del transmisor.
2. A continuación se procede a la instalación del *software*. Para ello se puede utilizar el interfaz gráfico de AirOS o bien mediante TFTP. De manera nativa todos los sistemas de Ubiquiti disponen de este protocolo de transmisión de archivos.

A continuación se relatan los comandos utilizados en la terminal de la computadora utilizada para la configuración general de los nodos.

De fábrica, los nodos vienen configurados con la IP 192.168.1.20/24. Para establecer comunicación con el nodo se debe configurar el interfaz de red del ordenador. Inicialmente, el interfaz que se utilizara para comunicar con los nodos es el *ethernet* puesto que, para las labores de instalación del SO, el interfaz cableado es el único con soporte para TFTP.

```
ifconfig eth0 inet 192.168.1.100 netmask 255.255.255.0
```

Posteriormente se procede a enviar el archivo que contiene el sistema operativo:

```
tftp 192.168.1.20
tftp> bin
tftp> put openwrt-atheros-ubnt5-squashfs.bin flash_update
Sent 1965199 bytes in 28.8 seconds
tftp> quit
```

Una vez transmitido el archivo mediante TFTP, el sistema se reinicia. Cuando vuelva a estar activo, se puede acceder a él con la IP 192.168.1.1/24. No es necesario configurar manualmente el interfaz de red del ordenador pues por defecto DHCP está activado y automáticamente el interfaz *eth0* adquiere como puerta de enlace el interfaz *ethernet* del nodo.

3. Una vez instalado OpenWrt, se procede a la instalación de los paquetes necesarios al protocolo de encaminamiento utilizado. Para ello, se recurre a la pagina oficial de OLSR [22]. En ella se puede encontrar las ultimas revisiones del *software*, así como diversos manuales que recomiendan unos valores estándar de funcionamiento para el protocolo de encaminamiento.

De nuevo, la fuente de referencia a la hora de la implementación del protocolo sobre el *software* en OpenWrt es [21]. A continuación, en la tabla 3-1 se indican los distintos módulos que hay que instalar para el funcionamiento del protocolo sobre OpenWrt.

Para la instalación de los módulos en el software de los nodos se procede a establecer conexión con el nodo mediante el protocolo SSH:

```
MacBook-Pro:~ ManuelMarin$ ssh root@192.168.1.1
The authenticity of host '10.0.30.10 (10.0.30.10)' can't be established.
RSA key fingerprint is 67:03:80:c9:2a:53:17:78:f5:5f:68:b3:9c:de:2a:5d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.30.10' (RSA) to the list of known hosts.
root@192.168.1.1's password:
BusyBox v1.19.4 (2013-03-14 11:28:31 UTC) built-in shell (ash)

_____
|   |.-----|.-----|.-----| | | |.----.| | _
| - || _ | -_| || | | || _|| _
|_____| || _|_____|_____|_____|_____|_____|
      |__| W I R E L E S S   F R E E D O M

-----

ATTITUDE ADJUSTMENT (12.09, r36088)

-----

root@LANCHA-3:~#
```

Se procede a instalar los paquetes de la tabla 3-1 mediante el gestor `opkg` utilizando el comando “`install`”:

```
root@LANCHA-3:~# opkg install luci-ssl pciutils luci-app-olsr
luci-app-olsr-services luci-app-olsr-viz olsrd olsrd-mod-arprefresh olsrd-mod-bmf
olsrd-mod-dot-draw olsrd-mod-dyn-gw olsrd-mod-dyn-gw-plain olsrd-mod-httpinfo
olsrd-mod-mdns olsrd-mod-nameservice olsrd-mod-p2pd olsrd-mod-pgraph luci-lib-json olsrd-mod-
jsoninfo wpad
```

Los paquetes “`luci-ssl luci-app-olsr luci-app-olsr-services luci-app-olsr-viz`” hacen referencia a la instalación de el interfaz gráfico necesario para poder gestionar el protocolo de encaminamiento

mediante LuCI. El paquete “wpad” es una extensión de funcionalidades para los sistemas de seguridad y cifrado en la capa de enlace, mientras “nano” y “pciutils” son dos paquetes destinados a facilitar la configuración.



Figura 3-7 Captura de pantalla del interfaz gráfico en la pestaña OLSR

En la figura 3-7 se muestra el interfaz gráfico basado en *web* de OpenWrt. La captura de pantalla se corresponde con la pestaña de información general del protocolo de encaminamiento. Disponer de un interfaz gráfico *web* que muestre el estado en tiempo real de las tablas de encaminamiento facilita la gestión y supervisión del protocolo de encaminamiento por personal sin conocimientos acerca de cómo interaccionar con el transmisor mediante línea de comandos.

Nombre	Descripción
olsrd	OLSR (Optimized Link State Routing) daemon
olsrd-mod-dyn-gw-plain	Dynamic internet gateway plain plugin
olsrd-mod-bmf	Basic multicast forwarding plugin
olsrd-mod-httpinfo	Small informative web server plugin
olsrd-mod-quagga	Quagga plugin
olsrd-mod-dyn-gw	Dynamic internet gateway plugin
olsrd-mod-txtinfo	Small informative web server plugin
olsrd-mod-nameservice	Lightweight hostname resolver plugin
olsrd-mod-dot-draw	Dot topology information plugin
olsrd-mod-mdns	Multicast DNS plugin
olsrd-mod-watchdog	Watchdog plugin
olsrd-mod-arprefresh	Kernel ARP cache refresh plugin
olsrd-mod-p2pd	Peer to Peer Discovery plugin
olsrd-mod-secure	Message signing plugin to secure routing domain

