FACULTAD DE INGENIERÍAS Y CIENCIAS AGROPECUARIAS

DISEÑO E IMPLEMENTACIÓN DE UNA RED MANET CON DISPOSITIVOS DE COMUNICACIÓN MÓVIL.

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieros en Electrónica y Redes de Información.

Profesor Guía

MSc. Jorge Wilson Granda Cantuña

Autores

Sebastián Marcelo Valencia Ayala

Erick Damián Risueño Benítez

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes orientando sus conocimientos y competencias para un eficiente desarrollo del tema elegido y cumpliendo con todas las disposiciones vigentes que regulan los Trabajos de titulación”

_____

Jorge Wilson Granda Cantuña

Máster en Ingeniería Eléctrica

C.I.: 1708594187

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber corregido este trabajo a través de reuniones periódicas con los estudiantes orientando sus conocimientos y competencias para un eficiente desarrollo del tema elegido y cumpliendo con todas las disposiciones vigentes que regulan los trabajos de titulación”

_____

Juan Andrés Vásquez Peralvo
Máster en Sistemas de Comunicación Inalámbrica
C.I.: 1717647588

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

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

_____	_____
Sebastián Marcelo Valencia Ayala	Erick Damián Risueño Benítez
C.I.: 1722488465	C.I.: 1720733789

AGRADECIMIENTO

A mis padres, que gracias a su sacrificio me han brindado la fuerza y la ayuda necesaria para culminar con mucha satisfacción mis estudios y forjarme como una persona de bien para la sociedad.

Un agradecimiento especial al Ingeniero Jorge Granda, quien con su guía y conocimiento se logró realizar esta tesis satisfactoriamente.

A mis compañeros de la universidad ya que sin ellos no se hubieran logrado tantos objetivos a lo largo de esta vida universitaria.

Sebastián Valencia.

AGRADECIMIENTO

Este proyecto es el resultado de varios años de esfuerzo los cuales han dejado experiencias y aprendizaje, quiero agradecer a mis padres, mi hermana y amigos que me han ayudado guiándome, apoyándome y haciendo que nunca decaiga en todo este camino para completar uno de mis objetivos más grandes; entendiendo que todo esfuerzo vale la pena al final.

Al Ingeniero Jorge Granda quien con paciencia y sabiduría supo guiar este proyecto para que se concluya con éxito.

Damián Risueño.

"La gratitud da sentido a nuestro pasado, trae paz al presente y crea una visión para el mañana."

DEDICATORIA

Este trabajo de titulación se la dedico a mis padres Marcelo y Narcisa, por ser los referentes en mi vida. Quienes con mucho sacrificio e incontables enseñanzas han sabido trazar un camino de rectitud y humildad.

Sebastián Valencia.

DEDICATORIA

Este proyecto lo dedico a mis padres quienes fueron la principal motivación para completar este gran objetivo, a mi hermana quien ha sido una guía muy importante en mi vida y a mis amigos y compañeros de Universidad quienes de una manera u otra han sido un apoyo para mí.

Damián Risueño.

"*El futuro mostrará los resultados y juzgará a cada uno de acuerdo a sus logros.*" – *Nikola Tesla*

RESUMEN

Debido al nuevo paradigma del internet de las cosas (IoT) y la necesidad de conectar cualquier objeto electrónico de manera inalámbrica en el hogar, campus universitarios, áreas de trabajo específicas, zonas de guerra o de catástrofes. Se debe pensar en otros mecanismos de interconexión en los que no siempre se dispondrá de una infraestructura fija, tomando en cuenta que existirán dispositivos u objetos que cambien de lugar, que desaparezcan o que se integren dinámicamente, así surge la idea de usar una red inalámbrica que permita solventar de manera adecuada las necesidades actuales de los usuarios; una de ellas es el uso de la red conocida como MANET.

Una red móvil Ad-Hoc o MANET (Mobile Ad-Hoc Network) es un sistema autónomo constituido por una cantidad "n" de nodos móviles, los cuales poseen propiedades de movilidad y auto-configuración que servirá para una conexión dinámica entre todos los nodos de la red, los mismos que se encuentran en iguales condiciones y se conectan para realizar actividades concretas. Esta igualdad de condiciones significa que no hay elementos que tengan funcionalidades específicas; es decir, pueden actuar como emisores y receptores indistintamente del tipo de dispositivo.

Este tipo de red se está convirtiendo cada vez más en una tecnología esencial para las comunicaciones inalámbricas debido al crecimiento en popularidad de los dispositivos móviles. Con los avances recientes en temas relacionados al rendimiento y movilidad, las tecnologías de computación y comunicaciones inalámbricas se expanden y puedan ser usados en diferentes tipos de aplicaciones. La visión de las redes móviles Ad-Hoc es apoyar el funcionamiento robusto y eficiente en las redes inalámbricas móviles mediante la incorporación de la funcionalidad de enrutamiento en los nodos que forman parte de la red.

ABSTRACT

Due to the new paradigm of the internet of things (IoT) and the need to connect any electronic object wirelessly whether at home, universities, specific work areas, war and catastrophes zones. It is necessary to think of other interconnection mechanisms in which fixed infrastructure will not always be available. We must also consider that there will be devices or objects that change places, disappear or are integrated dynamically. Therefore, arises the idea of using a Wireless network to adequately meet the current needs of users; one of them is the use of the network known as MANET.

An Ad-Hoc mobile network or MANET (Mobile Ad-Hoc Network) is an autonomous system consisting of an "n" number of mobile nodes which have mobility and self-configuration properties that will serve in a dynamic connection between all the nodes of the network, the same ones that are in equal conditions and are connected for a concrete activity. This equality of conditions means that there are no elements that have specific functionalities, for instance they can act as emitters and receivers regardless of the type of device.

This type of network is increasingly becoming an essential technology for wireless communications due to the growing popularity of mobile devices. With recent advances in topics related to performance and mobility, computer and wireless technologies in which this type of technology is expected to expand and be used in different types of applications. The vision of Ad-Hoc mobile networks is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into nodes that are part of the network.

ÍNDICE

Introducción

Alcance

El presente proyecto de titulación contempla la implementación de una red MANET con protocolos de comunicación dinámicos, utilizando sensores inalámbricos, aplicado a un escenario donde dichos sensores tengan movilidad. El objetivo general es el envío de datos en tiempo real en plataformas aéreas no tripuladas tomando en cuenta que el proyecto a realizarse será probado en plataformas terrestres las cuales servirán en un futuro para el desarrollo completo del proyecto macro donde se involucran más elementos entre ellos el uso de drones.

Para demostrar lo antes mencionado se usarán dispositivos conocidos como Raspberry Pi, los cuales van a servir como nodos de la red MANET, cada uno con los elementos necesarios para el funcionamiento independiente.

Justificación

Las redes MANET brindan una gran importancia a los elementos móviles que la conforman, así como el diseño e implementación de una pequeña red dotada de los elementos necesarios para su óptimo funcionamiento.

Estas redes pueden ser aplicadas para satisfacer diferentes necesidades de manera eficiente, rápida y remota, para el monitoreo de un área específica de territorio.

El presente proyecto presenta resultados y solventa los objetivos que se plantearon determinando el diseño, los protocolos de comunicación y los sensores más adecuados. Integrados para la realización del proyecto de titulación.

El proyecto es un aporte directo dentro de los campos de investigación que realiza el departamento de Redes y Telecomunicaciones y en general a la

Facultad de Ingeniería y Ciencias Agropecuarias de la Universidad de las Américas. Este proyecto cuenta con la información técnica necesaria para la implementación de futuras investigaciones en el campo de las redes inalámbricas.

Objetivos

Objetivo General

- Diseñar e implementar una red Mobile Ad-Hoc Network (MANET).

Objetivos específicos

- Realizar el estudio comparativo de dispositivos de comunicación móvil adaptables a plataformas terrestres con transmisión de datos en tiempo real.
- Procesamiento de señales, e identificación de nodos autenticados.
- Realizar pruebas de validación.

1. Capítulo I. Marco teórico

En este capítulo se presenta toda la información teórica necesaria para la implementación del proyecto.

1.1 Redes Inalámbricas

Las redes inalámbricas son redes que no se basan en una infraestructura de comunicación preexistente. Más bien, mantienen una topología de interconexión dinámica entre los usuarios móviles, este tipo de redes usan canales de radiofrecuencia como medio físico para la comunicación. Cada nodo en la red transmite información que puede ser recibida por todos los nodos dentro de su rango de transmisión directa. Puesto que los nodos transmiten y reciben a través del aire, estos no necesitan ser físicamente conectados a ninguna red. Por lo tanto, este tipo de redes ofrecen conectividad de datos junto con la movilidad del usuario.

Hoy en día están disponibles sistemas de comunicación muy avanzados. La radio y la televisión son algunas de las aplicaciones muy comunes que no pueden prescindir de las tecnologías inalámbricas. Se espera que las redes inalámbricas desempeñen un rol cada vez más importante en los futuros campos civiles y militares, donde el acceso inalámbrico a una red troncal cableada es ineficaz o imposible. (Murthy y Manoj, 2004, pp. 93)

En general, las redes inalámbricas se refieren al uso de señales infrarrojas o de radiofrecuencia para compartir información y recursos entre los dispositivos. Actualmente existe gran variedad de dispositivos inalámbricos disponibles; como, terminales móviles, PCs de bolsillo, PCs portátiles, teléfonos celulares, PDAs, sensores inalámbricos, entre otros. Debido a las diferencias encontradas en la capa física de estos sistemas, los dispositivos y redes inalámbricas muestran características distintas a las de sus homólogos de línea fija. Entre estas características tenemos:

- Mayor interferencia da lugar a menor fiabilidad.

  - Las señales infrarrojas sufren interferencia de fuentes de calor y luz solar, y pueden ser blindadas/absorbidas por varios objetos y materiales. Las señales de radio son generalmente menos propensas a ser bloqueadas; sin embargo, ellos pueden ser interferidos por otros dispositivos eléctricos.
  - La naturaleza de broadcast de medios de transmisión significa que todos los dispositivos están potencialmente interfiriendo entre sí.
  - Auto-interferencia debido a multipath.
- Disponibilidad de ancho de banda muy bajo y tasas de transmisión aún más bajas, en general mucho menos velocidad en comparación a las redes de telefonía fija, causando la degradación de la calidad del servicio, incluyendo mayor jitter, retrasos y tiempos más largos de la configuración de conexión.
- Condiciones de la red altamente variables:
  - Mayores tasas de pérdida de datos debido a la interferencia.
  - Movimiento del usuario causa frecuente desconexión.
  - Cambios en el canal dependiendo como los usuarios se mueven.
  - Potencia recibida disminuye con la distancia.
- Recursos limitados de energía y computación: limitada capacidad de procesamiento, memoria y tamaño del disco debido a la capacidad limitada de la batería, así como la limitación en el tamaño del dispositivo, peso y coso.
- Limitada cobertura del servicio.
  - Debido al dispositivo, distancia y limitaciones de la condición de red, el servicio de implementación para redes y dispositivos inalámbricos enfrenta muchas limitaciones y es más difícil en comparación con elementos y redes cableadas.
- Limitados recursos de transmisión.

  - Disponibilidad limitada de frecuencia con regulaciones restrictivas.
  - Espectro escaso y costoso.

- Limitación del tamaño del dispositivo debido a resultados de requisitos de portabilidad en interfaces de usuarios y pantallas.
- Seguridad más débil debido a que la interfaz de radio es accesible para todos, la seguridad de la red es más difícil de implementar ya que los atacantes pueden interactuar con mayor facilidad.

1.2 Tipos de redes inalámbricas

Existen muchos tipos de redes inalámbricas y se pueden clasificar de diversas maneras mencionando algunos a continuación dependiendo de varios criterios para su clasificación.

1.2.1 Por la formación de la red y la arquitectura

Las redes inalámbricas se pueden dividir en dos grandes categorías basados en cómo está construida la red y la arquitectura de la misma, así tenemos:

- Red basada en infraestructura
- Redes sin infraestructura (Ad Hoc)

1.2.2 Por el área de cobertura de comunicación

Como con las redes cableadas, las redes inalámbricas se pueden clasificar en diferentes tipos basados en las distancias sobre las cuales se transmiten los datos:

- Wireless Wide Area Networks (Wireless WANs)
- Wireless Metropolitan Area Networks (Wireless MANs)
- Wireless Local Area Network (Wireless LANs)

- Wireless Personal Area Network (Wireless PANs)

1.2.3 Por la tecnología de acceso

Según la norma específica, la frecuencia y el uso del espectro, las redes inalámbricas pueden ser clasificadas basándose en la tecnología de acceso utilizada. Estos incluyen:

- Redes GSM
- Redes TDMA
- Redes CDMA
- Redes Wi-Fi (802.11)
- Redes Hiperlan2
- Redes Bluetooth
- Redes Infrarrojas

Es así que las redes inalámbricas hoy en día se han vuelto parte fundamental del día a día de la humanidad. (Basagni, Conti, Giordano y Stojmenovic, 2004, pp. 22-25)

1.3 Redes Ad-Hoc

Una red ad hoc es una colección de nodos inalámbricos móviles (routers) que forman dinámicamente una red temporal sin el uso de cualquier infraestructura de red existente o administración centralizada. Los routers o nodos son libres de moverse aleatoriamente y organizarse arbitrariamente; por lo tanto, la topología de la red inalámbrica de puede cambiar rápidamente y de manera impredecible. Ad-Hoc puede operar de forma independiente, o puede estar conectado al internet. Uno de los mayores retos que tienen las redes Ad-Hoc es el diseño de los protocolos de enrutamiento adecuados ya que se debe tomar en cuenta varias características como: el multihop, la movilidad, el gran tamaño de la red combinada con la heterogeneidad del dispositivo, el ancho de banda y las limitaciones de potencia de la batería.

En la Figura 1 se muestra un ejemplo de topología de una red AD-HOC:

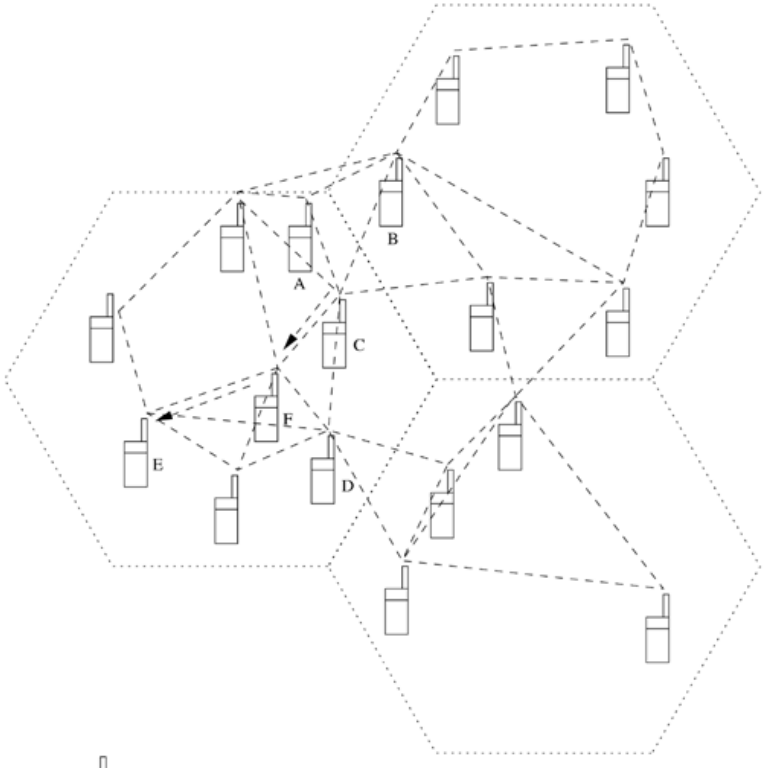


Figura 1. Redes Ad-Hoc

Tomado de Murthy y Manoj, 2004.

Las principales características de las redes Ad-Hoc son:

- Infraestructura de red no necesaria.
- No existen estaciones base.
- Rápido despliegue.
- Topologías de red altamente dinámicos con saltos múltiples (multihop).
- Ambiente hostil (ruido y pérdidas).
- Se adapta a cambios.
- Menor costo y menor tiempo de instalación. (Sarkar, Basavaraju y Puttamadappa, 2008, pp. 21-23)

1.3.1 Aplicaciones de las Redes Inalámbricas Ad Hoc

El campo de las redes inalámbricas surge de la integración de la informática personal, tecnología celular y la Internet. Esto es debido a la creciente interacción entre comunicación y computación, que está cambiando el acceso a la información de "en cualquier momento" a en "todo el tiempo, en todas partes." En la actualidad, existe una gran variedad de redes, que van desde la conocida infraestructura de redes celulares a redes inalámbricas ad hoc sin infraestructura existente. Las siguientes son algunas de las aplicaciones de las redes inalámbricas Ad Hoc:

- Red comunitaria
- Red empresarial
- Red doméstica
- Red de respuesta a emergencia
- Red de vehículos
- Red de sensores

Los nodos en una red ad hoc móvil son libres de moverse y organizarse en forma arbitraria. Cada usuario o nodo es libre de moverse mientras se está comunicando con otros. El camino entre cada par de usuarios puede tener múltiples enlaces y la radio entre ellos puede ser heterogénea. Esto permite una asociación de varios enlaces para ser una parte de la misma red. Las redes móviles ad hoc pueden funcionar de manera independiente o posiblemente podrían conectarse a una red más amplia como Internet.

Es apropiado usar las redes ad hoc en situaciones en las que una infraestructura no está disponible o implementarla si esta no es rentable. Uno de los muchos usos de las redes móviles ad hoc es en algunos entornos empresariales, dónde la necesidad de computación colaborativa podría ser más importante fuera del entorno de oficina que dentro. Una red móvil ad hoc también puede ser usada para proporcionar aplicaciones de servicios de gestión de crisis como en la recuperación ante desastres, dónde toda la

infraestructura de comunicación es destruida y recuperar rápidamente la comunicación es crucial. (Sarkar, Basavaraju y Puttamadappa, 2008, pp. 23-24)

1.4 Definición de MANET

Una red MANET (Mobile Ad-hoc Network), es una agrupación de nodos móviles, autónomos, que forman una red temporal sin verse en la necesidad de una administración centralizada o del uso de dispositivos de soporte como normalmente se ve en las redes convencionales. La característica más importante de este tipo de redes es su independencia de cualquier infraestructura fija, ya sea esta una estación base o un punto de acceso centralizado. Como funciones principales se tiene la determinación de la topología de red, acceso múltiple y el enrutamiento de datos sobre las rutas más adecuadas, siempre tomando en cuenta que las funciones antes mencionadas se deben realizar de forma distribuida. Estas tareas son particularmente difíciles debido al limitado ancho de banda disponible en un canal inalámbrico.

Al tener cada nodo generalmente un alcance de transmisión limitado, este busca la asistencia de nodos vecinos para el reenvío de paquetes y por lo tanto se puede afirmar que en este tipo de redes ad-hoc, los nodos pueden actuar como enrutadores y hosts a la vez. Esta propiedad importante de las redes MANET se la conoce como la capacidad multi-salto. Por ende cualquier nodo puede reenviar paquetes entre otros nodos, así como ejecutar aplicaciones de usuario.

Por su naturaleza este tipo de redes es adecuada para situaciones en donde no exista ninguna infraestructura fija o no sea posible el despliegue de una red convencional. Dando lugar a diferentes tipos de aplicaciones prácticas ya sea a nivel militar, catástrofes, etc. (Khosrow-Pour, 2005, PP.3090-3091)

En la figura 2 se muestra la topología clásica de una red MANET:

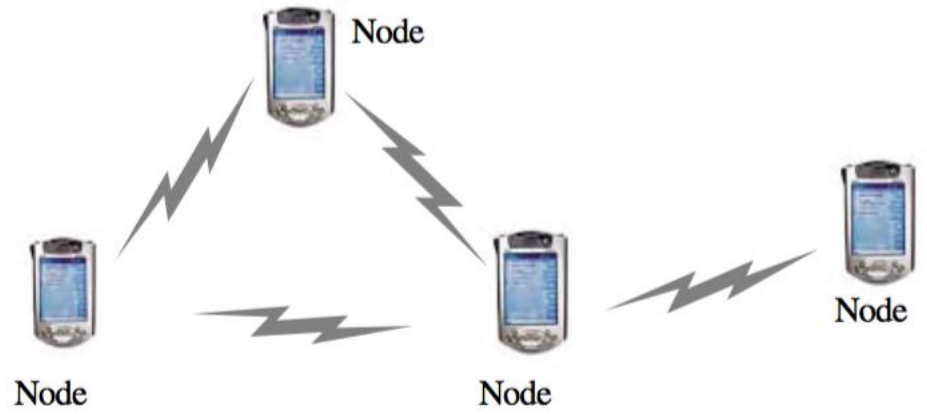


Figura 2. Nodos de una red MANET

Tomado de Khosrow-Pour, 2005

1.5 Escenarios y aplicaciones de MANET

Debido al incremento exponencial de dispositivos móviles en los últimos años, así como los avances en las tecnologías inalámbricas, las redes Ad Hoc han ganado gran importancia gracias al creciente número de aplicaciones para las cuales se las puede utilizar. Este tipo de redes pueden aplicarse en cualquier lugar y en cualquier momento, sin la necesidad de infraestructura y con redes muy flexibles. Las redes Ad Hoc facilitan las conexiones entre terminales, así como la habilidad de agregar o eliminar nodos desde y hacia la red. (Loo-Lloret-Hamilton, 2012, PP.8)

El conjunto de aplicaciones de redes MANET es variada, ya que van desde redes móviles altamente dinámicas y de gran escala, hasta redes pequeñas, que están restringidas por una potencia limitada. De igual manera se debe mencionar las aplicaciones que tienden a migrar de un entorno de infraestructura tradicional al contexto de las redes Ad Hoc debido a los beneficios que estas brindan. (Loo-Lloret-Hamilton, 2012, PP.8)

Las Aplicaciones típicas de este tipo de tecnologías se mencionan a continuación.

1.5.1 Aplicaciones Militares

En la actualidad los soldados de muchos ejércitos alrededor del mundo llevan algún tipo de equipamiento de cómputo. Las redes MANET pueden ser muy útiles para establecer la comunicación entre un grupo de soldados cumpliendo operaciones tácticas y también para las fuerzas armadas aprovechando la tecnología de red común que se tiene en Ad-Hoc para mantener comunicados a soldados, vehículos de guerra y otros equipos militares, con el cuartel general.

El otro factor importante que hace a las redes MANET muy importantes es el hecho de que los objetivos militares, tales como aviones, tanques y buques de guerra, que se mueven a alta velocidades requieren de una comunicación rápida y fiable que solo puede ser provista por una red MANET. (Loo, Lloret y Hamilton, 2012, PP.8)

Debido a que las aplicaciones militares requieren una comunicación muy segura a cualquier precio, los nodos montados en vehículos se asumen que son muy sofisticados y potentes. Pueden tener múltiples transcievers de alta potencia, cada uno con la capacidad de saltar entre diferentes frecuencias por razones de seguridad. Estos sistemas de comunicación se pueden suponer que están equipados con baterías de larga duración únicamente de uso militar y no para su uso comercial debido a los altos costos que conlleva su desarrollo. Pueden inclusive usar servicios de localización como es el caso del sistema global de posicionamiento (GPS) u otros servicios ofrecidos vía satélite para una comunicación y coordinación eficiente. (Murthy y Manoj, 2004, PP.210-211)

En resumen, la naturaleza principal de las comunicaciones militares impone ciertos requisitos importantes en las redes móviles ad hoc, por mencionar algunos de ellos: confiabilidad, eficiencia, comunicación y soporte que son

necesarios para el enrutamiento en multicast. (Murthy y Manoj, 2004, PP.210-211)

En la figura 3 se muestra el uso de una red MANET en aplicaciones militares en donde se interconectan múltiples nodos:

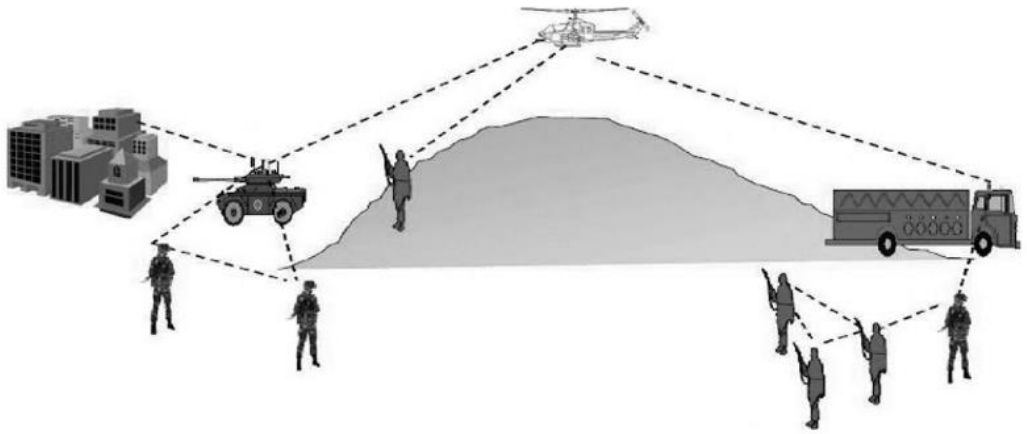


Figura 3. MANET en Aplicaciones Militares.