Tabla 3-4 Módulos necesarios en OLSR

4. Una vez instalados todos los módulos *software* necesarios se procede a la configuración del archivo principal del protocolo. La configuración se puede hacer bien mediante el interfaz gráfico LuCI o bien mediante línea de comandos vía ssh. Mediante ssh es necesario el acceso al archivo de configuración `/etc/config/olsrd`. En general, la configuración para todos los nodos es la misma exceptuando el nombre alfanumérico (resaltado en amarillo) para cada nodo.

```
root@LANCHA-3:/etc/config# vi olsrd
```

```
olsrd
```

```
option IpVersion '4'
```

```
option FIBMetric 'flat'
```

```
option LinkQualityLevel '2'
```

```
option LinkQualityAlgorithm 'etx_ff'
```

```
option OlsrPort '698'
```

```
option Willingness '3'
```

```
option NatThreshold '1.0'
```

```
option SmartGateway 'yes'
```

```
option SmartGatewayUplink 'both'
```

```
config LoadPlugin
```

```
option library 'olsrd_arprefresh.so.0.1'
```

```
option ignore '0'
```

```
config LoadPlugin
```

```
option library 'olsrd_dyn_gw.so.0.5'
```

```
option ignore
```

```
config LoadPlugin
```

```
option library 'olsrd_httpinfo.so.0.1'
```

```
option port '1978'
```

```
list Net '0.0.0.0 0.0.0.0'
```

```
option ignore '0'
```

```
config LoadPlugin
```

```
option library 'olsrd_nameservice.so.0.3'
```

```
option ignore '0'
```

```
list name 'LANCHA-3'
```

```
option interval '30'
```

```
option timeout '300'
```

```
option sighup_pid_file '/var/run/dnsmasq.pid'
```

```
option name_change_script '/touch/tmp/namechange'
```

```
config LoadPlugin
```

```
option library 'olsrd_txtinfo.so.0.1'
```

```
option accept '0.0.0.0'
```

```
option ignore '0'
```

```
config InterfaceDefaults
```

```
option Mode 'mesh'
```

```
config LoadPlugin
```

```
option library 'olsrd_pgraph.so.1.1'
```

```
option ignore '1'
```

```
config LoadPlugin
```

```
option library 'olsrd_jsoninfo.so.0.0'
```

```
option ignore '0'
```

```
config LoadPlugin
```

```
option library 'olsrd_p2pd.so.0.1.0'
```

```
option ignore '1'
```

```
config LoadPlugin
```

```
option library 'olsrd_sgwdynspeed.so.1.0.0'
```

```
option ignore '1'
```

```
config LoadPlugin
```

```
option library 'olsrd_pud.so.1.1.0'
```

```
option ignore '1'
```

```
config LoadPlugin
```

```
option library 'olsrd_watchdog.so.0.1'
```

<pre> option ignore '0' config LoadPlugin option library 'olsrd_secure.so.0.6' option keyfile '/etc/config/olsr.key' option ignore '0' config LoadPlugin option library 'olsrd_bmf.so.1.7.0' option ignore '1' config LoadPlugin option library 'olsrd_quagga.so.0.2.2' option ignore '1' config LoadPlugin </pre>	<pre> option library 'olsrd_dot_draw.so.0.3' option ignore '0' config LoadPlugin option library 'olsrd_mdns.so.1.0.1' option ignore '1' config LoadPlugin option library 'olsrd_dyn_gw_plain.so.0.4' option ignore '1' config LoadPlugin option library 'olsrd_mdns.so.1.0.0' option ignore '1' config Interface option ignore '0' option interface 'WLAN0' option Mode 'mesh' </pre>
--	---

5. Tal y como se presentó en las especificaciones de cada equipo, los nodos van equipados con dos interfaces físicas. Previo a la configuración, se verifica el reconocimiento por parte del sistema operativo de los dos interfaces mediante el comando “ifconfig”.

```
root@LANCHA-3:~# ifconfig
```

```

eth0    Link encap:Ethernet HWaddr 68:72:51:07:AE:F5
        inet addr:10.0.30.10 Bcast:10.0.30.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:897 errors:0 dropped:63 overruns:0 frame:0
        TX packets:653 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:158927 (155.2 KiB) TX bytes:163992 (160.1 KiB)
        Interrupt:4

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0

```

```
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:24906 errors:0 dropped:0 overruns:0 frame:0
TX packets:24906 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1699067 (1.6 MiB) TX bytes:1699067 (1.6 MiB)
```

```
wlan0 Link encap:Ethernet HWaddr 68:72:51:06:AE:F5
inet addr:192.168.1.30 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:1665 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:32
RX bytes:0 (0.0 B) TX bytes:139360 (136.0 KiB)
```

7. Una vez verificados, se procede a la configuración de los parámetros de red. A continuación se exponen unas pautas referentes a los interfaces físicos y sus nombres lógicos en el archivo de configuración “network”.

- El interfaz de red “WLAN0” está asociado al transmisor radio del sistema denominado “wlan0”. Por lo que será este interfaz el que utilice el protocolo de encaminamiento OLSR para inyectar sus tramas de control en la red MANET.
- Las direcciones IP de este interfaz son estáticas y la subred perteneciente a los interfaces WLAN0 es 192.168.1.0/24.
- Los nodos se identifican en múltiplos de 10. Es decir, que el nodo llamado “LANCHA-3” tiene como dirección IP en wlan0 a ‘192.168.1.30’.
- El interfaz lógico ‘lan’ se encuentra asociado al interfaz físico eth0 para realizar las funciones de transmisión de datos por el medio cableado. Es el responsable de extender la red MANET a los dispositivos de abordó. Se configura para ser la puerta de enlace de todos los dispositivos de abordó sirviendo direcciones IP mediante DHCP. Igualmente, la configuración es estática y tal y como se observa en la visualización del archivo “network” del nodo “LANCHA-y” se ubica en la subred 10.0.0.0/16. El conjunto denominador de cada nodo viene dado por 10.0.x.10/16, siendo $x = 10y$.
- Tanto el interfaz “lan” como “WLAN0” se configuran con las DNS “8.8.8.8, 8.8.4.4”.

A continuación se puede leer el contenido del archivo de configuración de uno de los nodos.

```
root@LANCHA-3:/etc/config# vi network
```

```

config interface 'loopback'
option ifname 'lo'
option proto 'static'
option ipaddr '127.0.0.1'
option netmask '255.0.0.0'

config interface 'lan'
option force_link '1'
option proto 'static'
option ip6assign '60'
option dns '8.8.8.8 8.8.4.4'
option _orig_ifname 'eth0'
option _orig_bridge 'true'
option ifname 'eth0'
option ipaddr '10.0.30.10'
option netmask '255.255.0.0'

config interface 'WLAN0'
option proto 'static'
option netmask '255.255.255.0'
option dns '8.8.8.8 8.8.4.4'
option ipaddr '192.168.1.30'

```

Asimismo, la configuración del nodo responsable de dar cobertura a los nodos embarcados tiene su interfaz ‘lan’ configurado en modo cliente de manera que sea otro dispositivo más de la red en tierra que va a extender.