Tomado de Loo-Lloret-Hamilton, 2012

1.5.2 Aplicaciones de Emergencia

Las redes MANET son muy útiles en operaciones de emergencia, ya sea en búsqueda y rescate, control de multitudes y operaciones de comando. Los principales factores que favorecen las redes móviles ad hoc para tales tareas son: auto-configuración del sistema con una sobrecarga mínima, independencia de la infraestructura fija o centralizada existente en la zona, poca importancia de la naturaleza del terreno para su implementación, libertad y flexibilidad de movilidad y la falta de infraestructura de comunicación convencional. En entornos en donde los servicios de comunicación que se basan en infraestructuras tradicionales se destruyen debido a una guerra o desastres naturales tales como terremotos, MANET sería una buena solución

para la coordinación de las diferentes actividades de rescate que se realicen en las áreas afectadas.

Puesto que las redes móviles ad hoc, tienen requisitos de configuración mínimas para empezar su funcionamiento, muy poco o casi ningún retraso está implicado en el montaje de dicha red y que esta esté totalmente operativa. Los escenarios que se mencionaron anteriormente suceden de manera inesperada, y en la mayoría de casos son inevitables y pueden afectar a un gran número de personas. Las redes ad hoc que son aprovechadas en estas instancias deben ser distribuidas y escalables para un gran número de nodos y también deben ser capaces de proporcionar vías de comunicación tolerante a fallos. La capacidad de comunicación en tiempo real es fundamental para este tipo de catástrofes debido que se debe usar constantemente la comunicación por voz para coordinar las acciones que se tengan que llevar a cabo. (Sarkar, Basavaraju y Puttamadappa, 2008, PP.297-298)

En la figura 4 se muestra el uso de una red MANET para aplicaciones de Emergencia:

Figura 4. MANET en aplicaciones de emergencia.

Tomado de Loo-Lloret-Hamilton, 2012

1.5.3 Aplicaciones de salud

El intercambio de información multimedia ya sea esta de audio, video y datos entre un paciente y los centros de salud es muy útiles en situaciones críticas de emergencia. Una persona que está siendo transportado a un hospital en una ambulancia puede intercambiar información a través del uso de redes de comunicación móviles ad hoc. Un profesional de la salud, en muchas situaciones, puede aprovechar de esta tecnología para dar un mejor diagnóstico y poder preparar un plan de tratamiento ya que el medico obtiene no solo información de audio sino también de video y datos. Por ejemplo, la información de video puede ser de gran utilidad en la evaluación de los reflejos del paciente, así como poder observar la capacidad de coordinación de la persona. Del mismo modo, el nivel de las lesiones de un paciente se pude establecer de mejor manera con la información visual que con otro tipo de información descriptiva solo de audio u de otro tipo.

Ecografías en tiempo real de los diferentes órganos de un paciente como pueden ser riñones, corazón u otros, y poder preparar un tratamiento adecuado para un paciente que está siendo transportado a un hospital. Dicha información puede ser transmitida a través de redes MANET o algún otro tipo de comunicaciones inalámbricas, la convergencia que es generada a través de las redes móviles ad hoc permite la conexión oportuna del personal adecuado de la casa de salud, así como hospitales y ambulancias.

Las redes móviles ad hoc establecidas dentro de una casa inteligente, también pueden ser útiles para el segmento de pacientes enfermos. Tales casas pueden ser capaces de tomar algunas decisiones básicas que se basen en información intercambiada entre varios sensores que participen en la red ad hoc. De este tipo de implementación se ven beneficiados de manera directa las personas de la tercera edad, ya que ellos requieren de un control más especializado para el cuidado de su salud.

Algunas de las acciones que pueden tomar las casas inteligentes incluyen el monitoreo de los patrones de movimiento dentro de una casa, reconocimiento

de una caída de una persona, reconocimiento de alguna situación inusual e informar a un organismo competente que pueda proporcionar la ayuda apropiada, de ser necesario. Cabe recalcar que los ejemplos mencionados anteriormente se los va poder llevar a cabo dependiendo de los sensores que estén implementados en dichas casas. (Sarkar, Basavaraju y Puttamadappa, 2008, PP.299)

1.5.4 Aplicaciones de ambiente académico

La mayoría de las instituciones educativas ya cuentan con redes de comunicación inalámbrica o están en un proceso de establecer dicho tipo de instalaciones. Tal escenario proporciona a los estudiantes y profesores un ambiente conveniente para interactuar y lograr los objetivos que se establezcan al principio de cada periodo educativo. Las redes inalámbricas ad hoc pueden realzar los escenarios de conectividad y añadir muchas otras características que sean atractivas para los usuarios, que en este caso son estudiantes y docentes de los planteles educativos. Por ejemplo, una red MANET puede establecerse entre los estudiantes y el docente que estén matriculados en una clase proporcionando de manera fácil y conveniente una distribución, por parte del docente, de folletos o alguna tarea en clase y también para los estudiantes que puedan presentar sus tareas y trabajos. El intercambio de información entre los participantes se facilita de manera considerable. (Sarkar, Basavaraju y Puttamadappa, 2008, PP.299-300)

1.5.5 Aplicaciones en entornos industriales

La mayoría de las empresas o industrias disponen ya de redes de comunicaciones inalámbricas, especialmente en entornos de manufactura. Las instalaciones de manufactura por lo general tienen numerosos dispositivos electrónicos que están interconectados. Tomando en cuenta que las conexiones de muchos de estos dispositivos suelen ser cableadas conduciendo así a ocupar espacio necesario y en ciertos casos a estorbar, lo que no solo

plantea riesgos para la seguridad sino también afectan de manera considerable la fiabilidad de la empresa. El uso de redes inalámbricas elimina muchas de estas preocupaciones.

Si la conectividad se la realiza a través de una red MANET, esta añade muchos aspectos atractivos, incluyendo la movilidad. Los dispositivos pueden ser trasladados fácilmente y se pueden reconfigurar las redes basados en las necesidades de movilidad que puedan surgir con el crecimiento continuo de la empresa. Brinda escalabilidad. (Sarkar, Basavaraju y Puttamadappa, 2008, PP.300)

1.6 Caracterisiticas de las Redes MANET

Las redes móviles ad hoc (MANET) disponen de las siguientes características que son necesarias al momento de sugerir o diseñar una solución en este tipo de paradigma.

- **Operación distribuida:** MANET tiene una característica de operación distribuida, en la cual cada nodo funciona de manera independiente y no hay un servidor centralizado o computadora para administrar la red. En su lugar, el trabajo se distribuye entre todos los nodos que se encuentren operativos al momento de la implementación de la red. Cada nodo trabaja en cooperación con los otros nodos para implementar las funciones ya sean estas de seguridad y enrutamiento.
- **Bajo consumo energético:** Otra característica de las redes MANET es el bajo consumo de energía, por lo que se pueda implementar dicha red fácilmente con dispositivos móviles los cuales no disponen de grandes baterías. Al ser estas baterías un recurso limitado, los nodos móviles tienen que utilizar la energía de manera eficiente y esto se logra gracias a los diferentes protocolos de comunicación que optimizan este recurso al máximo.
- **Seguridad:** La seguridad en este tipo de redes es la preocupación más importante, debido a que los nodos y a la información transmitida en

MANET no se encuentran protegidas de amenazas como, por ejemplo, ataques de negación de servicio, eavesdroping, suplantación de identidad (spoofing), entre otros. Al ser utilizados en este tipo de redes dispositivos móviles implica un riesgo de seguridad más alto comparado con dispositivos que operan de manera fija, debido a que los dispositivos portátiles pueden ser robados o el tráfico que generen puede cruzar enlaces inalámbricos de manera insegura y durante ese transcurso puedan ser interceptada la información que se transmite.

- **Topología Dinámica:** En MANET la topología de red siempre está cambiando porque los nodos de la red ad hoc alteran sus posiciones ya que son libres de moverse a cualquier lugar. Por lo tanto, los dispositivos de una red móvil ad hoc deben soportar topologías dinámicas. La movilidad de los nodos crea desconexiones frecuentes; por lo tanto se debe hacer frente a este problema y procurar que la red MANET pueda adaptarse a las nuevas condiciones de tráfico y transmisión de acuerdo a los patrones de movilidad que se tengan preestablecidos.
- **Ventajas:** Una red MANET dispone de varias ventajas con respecto a otras redes inalámbricas, incluyendo facilidad de instalación, velocidad de implementación y disminución de dependencias de una infraestructura fija. Las redes móviles Ad Hoc proporcionan un gran interés debido a la capacidad de formar una red de manera instantánea sin la presencia de estaciones base fijas ni llevar una administración del sistema. (Loo, Lloret y Hamilton, 2012, PP.9-10)

1.7 Seguridad en redes MANET

En MANET, la seguridad es uno de los temas más importantes ya que estas redes son más vulnerables a los ataques, inclusive mucho más que otras redes inalámbricas y de las redes cableadas. El diseño de un protocolo seguro en MANET es una tarea complicada debido a que este tipo de redes comparten un canal de radiofrecuencia sin protección, carecen de una autoridad central (nodo

central) y de mecanismos de asociación para usuarios y tienen limitados recursos y vulnerabilidades físicas. (Loo, Lloret y Hamilton, 2012, PP.241)

La investigación sobre la seguridad de las redes móviles ad hoc todavía está en su etapa temprana. Las propuestas existentes son típicamente orientadas a la identificación y análisis de varias amenazas de seguridad y posteriormente mejorar los protocolos ya existentes o se propone un nuevo protocolo para frustrar las amenazas de ataque. En cada paso de la operación del protocolo, el diseño se asegura de que todos los procedimientos realizados sigan el camino correcto. Cualquier procedimiento que se desvié de las operaciones validas, los protocolos lo deben tratar con la debida precaución. Inclusive cada vez que el sistema detecte una operación inconsistente, este pueda lanzar una alerta para las verificaciones adicionales que sean necesarias.

La solución también puede tomar un enfoque de seguridad colaborativa, que se basa en los múltiples nodos que una red MANET puede tener para proporcionar seguridad. A pesar de que se considera que ningún nodo solo por su cuenta es de plena confianza, solo un grupo de nodos se confiara colectivamente, este grupo de nodos pueden estar situados en un entorno de red local o a lo largo de una ruta de envío. (Sarkar, Basavaraju y Puttamadappa, 2008, PP.302-304)

Un estudio exhaustivo de la seguridad en MANET implica el análisis detallado de la seguridad para cada capa de esta arquitectura. Tal como se indica a continuación:

- **Capa Aplicación:** En esta capa, los temas de interés se basan en aplicaciones vulnerables que son ejecutadas en la máquina del usuario, en donde se podrían encontrar virus, gusanos y otros códigos maliciosos.
- **Capa de Transporte:** Esta capa autentica y asegura la comunicación end-to-end mediante el cifrado.
- **Capa de red:** La capa de red protege el enrutamiento de protocolos y paquetes de envío.

- **Capa enlace de datos:** La funcionalidad de esta capa es la de proteger el control de acceso al medio (MAC) y de proporcionar apoyo de seguridad para conectar protocolos que vengan de la capa de red.
- **Capa Física:** Esta capa previene los ataques de interferencia que buscan causar es la negación o deterioro de los servicios que se puedan ofrecer sobre una red MANET.

1.8 Protocolos de Enrutamiento en redes MANET

Dentro de una red existen varias rutas generalmente para la transmisión de un paquete desde un origen a un nodo de destino. El objetivo de un protocolo de enrutamiento es encontrar una o más rutas óptimas de una lista de posibilidades, reduciendo así la función de costo. (Frikha 2011, pp. 23)

En el trabajo realizado por la IETF sobre MANET, rápidamente se identificaron distintas familias de protocolos. En ese caso, cada protocolo puede ser clasificado como reactivos, proactivos o híbridos.

En la figura 5 se indica el enrutamiento dinámico de una red MANET.

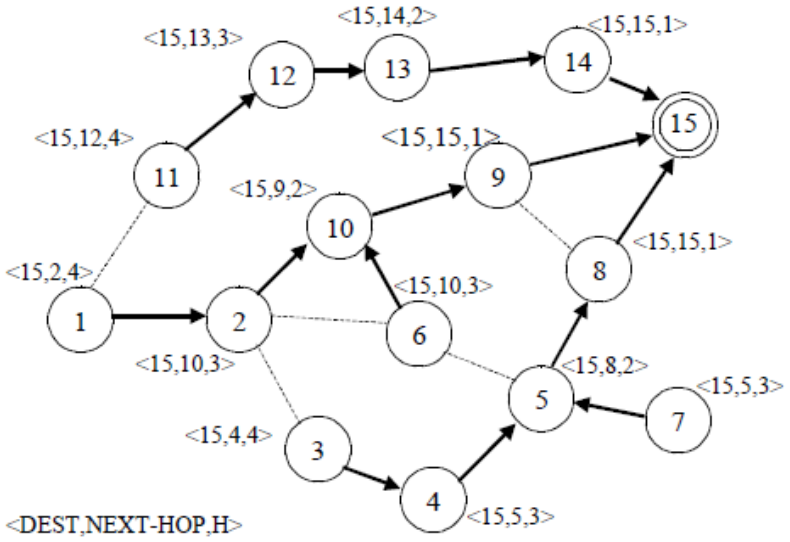


Figura 5. Ejemplo de enrutamiento en una red MANET

Tomado de Beraldi y Baldoni, 2003

1.9 Protocolos de Enrutamiento Proactivos (Basados en Tablas)

Estos protocolos son los sucesores de los protocolos vector-distancia y de estado de enlace. Los protocolos proactivos mantienen tablas de enrutamiento que contiene información sobre la topología de la red. La principal desventaja de éste tipo de protocolo es la señalización, la cual puede tener un efecto negativo sobre el ancho de banda que se esta manejando en la red. La ventaja es que una ruta de origen a destino siempre está disponible sin tener que recurrir a los mecanismos de búsqueda de ruta. Sin embargo, los protocolos de enrutamiento proactivos tienen ciertas deficiencias en casos de frecuente y rápido desarrollo topológico dentro de la red, o cuando la red es relativamente grande. (Frikha, 2011, pp. 20)

En este tipo de protocolos de enrutamiento, los nodos evalúan continuamente las rutas a todos los nodos alcanzables e intentan mantener constante y actualizada información de enrutamiento. Por lo tanto, un nodo de origen puede obtener un camino de enrutamiento de inmediato si necesita uno. Es así que en este tipo de protocolos todos los nodos necesitan mantener una consistente vista de la topología de la red. Cuando ocurre un cambio en la topología de la red, las respectivas actualizaciones deben ser propagadas por toda la red para notificar el cambio. La mayoría de los protocolos de enrutamiento proactivos propuestos para redes MANET han heredado propiedades de los algoritmos utilizados en las redes cableadas. (Sarkar, Basavaraju y Puttamadappa, 2008, pp.68)

Los principales mecanismos adoptados en protocolos proactivos son los siguientes:

- Incrementando la cantidad de información almacenada en cada nodo (para evitar bucles y acelerar la convergencia de protocolo).
- Variando dinámicamente el tamaño de ruta de actualizaciones o la frecuencia de actualización.
- Optimizando el flooding de la red.
- Combinando las características de DV y LS.

Es así que a continuación se mencionará a los protocolos más importantes en cada clasificación. Entre los protocolos de enrutamiento proactivos más importantes se tiene:

- WRP
- DSDV
- OLSR (Optimized Link State)
- FSR
- HSR
- TBRF (Topology Broadcast Reverse Forwarding)

1.9.1 WRP (Wireless Routing) Protocol

Es un protocolo de enrutamiento unicast proactivo para redes MANET. WRP utiliza un algoritmo de enrutamiento mejorado Vector-Distancia de Bellman-Ford, además pertenece a la clase general de Path-Finding Algotithms (PFA), que se define como el conjunto de algoritmos de la ruta más corta distribuidos que calculan las rutas que utilizan la información con respecto a la longitud y el segundo a último salto (predecesor) del camino más corto a cada destino. Los algoritmos PFA eliminan el problema del conteo a infinito del algoritmo de Bellman-Ford Distribuido (DBF - Distributed Bellman-Ford Algorithm). WRP también aborda el problema de evitar bucles a corto plazo que aún pueden estar presentes en este tipo de algoritmos especificadas por el nodo predecesor. El protocolo utiliza las siguientes cuatro estructuras de datos:

- Tabla de Distancia.
- Tabla de Enrutamiento.
- Tabla de Costo-Enlace.
- Lista de Mensaje de Retransmisión (MRL). (Beraldi y Baldoni, 2003, pp.138)

En WRP, los nodos móviles intercambian las tablas de enrutamiento con sus vecinos mediante mensajes de actualización. Los mensajes de actualización se pueden enviar de forma periódica o cuando ocurren cambios de estado de enlace. El MRL contiene información acerca de que vecino no ha reconocido un mensaje de actualización. Si es necesario, el mensaje de actualización vuelve a ser transmitido al vecino. Además, si no hay ningún cambio en su tabla de enrutamiento desde la última actualización, se requiere que un nodo envíe un mensaje de “Hello” para asegurar la conectividad. Al recibir un mensaje de actualización, el nodo modifica su tabla de distancias y busca mejores rutas de enrutamiento de acuerdo con la información actualizada. (Sarkar, Basavaraju y Puttamadappa, 2008, pp.69)

1.9.2 DSDV (Destination-Sequenced Distance Vector) Protocol

DSDV es un protocolo de enrutamiento unicast proactivo para MANET. Como WRP, DSDV también se basa en el tradicional algoritmo de Bellman-Ford. Sin embargo, sus mecanismos para mejorar el rendimiento de enrutamiento en redes MANET son muy diferentes. Los elementos clave de DSDV son:

1. Un mecanismo basado en una secuencia de números que se incrementa monótonamente, que indica la frescura de la ruta y que se utiliza para evitar bucles de enrutamiento y el problema del conteo a infinito.
2. El uso de actualizaciones de ruta completas, enviando periódicamente cada intervalo de actualización o enviando actualizaciones de ruta incrementales en los cambios topológicos.
3. El retraso de actualizaciones de ruta para las rutas que suelen ser inestables, es decir, aquellos para los que una nueva actualización está en camino hacia un nodo.

En las tablas de enrutamiento de DSDV, una entrada almacena el siguiente salto hacia un destino, la métrica de coste para el camino de enrutamiento para el destino y un número de secuencia del destino que es creado por el destino. Los números de secuencia son usados en DSDV para distinguir rutas obsoletas

de rutas nuevas y así evitar la formación de bucles de ruta. Las actualizaciones de ruta de DSDV pueden ser conducidas por tiempo o por eventos. Cada nodo transmite periódicamente actualizaciones, incluyendo su información de enrutamiento, a sus vecinos inmediatos. Mientras se produce un cambio significativo desde la última actualización, un nodo puede transmitir su tabla de enrutamiento cambiada en un estilo activado por eventos. Por otra parte, el protocolo DSDV tiene dos formas para enviar actualizaciones de tabla de enrutamiento. Uno es el tipo de actualización full-dump" en el que la tabla de enrutamiento completa es incluida dentro de la actualización. Una actualización incremental, por el contrario, contiene sólo las entradas con las métricas que se han cambiado desde que se envió la última actualización. Además, la actualización incremental cabe en un paquete. (Sarkar, Basavaraju y Puttamadappa, 2008, pp.72)

1.9.3 Optimized Link State Routing (OLSR) Protocol

OLSR es una optimización del clásico protocolo de estado-enlace, adaptado para redes ad hoc móviles (MANET), este intercambia información con otros nodos de la topología de la red regularmente. La idea clave de OLSR es el uso de nodos de retransmisión multipunto (MPR) para inundar la red de una manera eficiente mediante la reducción de paquetes duplicados en la misma región. En OLSR, únicamente los nodos seleccionados como MPRs, son responsables de controlar el tráfico de reenvío, destinado a la difusión en toda la red. MPR proporcionan un mecanismo eficiente para inundar el tráfico de control mediante la reducción del número de transmisiones requeridas. Los nodos, seleccionados como MPRs, también tienen una responsabilidad especial cuando se declara la información de estado de enlace en la red. De hecho, el único requisito de OLSR para proporcionar rutas de camino más cortas a todos los destinos es que los nodos de MPR declaran información de estado de enlace para sus selectores MPR.

Los nodos que han sido seleccionados como relés multipuntos por algunos nodos vecinos anuncian esta información periódicamente en sus mensajes de

control. Por lo tanto, un nodo anuncia a la red que tiene acceso a los nodos que ha seleccionado como un MPR. En el cálculo de ruta, los MPRs se utilizan para formar la ruta desde un nodo dado a cualquier destino en la red. Además, OLSR utiliza los MPRs para facilitar el flooding eficiente de mensajes de control en la red.

Un nodo selecciona MPRs de entre sus vecinos con un salto (es decir, bidireccional) de vínculos "simétricos". Por lo tanto, seleccionar la ruta a través de MPRs automáticamente evita los problemas asociados con la transferencia de paquetes de datos sobre enlaces unidireccionales (tales como el problema de no conseguir acuses de recibo de capa de enlace de paquetes de datos en cada salto, para capas de enlace que emplean esta técnica para el tráfico de unidifusión).

Una de las ventajas que más sobresale en OLSR es su diseño el cual hace que este protocolo trabaje de una manera completamente distribuida y no necesite de ninguna entidad central. En OLSR no se necesita de una transmisión segura ya que cada nodo que forma parte de la red se encarga de enviar mensajes de control de una manera periódica, así puede existir una pérdida bastante razonable de algunos mensajes. También, OLSR no requiere la entrega secuenciada de mensajes. Cada mensaje de control contiene un número de secuencia, que se incrementa para cada mensaje. Así, el destinatario de un mensaje de control puede, si es necesario, identificar fácilmente qué información es más reciente, incluso si los mensajes han sido reordenados en la transmisión. Además, OLSR proporciona soporte para las extensiones de protocolo como operación en modo sleep y enrutamiento multicast. Estas extensiones pueden introducirse como adiciones al protocolo sin romper hacia atrás la compatibilidad con versiones anteriores. OLSR no requiere cambios en el formato de los paquetes de protocolo Internet (IP). Así, cualquier pila IP existente puede utilizarse tal como está; el protocolo sólo interactúa con la gestión de la tabla de enrutamiento.

En la figura 6 se muestra el diagrama de funcionamiento del protocolo OLSR:

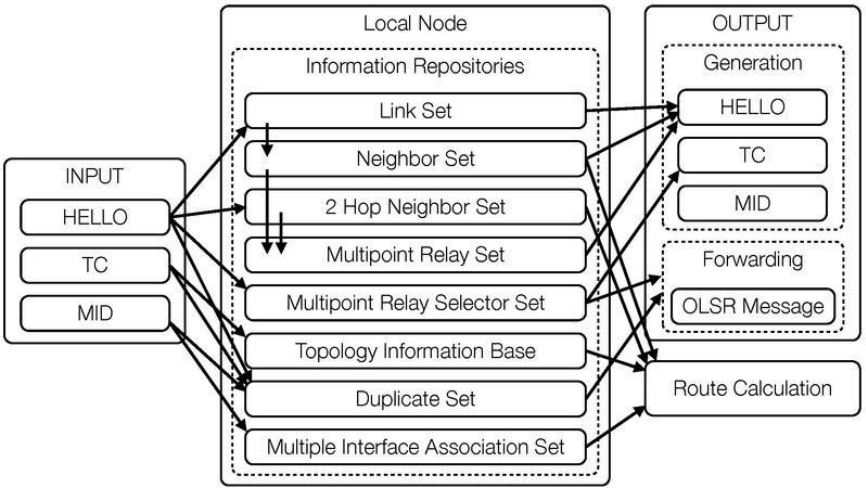


Figura 6. Diagrama de flujo de datos OLSR.

Tomado de Sarkar, Basavaraju y Puttamadappa, 2008

En la figura 7 se muestra la selección del nodo MPR y como el mismo realiza el proceso de flooding en la red:

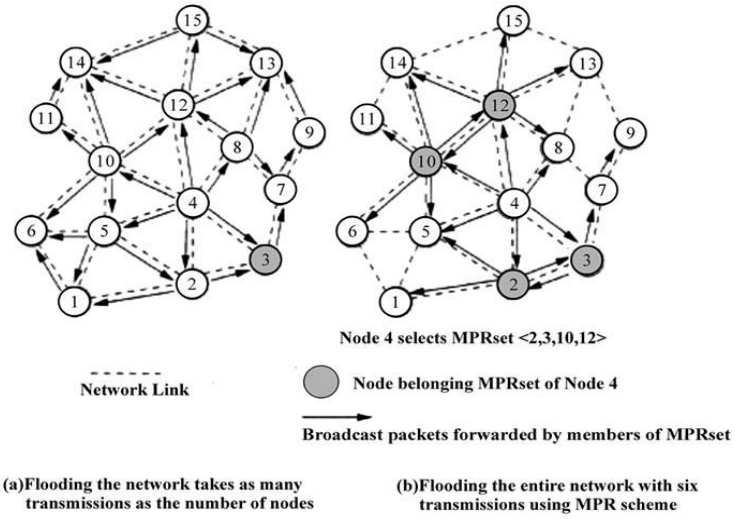


Figura 7. Selección nodos MPR.

(a) El flooding en la red toma tantas transmisiones como el número de nodos.

(b) El flooding de toda la red con seis transmisiones mediante esquema de MPR.

Tomado de Enneya, Oudidi y Elkoutbi, 2009.

1.9.3.1 Multipoint Relays (MPRs)

La idea de relés multipunto (MPRs) es reducir los mensajes de flooding enviados a todos los nodos de la red evitando así la redundancia de retransmisiones. Cada nodo de la red selecciona un conjunto de nodos en su zona simétrica de un solo salto, que puede retransmitir sus mensajes. Este conjunto de nodos vecinos seleccionados se llama el conjunto MPR de ese nodo. Los vecinos del nodo N que no están en su conjunto MPR reciben y procesan mensajes de difusión, pero no retransmiten los mensajes de difusión recibidos del nodo N. Cada nodo selecciona su conjunto MPR de entre sus vecinos simétricos de un salto. Este conjunto se selecciona de tal manera que cubre (en términos de alcance de radio) todos los estrictos nodos simétricos de dos saltos. El conjunto MPR de N, denotado como MPR (N), es entonces un subconjunto arbitrario de la simétrica zona de un salto de N que satisface la siguiente condición: cada nodo de la estricta zona de dos saltos simétrica de N debe tener una relación simétrica hacia MPR (N). Cuanto más pequeño es un conjunto MPR, menos tráfico de control superior resulta del protocolo de enrutamiento. Cada nodo mantiene información sobre el conjunto de vecinos que han seleccionado este como un MPR. Este conjunto se llama el "conjunto selector MPR" de un nodo. Un nodo obtiene esta información de los mensajes periódicos “Hello” recibido de los vecinos. Al recibir esta información del selector MPR, cada nodo calcula y actualiza su ruta a cada destino. Por lo tanto, la ruta es una secuencia de saltos a través de los relés multipuntos desde origen a destino.

1.9.3.2 Algoritmo de selección MPR

El cálculo del MPR con tamaño mínimo es un problema completo de NP. Para ello, el algoritmo de selección MPR estándar actualmente utilizado en las implementaciones del protocolo OLSR es el siguiente:

Para un nodo x, sea $N(x)$ el vecindario de x. $N(x)$ es el conjunto de nodos que están en el rango de x, los cuales comparten con x un enlace bidireccional. Se denota $N2(x)$ el vecindario 2 de x, es decir, el conjunto de nodos que son vecinos de al menos un nodo de $N(x)$ pero que no pertenecen a $N(x)$. Basándose en las notaciones anteriores, el algoritmo estándar para la selección de MPR se define de la siguiente manera:

1. $U \leftarrow N^2(x)$ **(Ecuación 1)**
2. $MPR(x) \leftarrow \emptyset$ **(Ecuación 2)**
3. $while\ \exists v : v \in U\ \wedge\ \exists! w \in N(x) : v \in N(w) do$ **(Ecuación 3)**
    a) $U \leftarrow U - N(w)$
    b) $MPR(x) \leftarrow MPR(x) \cup \{w\}$
4. $while(U \neq \emptyset) do$ **(Ecuación 4)**
    a) $choose\ w \in N(x) such\ as: CRITERIA(w) = |N(w) \cap U| = \max(|w \cap U| : w \in N(x))$
    b) $U \leftarrow U - N(w)$
    c) $MPR(x) \leftarrow MPR(x) \cup \{w\}$
5. $return\ MPR(x)$ **(Ecuación 5)**

En la figura 8 se muestra un ejemplo del calculo realizado para la selección del nodo MPR.

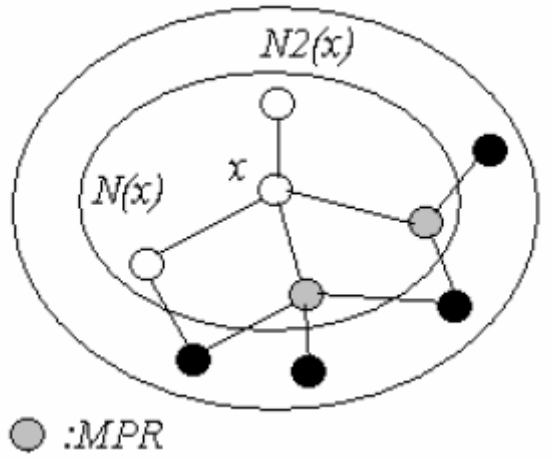


*Figura 8***.** Ejemplo de cálculo de MPRset.
Tomado de Enneya, Oudidi y Elkoutbi, 2009.

1.9.3.3 Grado de movilidad del nodo propuesto

Cada nodo en una red móvil ad-hoc puede encontrarse en cuatro estados con sus nodos vecinos: el nodo se mueve y sus vecinos están estáticos, el nodo está estático y sus vecinos se mueven, el nodo y sus vecinos se mueven, el nodo y sus vecinos están estáticos. En consecuencia, estos cuatro posibles estados dan lugar a un cambio del estado del enlace del nodo con sus vecinos. Por lo tanto, a medida que los nodos se mueven en la red móvil ad-hoc, el estado del enlace cambia en el tiempo.

Basado en esta observación, se define una medida de movilidad que representa el grado de movilidad del nodo en la red. Esta medida de movilidad no tiene ninguna unidad y no depende de artefactos de simulación como parámetros del modelo de movilidad o patrones de movimiento. Por otra parte, su evaluación se realiza en intervalos de tiempo discretos. Se define el grado de movilidad de un nodo móvil i en un tiempo t por la siguiente fórmula:

$$M_i^{\lambda}(t) = \lambda \frac{NodesOut(t)}{Nodes(t-\Delta t)} + (1-\lambda)\frac{NodesIn(t)}{Nodes(t)} \qquad \textbf{(Ecuación 6)}$$

Dónde:

$NodesIn(t)$: El número de nodos que se unieron al rango de comunicación de i durante el intervalo $[t-\Delta t, t]$.

$NodesOut(t)$: El número de nodos que salieron del rango de comunicación de i durante el intervalo $[t-\Delta t, t]$.

$Nodes(t)$: El número de nodos in el rango de comunicación de i en el tiempo t.

λ: El coeficiente de movilidad entre 0 y 1 definido por adelantado.

Este grado de movilidad del nodo se cuantifica localmente e independientemente de la localización de un nodo dado en la red. Se representa esta cuantificación local y relativa por el cambio de los vecinos de cada nodo. El grado de movilidad del nodo en un tiempo dado t para el nodo i en la red móvil ad-hoc se define como el cambio en sus vecinos en comparación con el estado anterior en el momento $t-\Delta t$. Por lo tanto, los nodos móviles que se unen y/o dejan a los vecinos de un nodo i sin duda

tendrán un impacto en la evaluación de su grado de movilidad. Además, se eligió el coeficiente de movilidad λ entre 0 y 1 para tener el grado de movilidad del nodo en el intervalo [0,1].

Para ilustrar, se ha tomado un ejemplo cuando el nodo está en el estado mostrado en la Figura 11(a) con 10 vecinos, y durante el intervalo Δt, sus vecinos sufrirán los cambios de estado mostrados en la Figura 11(b): cuatro nodos (de color azul) dejarán el rango de comunicación, y dos nodos (de color rojo) se unirán a este. En consecuencia, el nodo estará después de Δt (en el tiempo t) en el estado (Figura 11(c)) con seis cambios. Al final de cada intervalo de tiempo, el nodo será capaz de hacer una evaluación del cambio de sus vecinos representados por esta movilidad relativa, que en este ejemplo es igual a 13/40 = 32,5% (con λ = 1/2).

Cada de la red móvil ad-hoc puede realizar una evaluación autónoma y automática de su movilidad a intervalos de tiempo regulares (esta evaluación se puede realizar periódicamente mientras intercambia los mensajes Hello). Además, el cálculo y el recalculo de la movilidad del nodo es rápido y no requiere suficiente consumo de recursos (CPU y memoria).

En la figura 9 se muestra el análisis del grado de movilidad de la red usando dicho protocolo:

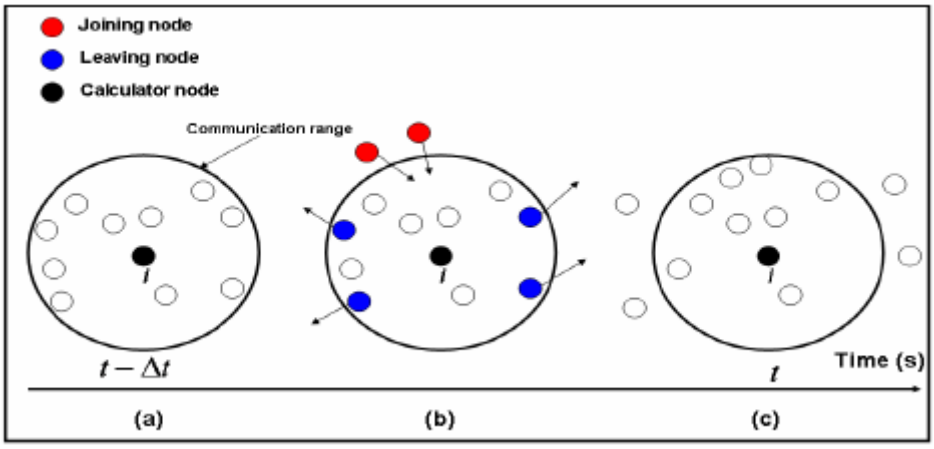


Figura 9. Cuantificación del grado de movilidad de la red.
Tomado de Enneya, Oudidi y Elkoutbi, 2009.

1.9.3.4 Mejora

La movilidad es un problema crucial en MANET, y hasta ahora, la mayoría de los protocolos de enrutamiento han mostrado algunas debilidades para hacer frente a una alta movilidad en algunas partes de la red. El objetivo consiste en utilizar positivamente la movilidad, para adaptar y mejorar el desempeño del protocolo OLSR.

a. Estimación de movilidad de enlaces

Algunos experimentos OLSR muestran que los enlaces deben ser más estables y menos móviles para evitar conexiones frágiles que implica la pérdida de datos y cambios frecuentes de ruta. El protocolo OLSR mantiene constantemente las rutas más cortas para llegar a todos los destinos posibles de la red. Por lo tanto, es más prudente estimar la calidad de los enlaces antes de agregarlos en la información topológica que sirve para calcular las mejores rutas. La calidad de un enlace puede estimarse basándose en la potencia de la señal recibida. Esta información es proporcionada por algunas tarjetas inalámbricas. Si esta información no está disponible, el protocolo OLSR estima la calidad del enlace en función del número de mensajes de control perdidos. Se puede detectar un fallo de enlace utilizando la caducidad del temporizador o la capa de enlace que informa a las capas superiores del fallo con un nodo vecino después de alcanzar el número máximo de reintentos. Con el objetivo de estimar la calidad de los enlaces en términos de movilidad, se define la movilidad de un enlace L entre dos nodos A y B como la movilidad media de los nodos implicados (ver Figura 12), como se muestra en la siguiente ecuación:

$$M^{\lambda}_{L(A,B)} = \frac{M^{\lambda}_{A}(t)+M^{\lambda}_{B}(t)}{2} \qquad \textbf{(Ecuación 7)}$$

En la figura 10 se muestra el porcentaje total de movilidad de un enlace punto a punto:

Figura 10. Movilidad del enlace $L(A,B)\ is\ (40\% + 50\%)/2 = 45\%$.
Tomado de Enneya, Oudidi y Elkoutbi, 2009.

Esta evaluación de la movilidad del enlace por sí sola no es significativa, ya que se puede tener un valor normal de la movilidad del enlace con un alto valor de movilidad de uno de los nodos involucrados. La dependencia entre la movilidad de los nodos que componen un enlace (en el núcleo de la red) en el tiempo t puede ser vista como dependencia de la movilidad del enlace L (A, B) de la siguiente manera:

$$P^{\lambda}_{L(A,B)}(t) = |M^{\lambda}_{A}(t) - M^{\lambda}_{B}(t)| \quad \textbf{(Ecuación 8)}$$

Por lo tanto, un enlace simétrico fiable en términos de movilidad puede ser visto como un enlace que satisface las dos condiciones siguientes:

1) La movilidad media del enlace L (i, j) es inferior a un umbral THRESHOLD_Link que depende de las características de la red inalámbrica (densidad de red, movilidad de red, escalabilidad de red, dimensión de red, etc):

   $$M^{\lambda}_{L(i,j)}(t) \leq THRESHOLD\_Link \quad \textbf{(Ecuación 9)}$$

2) La dependencia de la movilidad del enlace L (i, j) es cercana a cero:

   $$P^{\lambda}_{L(i,j)}(t) \to 0 \quad \textbf{(Ecuación 10)}$$

La elección de tal enlace que satisface estas dos condiciones asegura que el enlace tenga una baja movilidad, con una fuerte dependencia entre los nodos implicados.

b. Criterios de movilidad

El primer criterio es directo porque selecciona como MPRs establecidos a los nodos vecinos y que tengan una menor movilidad (Figura 13 (a)). Precisamente el nodo seleccionado como MPR es el nodo en donde su movilidad es la más pequeña tal como se observa en la ecuación 11. Mientras que los dos criterios restantes se basan en la estimación de la calidad de enlace entre vecinos one-hop y multi-hop. La calidad del enlace en los términos de movilidad depende de dos condiciones mencionadas anteriormente y por lo tanto la nueva selección MPR se combina entre el número de enlaces hacia los nodos en dos saltos y la confiabilidad en términos de movilidad. El segundo y tercer criterio comentados se basan en la ecuación 12 y 13 respectivamente. Al aplicar estos tres criterios se brinda una ventaja en la facilidad de cálculo y evita el consumo excesivo de recursos de memoria y CPU.

En la figura 11 muestra criterios de selección de nodos MPRs una vez realizada la evaluación de movilidad de los nodos de la red:

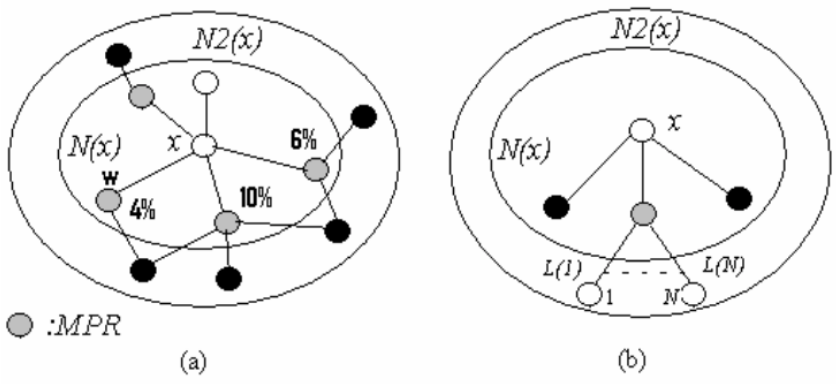


Figura 11. Criterios de evaluación.

Tomado de Enneya, Oudidi y Elkoutbi, 2009.

$Criterio - DIR(\omega) = \min_{\omega \epsilon N(x)} M_{\omega}^{\lambda}$ (t)
(Ecuación 11)

$$Criterio - SUM(\omega) = 1 - \frac{\sum_{i=1}^{N} M_{(\omega,i)}^{\lambda}(t)}{N} \quad \textbf{(Ecuación 12)}$$

$Criterio - PRD(\omega) = 1 - \prod_{i=1}^{N} M_{(\omega,i)}^{\lambda}$ (t) **(Ecuación 13)**

1.9.3.5 Métricas de Rendimiento

Se ha considerado las métricas más importantes para analizar y evaluar el rendimiento de los protocolos de enrutamiento MANET. Estas métricas consideradas son:

1) Normalized Routing Overhead (NRL): Representa la relación entre el número de paquetes de control propagados por cada nodo de la red y el número de paquetes de datos recibidos por los nodos de destino. Esta métrica refleja la eficiencia de los protocolos de enrutamiento implementados en la red.
2) Packet Delivery Fraction (PDF): Se trata de un número total de paquetes de datos entregados divididos por el número total de paquetes de datos transmitidos por todos los nodos. Esta métrica de rendimiento nos dará una idea de lo bien que el protocolo está realizando en términos de entrega de paquetes mediante el uso de diferentes modelos de tráfico.

Average End-to-End delay (Avg-End-to-End): Este es el retardo medio de los paquetes de datos desde el nodo de origen al nodo de destino. Esta métrica se calcula restando "tiempo en el que se transmitió el primer paquete por fuente" desde "tiempo en el que el primer paquete de datos llegó al destino". Esto incluye todos los posibles retrasos causados por el almacenamiento en búfer durante la latencia de descubrimiento de ruta, las colas en la cola de interfaz, los retrasos de retransmisión en la capa MAC, los tiempos de propagación y transferencia. (Enneya, Oudidi y Elkoutbi, 2009, pp. 1-5)

1.9.3.6 Funcionamiento del Protocolo

OLSR es modularizado en un "núcleo" de funcionalidad, que siempre es necesario para que el protocolo desempeñe de manera correcta y con la ayuda de funciones auxiliares. Cada función auxiliar proporciona funcionalidad adicional, que puede ser aplicable en situaciones específicas (por ejemplo, en caso de que un nodo está proporcionando conectividad entre la MANET y otro dominio de enrutamiento). Todas las funciones auxiliares son compatibles, en

la medida en que cualquier (sub) conjunto de funciones auxiliares se puede implementar con el núcleo. Además, el protocolo permite a los nodos heterogéneos, es decir, nodos que implementan diferentes subconjuntos de funciones auxiliares para coexistir en la red. El propósito de dividir el funcionamiento del OLSR en funcionalidad del núcleo y un conjunto de funciones auxiliares es proporcionar un protocolo sencillo y fácil de comprender, y para proveer una forma de sólo agregar complejidad donde se requiere funcionalidad adicional específica.

1.9.3.7 Funcionamiento del Núcleo

La funcionalidad básica de OLSR especifica el comportamiento de un nodo, equipado con interfaces OLSR participando en la MANET y corriendo OLSR como un protocolo de enrutamiento. Esto incluye una especificación universal de mensajes de protocolo OLSR y su transmisión a través de la red, así como detección de enlace, difusión de la topología y cálculo de la ruta. Específicamente, el núcleo se compone de los siguientes componentes: Formato de paquete y reenvío, Detección de Enlace, Detección de Vecino, Selección y Señalización de MPR, Difusión de mensaje de Control de topología y Cálculo de ruta. (Sarkar, Basavaraju y Puttamadappa, 2008, pp.77-81)

1.9.4 Fisheye State Routing (FSR)

FSR es un protocolo proactivo basado en la denominada "técnica ojo de pez," propuesta para reducir el tamaño de la información necesaria para representar los datos gráficos. Las novedades en FSR son:

1. La transmisión de paquetes de estado de enlace a los vecinos en lugar de hacerlo por flooding (un método tomado del protocolo de enrutamiento de estado global, GSR).

2. La introducción de la noción de alcance para definir regiones de redes con diferente precisión en la información de enrutamiento.

FSR es similar a los protocolos de estado de enlace, ya que cada nodo mantiene una tabla de topología de la red. Un nodo también mantiene una tabla de rutas y una lista de vecinos. A diferencia de los protocolos de estado de enlace, que realiza flooding en las actualizaciones de ruta de la red, en los paquetes de estado de enlace FSR se intercambian con los únicos vecinos, mientras que los números de secuencia se utilizan para indicar la frescura de la información, como en DSDV. Un mensaje de actualización de ruta incluye una secuencia de (dirección de destino, lista de vecinos) pares. Para llevar a cabo la técnica de ojo de pez, FSR introduce la noción de alcance. El alcance a un nodo N se define como el conjunto de nodos que se puede llegar en X saltos de N.

Las actualizaciones de enrutamiento se generan a un ritmo diferente, con la mayor frecuencia de los nodos con el alcance más pequeño. Esto produce una reducción en el número y tamaño de los mensajes de actualización y en la sobrecarga del protocolo. FRS se basa en un equilibrio de los costos óptimos de la ruta. Este mantiene la distancia y la calidad de la información sobre el vecindario o zona de un nodo con progresivamente menos detalle a medida que aumenta la distancia. Tal conocimiento impreciso de la mejor ruta hacia el destino puede llevar a la utilización de algunas rutas no óptimas; sin embargo, el protocolo tiene un buen potencial para escalar hasta grandes redes, ya que los cambios topológicos que ocurren en las regiones situadas lejos de un nodo no producen la misma cantidad de tráfico como lo harían en un protocolo proactivo de un solo ámbito. Por otra parte, cuando el paquete se acerca al destino, llega a alcances con conocimiento cada vez más preciso sobre el destino, y esto mitiga la falta de información precisa. Es evidente cómo el ámbito de aplicación es una nueva dimensión en el espacio de diseño de protocolo. (Beraldi y Baldoni, 2003, pp.137)

En la figura 12 muestra el funcionamiento y el alcance del protocolo FSR:

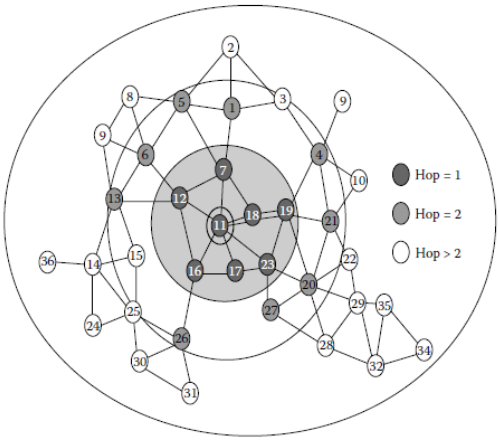


Figura 12. Alcance de la técnica Ojo de Pez (Fisheye).

Tomado de Sarkar, Basavaraju y Puttamadappa, 2008.

En la figura 13 la reducción de la tabla de enrutamiento de los nodos la red utilizando el protocolo FSR:

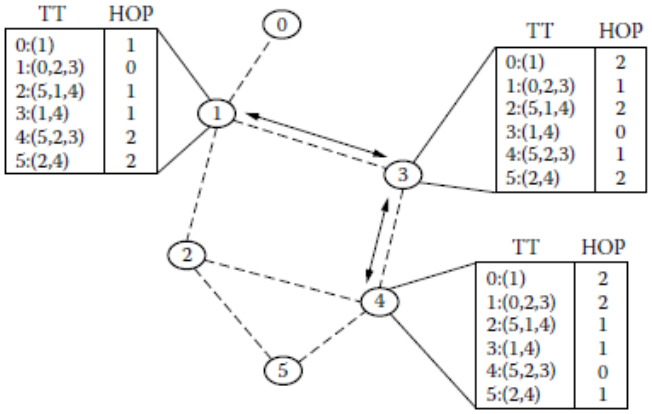


Figura 13. Reducción de tabla de enrutamiento en nodos usando FSR.