8. El cortafuegos debe configurarse de manera que el tráfico que provenga del interfaz inalámbrico (WLAN0) se redirija hacia el eth0. Si se configura de manera que acepte tráfico en ambas direcciones se resuelve la configuración para los nodos embarcados y para el nodo en tierra que haga funciones de puerta de enlace.

```
root@LANCHA-3:/etc/config# vi firewall
```

```
config defaults
```

```

option syn_flood '1'
option input 'ACCEPT'
option output 'ACCEPT'

```

<pre> option forward 'REJECT' config include option path '/etc/firewall.user' config zone option input 'ACCEPT' option output 'ACCEPT' option name 'mesh' </pre>	<pre> option forward 'ACCEPT' option masq '1' option mtu_fix '1' option network 'WLAN0 lan' config zone option name 'newzone' option input 'ACCEPT' option output 'ACCEPT' </pre>
--	--

9. Se procede a la configuración de los parámetros del interfaz radio “radio1” mediante el archivo “wireless”.

<pre> root@LANCHA-3: vi /etc/config/wireless config wifi-device 'radio1' option type 'mac80211' option macaddr '68:72:51:06:ae:f5' list ht_capab 'SHORT-GI-40' list ht_capab 'TX-STBC' list ht_capab 'RX-STBC1' list ht_capab 'DSSS_CCK-40' option txpower '27' option hwmode '11g' </pre>	<pre> option country 'BO' option channel '10' config wifi-iface option device 'radio1' option ssid 'NW-MESH' option mode 'adhoc' option network 'WLAN0' option key 'manolito' option encryption 'psk2' </pre>
---	--

En la opción “encryption” se indica al módulo wpad que habilite la seguridad en la capa de física mediante el estándar 802.11i en su variante de clave precompartida utilizando AES como método de cifrado de datos.

10. Finalmente, se configura el módulo de seguridad basado en la firma de los paquetes de protocolo OLSR que proporciona integridad a la MANET. Para ello, se crea el archivo mediante el siguiente comando: “vi/etc/config/olsr.key”. En él se pega la clave en hexadecimal.

3.4 Acceso desde dispositivos cliente a bordo de buques

Una vez establecida la Red MANET entre los buques y el nodo en tierra se presenta el problema de proporcionar servicio a cualquier dispositivo cliente que necesite conectividad. Ya que los nodos instalados en los buques funcionan en modo *ad-hoc* y utilizan un sistema de señalización distinto al modo *ad-hoc* integrado en cualquier dispositivo doméstico es necesario extender la red MANET a los dispositivos a bordo del buque de manera inalámbrica.

Como funcionalidad añadida a los servicios prestados a los cliente de a bordo se configura un servidor *proxy-web* para optimizar el tráfico referente a los puertos 80 y 443, correspondientes a los servicios *web* y SSL (*Socket Secure Layer*). Para ello, se utiliza un punto de acceso inalámbrico (AP) conectado al puerto *ethernet* de cada uno de los nodos de la red MANET de la lancha. El dispositivo elegido para desempeñar las funciones de punto de acceso Wi-Fi es el siguiente:

TP-LINK WDR3500

Es un encaminador inalámbrico de banda dual simultáneo de desempeño optimizado que combina velocidades de 300Mbps en la banda de 5GHz y de 2,4 GHz. Con la banda dual simultánea, los usuarios disponen de hasta 600Mbps.



Figura 3-8 TP-LINK WDR3500

Arquitectura	MIPS 74Kc
Ensamblador	Qualcomm Atheros
Chip	AR9344 (MIPS)
Vel. CPU	560 MHz
Flash-Chip:	cFeon Q64-104HIP
TamañoFlash	8192 KiB
RAM:	128 MiB
Wireless	Atheros AR9340 2.4GHz
Ethernet	Atheros AG71xx: eth0
Switch:	AR934X built-in switch
USB:	1 x 2.0 usb

Tabla 3-5 Especificaciones técnicas del AP

3.4.1 Configuración

Al igual que los dispositivos integrantes de la red MANET, este AP viene de fábrica con un software propietario. Atendiendo a las tablas de comprobación de hardware compatible con OpenWrt se procede a la instalación de la versión 14.07 de OpenWrt.

A continuación se exponen los pasos a seguir para la configuración:

1. Se procede a la instalación del sistema operativo OpenWrt. El primer paso es común a los dos primeros pasos de el apartado 3.3.

2. Iniciar sesión en el router a través de SSH.

```
ssh root@192.168.1.1
```

3. Si existe alguna interfaz WAN ya definida, se debe eliminar.

```
uci del network.wan
```

4. Cambiar la subred de la interfaz LAN del router a una distinta a la del router principal.

```
uci set network.lan.ipaddr=192.168.2.1
uci set network.lan.netmask=255.255.255.0
uci set network.lan.dns=8.8.8.8
uci set network.lan.nat=1
uci set network.lan.accept_ra=1
```

5. Permitir las concesiones dinámicas en el servidor DHCP:

```
uci set dhcp.lan.dynamicdhcp=1
```

6. Crear una interfaz para el WLAN.

```
uci set network.wan=interface
uci set network.wan.proto=
```

7. Habilitar la interfaz wireless:

```
uci set wireless.radio0.disabled=0
uci commit wireless wifi
```

8. Cambiar la configuración del wifi:

El dispositivo a editar es el "radio0" (Driver OpenSource de Broadcom).

```
uci set wireless.radio0.channel=1
uci set wireless.@wifi-iface[0].ssid=WLAN
uci set wireless.@wifi-iface[0].mode=sta
uci set wireless.@wifi-iface[0].network=wan
uci set wireless.@wifi-iface[0].encryption=psk2
uci set wireless.@wifi-iface[0].key=manolito
```

9. El firewall quedará configurado de la misma manera que el punto 8 del apartado 3.3.

4 RESULTADOS

Una vez configurado el material, se realizan dos pruebas que se detallan a continuación. La ENM, situada en la ría de Pontevedra es el entorno de pruebas. Los nodos en tierra pueden instalarse en cualquier ubicación de la ENM con el objeto de extender la cobertura hacia el oeste, dirección en la cual las embarcaciones realizan sus adiestramientos. La monitorización en tiempo real de las pruebas se realiza desde un único nodo, siendo en ambas pruebas el nodo “LANCHA-1”. Las pruebas abarcan a la red MANET, dejando en segundo plano el funcionamiento de los puntos de acceso inalámbricos que tienen que extender la red a los dispositivos cliente de abordó. Los objetivos que persiguen la pruebas son los siguientes:

- Dotar a la red MANET de acceso a internet mediante la conexión de uno de los nodos en tierra al servicio de Internet prestado en uno de los cuarteles de la ENM.
- Alcance máximo del nodo TIERRA-1.
- Tasa de datos en la máxima distancia.
- Operación del *hardware* en el ambiente marino.
- Viabilidad de una instalación fija.

Durante las dos pruebas, se da la circunstancia de que el nodo con mejor situación geográfica y por lo tanto, que se encuentra en predisposición de extender la cobertura a mayor distancia es el nodo denominado “TIERRA-1”.