Tomado de Sarkar, Basavaraju y Puttamadappa, 2008

1.10 Protocolos de Enrutamiento Reactivos o de demanda

Estos protocolos son la oferta más reciente en la búsqueda de soluciones confiables de enrutamiento en redes inalámbricas. Su característica distintiva es que llevan a cabo una búsqueda de ruta cuando una fuente desea comunicarse con un destino y no sabe cómo alcanzarlo. El descubrimiento de

la ruta se realiza mediante mensajes de “flooding”: el nodo de origen, en busca de una ruta hacia un destino, emite una solicitud de información a través de la red. Al recibir la solicitud, los nodos intermediarios (o de tránsito) intentan enseñar al nodo de origen la ruta y guardarla en la tabla enviada. Una vez que se ha alcanzado el nodo de destino, este es capaz de responder usando la ruta trazada por la solicitud, estableciendo una ruta full dúplex entre nodos de origen y de destino. El esfuerzo involucrado es reducido en casos donde un nodo de tránsito ya posee una ruta hacia el destino. Una vez calculada la ruta, esta debe ser guardada y actualizada a nivel de la fuente durante el tiempo que permanece en uso. Otra técnica utilizada para trazar una ruta solicitada es la ruta de origen, como se utiliza en el protocolo de enrutamiento de origen dinámico. AODV es un ejemplo de un protocolo reactivo.

Entre los protocolos de enrutamiento reactivos más importantes se tiene:

- AODV
- DSR
- TORA (Temporally Ordered Routing Algorithm)
- CBRP
- LAR
- ARA (Ant-Colony-Based Routing Algorithm)

1.10.1 AODV (Ad Hoc On Demand Distance Vector routing)

AODV pide el uso de la secuencia numérica de DSDV para reemplazar antiguos rutas en caché y para evitar bucles, mientras que el procedimiento de descubrimiento se deriva de la adoptada en DSR. La principal diferencia con DSR es que una ruta descubierta se almacena localmente en los nodos en lugar de incluirse en el encabezado del paquete. El proceso mismo de rutas del disco se desencadena por un nodo S cuando se necesita enviar un paquete a un nodo D para el que no tiene información de enrutamiento en su tabla de enrutamiento. El descubrimiento de ruta se basa en realizar flooding de paquetes RREQ de una manera similar a DSR. Como un nodo reenvía el

paquete de solicitud, este establece una trayectoria inversa a partir de sí mismo a S mediante el registro de la dirección del vecino del que haya recibido la primera copia del paquete RREQ. Del mismo modo, cuando un paquete de control de RREQ se envía hacia el destino, un nodo configura automáticamente el camino inverso desde todos los nodos de nuevo a la fuente. Los otros caminos de vuelta se eliminan después de un período de tiempo de espera. (Beraldi y Baldoni, 2003, pp.141)

Figura 14 se muestra un ejemplo de propagación de un mensaje RREQ con el protocolo AODV:

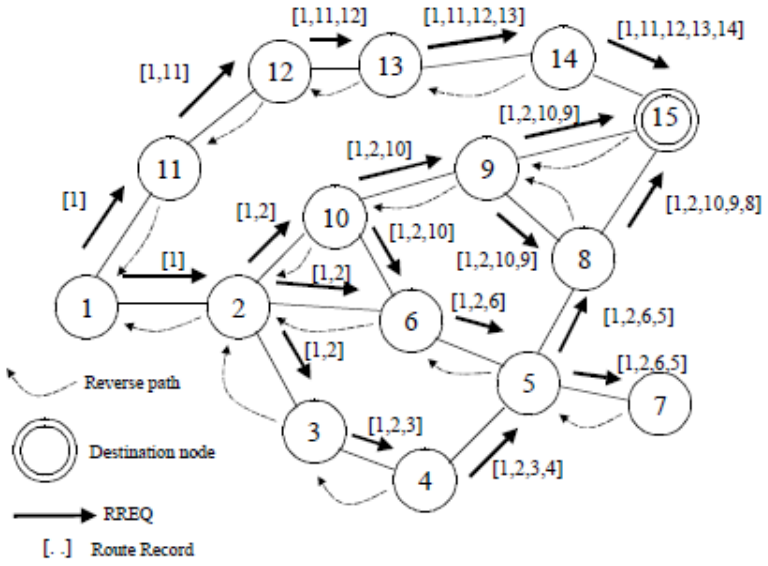


Figura 14. Ejemplo de propagación de RREQ en AODV y configuración de la ruta de reserva.

Tomado de Beraldi y Baldoni, 2003

En la figura 15 se muestra un ejemplo de la transmisión mediante una ruta seleccionada usando el protocolo AODV.

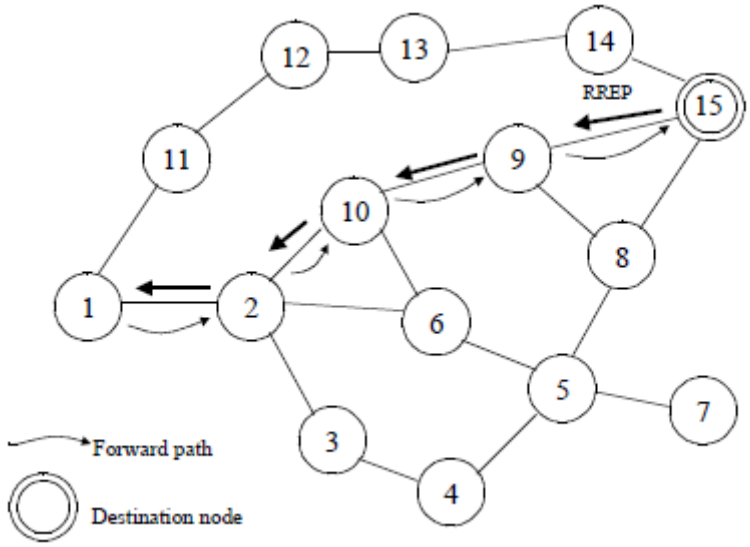


Figura 15. Ejemplo de configuración de la ruta hacia adelante en AODV.

Tomado de Beraldi y Baldoni, 2003

Al final de la fase de descubrimiento, como resultado de las transmisiones de paquetes de petición-respuesta, un nuevo estado de enrutamiento se crea en los nodos. El estado se compone de las entradas de la tabla de enrutamiento que registra el nodo del siguiente salto hacia el destino de la ruta a seguir. Se elimina un camino a seguir si no se utiliza dentro de un intervalo de tiempo de caducidad determinada ruta. Cada vez que se utiliza la ruta, el intervalo de tiempo de caducidad se restablece. El mantenimiento de una ruta se basa en la transmisión periódica de mensajes de “HELLO”. Al detectar una falla en el enlace, un nodo envía un paquete de respuesta no solicitado de ruta a todos sus vecinos upstream activos invalidando todas las rutas con el enlace roto. Esos nodos, a su vez, transmiten los paquetes a sus respectivos nodos upstream para que, finalmente, todas las fuentes activas sean notificadas. Después de recibir la respuesta solicitada de ruta, la fuente emite otra solicitud de ruta. (Beraldi y Baldoni, 2003, pp.142)

1.10.2 TORA (Temporally Ordered Routing Algorithm)

TORA pertenece a una familia general de algoritmos de "revocación de enlace". TORA está diseñado para reaccionar de manera eficiente a los cambios topológicos y para hacer frente a las particiones de red. El nombre del protocolo se deriva de la suposición de tener relojes sincronizados (por ejemplo a través de GPS), requeridos en orden a los eventos que ocurren en la red. TORA proporciona enrutamiento mediante la explotación de un enfoque completamente diferente de los descritos hasta ahora. La optimización de ruta es una preocupación secundaria en TORA. El objetivo principal es encontrar rutas estables que pueden ser reparados de forma rápida y localmente. El protocolo construye un grafo acíclico dirigido (DAG) enrutado al destino deseado para este propósito. DAG se obtiene mediante la asignación de una dirección lógica a los enlaces, sobre la base de una "altura" o nivel de referencia asignado a los nodos. Si (X, Y) es un enlace directo de DAG, X es llamado el nodo upstream e Y el nodo downstream. DAG tiene la siguiente propiedad: sólo hay un nodo receptor (el destino), mientras que todos los demás nodos tienen al menos uno, pero por lo general, muchos enlaces salientes. Al nodo de destino se puede llegar desde un nodo siguiendo cualquiera de sus enlaces salientes. Los bucles son trivialmente evitados debido a la propiedad de DAG. Funcionamiento del Protocolo puede dividirse en tres fases separadas: descubrimiento de ruta, mantenimiento de ruta y eliminación ruta.

La primera fase se basa en un intercambio de paquetes cortos de control de consulta-respuesta. Durante la transmisión de los mensajes de respuesta, que también se lleva a cabo por el flooding, los enlaces reciben una dirección lógica (upstream o downstream) en función de su altura relativa lógica, así ese DAG, enrutado al destino es creado al final de la fase. Este estado de enrutamiento puede ser vista como la red de tubos, con el agua que fluye hacia abajo hacia el nodo de destino, que tiene la altura más baja en la red. Mantenimiento de la ruta se activa para mantener el DAG y se basa en una secuencia finita de operaciones de "cambio de enlace". Una característica clave de TORA es que

muchos cambios topológicos no pueden provocar ninguna reacción en absoluto. De hecho, si uno de los enlaces de salida de un nodo se rompe, pero el nodo tiene al menos otro nodo de downstream, el destino puede todavía ser alcanzable a través de otro camino, y por lo tanto no se requieren actividades de reparación. Por el contrario, cuando un nodo detecta que no tiene nodos de downstream, se genera un nuevo nivel de referencia con el fin de convertirse en un máximo global. El nuevo nivel de referencia se propaga en la red, causando la reversión parcial del enlace para aquellos nodos que, como resultado del nuevo nivel de referencia, han perdido todas las rutas hacia el destino. Al final de las actividades de reparación, localizados cerca del nodo, el DAG se restablece. TORA es capaz de detectar particiones de red. En la detección de una partición de la red, un nodo inunda un paquete claro que restablece el estado de enrutamiento. (Beraldi y Baldoni, 2003, pp.142-143)

En la figura 16 se muestra un ejemplo de asignación de DAG en el nodo 8:

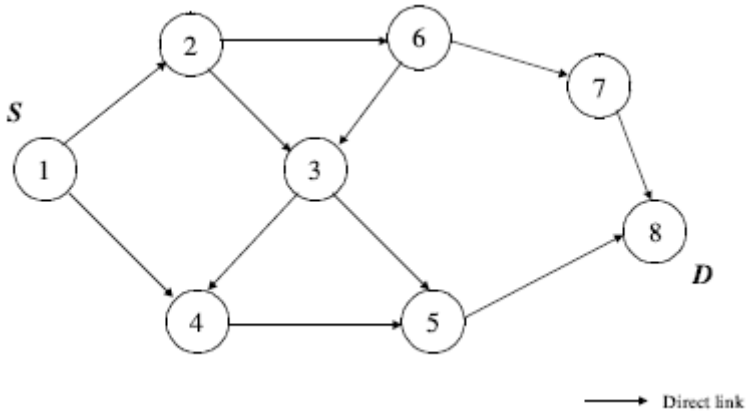


Figura 16. Ejemplo de DAG arraigado al nodo 8.

Tomado de Beraldi y Baldoni, 2003.

1.11 Protocolos de Enrutamiento Híbridos

El protocolo de enrutamiento de zona es un ejemplo de un protocolo híbrido, que intenta combinar las ventajas de las dos familias de protocolos

anteriormente vistas. Los nodos tienen un enfoque proactivo para enrutamiento en sus inmediaciones, hasta cierta distancia (por ejemplo, tres o cuatro saltos). Si una aplicación quiere enviar algo a un nodo fuera de esta zona, se desencadena una búsqueda reactiva. Mediante este sistema, las rutas en las cercanías de un nodo están disponibles inmediatamente, y cuando la búsqueda deba ampliarse, este es optimizado: cuando un nodo recibe un paquete de búsqueda de ruta, sabe inmediatamente si el destino está dentro de su propia zona; en este caso, puede responder, o si no propaga la solicitud de una manera optimizada fuera de su zona activa. Dependiendo del tipo de tráfico y las rutas solicitadas, sin embargo, los protocolos híbridos de este tipo pueden combinar las desventajas de los métodos de enrutamiento proactivos y reactivos: el intercambio regular de monitoreo de paquetes y de flooding de toda la red al buscar una ruta a un nodo distante. (Frikha 2011, pp. 20-22)

Otro método de clasificación se basa en los roles que los nodos pueden tener en un esquema de enrutamiento. En un protocolo de enrutamiento uniforme, todos los nodos móviles tienen el mismo rol, importancia y funcionalidad. Algunos ejemplos de protocolos de enrutamiento uniforme incluyen los protocolos de enrutamiento WRP, DSR, AODV y DSDV. Los protocolos de enrutamiento uniforme normalmente asumen una estructura de red plana. En protocolos de enrutamiento no uniformes para redes MANET, algunos nodos llevan a cabo distinta gestión o funciones de enrutamiento. Normalmente, los algoritmos distribuidos son explotados para seleccionar los nodos especiales. En algunos casos, los enfoques del enrutamiento no uniforme están relacionados con la estructura de red jerárquica para facilitar la gestión y la organización del nodo. Los protocolos de enrutamiento no uniformes adicionales se pueden dividir de acuerdo a la organización de los nodos móviles y cómo se llevan a cabo las funciones de gestión y de instalación. Así, siguiendo estos criterios los protocolos de enrutamiento no uniformes para redes MANET se dividen en enrutamiento jerárquico basado en la zona, enrutamiento jerárquico basado en clúster y enrutamiento basado en el nodo principal. (Sarkar, Basavaraju y Puttamadappa, 2008, pp. 66)

Se debe empezar por examinar si los protocolos de enrutamiento de internet están adaptados para ser usados en MANET. Así también, hay que revisar los protocolos usados en redes con infraestructura de enrutamiento y estudiar la posibilidad de adaptar estos protocolos a una red MANET. (Frikha 2011, pp. 23)

Entre los protocolos de enrutamiento híbridos más importantes tenemos:

- ZRP
- ZHLS
- SLURP (Scalable Location Updates Routing Protocol)
- DST (Distributed Spanning Trees Based Routing Protocol)
- Distributed Dynamic Routing (DDR) Protocol

1.11.1 Zone Routing Protocol (ZRP)

ZRP es un protocolo de enrutamiento híbrido que tiene como objetivo combinar las ventajas tanto de los enfoques proactivos y reactivos, es decir, principalmente para reducir la latencia necesaria para adquirir una nueva ruta y la sobrecarga de protocolo. El punto central de un protocolo de este tipo es la noción de zona. Una zona Z (k, n) para un nodo n con el radio k, se define como el conjunto de nodos a una distancia no mayor de saltos k:

$$Z(k,n) = \{i \mid H(n,i) \leq k\},$$

Dónde: H (i, j) es la distancia en número de saltos entre el nodo i y el nodo j. El nodo n se llama el nodo central de la zona de encaminamiento, mientras que el nodo b tal que H (n, b) = k se denomina nodo periférico de n. El valor de k es generalmente pequeño en comparación con el diámetro de la red y se puede optimizar en diferentes escenarios caracterizados por diversos grados de movilidad y de tráfico. La arquitectura del protocolo está organizada en cuatro componentes principales: el Protocolo de Enrutamiento Intrazona (IARP), el Protocolo de Enrutamiento Interzona (IERP), el Protocolo de Bordercast (BRP)

y un Protocolo de Descubrimiento/Mantenimiento de Vecino (NDP). El IARP ofrece rutas de forma proactiva a los nodos situados dentro de la zona de encaminamiento del origen. Puede estar basada en cualquier protocolo proactivo con la diferencia de que las actualizaciones de ruta se propagan a una distancia no mayor que los saltos k. IARP utiliza NDP para aprender acerca de los vecinos de un nodo.

Para aquellos nodos situados a una distancia $k' > k$ del origen, ZRP se basa en IERP para calcular la demanda de una ruta entre zonas. IERP utiliza una forma de flooding selectivo para explotar la estructura de la zona subyacente generada por el IARP. Específicamente, las inundaciones se basan en el envío de paquetes de consulta sólo a los nodos periféricos (también llamados nodos de frontera), utilizando un tipo especial de transmisión de multidifusión, denominado bordercast. Cuando un nodo recibe el paquete de consulta, se puede o bien responder al origen – si D es un miembro de su zona de enrutamiento – o bordercast el paquete de consulta a sus nodos periféricos. Finalmente, el paquete de consulta llega a un nodo que tiene D como miembro de su zona, de modo que se genera un paquete de control de respuesta y enviado de vuelta a la fuente. Una ruta a D puede ser acumulado en el paquete de consulta durante el reenvío (como por DSR) o – para reducir la longitud del paquete de consulta – en el paquete de control de respuesta durante la fase de respuesta. El reenvío de paquetes a lo largo de una ruta entre zonas adopta un enrutamiento de partida modificado. Un camino de enrutamiento contiene sólo los nodos de borde que tienen que ser atravesados. Reenvío a lo largo de los nodos de frontera está determinado por tablas, ya que la distancia entre los nodos de frontera es k. Ya que no existe ninguna coordinación entre los nodos, las zonas se superponen fuertemente. Un nodo puede ser un miembro, así como un nodo de frontera de muchas zonas. De esta manera, el mecanismo de búsqueda básica se puede desempeñar incluso peor que un flooding estándar. La literatura ofrece varias soluciones para hacer frente a este problema al detener y controlar los hilos de consulta redundantes. El mantenimiento de ruta es responsable del mantenimiento de caminos entre zonas. El uso de un procedimiento de reparación local con el objetivo de reparar el enlace roto por

una búsqueda de mini-ruta también se sugiere para reducir la necesidad del descubrimiento global de ruta. Una mejora sobre ZRP – el algoritmo de enrutamiento dinámico distribuido (DDR) – también ha sido propuesto. El protocolo se basa en la construcción de un bosque de zonas dinámicas que no se superponen. (Beraldi y Baldoni, 2003, pp.146-147)

En la figura 17 se muestra un ejemplo de una zona determinada por el protocolo ZRP:

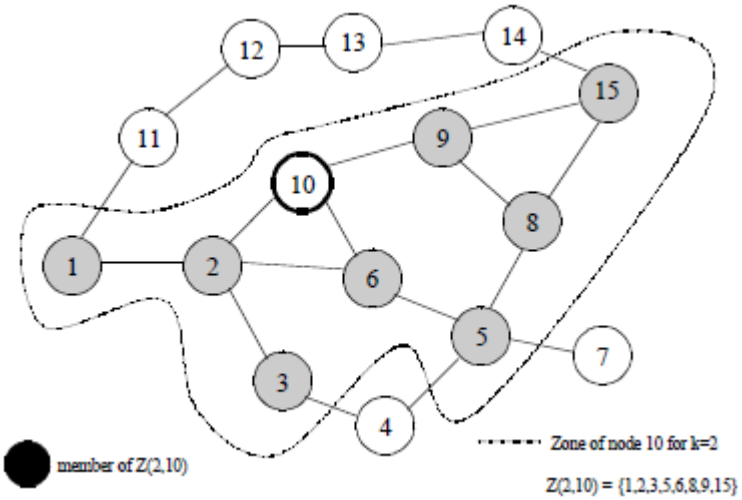


Figura 17. Ejemplo de una zona en ZRP.

Tomado de Beraldi y Baldoni, 2003.

En la figura 18 se muestra la comunicación entre zonas de una red utilizando bordercast con el protocolo ZRP:

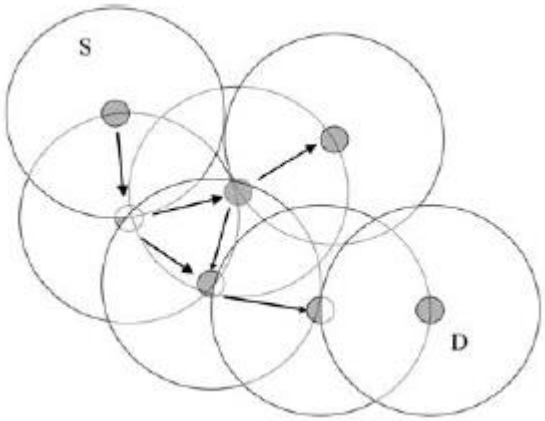


Figura 18. Bosquejo de la propagación de consulta mediante bordercast.

Tomado de Beraldi y Baldoni, 2003.

1.12 Seguridad en protocolos de enrutamiento en MANET

Uno de los estudios más relevantes en el campo de las redes MANET es la de proporcionar mecanismos de seguridad para los protocolos de enrutamiento. Los ataques contra la seguridad de este tipo de redes se las pueden clasificar como activos y pasivos.

- **Ataques Activos:** Este tipo de ataques se basa en la modificación de los paquetes o la introducción de información falsa. Dichos ataques pueden ser internos o externos ya sean estos realizados por un nodo infectado dentro de la red o por un nodo que se encuentre fuera de la red MANET.
- **Ataques Pasivos:** Un ataque pasivo no afecta al funcionamiento normal del protocolo de enrutamiento, simplemente obtienen información valiosa al interceptar el tráfico de enrutamiento. Esto los hace difíciles de detectar.

2. CAPITULO II. Diseño e Implementación Red MANET

En el siguiente capítulo se detalla todos los elementos que fueron necesarios para la implementación de la red MANET, desde la instalación del sistema operativo de Raspberry Pi hasta la implementación del protocolo necesario para la creación de la red.

2.1 Hardware

2.1.1 Estudio Comparativo

Para seleccionar el dispositivo que se utilizó en la implementación de la red MANET propuesta se realizó un estudio comparativo de características de los equipos, de sus antenas y procesadores, y así seleccionar el dispositivo apropiado que cubra las necesidades del proyecto.

2.1.1.1 Antenas

a. Módulo Xbee S2 OEM RF

Los módulos Xbee Serie 2 OEM RF fueron diseñados para operar dentro del protocolo ZigBee y soportar las necesidades únicas de redes de sensores inalámbricos de bajo costo y consumo. Los módulos requieren una potencia mínima y proporcionan una entrega confiable de datos entre dispositivos remotos. Los módulos funcionan dentro de la banda de frecuencia ISM 2.4 GHz.

En la tabla 1 se muestra las especificaciones del módulo Xbee S2:

Tabla 1.

Especificaciones Xbee.

	
Especificación	
Rendimiento	
Rango Interior/Urbano	Sobre los 40 m
Rango Exterior con línea de vista	Sobre los 120 m
Salida de Potencia de Transmisión	2mW (+3dBm)
Tasa de Datos RF	250000 bps
Tasa de Datos de la Interface Serial	1200 – 230400 bps
Sensibilidad Recibida	-95 dBm (1% tasa de error por paquete)
Requerimientos de Energía	
Suministro de Voltaje	2.8 – 3.4 V
Corriente de Transmisión (Típica)	40 mA (@ 3.3 V)
Corriente de Recepción (Típica)	40 mA (@ 3.3 V)
Corriente de Desconexión	< 1 μA @ 25°C
General	
Frecuencia de Operación	ISM 2.4 GHz

Dimensiones	0.960” x 1.087” (2.438 cm x 2.761 cm)
Temperatura de funcionamiento	-40 to 85º C (industrial)
Opciones de Antenas	Whip Integrado, Chip, RPSMA y conector UFL
Red y Seguridad	
Topologías de Red Soportadas	Punto a Punto, Punto Multipunto, Peer-to-Peer & Mesh.
Número de canales	16 Canales de Secuencia Directa.
Opciones de direccionamiento	PAN ID y Direcciones,

Adaptado de Digi Internacional, s.f.

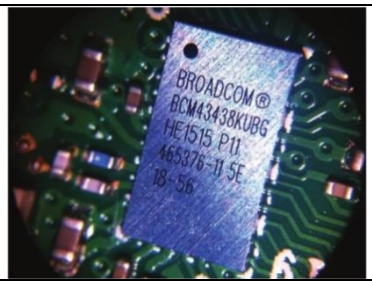
b. Broadcom BCM43438

El BCM43438 incluye un radio de conversión directa integrado que soporta la banda de 2,4 GHz.

En la tabla 2 se muestran las especificaciones de la antena BCM433438 integrada en cada Raspberry PI 3.

Tabla 2.

Especificaciones antena raspberry.



Especificación	
Rendimiento	
Frecuencia	Mínimo 2.4 GHz, Máximo 2.5 GHz
Variación de potencia de TX de lazo cerrado en el nivel de potencia más alto.	• En amplia gama de temperatura y voltaje. Se aplica en toda la gama de potencia de salida de 5 a 21 dBm. • Puede ser típicamente $\pm$1.5 dB.
Control de Ganancia	0.25 dB (Típico)
Pérdida de Retorno	• $Z_0 = 50\ ohm.$ • Mínimo 4 dB, Máximo 6 dB.
Emisiones de TX	• 30 MHz < f < 1 GHz RBW (Resolución de ancho de banda) = 100 kHz; Típico: -99 dBm; Máximo: -96 dBm. • 1 GHz < f < 1.75 GHz RBW = 1 MHz; Típico: -44 dBm; Máximo: -41 dBm. • 1.8 GHz < f < 1.9 GHz RBW = 1 MHz; Típico: -68 dBm; Máximo: -65 dBm. Máximo: -96 dBm. • 1 GHz < f < 1.75 GHz RBW

	= 1 MHz; Típico: -44 dBm; Máximo: -41 dBm. • 1.8 GHz < f < 1.9 GHz RBW = 1 MHz; Típico: -68 dBm; Máximo: -65 dBm.
Emisiones de RX	• 30 MHz < f < 1 GHz RBW (Resolución de ancho de banda)) = 100 kHz; Típico: -99 dBm; Máximo: -96 dBm. • 1 GHz < f < 1.75 GHz RBW = 1 MHz; Típico: -54 dBm; Máximo: -51 dBm. • 1.8 GHz < f < 1.9 GHz RBW = 1 MHz; Típico: --88 dBm; Máximo: -85 dBm.

Adaptado de Raspberry Foundation, s.f.

c. Antena Arduino WiFi Shield Verion 022

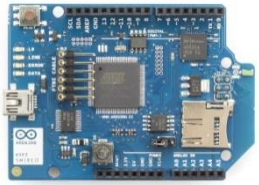
Se ha añadido esta antena ya que el Arduino Uno no cuenta con una antena incorporada, por lo tanto, esta antena externa es una solución para cumplir con los requerimientos para implementar la red MANET.

La antena Arduino WiFi permite a una placa Arduino conectarse a internet a través de la biblioteca de WiFi y a leer y escribir una tarjeta SD usando la biblioteca de la SD, a continuación, sus especificaciones.

En la tabla 3 se muestran las especificaciones de una antena Arduino WIFI shield versión 022:

Tabla 3.

Especificaciones antena de Arduino WIFI Shield V022.


Especificación
General
Requiere una tarjeta Arduino.
Voltaje de operación 5V (suministrada desde la placa Arduino).
Compatible con Arduino Due.
Conexión a través de redes 802.11b/g.
Tipos de cifrado: WEP y WPA2 Personal.
Conexión con Arduino en el puerto SPI.
Ranura micro SD integrada.
Encabezados ICSP.
Conexión FTDI para la depuración serial de WiFi shield.
Mini-USB para actualizar el firmware de WiFi shield.

Adaptado de Arduino, s.f.

2.1.1.2 Procesador

a. Arduino Uno

Arduino Uno es una placa de microcontrolador basada en el ATmega328. Tiene 14 pines de entradas/salidas digitales (de los cuales 6 pueden utilizarse como salidas PWM), 6 entradas analógicas, un oscilador de cristal de 16 MHz, conexión USB, un conector de alimentación, un encabezado ICSP y un botón de reset. Contiene todo lo necesario para soportar el microcontrolador; simplemente conéctelo a un ordenador con un cable USB o conéctelo con un adaptador AC-DC o batería para empezar. El Uno se diferencia de todas las placas anteriores en que no utiliza el chip controlador FTDI USB-a-serial. En su lugar, cuenta con el Atmega8U2 programado como un convertidor de USB a serie.

En la tabla 4 se muestran las especificaciones de la placa Arduino UNO.

Tabla 4.

Placa Arduino UNO.

	
Especificación	
Técnica	
Microcontrolador	ATmega328
Voltaje de funcionamiento	5V
Voltaje de entrada (recomendado)	7-12V
Voltaje de entrada (límites)	6-20V

Pines Digitales E/S	14 (de los cuales 6 proporcionan salida PWM)
Pines de entrada analógicos	6
Corriente DC por Pin de E/S	40 mA
Corriente DC por Pin de 3.3V	50 mA
Memoria Flash	32 KB de los cuales 0.5 KB utilizados por bootloader
SRAM	2 KB
EEPROM	1 KB
Velocidad de reloj	16 MHz

Adaptado de Arduino. s.f.

b. Raspberry Pi 3

Raspberry Pi 3 Modelo B es la tercera generación de Raspberry Pi. Esta poderosa computadora del tamaño de una tarjeta de crédito se puede utilizar para muchas aplicaciones y sustituye a la original Raspberry Pi Modelo B+ y Raspberry Pi 2 Modelo B. Manteniendo el popular formato de tablero el Raspberry Pi 3 Modelo B te trae un procesador más potente, 10 veces más rápido que la primera generación de Raspberry Pi. Además, añade LAN inalámbrica y conectividad Bluetooth, lo que la convierte en la solución ideal para diseños conectados de gran alcance.

En la tabla 5 se muestra las especificaciones de Raspberry PI 3

Tabla 5.

Raspberry PI 3.

	
Especificación	
Procesador	• Broadcom BCM2387 chipset. • 1.2GHz Quad-Core ARM Cortex-A53 802.11 b/g/n Wireless LAN and Bluetooth 4.1
GPU	• Co-procesador multimedia Dual Core VideoCore IV. Proporciona Open GL 2.0, acelerado por hardware. • OpenVG y decodificación de alto perfil H.264 de 1080p30. • Capaz de 1Gpixel / s, 1.5Gtexel / s o 24GFLOPs con filtro de textura y la infraestructura DMA.
Memoria	1GB LPDDR2
Sistema Operativo	Inicio desde de la tarjeta Micro SD, ejecutando una versión del sistema operativo Linux o Windows 10 IoT.
Dimensiones	85 x 56 x 17mm
Energía	Micro USB 5V1, 2.5ª
Conectores	

Ethernet	Conector Ethernet 10/100 BaseT
Salida de vídeo	HDMI (rev 1.3 & 1.4. Composite RCA (PAL and NTSC)
Salida de audio	• 40-pin 2.54 mm (100 mil) expansion header: 2x20 strip. • Providing 27 GPIO pins as well as +3.3 V, +5 V and GND supply lines.
Conector GPIO	• 40-pin 2.54 mm (100 mil) expansion header: 2x20 strip. • Providing 27 GPIO pins as well as +3.3 V, +5 V and GND supply lines.
Conector de Cámara	Interfaz serie serie MIPI de 15 polos (CSI-2).
Ranura para tarjeta de memoria	Push/pull Micro SDIO.
Beneficios Clave	• Bajo costo. • Formato consistente del raspberry. • Procesamiento 10x más rápido. • Conectividad añadida.
Aplicaciones Clave	• PC/Tablet/Laptop de bajo costo. • Aplicaciones IoT. • Centro de Medios. • Robótica.

	• Automatización Industrial/Hogar. • Servidor/Servidor Cloud. • Servidor de impresión. • Supervisión de la seguridad. • Cámara web. • Juegos. • Punto de acceso inalámbrico. • Sensibilización ambiental/Monitoreo (por ejemplo, estación meteorológica).

Adaptado de Raspberry Foundation, s.f.

Después de haber comparado especificaciones de cada dispositivo se pudo llegar a la conclusión de cuál sería el mejor para poder realizar de forma óptima la red MANET propuesta.

Se ha descartado el uso del módulo Xbee S2 ya que la tasa de ancho de banda es de máximo 250 kbps por lo que imágenes y audio sería posible transmitir, inclusive video de muy baja calidad se podría transmitir, pero no de la manera óptima que se requiere que en este caso es de 1000 mbps.

El uso de Arduino Uno también ha sido descartado para la implementación de este proyecto puesto que a diferencia del Raspberry Pi 3, dispositivo seleccionado para ser usado en la implementación de este proyecto el mismo que cuenta con una antena WiFi incorporada que soporta el envío de video en tiempo real y cubre la tasa de ancho de banda solicitada que es mínimo 1000 mbps; se ha podido cubrir así los requerimientos necesarios para que el proyecto sea implementado y su funcionamiento sea óptimo.

2.1.2 Raspberry Pi

2.1.2.1 Definición e Historia

La placa Raspberry Pi es un pequeño computador personal, del tamaño de una tarjeta de crédito y con un costo relativamente bajo. Aunque carece de la capacidad de expansión de memoria y no puede acomodar a bordo dispositivos tales como CDs, DVDs y unidades de discos duros, tiene todos los elementos necesarios para el funcionamiento de un ordenador personal. Entre los más conocidos se pueden encontrar, Puertos USB, un Puerto Ethernet, entrada HDMI, Conector de Audio, Procesador, entre otros.

Como se menciona anteriormente al ser un computador personal, éste realiza las tareas básicas que un computador hace, las cuales pueden ser desde el procesamiento de hojas de cálculo y texto, navegación en Internet, reproducción de video de alta calidad, etc. Inclusive con un conocimiento superior en temas referentes a electrónica programación y redes, se pueden desarrollar muchos proyectos interesantes en los diferentes paradigmas que existen en el mundo tecnológico, como puede ser el caso del Internet de las Cosas (IoT).

Sus orígenes pueden encontrarse en los laboratorios de computación de la Universidad de Cambridge en 2006. Bajo la premisa de impulsar el aprendizaje de la electrónica y la programación de la mano de elementos sencillos como es el caso de la plataforma Raspberry y el lenguaje de programación Python. Bajo este objetivo se origina la fundación Raspberry y durante los siguientes 6 años se dedicó al desarrollo de dicho computador saliendo a la venta en el 2012 a un precio muy accesible. En la actualidad existen dos modelos de Raspberry Pi conocidos como Model A y Model B y cada uno con diferentes revisiones en donde se mejoró procesamiento, capacidad, velocidad entre otros elementos. Para este proyecto de titulación va a usar Raspberry Pi Model B versión 3.

2.1.2.2 Placa Raspberry Pi versión 3

La Raspberry Pi 3 con sus dimensiones de 85[mm] x 56[mm] x 17[mm] y un peso de aproximadamente 45[g]. Este pequeño tamaño lo hace adecuado para proyectos integrados, dispositivos de automatización del hogar, máquinas de arcade o la construcción de pequeños clusters de múltiples dispositivos.

En la figura 19 se muestra el esquema del Raspberry PI 3

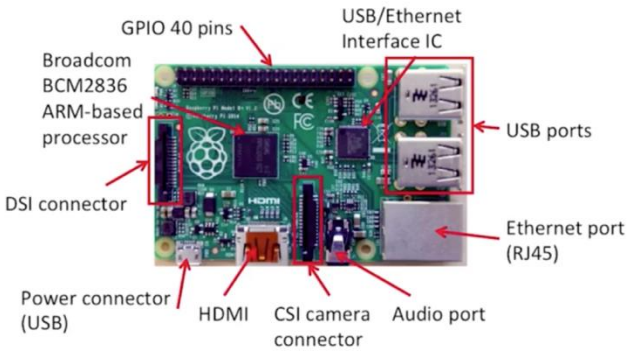


Figura 19. Esquema Raspberry Pi 3.

Tomada de Raspberry Foundation, 2016.

2.1.2.3 Arquitectura System on Chip (SoC)

La arquitectura de System on Chip (SoC) que se encuentra implementada en la tercera generación de Raspberry se la conoce como Broadcom BCM2837, la cual está compuesta de una CPU, GPU, SDRAM.

a. CPU

La unidad central de procesamiento, también conocida como procesador, es el cerebro de la Raspberry Pi y responsable de procesar e interpretar todo tipo de instrucciones de los programas que se encuentren almacenados en el computador. El SoC implementa un procesador quad-core ARM Cortex-A53 de 1.2 GHz y con arquitectura de 64 bits.

b. GPU

La unidad de procesamiento de gráficos es un chip especializado para manejar la matemática compleja que es requerida al momento de renderizar gráficos ya sean estos del sistema operativo o de algún programa que involucre procesamiento gráfico.

c. SDRAM

Raspberry Pi viene integrada con 1 GB de SDRAM, que puede ser compartida entre la CPU y GPU

d. Puertos USB

Esta placa viene incluida con 4 puertos USB 2.0 con una salida de 1.2 [A] que permite conectar teclado, mouse, memorias flash, entre otros elementos.

e. Ranura para MicroSD

La tarjeta microSD es el principal mecanismo de arranque y de almacenamiento de Raspberry PI. Es sobre esta tarjeta que se carga el sistema operativo y en donde se almacenan todos los datos, programas, etc.

f. Puerto Ethernet

Uno de los beneficios del modelo B de Raspberry Pi es la inclusión de un puerto Ethernet. Al ser una conexión física esta se limita a la distancia del cable Ethernet. La versión dos y tres de Raspberry Pi modelo B es compatible con Ethernet 10/100 Mbps.

g. Audio

Raspberry Pi dos y tres implementa el estándar Inter-IC Sound (I2S) para la entrada y salida de audio. Esto permite que el dispositivo se conecte a varios aparatos de audio digital. Un conector de 3.5 mm TRSS permite la salida de audio de forma análoga, mientras que el componente HDMI ofrece una salida de audio digital.

h. Puerto HDMI

De igual manera se incluye una interfaz multimedia de alta definición o por sus siglas en ingles HDMI. Permite que la placa raspberry se conecte a un monitor o televisor de alta definición. Este puerto es de suma importancia ya que la manera más sencilla de instalar el sistema operativo se la realiza cuando se conecta el dispositivo a un televisor y así poder seguir los pasos de instalación con la interfaz gráfica.

i. Interfaz de Cámara CSI

Es un puerto con 15 pines que sirve para la conexión dedicada de la PiCamera. Fue diseñada por la fundación raspberry. Al ser creada por la misma fundación su compatibilidad hace que se facilite su implementación en proyectos donde sea necesario el uso de una cámara. Su modelo más actual cuenta con sensor Sony de 8 megapíxeles.

j. Interfax de monitor DSI

Es un puerto con 15 pines que sirve para la conexión de monitores LCD.

k. Pines GPIO

El método principal para interactuar con diferentes componentes electrónicos es a través del uso de estos pines conocidos como **General Purpose Input/Output (GPIO).** Se dispone de 40 pines la mayoría de los cuales se pueden controlar, mediante el lenguaje de programación Python, para distintos usos de acuerdo al proyecto en el que se esté trabajando. (Raspberry Foundation, 2015, pp.6-13)

2.1.3 Elementos Adicionales

a. Raspberry Pi Camera v2

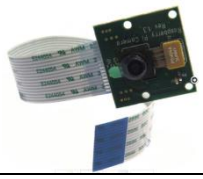
Como elemento extra se adquirió una cámara propia de Raspberry para tener una mayor compatibilidad y facilitar el proceso de instalación y uso con el proyecto de la red MANET. Esta cámara se puede utilizar para tomar vídeo de

alta definición, así como fotografías, se conecta directamente en el conector CSI del Raspberry Pi 3.

En la tabla 6 se muestran las especificaciones del módulo Raspberry Pi camera v2:

Tabla 6.

Pi cámara V2.

	
Especificación	
Tamaño	Alrededor de 25 x 24 x 9 mm
Peso	3g
Resolución	8 Megapíxeles
Modos de Video	1080p30, 720p60 and 640 × 480p60/90
Sensor	OmniVision OV5647
Sensibilidad	680 mV/lux-sec

Adaptado de Raspberry Foundation, s.f.

2.2 Software

2.2.1 Interfaz Grafica

Para realizar las pruebas sobre la red MANET se va usar la transmisión de video en vivo. Su manejo viene contemplado dentro de un aplicativo .NET usando el IDE de desarrollo de Visual Studio.

Este proceso consta de dos partes una de ellas se configura en el computador y la otra dentro de cada Raspberry.

2.2.1.1 Framework Eneter

Eneter es un Framework ligero que sirve para la comunicación entre procesos. Su amplia compatibilidad entre plataformas de desarrollo permite una interacción más sencilla entre los elementos necesitados en la red MANET.

Las plataformas soportadas son las siguientes.

- Java 6
- Android 2.3.3 (or later)
- JavaScript
- .NET 3.5, 4.0, 4.5
- Windows Phone 7, 7.1, 8.0, 8.1
- Compact Framework 2.0, 3.5
- Silverlight 3, 4, 5
- Xamarin for Android 4.0.3 (or later)
- Xamarin for iOS
- Mono 2.6.4 (or later)
- HTML5 Javascript

Para conectar las aplicaciones entre raspberry y Visual Studio es necesario de un protocolo de comunicación; los siguientes se encuentran implementados en el Framework.

- TCP
- *Websockets*
- *HTTP*
- *UDP*

En la figura 20 se muestra el diagrama de conexión entre emisor y receptor del framework Eneter:

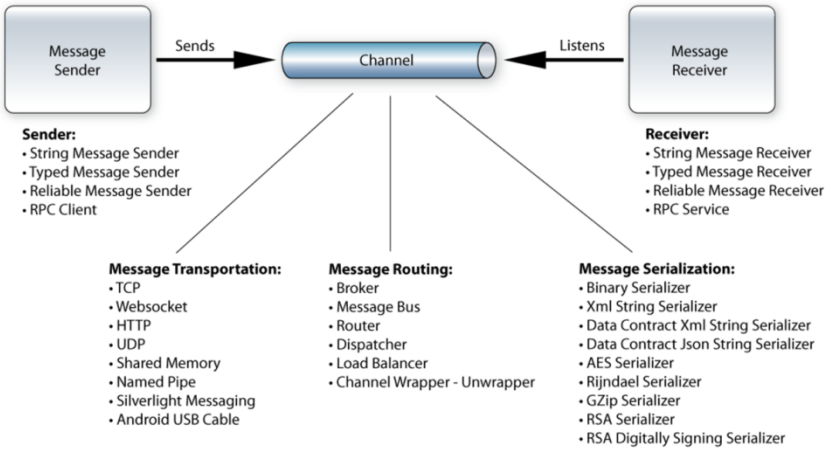


Figura 20. Diagrama del Framework Eneter

Tomado de Eneter Messaging Network, 2016.

Se necesita descargar el framework Eneter para java y .NET de la siguiente dirección: http://www.eneter.net/ProductDownload.htm.

Eneter para .NET será de gran uso en la aplicación del lado del cliente mientras tanto Eneter para Java será usado del lado del script de streaming de video que corre en cada uno de los nodos de la red MANET, formando una conexión como se muestra en el siguiente diagrama.

En la figura 21 se muestra el diagrama de conexión entre un cliente y el servicio de video de raspivid:

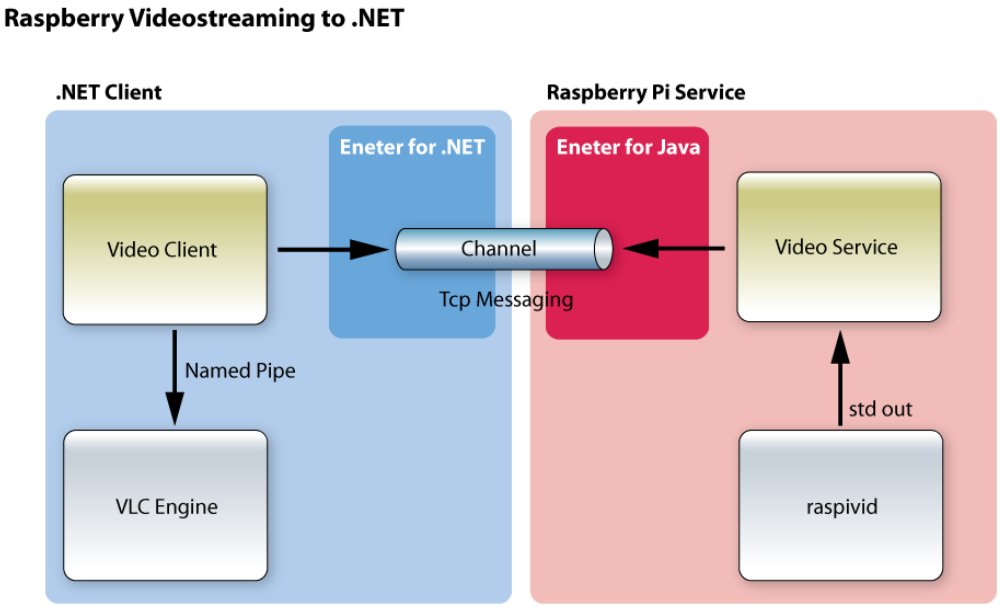


Figura 21. Diagrama de Streaming de video entre cliente .NET y Raspberry

Tomado de Eneter Messaging Network, 2016.

2.2.1.2 Librería de VLC

Raspberry Pi genera la transmisión de video usando el Códec H.264, por esta razón es necesario implementar alguna especie de decodificador de video del lado del cliente, existen varias opciones que se podrían incluir dentro del aplicativo, pero al ser muy compleja su programación es preferible usar las librerías de VLC en donde se tienen una cantidad considerable de los Codecs necesarios para la reproducción de video. Cabe recalcar que poder aprovechar los Codecs antes mencionados se debe tener instalado el reproductor de video VLC el cual se puede conseguir desde la página web oficial.

Se usó una implementación open source en donde se aprovechan las librerías de VLC, tales como:

- LibVlc
- VlcException

- VlcInstance
- VlcMedia
- VlcMediaPlayer

El cambio que se realizó en este código fue únicamente el de la ruta de acceso en donde se especifica en qué dirección se encuentra VLC.

2.2.1.3 Aplicativo Cliente

Usando las herramientas que proporciona Visual Studio se usó un aplicativo en donde se incluye un Form de video y dos botones el uno para iniciar la transmisión y el otro para detenerla. Tal como se observa en las figuras 25, 26 y 27.

Al tener tres nodos en la red MANET se crearon tres aplicativos con un ligero cambio en el nombre en donde se asignó lo siguiente:

En la tabla 7 se muestra el direccionamiento IP y puertos de cada nodo utilizado en la implementación del proyecto:

Tabla 7.

Direcciones IP y Puertos

Nombre de Aplicativo	**Dirección IP/ Puerto**
Cliente Raspberry 1	192.168.1.1/8093
Cliente Raspberry 2	192.168.1.2/8094
Cliente Raspberry 3	192.168.1.3/8095

Adaptado de Autor

En las figuras 22, 23 y 24 se muestra la interfaz gráfica de cada cliente respectivamente.

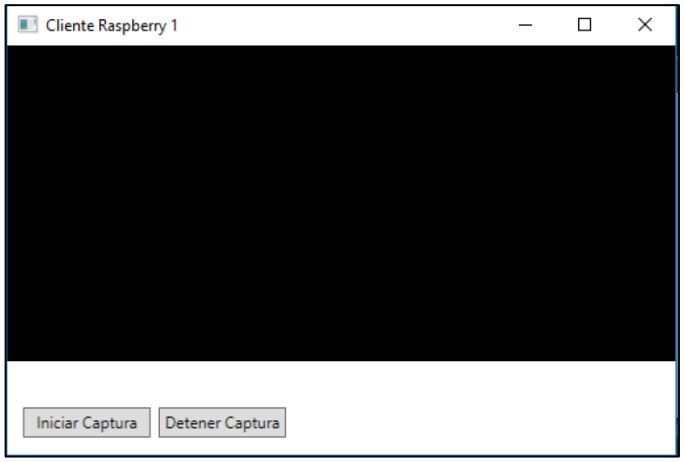


Figura 22. Interfaz gráfica cliente 1.

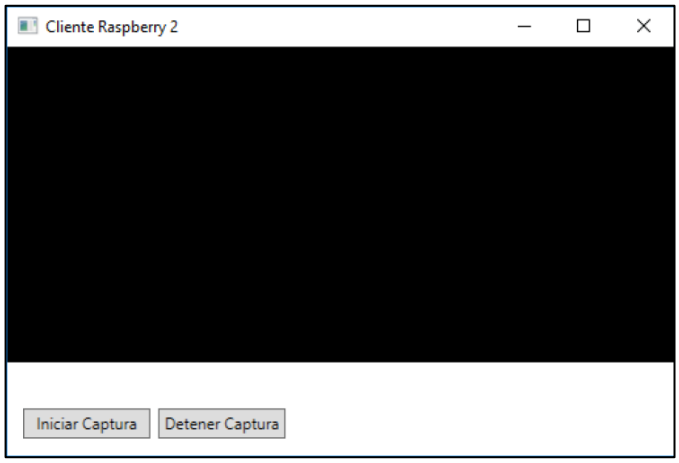


Figura 23. Interfaz gráfica cliente 2

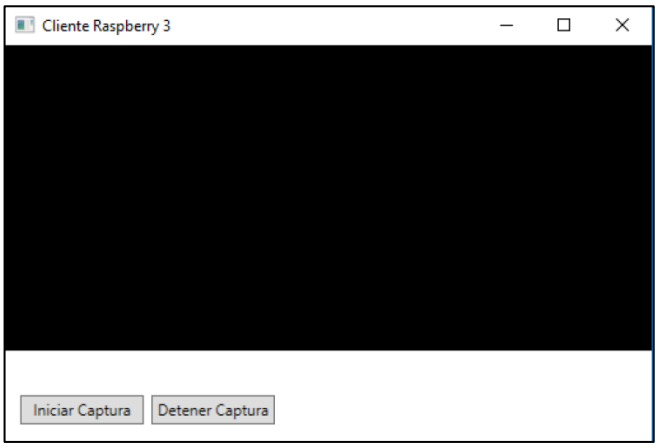


Figura 24. Interfaz gráfica cliente 3.