4.1 Realización de la 1ª Prueba

La disposición del material y PIRE es la siguiente:

NODO	TRANSMISOR	ANTENA	PIRE	DIRECCIÓN IP	
				WLAN0	ETH0
TIERRA-1	Bullet M2 Titanium	Antena Omnidireccional AOA-2415	42 dBm	192.168.1.30/24	192.168.3.200/22
LANCHA-1				192.168.1.10/24	10.0.10.10/16
LANCHA-2				192.168.1.40/24	10.0.40.10/16
LANCHA-3				192.168.1.20/24	10.0.20.10/16

Tabla 4-1 Organización del material. 1ª Prueba

En la primera prueba el nodo TIERRA-1 se instala en la fachada norte del cuartel Almirante Francisco Moreno. La visión de su antena omnidireccional se observa en la figura 4-1. El principal inconveniente de este escenario de radica en que el edificio del Centro de Medidas Electromagnéticas se encuentra en la trayectoria del haz de la antena hacia el exterior de la ría de Pontevedra. Este nodo es la puerta de enlace de acceso a Internet de toda la red MANET, extendiendo la red del cuartel Almirante Francisco Moreno que se encuentra en la subred 192.168.0.0/22.



Figura 4-1 Visión de nodo “TIERRA-1”

Los nodos embarcados denominados como LANCHA-X se instalan provisionalmente en el puente alto de las lanchas de instrucción. Se procura que el haz omnidireccional de la antena tenga en visión a todo horizonte para que no haya ángulos muertos que condicionen al gobierno de la embarcación.

Aunque en la figura 4-1 ya se pueden intuir los sectores con obstáculos de la ría, en la figura 4-2 se realiza una representación aérea de dichos sectores. Los sectores en color morado son aquellos en los que un observador situado en el mar, no tiene visión directa de la antena. Esta situación no ayuda a conocer la máxima distancia posible de los enlaces, ya que algunos nodos se pueden encontrar en las áreas moradas de la figura 4-2 y puede resultar engañoso.

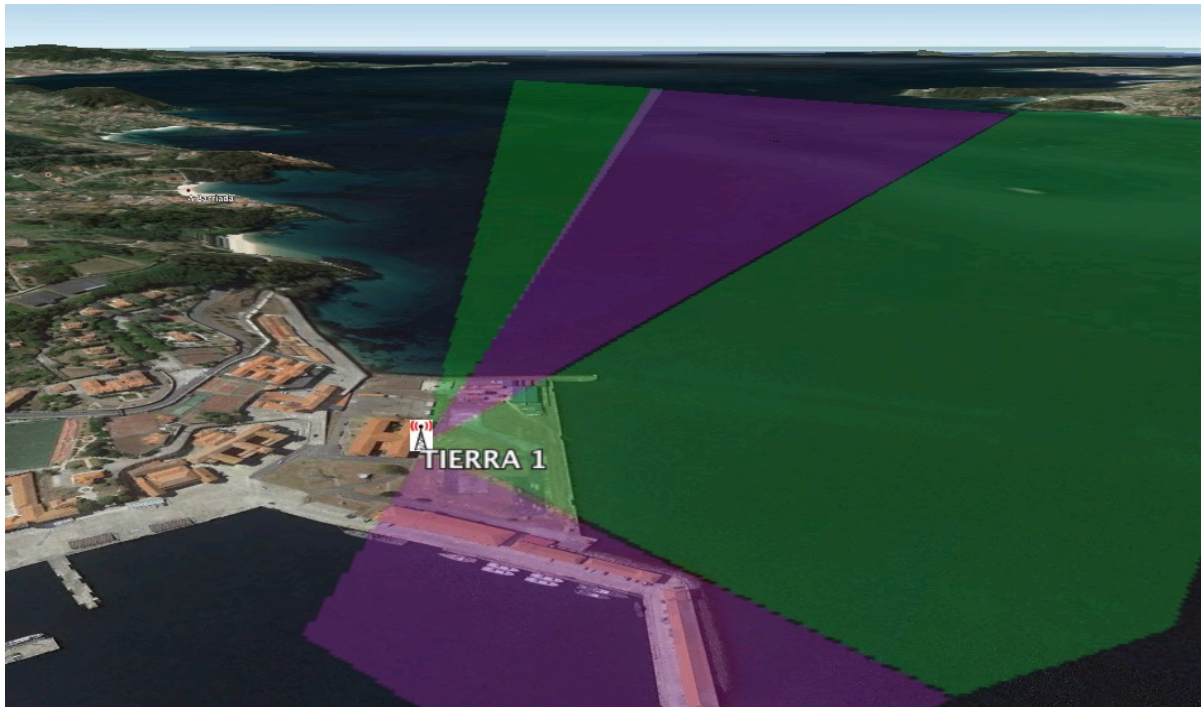


Figura 4-2 Situación y representación de sectores con obstáculos

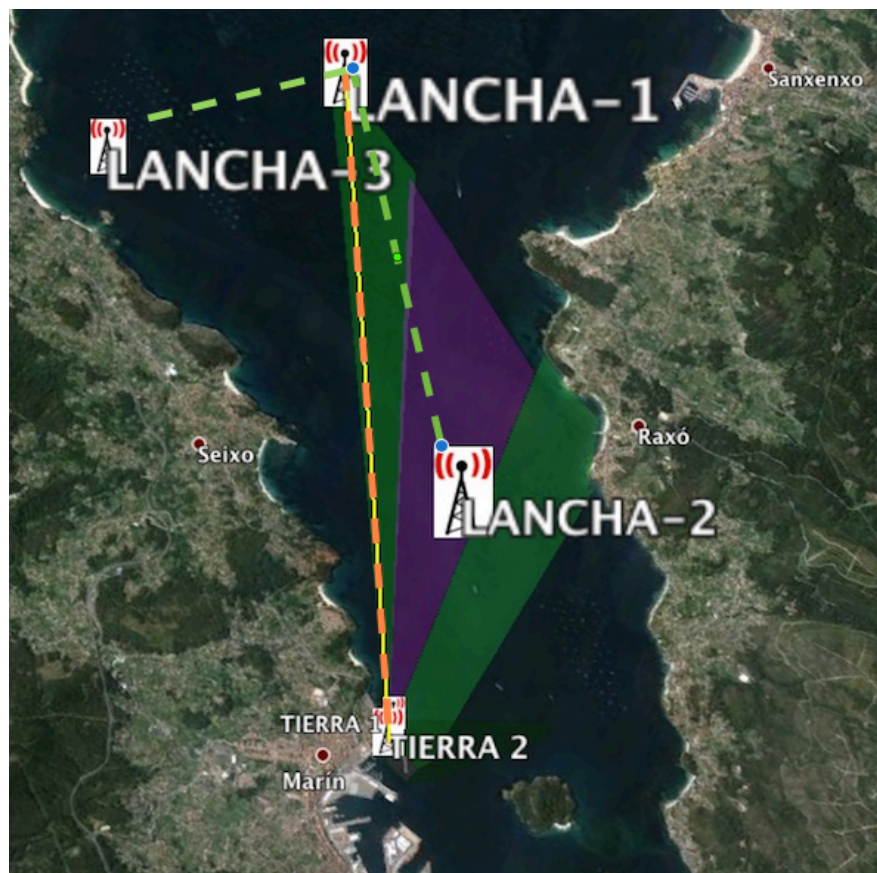


Figura 4-3 Cobertura de los nodos. Escenario de prueba 1º

4.2 Realización de la 2ª Prueba

La disposición del material será la siguiente:

NODO	TRANSMISOR	ANTENA	PIRE	DIRECCIÓN IP	
				WLAN0	ETH0
TIERRA-2	NanoStation M2		16 dBm	192.168.1.50/24	192.168.3.200/22
TIERRA-1	Bullet M2 Titanium	Antena Omnidireccional AOA-2415	42 dBm	192.168.1.10/24	/
LANCHA-1				192.168.1.40/24	10.0.40.10/16
LANCHA-2				192.168.1.20/24	10.0.20.10/16

Tabla 4-2 Organización del material. 2ª prueba

Se instala el nodo “TIERRA-2” en la fachada norte del cuartel Almirante Francisco Moreno. Su antena direccional está apuntada con un azimut de 305° y una elevación de 0° (haz de radiación paralelo al plano de tierra). Este nodo es el encargado establecer un enlace *ad-hoc* con el nodo “TIERRA-1”, que dista a una distancia de 190 metros. Está conectado mediante cable CAT5 al conmutador principal del mismo cuartel, por lo que es la puerta de enlace de la red MANET para todo el tráfico que tenga como destino Internet.

El nodo “TIERRA-1”, situado en las instalaciones del Centro de Medidas Electromagnéticas con base en la ENM es el nodo con mejor línea de visión a la ría de Pontevedra. En su emplazamiento, el nodo “TIERRA-1” solo dispone de toma de alimentación a la red. En un principio, este nodo es el que tendrá mayor radio de cobertura dada su situación, expuesta en la figura 4-4. Este nodo tendrá en todo momento enlace con su homólogo situado en el cuartel Almirante Francisco Moreno. Asimismo, esta disposición permite comprobar de manera rápida el rendimiento del sistema a dos saltos de distancia, puesto que el nodo “TIERRA-2” tiene ajustada la potencia de transmisión para que establezca enlace a 54 Mbps de acuerdo a la tabla contenida en el anexo I. Este ajuste de potencia fuerza a los nodos embarcados a establecer contacto con la puerta de enlace mediante el nodo intermedio “TIERRA-1”.

Tal y como se observa en la tabla 4-2, el interfaz “ETH0” del nodo “TIERRA-2” no tiene asignada ninguna dirección IP puesto que no tiene que encaminar ninguna información por ese interfaz. Todo trabajo de encaminar tráfico es realizado por el interfaz inalámbrico “WLAN0”, ya sea proveniente de “TIERRA-1”



Figura 4-4 Disposición de nodos en tierra. 2º prueba

1- Edificio Almirante Francisco Moreno

2- Instalaciones CEMEDEN

Los nodos embarcados denominados como LANCHA-X se instalan de la misma manera que en la primera prueba.



Figura 4-5 Cobertura de los nodos de tierra. Escenario de prueba 2º

4.3 Datos obtenidos

Una vez presentados los dos escenarios de prueba, se exponen los resultados obtenidos durante las dos pruebas realizadas.

Durante la primera prueba, a pesar de los sectores sin visión directa de la ría, expuestos en la figura 4-2, se alcanza una distancia máxima sin retransmisiones de 8,2 Km. La tablas de encaminamiento se actualizan satisfactoriamente experimentándose un retardo de no más de 10 segundos en la actualización de la topología de la red. La realidad en este escenario es que se producen grandes pérdidas debido a la cercanía de los obstáculos en las proximidades de la antenna. Otro hecho determinante es el uso de una antena omnidireccional en lugar de un equipo NanoStation M2, el equipo especialmente adquirido para realizar esta función.

La herramientas utilizada para examinar la topología de la red en tiempo real se corresponde con el modulo “olsr-viz”, que realiza una representación gráfica de la topología tal y como se observa en la imagen.

La tasa de transferencia en enlace directo resultó ser de 6 Mbps y una latencia de no más de 60ms. Esto permitía hacer un uso fluido de servicios disponibles en Internet como navegación normal *web* e incluso la visualización de vídeos en *streaming*, lo cual demuestra la capacidad del radioenlace para soportar otras aplicaciones. Sin embargo, durante esta prueba el nodo desde donde se realizaba la monitorización no estuvo en ningún momento a dos saltos de distancia de la puerta de enlace, puesto que el algoritmo de encaminamiento consideraba en todo momento que el mejor enlace era el directo.