2.2.2 Sistema Operativo Raspbian

Como cualquier otro computador, Rasperry Pi necesita de un sistema operativo y las diferentes distribuciones de Linux son las preferidas por los usuarios de Raspberry, en su mayoría debido a que dichas distribuciones son gratuitas y también por la compatibilidad que estos sistemas tienen con la arquitectura ARM integrada en Raspberry. Rasbian es la distribución oficial y la más usada ya que esta fue desarrollada en conjunto con la placa. Tiene como base el sistema operativo Debian y se incluyen instrucciones y características únicas para ser aprovechadas por Raspberry Pi. Ya sea este en el uso de los pines GPIO o los puertos de cámara y display.

A continuación, se muestran varias distribuciones optimizadas para el uso de esta placa incluyendo una versión de Windows 10 pensado ya para la creación de proyectos en IoT o Internet de las Cosas por sus siglas en ingles.

En la figura 25 se muestran los distintos tipos de sistemas operativos existentes para raspberry:

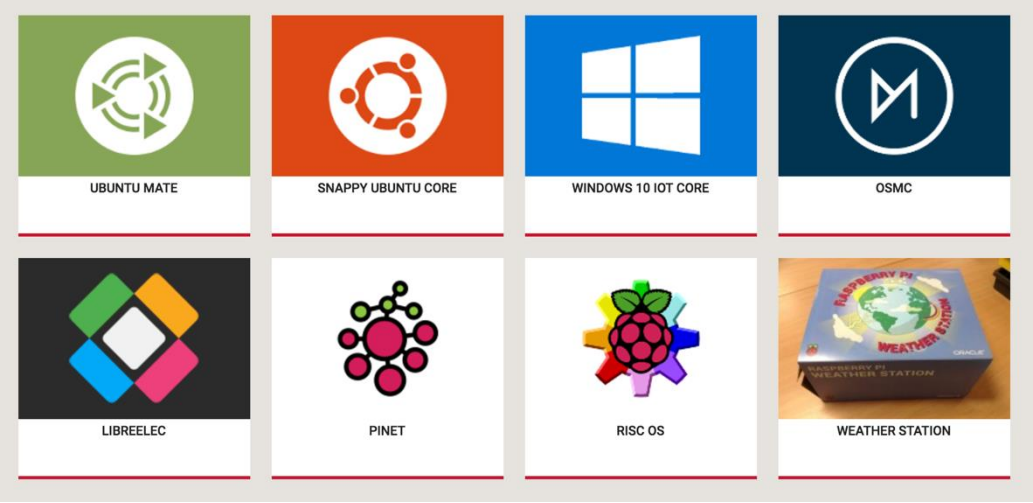


Figura 25. Sistemas Operativos para Raspberry.

Tomado de Raspberry Foundation, 2016.

2.2.2.1 Instalación Sistema Operativo Raspbian

Luego de realizar un análisis comparativo entre los sistemas operativos existentes se decidió instalar Raspbian, ya que incluye las librerías necesarias para la implementación de la red, cámaras de transmisión de video y como punto más importante es la única en raspberry que es compatible con HSMM-PI el cual es esencial para la implementación de la red MANET.

Rasbian se lo puede descargar de la página oficial de Raspberry Pi a través del siguiente link https://www.raspberrypi.org/downloads/. Allí se pueden encontrar dos opciones la una que se conoce como noobs y la otra que es la distribución de Raspbian.

En la figura 26 se muestra las opciones de instalación del sistema operativo seleccionado (raspbian)

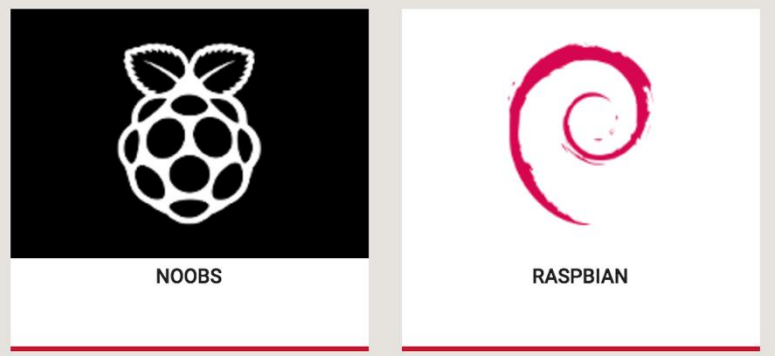


Figura 26. Opciones de instalación de Raspbian.

Tomado de Raspberry Foundation, 2016.

Hay que tomar en cuenta que Noobs no es más que una versión ligera de Raspbian, donde es necesario tener ciertos elementos para poder instalar el sistema operativo completo entre ellos se puede mencionar los siguientes.

- Televisor o display con una entrada HDMI.
- Cable HDMI.

- Mouse.
- Teclado

Otros elementos van a ser requeridos dependiendo del tipo de Raspberry que se tenga. En este caso se usa la versión 3, ya que esta permite la conectividad a internet a través del wifi integrado para la descarga del sistema operativo completo.

La versión completa se llama Raspbian Jessie y lo primero que se debe realizar es la descarga de dicha distribución se recomienda descargar la versión ZIP de la imagen para evitar tener que instalar otro tipo de programas de descarga.

En la figura 27 se muestra la versión del sistema operativo raspbian seleccionado.

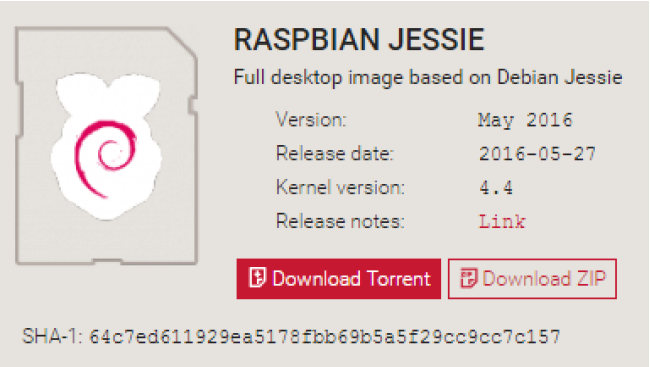


Figura 27. Sistema operativo Raspbian Jessie.

Tomado de Raspberry Foundation, 2016.

Dicha imagen que lleva como formato .img, se debe instalar en una tarjeta micro SD, con la ayuda del programa Win32 Disk Imager el cual va a montar el sistema operativo dentro de la tarjeta micro SD creando un dispositivo booteable.

En la figura 28 muestra el programa utilizado para montar el sistema operativo raspbian:

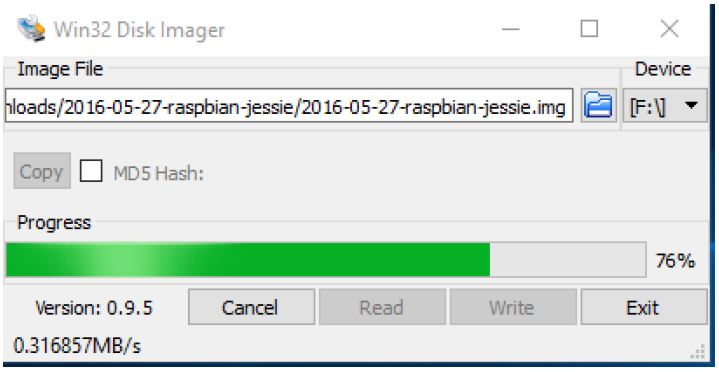


Figura 28. Win32 Disk Imager.

Una vez instalado el sistema operativo se coloca la tarjeta micro SD en la ranura existente en la Raspberry Pi. La manera más sencilla de configurar el resto de elementos ya sea la conexión a una red Wireless, cambio de claves y creación de usuarios se las realiza conectando periféricos como: Teclado, Mouse, Pantalla. El proceso de configuración se lo puede realizar a través de un terminal ssh sabiendo la dirección IP del dispositivo.

Terminadas las configuraciones preliminares es necesario realizar la expansión de la tarjeta micro SD para que el sistema operativo ocupe toda la capacidad de la tarjeta. Es un paso sumamente necesario para la correcta implementación del protocolo utilizado para la red MANET.

Es necesario habilitar la interfaz de la cámara ya que por defecto viene deshabilitada, para realizar esta configuración se debe abrir la pestaña de Menú, Posteriormente a preferencias y se abre la última opción que lleva por nombre Raspberry Pi Configuration. Se abre una ventana de configuración y en la pestaña de interfaces se procede con la activación de la cámara.

En la figura 29 muestra la interfaz gráfica del sistema operativo Raspbian:

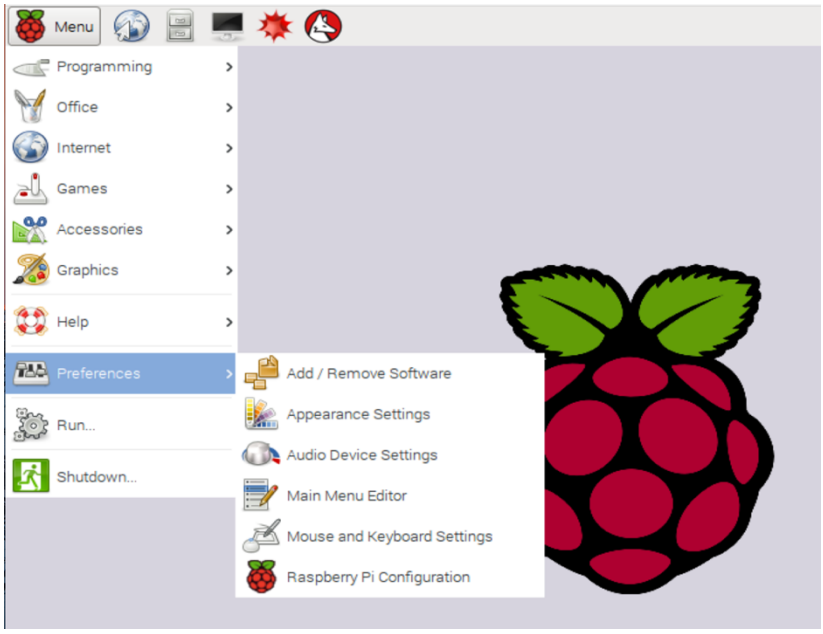


Figura 29. Pasos para activar interfaz de cámara.

En la figura 30 se muestra la interfaz gráfica para la activación de interfaces dentro de Raspberry PI:

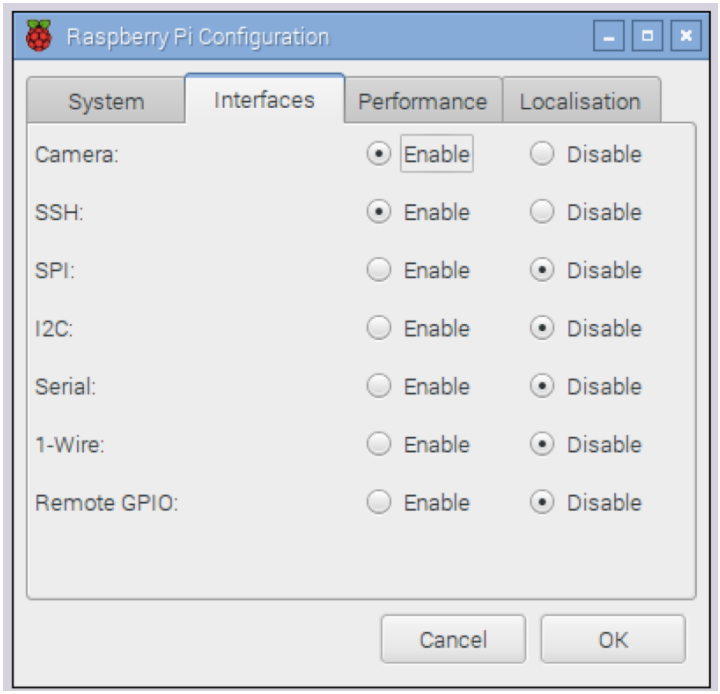


Figura 30. Activación de cámara.

2.2.3 Red MANET

Para la creación de la red MANET se usaron 3 módulos Raspberry Pi con 3 cámaras para probar funcionalidad de la red transmitiendo video en vivo mientras los nodos se encuentran en movimiento probando así la habilidad del protocolo OLSR de buscar y reconectar la red entre los nodos más cercanos y en caso del ingreso de un nuevo nodo esta pueda reestructurarse de manera automática.

Además, se implementa un servidor FTP con la única finalidad de transferir desde un computador el script de transmisión de video que contiene una dirección IP y puerto necesarios para que el Streaming funcione de manera correcta.

Un computador con Windows 10 que va a servir como centro de control en donde se observa calidad de enlace de los nodos, reproducción del video transmitido en una aplicación creada en Visual Studio. El programa contiene la dirección IP de cada nodo de la red MANET, así como un puerto necesario para la transmisión.

En la siguiente figura se observa un esquema de la red MANET diseñada, cada nodo tiene una dirección IP estática, al igual que el computador de pruebas. El enrutamiento dentro de la red lo maneja el protocolo OLSR.

En la figura 31 se muestra el esquema del diseño propuesto de la red MANET:

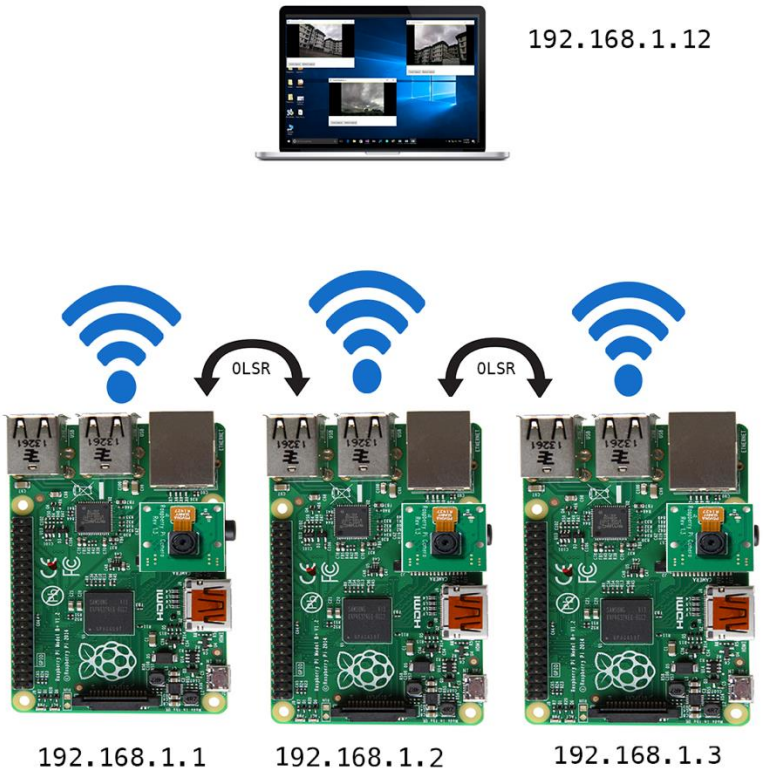


Figura 31. Esquema de Diseño de red MANET

2.2.3.1 HSMM (High Speed MultiMedia)

HSMM conocido también como “hinternet” se basa en lo que comercialmente se conoce como tecnología de Radio red de área Local (RLAN). HSMM es la implementación de redes inalámbricas de datos sobre radiofrecuencias de aficionados usando hardware comercial (COTS) como puntos de acceso 802.11 y equipos D-Star. Los operadores de radio aficionados con licencia pueden utilizar amplificadores y antenas especializadas para aumentar la potencia y la cobertura de la señal 802.11. El nombre “hinternet” proviene de la combinación de las palabras “ham” e “internet” y puede utilizarse para referirse a cualquier red de datos de alta velocidad sobre radioaficionados, no sólo redes 802.11.

HSMM soporta la mayor parte del tráfico que actualmente realiza Internet, incluyendo video chat, voz, mensajería instantánea, Web (HTTP) y

transferencia de archivos (FTP), puede incluso conectarse a Internet y usarse para "navegar por la Web".

En la figura 32 se muestra el esquema del diseño de una red HSMM-MESH:

a. HSMM-Mesh

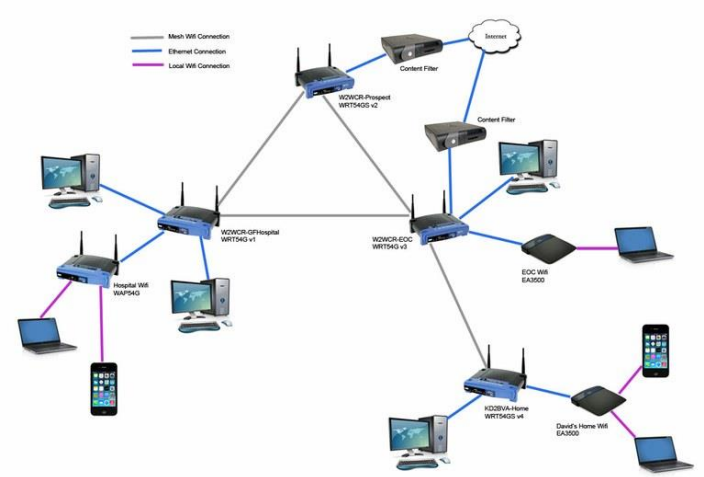


Figura 32. Esquema red HSMM-Mesh.

Tomado de W2WCR, 2008.

Es una red de datos inalámbrica de alta velocidad, auto descubrimiento, auto configuración, tolerante a fallos que utiliza muy poca energía. HSMM-MESH combina las capacidades Multi Media de alta velocidad de Ethernet inalámbrica con routers que pueden realizar la configuración automática de red (MESH). Una red HSMM-MESH utiliza un conjunto de routers inalámbricos especialmente programados que buscan routers "vecinos" y luego intercambian información entre ellos sobre qué routers están en la red y qué otros routers pueden contactar cada uno y con qué nivel de calidad de señal. Utilizando esta tecnología, los routers pueden llegar a un sitio y conectarse a una red en pocos segundos. Esto se hace mediante un proceso de reconfiguración periódico, pero automático, para convertirse en parte de la red. Permite que los datos del usuario y los dispositivos muevan sus datos de forma automática y transparente a través de un conjunto de routers. (Gordon, 2013, PP.26)

b. HSMM-Pi

HSMM-PI es una implementacion de software libre cuyo codigo fuente y todas los aportes por parte de la comunidad HSMM se encuentran en GITHUB.

HSMM-Pi es un conjunto de herramientas diseñado para configurar fácilmente el Raspberry Pi para funcionar como un nodo inalámbrico de alta velocidad Multimedia (HSMM) compatible with Broadband Hamnet (BBHN) and AREDN. Las redes mesh ofrecen a los operadores de radio aficionados (hams) la capacidad de operar redes de datos de alta velocidad en las frecuencias compartidas con los usuarios sin licencia de equipos de red 802.11 b/g/n. Hams pueden operar HSMM o BBHN con mayor potencia con antenas de mayor tamaño que los que están disponibles para los usuarios sin licencia. HSMM-Pi permite ejecutar un nodo mesh HSMM en el Raspberry Pi.

HSMM-Pi consiste en una aplicación web PHP que se utiliza para configurar y supervisar cada nodo y la instalación de un script Shell el cual crea dependencias y pone las cosas en los lugares correctos. Además, HSMM-Pi está diseñado para ejecutarse en sistemas Ubuntu 12.04. En lugar de proporcionar una imagen de sistema operativo para HSMM Pi, se ha creado un script de instalación que transformará un host común en un nodo HSMM-Pi. Esto tiene varios beneficios:

- Transparencia: Se podrá ver exactamente qué cambios se realizan en el sistema base mirando el script shell de instalación.
- Más fácil de trasladar a más plataformas: Cualquier plataforma que ejecute las versiones de Ubuntu soportadas debería ser capaz de ejecutar HSMM-Pi.
- Más fácil para los hosts: Solo se tendrá que publicar el script de instalación y los archivos webapp en Github y estará listo.

Modos HSMM-Pi

HSMM-Pi tiene 2 modos: Internal y Gateway. A continuación, una descripción de cada uno.

Modo Internal

Un nodo en modo Interno encamina el tráfico a través de la red MANET y proporciona acceso a todos los hosts conectados a su puerto Ethernet cableado. El nodo en este modo ejecuta un servidor DHCP que emite concesiones DHCP a cualquier host de la conexión cableada. También ejecuta un servidor DNS que puede proporcionar resolución de nombres tanto para los nodos de la red como para los hosts de Internet.

Modo Gateway

Un nodo en modo Gateway enruta el tráfico a lo largo de la red y proporciona a la misma con acceso a Internet a través del puerto Ethernet por cable. El Gateway obtiene DHCP en la interfaz cableada y anuncia su enlace de internet a los nodos de la red utilizando enrutamiento OLSR.

En la Figura 36 se muestra un ejemplo de un esquema de la red MANET usando los dos modos que HSMM-PI, ya sea este en Modo Gateway o Internal.

En la figura 33 se muestra el esquema del diseño de la red HSMM-PI:

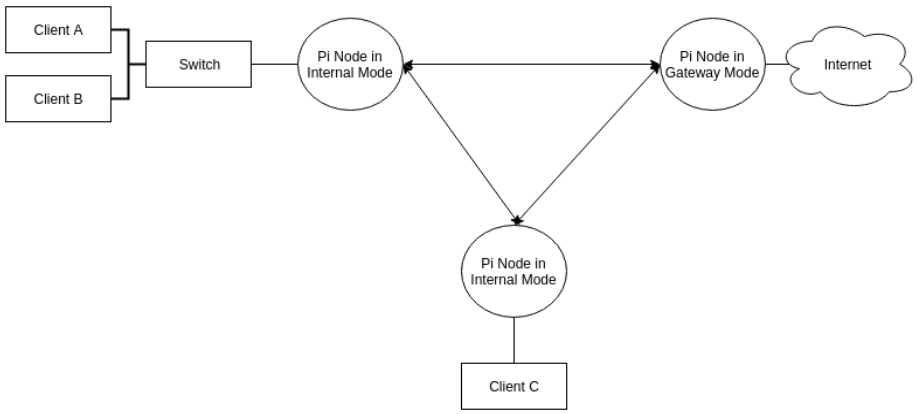


Figura 33. Esquema General red HSMM-Pi (MANET).

Tomado de HSMM-PI,2016

2.2.3.2 Implementación HSMM-PI

Antes de instalar HSMM-PI se necesita expandir el sistema de archivos para ocupar todo el espacio de la tarjeta de memoria, se usa el comando *sudo raspi-config*, este comando muestra todas las configuraciones y modificaciones que se pueden realizar al sistema operativo Raspbian entre ellas la expansión del sistema de archivos.

En la figura 34 se muestra el proceso para la expansión del sistema operativo y así ocupe toda la memoria de la tarjeta micro SD:

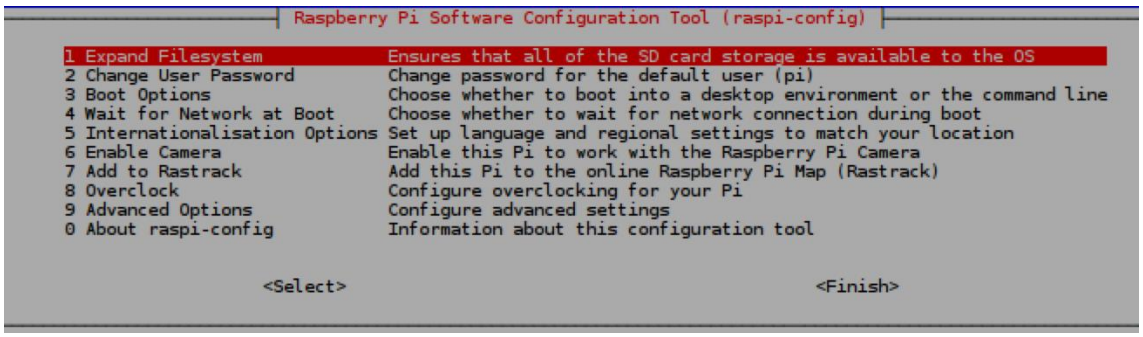


Figura 34. Expansión de sistema de archivos.