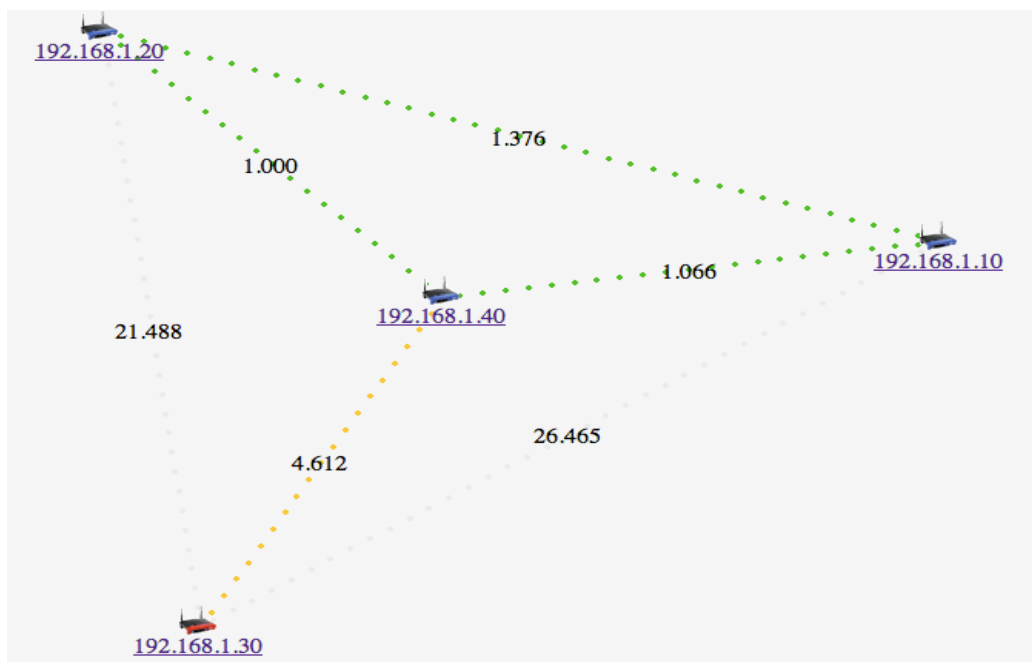


Figura 4-6 Topología mostrada por el interfaz gráfico durante la 1ª prueba

La imagen 4-6 muestra la situación en la cual el nodo “LANCHA-2” (IP: 192.168.1.40) es el único en alcance radio con el nodo en tierra. Esta situación se monitoriza remotamente desde el nodo “LANCHA-1”(IP: 192.168.1.10).

A continuación se exponen los criterios seguidos por el algoritmo de encaminamiento para la elaboración de las tablas de encaminamiento.

LQ: Success rate of packages received from the neighbour

NLQ: Success rate of packages sent to the neighbour

ETX: Expected retransmission count

Green: Very good ($ETX < 2$)

Yellow: Good ($2 < ETX < 4$)

Orange: Still usable ($4 < ETX < 10$)

Red: Bad ($ETX > 10$)

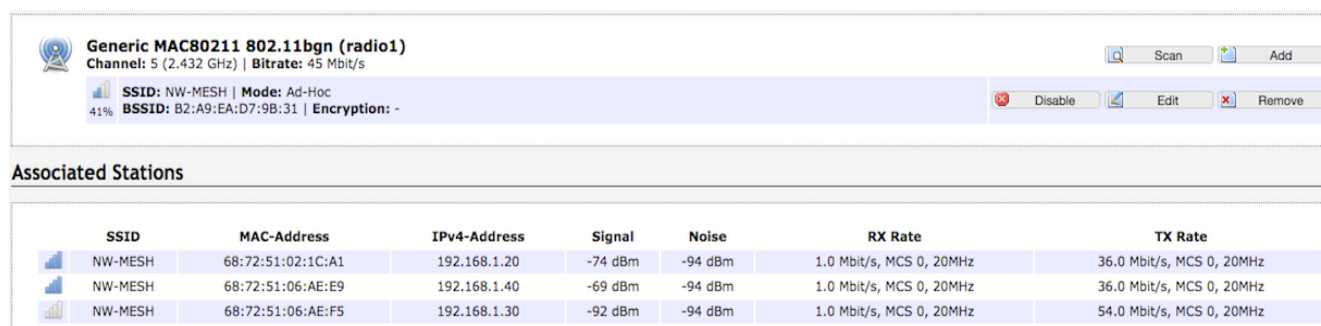


Figura 4-7 Potencia Rx a bordo de “LANCHA-1”

En la figura 4-7 se observa la baja potencia recibida del nodo en tierra: -92dBm de potencia en la recepción no es suficiente para que el transmisor enlace directamente con tierra. Automáticamente, “LANCHA-2” comienza a retransmitir hacia los demás nodos fuera de alcance.

Durante la segunda prueba, las condiciones meteorológicas eran de lluvia intensa. Pese a ello, la antena omnidireccional AOA-2415 del nodo “TIERRA-1” demostró tener un alcance de 11 km. En esta situación de enlace a dos saltos de distancia en el punto más lejano donde el sistema demostró seguir teniendo enlace se logró una tasa de transferencia de 1.3 Mbps con una latencia en torno a 100 ms.

En la figura 4-8 se observa como el algoritmo valora el enlace entre las dos lanchas (lado izquierdo de la figura) encontrándose a 1200 metros de distancia de forma satisfactoria. Sin embargo, el nodo “LANCHA-2” (192.168.1.40) se encuentra en muy malas condiciones debido a que la antena sectorial (192.168.1.50) está limitada en potencia.

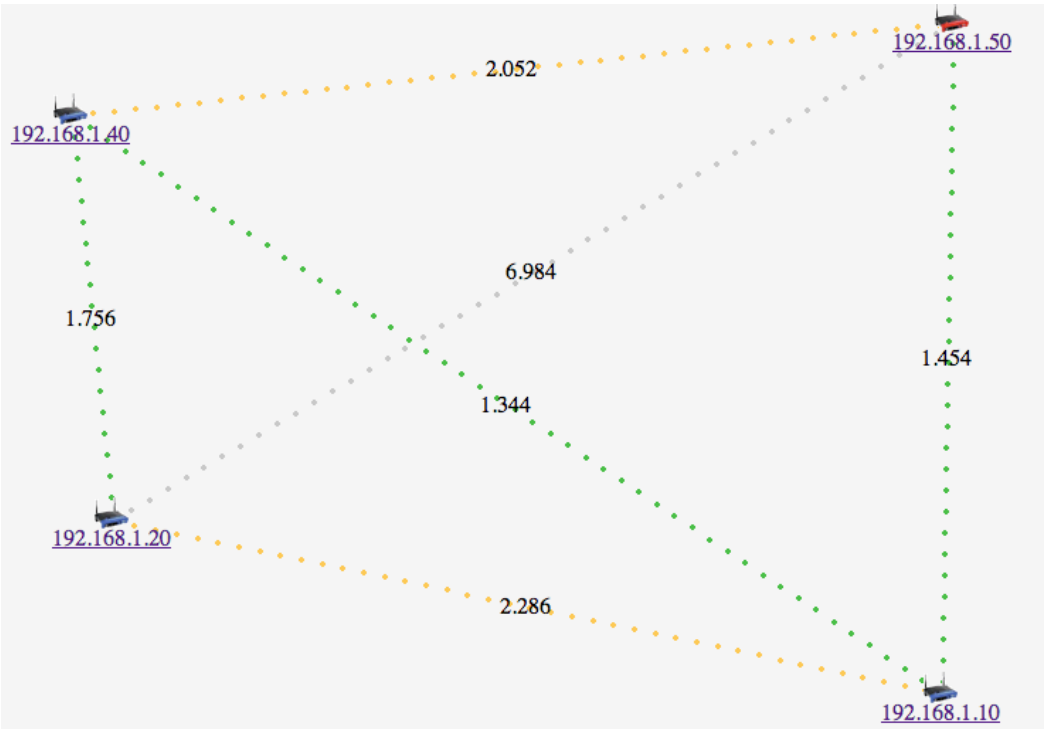


Figura 4-8 Topología mostrada por el interfaz gráfico durante la 2ª prueba

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones extraídas

Tras el estudio del escenario de despliegue de la red y realizar dos pruebas a bordo de las lanchas de instrucción, las conclusiones son las siguientes:

A pesar de que previamente a la adquisición de los equipos se realizó un estudio previo para definir las necesidades y especificaciones técnicas que los equipos de radio debían tener, no estaba claro el rendimiento que finalmente iban a mostrar en el escenario de pruebas. Se trata de una tecnología muy económica ya que los transmisores en la banda ISM de 2,4GHz están muy extendidos en aplicaciones domésticas y semiprofesionales. Las limitaciones de PIRE en esta banda de frecuencias son un factor relevante. De la misma manera, la saturación y ruido producido en su mayor parte por el masivo empleo de esta banda, en un principio, tampoco la hacían la ideal. No obstante, se apostó por equipos de exterior que estuvieran directamente conectados a la antena de manera que se minimizaran las pérdidas en el sistema referentes a conectores y cables coaxiales. Esto se traduce en equipos que entregan toda la potencia a la antena sin apenas pérdidas, resultando óptimos a la hora de transmitir y recibir. El término óptimo se refiere al logro de una elevada PIRE, además de, tal y como se puede ver en las tablas del anexo I, las sensibilidades de recepción de los dispositivos son del orden de -90 dBm. Finalmente, esto se ha traducido en alcance de hasta 12 km entre nodos, lo cual para el escenario de pruebas resulta muy exitoso, pues el punto más externo de la ría de Pontevedra se encuentra a 13 km. No obstante, no se ha tenido la oportunidad de comprobar los parámetros de operación de los transmisores en mayores distancias.

Con respecto al tema de la seguridad e integridad de la red MANET, desde un principio se anticipaba el poco desarrollo existente en protocolos de seguridad para este tipo de redes. La dificultad añadida de no poder implantar protocolos de seguridad en la capa de red como IPsec debido a la naturaleza de las redes MANET es el comienzo para la experimentación de estándares que aporten integridad y confidencialidad. En este sentido, la existencia en el protocolo OLSR de un módulo que aporta integridad a nivel de encaminamiento es un punto a favor. No obstante, a día de hoy, el número de usuarios que disponen de un transceptor de la banda ISM de 2,4GHz es elevadísimo y supone una seria amenaza de la existencia de usuarios malintencionados que sean capaces de monitorizar la

información que viaja a través del medio. Es por ello, que resultaba imprescindible cifrar la información contenida en los paquetes de red.

Finalmente, en un escenario como la ría de Pontevedra se ha comprobado que durante una salida rutinaria a la mar, ningún nodo embarcado se queda fuera del alcance radio de los demás nodos. Esto quiere decir que cualquier embarcación puede alcanzar a otra utilizando comunicación directa (un solo salto) , lo cual se traduce en una baja latencia de comunicación y buen aprovechamiento de la tasa de datos del estándar 802.11. De cara a implantar comunicaciones mediante voz IP entre los nodos embarcados supondría tener una latencia muy baja, parámetro meramente determinante de cara a la comunicaciones por voz en tiempo real.

5.2 Líneas futuras

Las líneas de avance en el despliegue de una red MANET de ámbito docente se analizan en dos vertientes, *hardware* y *software*.

En cuanto a equipos, una vez comprobado el funcionamiento con un fin docente se plantean diversas ideas para incorporarlo con un fin profesional. Es obvio que la banda libre de 2,4 Ghz ha servido para comprobar el funcionamiento del estándar inalámbrico de transmisión de datos y del protocolo de encaminamiento, pero sus características de banda libre impide transmitir con potencias elevadas que permitan aumentar el alcance. Una línea futura de investigación sería la portabilidad de este estándar a una banda militar UHF en la cual no exista la limitación de potencia de la banda de 2,4 Ghz. El principal problema de las bandas de menor frecuencia radica en la menor disponibilidad de ancho de banda, aunque numerosas pruebas experimentales muestran [23] buenas tasas de transmisión con la mitad del ancho de banda.

Asimismo, mudarse a frecuencias inferiores suele ser la solución más fácil pues se reducen pérdidas por atenuación del medio. Probablemente, la solución de mudarse a UHF no resultase tremendamente beneficiosa en redes de *ad-hoc* debido al problema del ruido generado por todos los demás nodos que se encuentran en el canal. Tal y como se muestra en [4], existe la posibilidad de desplegar redes MANET multicanal de manera que aumentar el radio de alcance de los nodos no suponga un aumento exponencial del ruido en el canal de transmisión.

En cuanto a *software*, una meta a conseguir es la optimización de las aplicaciones de a bordo estableciendo una jerarquía de utilización de recursos. Esto es conocido como QoS. Numerosos protocolos de encaminamiento contemplan la posibilidad de configuración en este ámbito.

Una vez lograda una conectividad robusta entre las lanchas y entre estas y tierra, se puede contribuir a dotar a las lanchas de instrucción de aplicaciones docentes con necesidades de conectividad. Entre las numerosas aplicaciones, las líneas de trabajo futuras serían la incorporación de un *chat* seguro entre embarcaciones, desarrollo de sistema táctico para compartición de información de los sensores, conferencias de voz y vídeo en tiempo real mediante aplicaciones basadas en IP.

6 BIBLIOGRAFÍA

- 1] | Stanford Education. Stanford Education. [Online].
<http://cs.stanford.edu/people/eroberts/courses/soco/projects/risc/whatis/index.html>
- 2] | OpenWrt. OpenWrt. [Online]. <http://wiki.openwrt.org/toh/buyerguide>
- 3] | IEEE Computer Society, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications □ □ □," in *IEEE Std 802.11TM-2012*. EEUU.
- 4] | Auerbach Publications, *Wireless Mesh Networking*, Jijun Luo, Honglin Hu Yan Zhang, Ed. New York, 2007.
- 5] | R. Ramanathan, *On the performance of ad hoc networks with beamforming antenas.:* ACM MobiHoc, 2001.
- 6] | Tarek Saadawi Shugong Xu, *Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?* New York, EEUU, 2001.
- 8] | C.K. Toh. E.M. Royer, *A review of current routing protocols for ad hoc mobile wireless networks*. 1999: IEEE Wireless Communications, vol. 6.
- 7] | Shugong Xu. Tarek Saadawi, *Revealing the problems with 802.11 medium access control protocol in multi-hop wireless ad hoc networks.:* The International Journal of Computer and telecommunications Networking, 2002.
- 9] | K. Petteri, *Classification of ad hoc routing protocols*. Finland: Finish Defence Forces, Naval Academy, 2002.
- 10] | G D Holland, *Adaptive models for Mobile Ad Hoc Networks*. Texas: Department of Computer Science, 2004.
- 1] | E. Ancillotti, M. Conti, A. Passarella G. Anastasi, *A Transport Protocol for Ad Hoc*