Una vez realizado este paso se prosigue con la instalación de HSMM-PI, se recomienda ejecutar los siguientes comandos para actualizar el sistema operativo y todos los ficheros necesarios con la finalidad de evitar cualquier error durante la instalación.

“Sudo apt-get update”

“Sudo apt-get upgrade”

El siguiente paso es opcional ya que en las versiones recientes de Raspbian, GIT ya viene instalado por defecto, se recomienda ejecutar el comando solo para asegurar que GIT esté instalado.

“Sudo apt-get install -y git”

Para iniciar con la instalación de HSMM-PI se debe tener una conexión a wifi ya sea vía USB en el caso de raspberry pi modelo B+ 1 y 2 y para Raspberry Pi 3 se usa la conexión interna que ya vienen incluida.

Se ejecutan los siguientes comandos:

“Git clone https://github.com/urlgrey/hsmm-pi.git*”*

Este comando descarga desde GIT el directorio con todos los archivos necesarios para la instalación. La descarga debería durar algunos segundos y al completarse hay que ingresar al directorio descargado con el siguiente comando *cd hsmm-pi* dentro del directorio se procede con la instalación usando *sh install.sh* este comando ejecuta el script install.sh.

En la figura 35 se muestra la ejuccion del script install.sh:

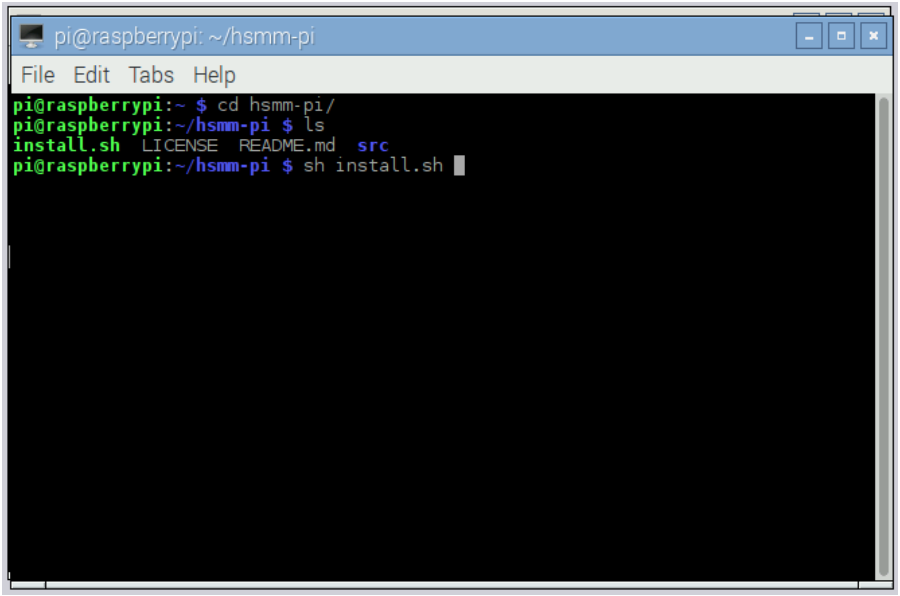


Figura 35. Ejecución de script install.sh.

Este script descarga una variedad de ficheros nuevos y construye la infraestructura necesaria para el funcionamiento del protocolo, también crea una aplicación web para el control y visualización de los nodos de la red MANET.

En la figura 36 se muestra la ejuccion del script install.sh:

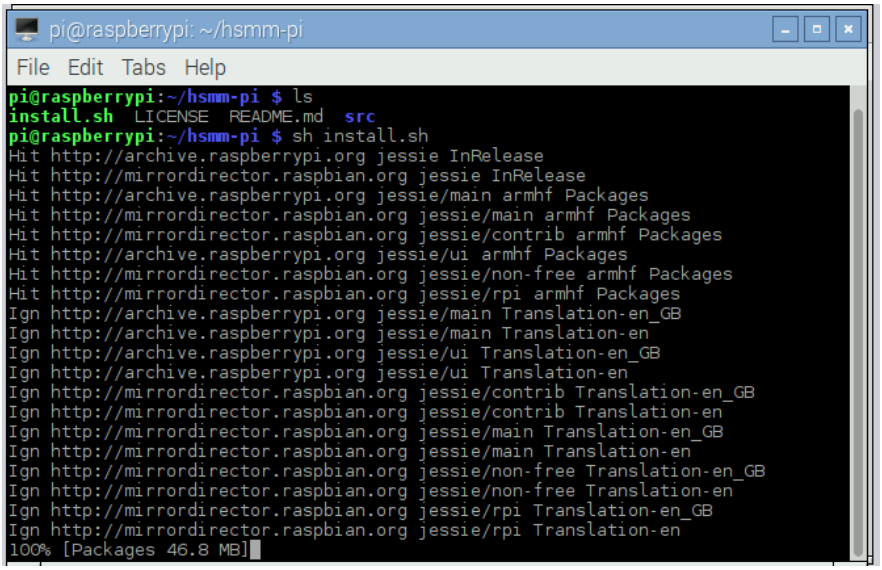


Figura 36. Descarga de ficheros.

A continuación, se muestra una lista con todas las dependencias descargadas por el script y que posteriormente son configuradas.

- Apache2
- Php5
- Sqlite
- Php5-mcrypt
- Php5-sqlite
- Dnsmasq
- Sysv-rc-conf
- Make
- Bison
- Flex
- Gpsd
- Libnet-gpsd3-perl
- Ntp

En la figura 37 se muestra la compilación del codigo de enrutamiento OLSR:

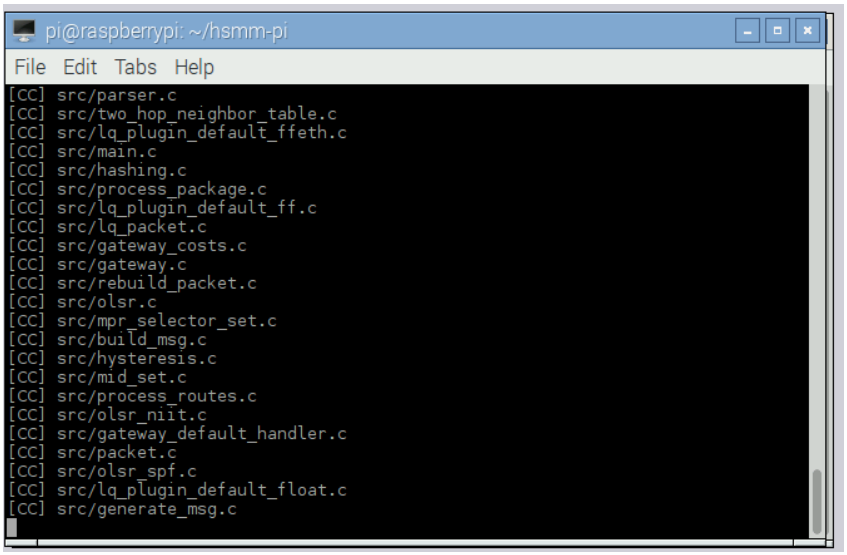


Figura 37. Compilación de código de protocolo OLSR.

El tiempo de instalación dependerá de la velocidad de la conexión a internet y el poder de procesamiento que tenga cada Raspberry PI. Al finalizar con la instalación se despliega un mensaje de éxito como se muestra en la siguiente imagen.

En la figura 38 se muestra un mensaje de instalacion exitosa de HSMM-PI:

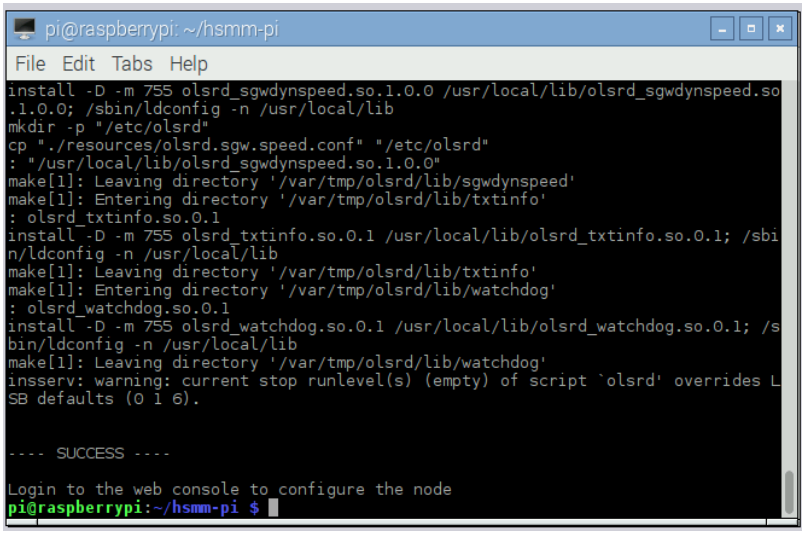


Figura 38. Instalación exitosa de HSMM-PI.

Configuración de Nodos

Al concluir la instalación se puede acceder a la interfaz web para la configuración de nodos, simplemente se abre un buscador y se ingresa la dirección IP asignada al nodo. Se puede visualizar una interfaz como la siguiente.

En la figura 39 y 40 se muestra el proceso de inicio y login de la interfaz de control de cada nodo que forma parte de la red MANET:

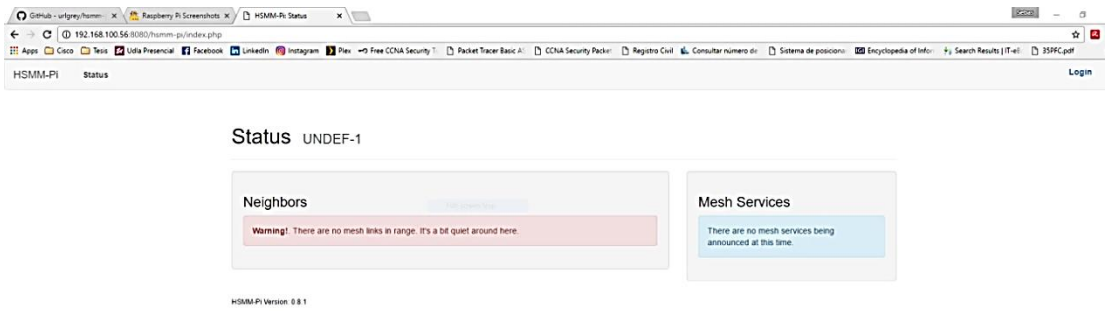


Figura 39. Página inicial HSMM-PI.

Para acceder a las configuraciones es necesario autenticarse en una interfaz de login. El usuario y contraseña por defecto es “admin” y “changeme” respectivamente. Se recomienda cambiar estas credenciales por seguridad.

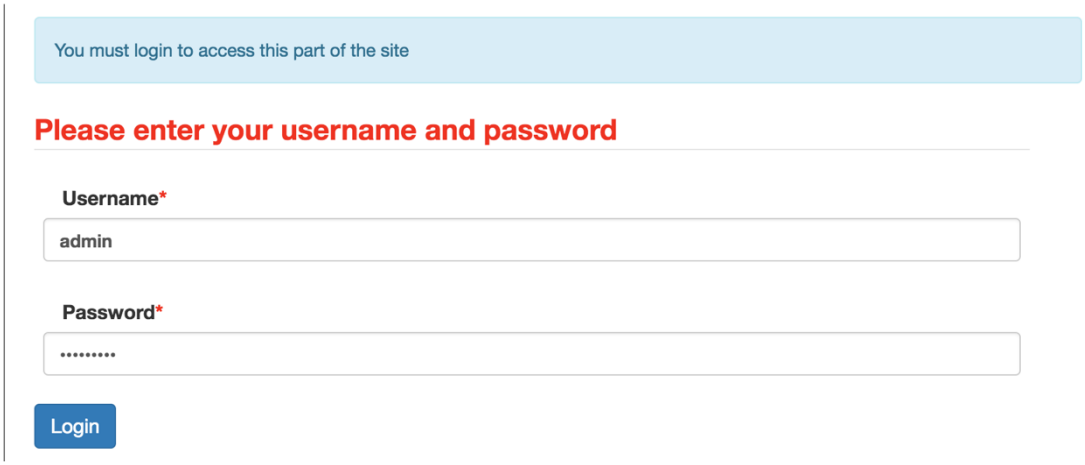


Figura 40. Login HSMM-PI.

Dentro de admin existen las siguientes opciones

- Red
- Servicios
- Localización
- Cuenta de Usuario
- Escaneo de Wifi
- Reinicio y apagado de nodo

Red

Dispone de 4 botones, Wifi, Wired, Mesh, Time

Wifi

Se configura la dirección IP del nodo, mascara de red, el adaptador por defecto que en la mayoría de casos va a ser wlan0, un nombre para la red (SSID) este debe ser el mismo para todos los nodos.

En la figura 41 se muestra un ejemplo de configuración de lo mencionado anteriormente:

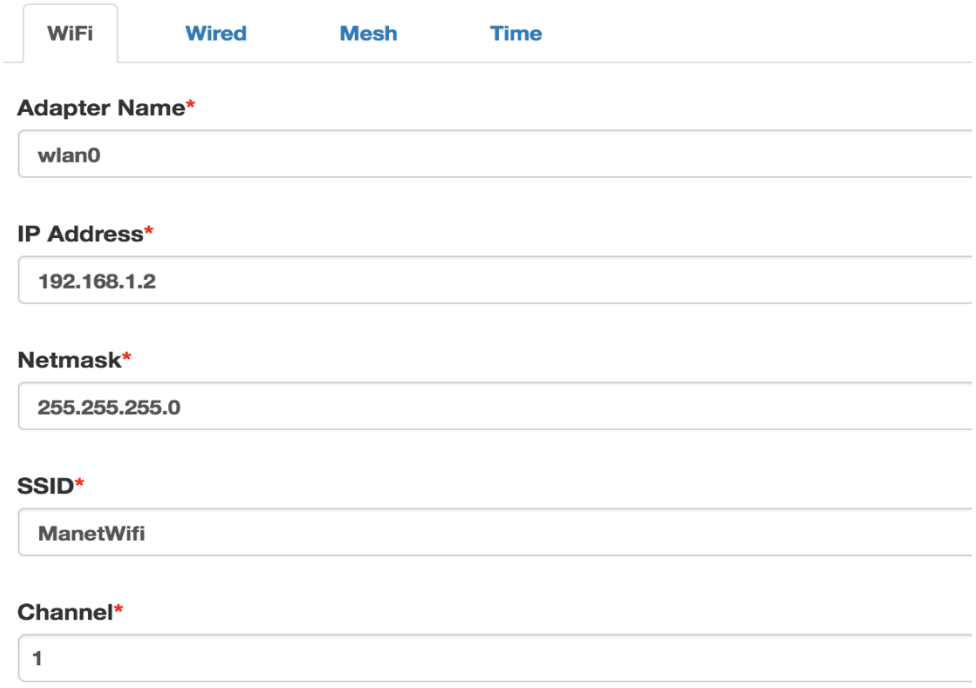


Figura 41. Configuración WiFi.

Wired

Parecida a la primera pestaña de configuraciones, en esta se elige el modo de configuración del nodo.

- Modo Gateway con interfaz WAN
- Modo Internal con interfaz LAN

Se puede ingresar una dirección IP o dejar la que viene incluida por defecto, asi mismo existe la posibilidad de habilitar o deshabilitar el servidor DHCP. Debido a que la red a implementarse es una red MANET no es necesario que los nodos proporcionen DHCP ya que no van a tener clientes conectados. A continuación, se muestra la configuración predeterminada.

En la figura 42 se muestra un ejemplo de configuración de lo mencionado anteriormente:

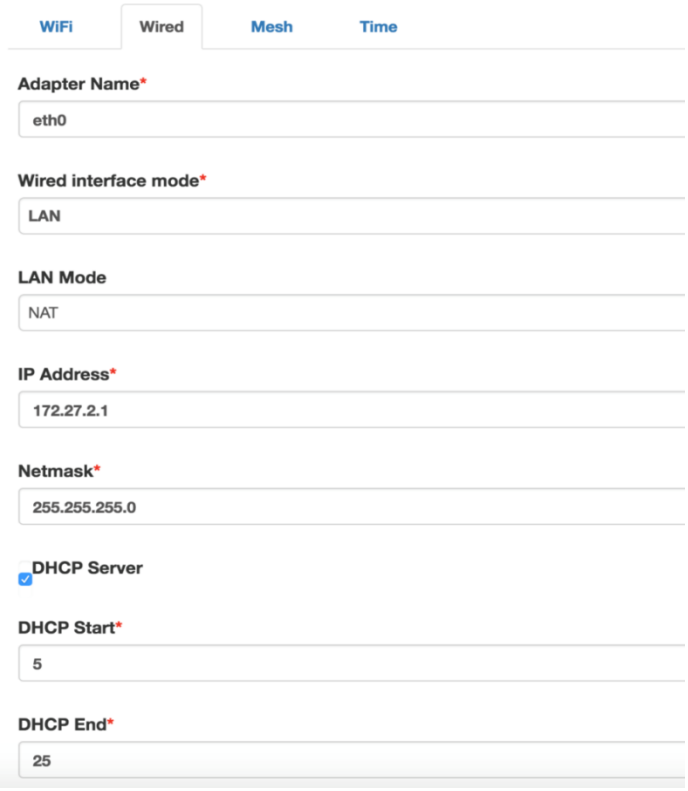


Figura 42. Configuración Wired.

Mesh

Se proporciona un nombre para el nodo que sirva como identificador, además adiciona una capa de seguridad que es opcional y sirve para validar nodos que se quieran incorporar a la red.

En la siguiente imagen se configura el nombre del nodo como ManetTesis y se procede a desactivar OLSRD Secure debido a que provoca errores de conexión de los nodos.

En la figura 43 se muestra un ejemplo de configuración de lo mencionado anteriormente:

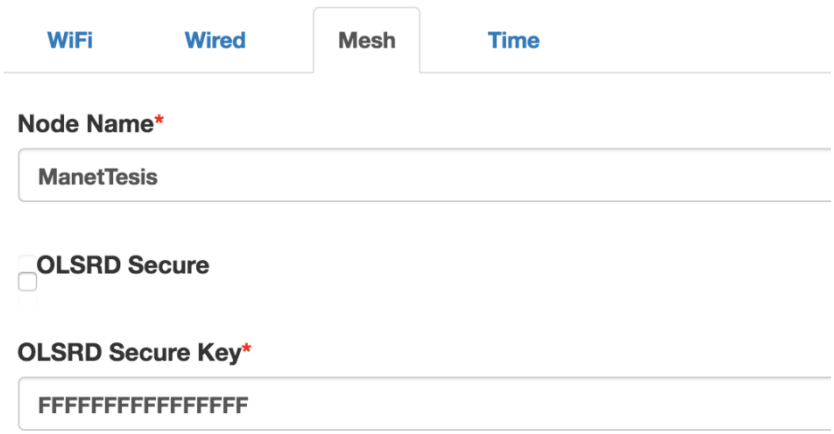


Figura 43. Configuración Mesh.

Servicios en la red

HSMM-PI abre la posibilidad de agregar cualquier servicio que involucre los protocolos TCP y UDP.

En la figura 44 se muestra un ejemplo de configuración de lo mencionado anteriormente:

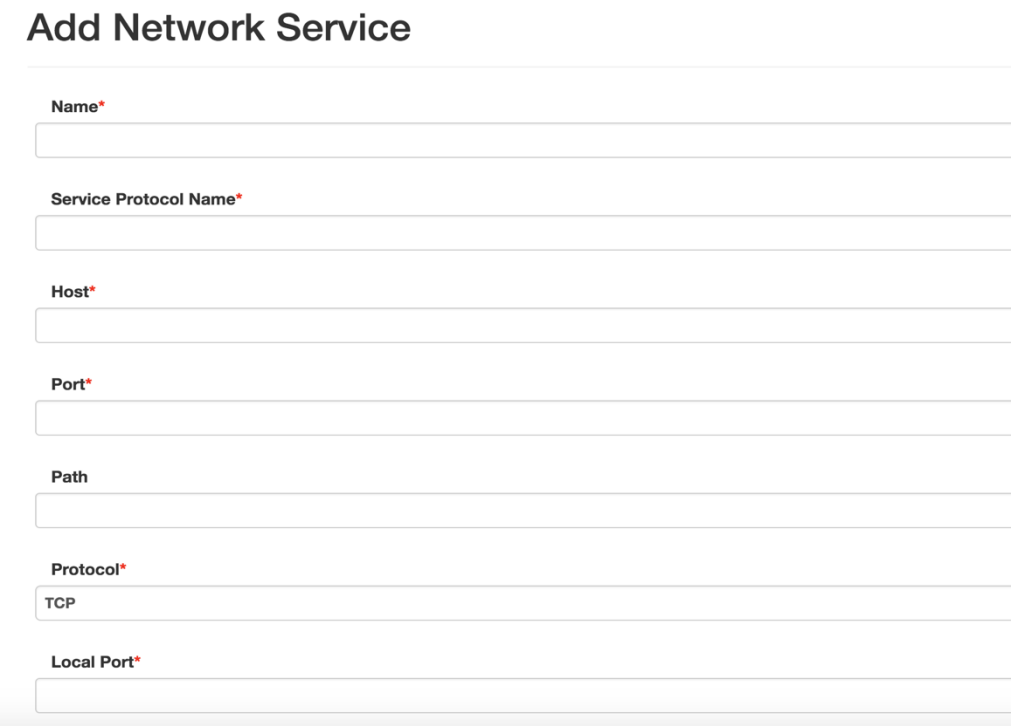


Figura 44. Creación de servicios dentro de la red**.**

2.2.4 Script de Streaming de Video

Como se mencionó anteriormente, la transmisión de video consta de dos partes, del lado del cliente existe el aplicativo desarrollado visual studio mientras que del lado del nodo existe un script creado en java, en donde se usan las mismas librerías de Eneter para establecer la comunicación. De igual manera el código utilizado es open source.

Dentro de este script se encuentran una serie de comandos para la captura de video desde Raspberry Pi. Dicha herramienta basado en líneas de comando lleva como nombre “Raspivid”.

El servicio ejecuta raspivid con los siguientes parámetros:

“raspivid -n -vf -hf -co -br -ih -w 640 -h 380 -fps 24 -t 0 -o – “

- **-n:** Evita generar vista previa
- **-vf –hf:** Voltea el video de manera vertical y horizontalmente
- **-ih:** Genera cabeceras SPS y PPS para evitar problemas en el caso de que un segundo cliente desee conectarse a la misma transmisión.
- **-w 640 –h 380:** Genera un video de 680 x 380 pixeles.
- **-fps 24:** Produce video a 24 cuadros por segundo.
- **-t 0:** Captura de video por un tiempo indefinido
- **-o –:** Produce el video por la salida estándar stdout para que pueda ser capturado por la aplicación del cliente.

Una vez configurado los parámetros de video que se consideren necesarios, se debe generar un archivo .jar que va a ser ejecutado dentro de cada nodo de la siguiente manera.

“Java –jar raspberry-camera-service.jar.

2.3 Diagramas de Interconexión

2.3.1 Diagrama General

En la figura 45, 46, 47 y 48 se muestra un diagrama general, diagrama de la red MANET, diagrama de los nodos de la red y diagrama de software de gestión respectivamente implementados en el proyecto.

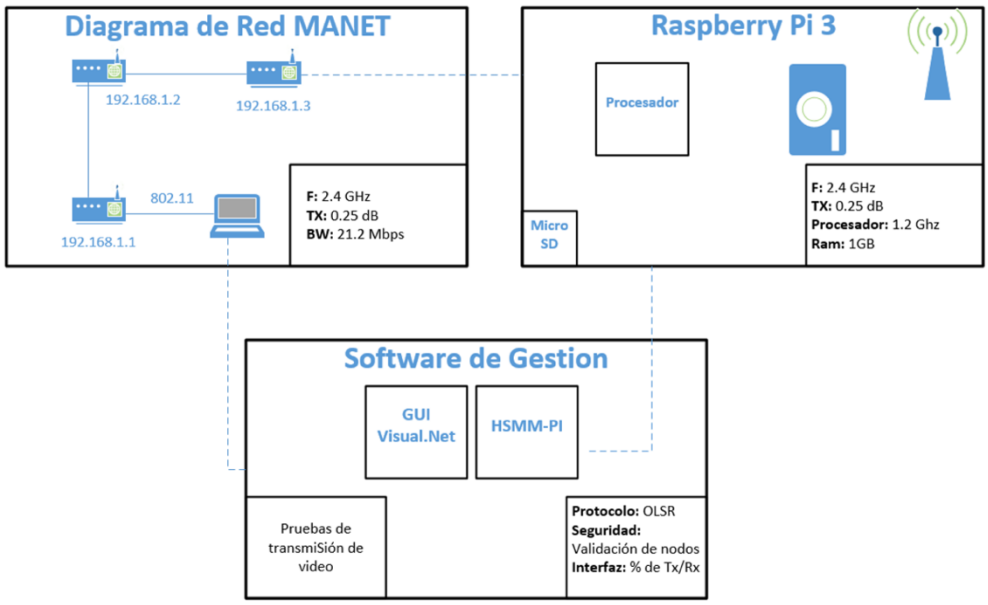


Figura 45. Diagrama General.