- 11] *Networks*. 2005: Computers and Communications.
- 12] | Godred. Fairhurst, *Best Effort*. UK: Internet Communications Engineering, 2013.
- 13] | P. Jacquet T. Clausen. RFC3626. [Online]. <https://tools.ietf.org/html/rfc3626>
- 14] | Andreas Tønnesen. (2003, Febrero) Mobile Ad-Hoc Networks. [Online]. <http://www.olsr.org/docs/wos3-olsr.pdf>
- 15] | IEEE,. 2004.
- 16] | S. Kent and R. Atkinson, *Security architecture for the Internet Protocol*. RFC 2401., 1998.
- 18] | John Marshall., *An analysis of SRP for mobile ad hoc networks*. Las Vegas, EEUU, 2002, In Proceedings of the 2002 International Multiconference in Computer Science.
- 17] | Ludovic Me, and Rafael Timóteo de Sousa. Ricardo Staciarini Puttini, "Certification and authentication services for securing MANET routing protocols.," International Conference on Mobile and Wireless Communications Networks, Singapore, Singapore, 2003.
- 19] | Adrian Perrig, and David B. Johnson Yih-Chun Hu, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks.," Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, 2003.
- 20] | Eriko Ando, and Yasuko Fukuzawa Shuichi Isida, "Secure routing functions for OLSR protocol.," n 2005 OLSR Interop and Workshop, Ecole Polytechnique, Palaiseau., 2005.
- 21] | OpenWrt. (2015, Febrero) [Online]. <http://wiki.openwrt.org/toh/start>
- 22] | Andreas Tønnesen. Sitio web del protocolo OLSR. [Online]. <http://www.olsr.org>
- 23] | David Bern. <http://www.tapr.org/>. [Online]. <http://www.tapr.org/pdf/DCC2012-Experimenting--Wireless-Networking-in-420-MHz-Band-W2LNX.pdf>
- 24] | David J. Wetherall Andrew S. Tanenbaum, *Redes de Computadoras*, Quinta Edición ed. México: Pearson, 2012.

ANEXO I: ESPECIFICACIONES DE EQUIPOS

Bullet M2 HP - Operating Frequency 2412-2462 MHz							
OUTPUT POWER: 28 dBm							
2.4 GHz TX POWER SPECIFICATIONS				2.4 GHz RX POWER SPECIFICATIONS			
	DataRate	Avg. TX	Tolerance		DataRate	Sensitivity	Tolerance
11b/g	6-24 Mbps	28 dBm	+/- 2 dB	11b/g	24 Mbps	-83 dBm	+/- 2 dB
	36 Mbps	25 dBm	+/- 2 dB		36 Mbps	-80 dBm	+/- 2 dB
	48 Mbps	24 dBm	+/- 2 dB		48 Mbps	-77 dBm	+/- 2 dB
	54 Mbps	23 dBm	+/- 2 dB		54 Mbps	-75 dBm	+/- 2 dB
11n	MCS0	28 dBm	+/- 2 dB	11n	MCS0	-96 dBm	+/- 2 dB
	MCS1	28 dBm	+/- 2 dB		MCS1	-95 dBm	+/- 2 dB
	MCS2	28 dBm	+/- 2 dB		MCS2	-92 dBm	+/- 2 dB
	MCS3	28 dBm	+/- 2 dB		MCS3	-90 dBm	+/- 2 dB
	MCS4	27 dBm	+/- 2 dB		MCS4	-86 dBm	+/- 2 dB
	MCS5	25 dBm	+/- 2 dB		MCS5	-83 dBm	+/- 2 dB
	MCS6	23 dBm	+/- 2 dB		MCS6	-77 dBm	+/- 2 dB
	MCS7	22 dBm	+/- 2 dB		MCS7	-74 dBm	+/- 2 dB

Tabla 6-1 Sensibilidades en recepción frente a Tasas de transmisión. BulletM2

Fuente: Fabricante *Ubiquiti Networks*

NanoStationM2 Specifications

Output Power: 28 dBm							
2.4 GHz TX POWER SPECIFICATIONS				2.4 GHz RX POWER SPECIFICATIONS			
	Data Rate/MCS	Avg. TX	Tolerance		Data Rate/MCS	Sensitivity	Tolerance
11b/g	1-24 Mbps	28 dBm	± 2 dB	11b/g	1-24 Mbps	-83 dBm	± 2 dB
	36 Mbps	26 dBm	± 2 dB		36 Mbps	-80 dBm	± 2 dB
	48 Mbps	25 dBm	± 2 dB		48 Mbps	-77 dBm	± 2 dB
	54 Mbps	24 dBm	± 2 dB		54 Mbps	-75 dBm	± 2 dB
airMAX	MCS0	28 dBm	± 2 dB	airMAX	MCS0	-96 dBm	± 2 dB
	MCS1	28 dBm	± 2 dB		MCS1	-95 dBm	± 2 dB
	MCS2	28 dBm	± 2 dB		MCS2	-92 dBm	± 2 dB
	MCS3	28 dBm	± 2 dB		MCS3	-90 dBm	± 2 dB
	MCS4	27 dBm	± 2 dB		MCS4	-86 dBm	± 2 dB
	MCS5	25 dBm	± 2 dB		MCS5	-83 dBm	± 2 dB
	MCS6	23 dBm	± 2 dB		MCS6	-77 dBm	± 2 dB
	MCS7	22 dBm	± 2 dB		MCS7	-74 dBm	± 2 dB
	MCS8	28 dBm	± 2 dB		MCS8	-95 dBm	± 2 dB
	MCS9	28 dBm	± 2 dB		MCS9	-93 dBm	± 2 dB
	MCS10	28 dBm	± 2 dB		MCS10	-90 dBm	± 2 dB
	MCS11	28 dBm	± 2 dB		MCS11	-87 dBm	± 2 dB
	MCS12	27 dBm	± 2 dB		MCS12	-84 dBm	± 2 dB
	MCS13	25 dBm	± 2 dB		MCS13	-79 dBm	± 2 dB
	MCS14	23 dBm	± 2 dB		MCS14	-78 dBm	± 2 dB
	MCS15	22 dBm	± 2 dB		MCS15	-75 dBm	± 2 dB

Tabla 6-2 Sensibilidades en recepción frente a Tasas de transmisión. NanoStationM2

Fuente: Fabricante *Ubiquiti Networks*