2.3.2 Diagrama Red MANET

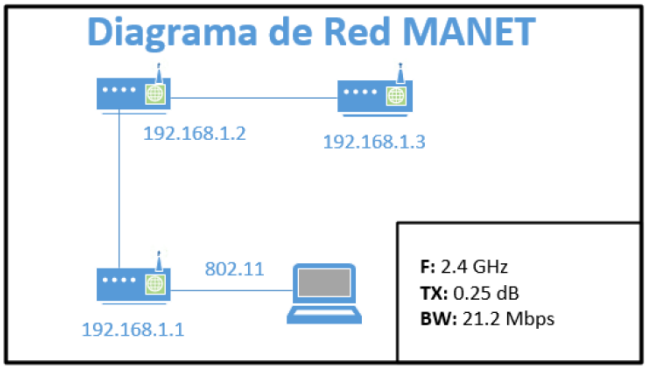


Figura 46. Red MANET.

2.3.3 Diagrama de Nodos de Red

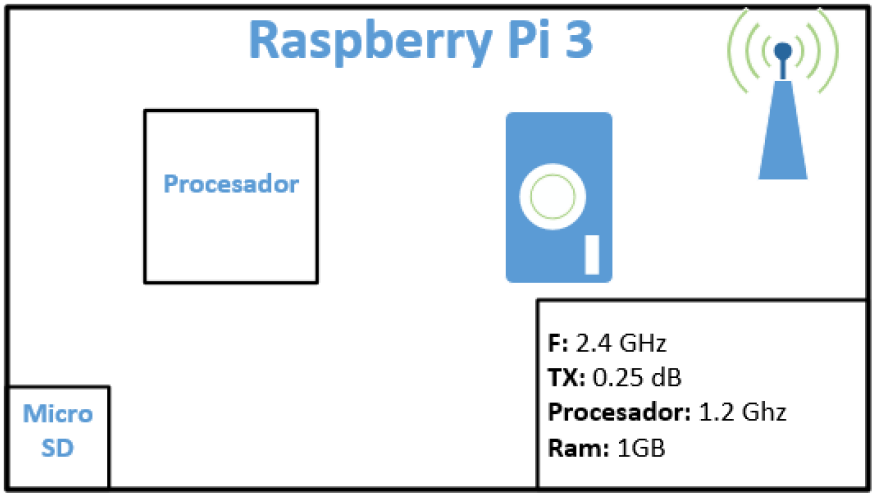


Figura 47. Nodos de Red.

2.3.4 Diagrama de Software de Gestión

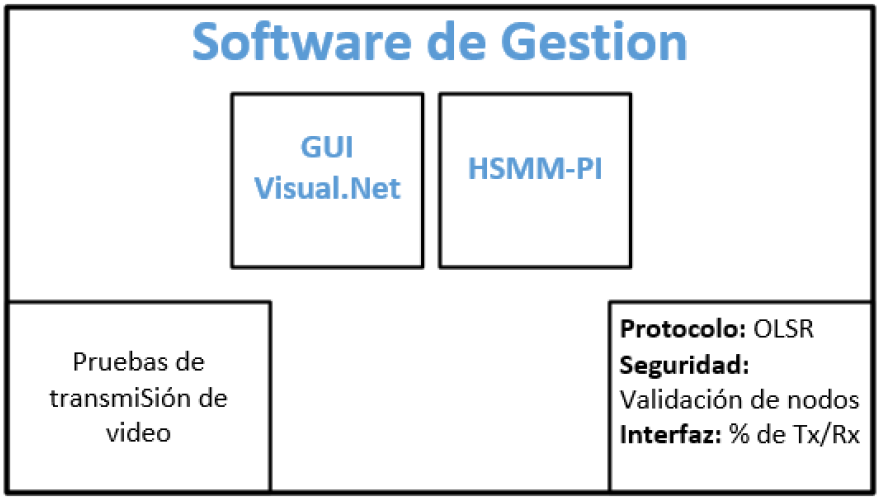


Figura 48. Software de Gestión.

3. CAPITULO III. Presentación de resultados

En este capítulo se presentan todos los resultados de las pruebas realizadas en los distintos tipos de escenarios que fueron propuestos y se realizaron tabulaciones del presente proyecto.

En la tabla 8 se muestra el plan de pruebas para la validación del proyecto.

Tabla 8.

Plan de Pruebas

Plan de Pruebas				
Hardware	**Software**	**Documentos**	**Instalaciones**	**Ambientes**
Laptop Macbook Pro 15''	Máquina Virtual Windows 10	Datasheet Raspberry Pi 3	Laboratorio UITEC/UDLA	Laboratorio UITEC/UDLA
3 Raspbery Pi 3	Raspbian Jessie	Datasheet Raspberry Pi Camera v2	Universidad de Las Americas	Exteriores Campus Sede Queri
3 Raspberry Pi Camera v2	HSMM-PI		Conjunto Habitacional Granados	Cancha de Basquet Condominios El Batan
3 Baterías portátiles de 4000 mah	Visual Studio			

3.1 Escenario de pruebas.

3.1.1 Escenario 1

Laboratorio UITEC (UDLA)

La primera prueba fue realizada en el Laboratorio de la Unidad de Innovación Tecnológica (UITEC).

Cuyas coordenadas geográficas son las siguientes para los 3 nodos.

Nodo 1: 0° 10' 12.004" S 78° 28' 15.298" W.

Nodo 2: 0° 10' 12.004" S 78° 28' 15.298" W.

Nodo 3: 0° 10' 12.004" S 78° 28' 15.298" W.

En la figura 49 se muestra un mapa mostrando el escenario 1:

Figura 49. Escenario de Prueba 1.

3.1.2 Escenario 2

Áreas Verdes Universidad de las Américas Sede Queri.

La segunda prueba fue realizada en los exteriores de la Universidad de las Américas sede Queri tal como se muestra en el mapa a continuación. Los pines

de color amarillo indican la posición de los 3 nodos de la red MANET y cuyas coordenadas son las siguientes.

Cuyas coordenadas geográficas son las siguientes para los 3 nodos.

Nodo 1: 0° 10' 10.322" S 78° 28' 15.125" W.

Nodo 2: 0° 10' 9.826" S 78° 28' 15.175" W.

Nodo 3: 0° 10' 8.357" S 78° 28' 15.118" W.

En la figura 50 se muestra un mapa mostrando el escenario 2:

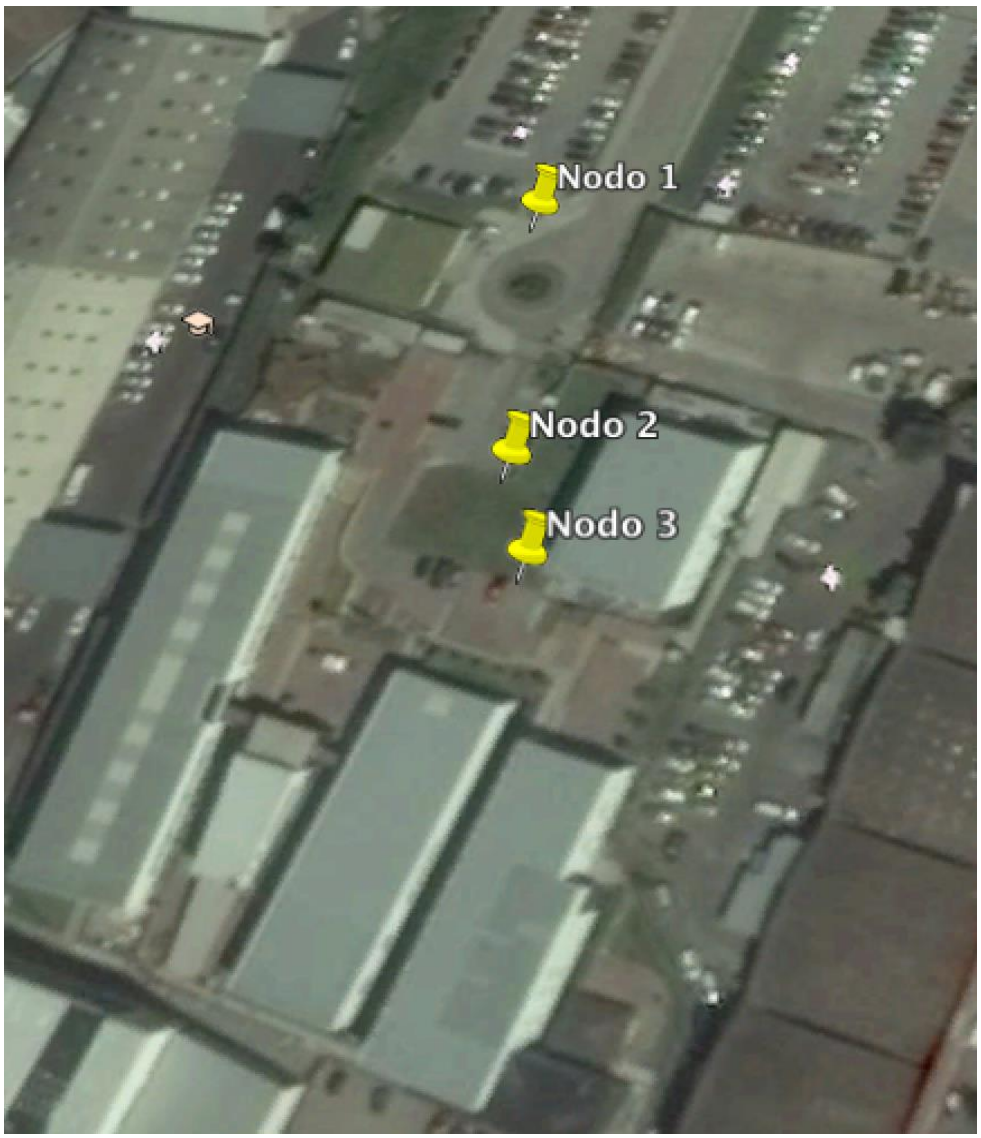


Figura 50. Escenario de Prueba 2.

3.1.3 Escenario 3

Cancha de básquet conjunto habitacional Granados.

La tercera prueba fue realizada en dentro del conjunto habitacional Granados tal como se muestra en el mapa a continuación. Los pines de color amarillo indican la posición de los 3 nodos de la red MANET.

Cuyas coordenadas geográficas son las siguientes para los 3 nodos.

Nodo 1: 0° 9' 57.654" S 78° 28' 13.876" W.

Nodo 2: 0° 9' 57.154" S 78° 28' 13.519" W.

Nodo 3: -0° 9' 56.563" N 78° 28' 13.944" W.

En la figura 51 se muestra un mapa mostrando el escenario 3:

Figura 51. Escenario de Prueba 3.

3.2 Inicio de Pruebas

3.2.1 Escenario 1

A continuación, se muestra el diagrama del escenario 1 con las respectivas distancias entre los nodos de la red MANET. Dicha prueba se realizó en las instalaciones de la Unidad de Innovación Tecnológica UITEC.

En la figura 52 se muestra un esquema de prueba realizada en el escenario 1:

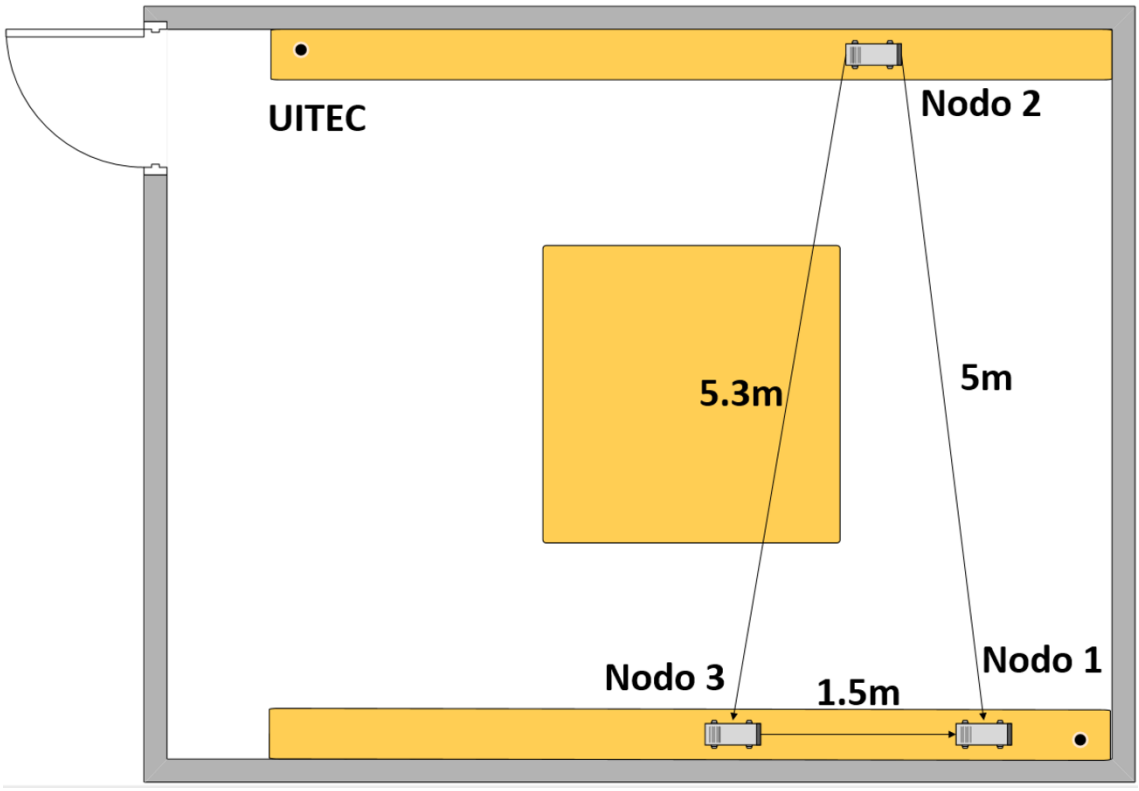


Figura 52. Red MANET prueba 1.

Se realizó la prueba de transmisión de video en tiempo real dando esta un resultado 100 % satisfactorio por parte de cada uno de los nodos que forman la red MANET.

En la figura 53 se muestra la transmisión de video en tiempo real de la prueba en escenario 1:

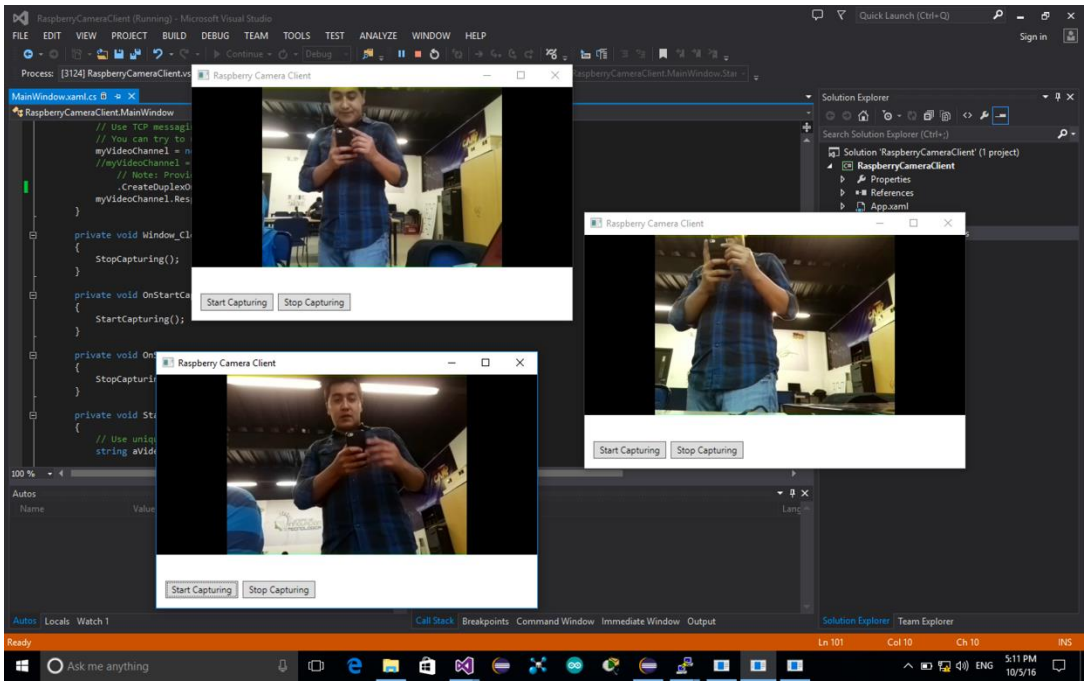


Figura 53. Prueba transmisión de video en tiempo real.

De igual manera se realizó una medición de calidad del enlace usando la interfaz gráfica de HSMM-PI respecto a cada nodo de la red.

En la figura 57 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.1, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres.

En la figura 54, 55, 56 se muestra la calidad del enlace de los 3 nodos medidos en el escenario 1 respectivamente:

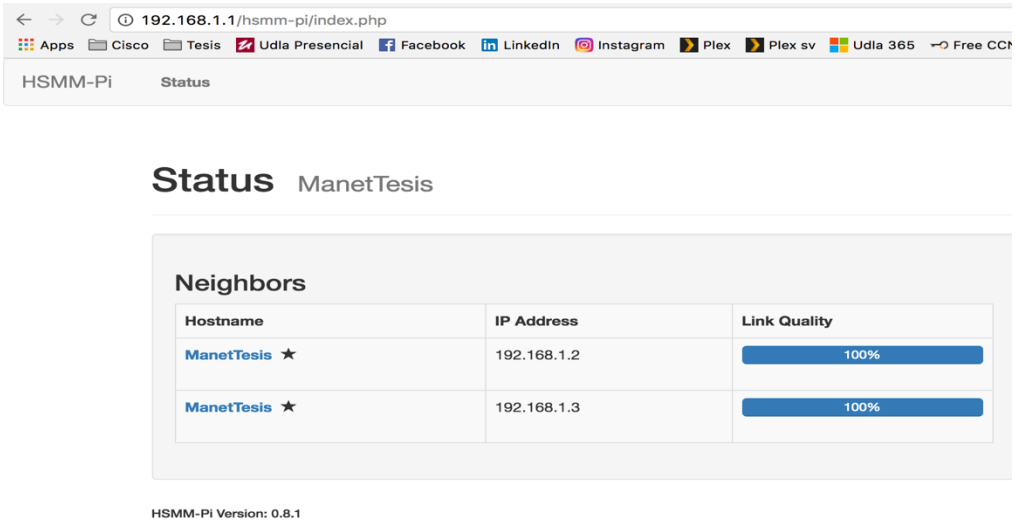


Figura 54. Prueba de enlace Nodo 1.

En la figura 58 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.2, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres.

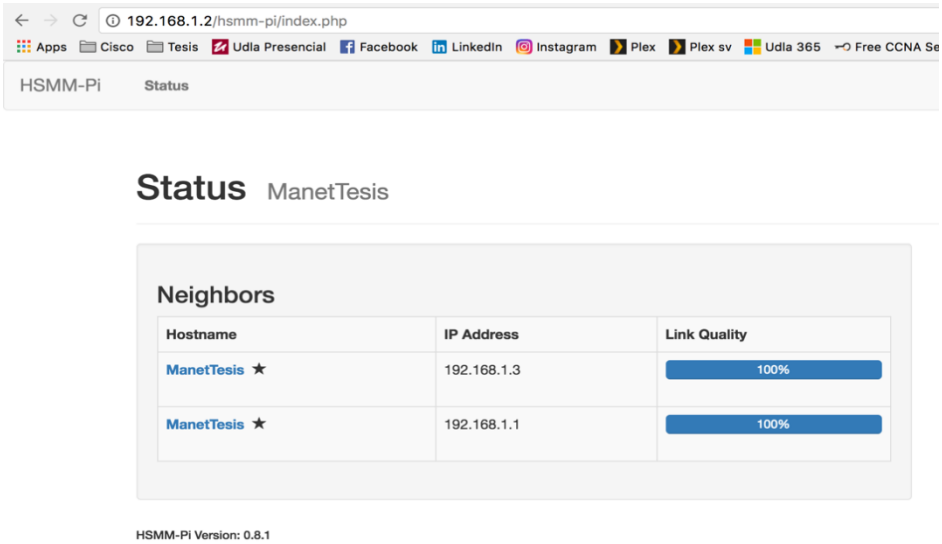


Figura 55. Prueba de enlace Nodo 2.

En la figura 59 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.3, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres.

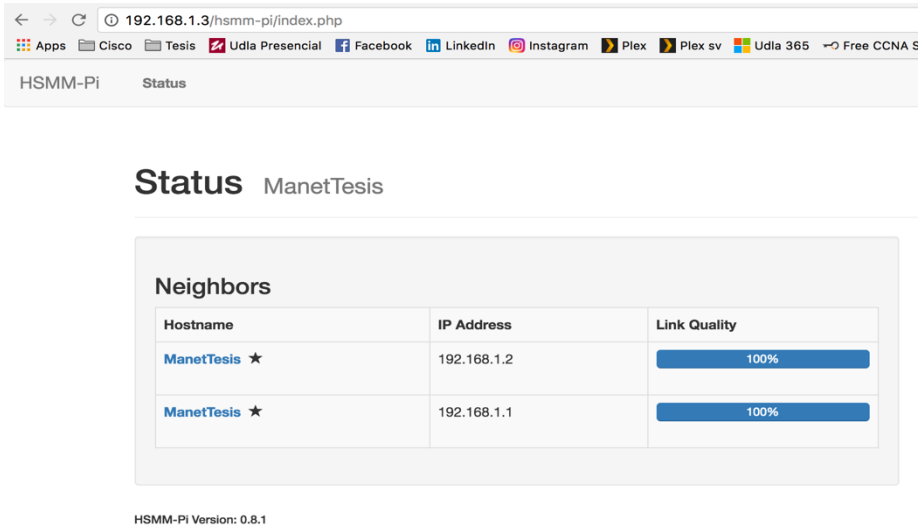


Figura 56. Prueba de enlace Nodo 3.

Finalizando las pruebas en el escenario 1 se realizó el análisis de potencia de la red MANET dando los siguientes resultados.

Primero se realiza un estudio con el software de gestión de redes NETSPOT para Windows 10 en donde como se observa en la figura 60 esta solo muestra un solo canal usado por la red. El software analiza los 3 nodos de la red MANET como uno solo los cuales trabajan en el mismo rango de frecuencia y tienen una potencia de -40dB.

En la figura 57 se muestra la frecuencia y canal de funcionamiento de la red MANET para el escenario 1:

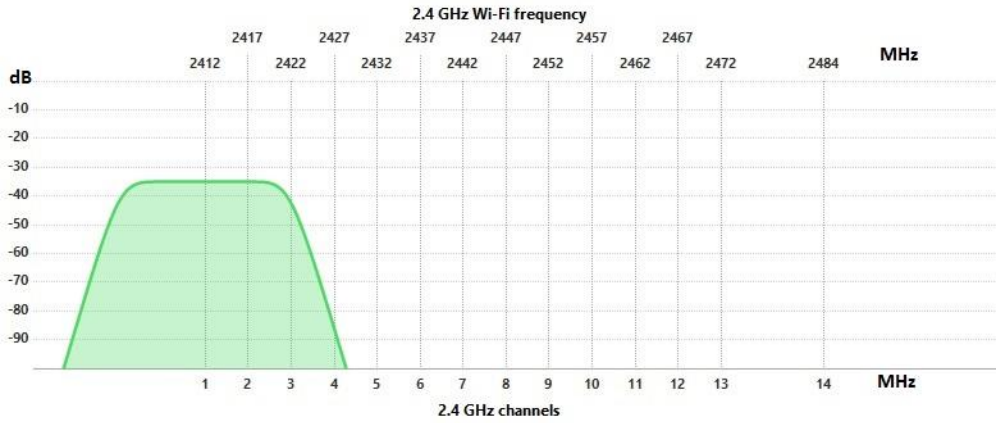


Figura 57. Frecuencia y canal de funcionamiento de red MANET.

Posteriormente en la figura 61 se utiliza es mismo programa y se realiza un análisis de potencia, pero esta vez respecto al tiempo. Esta prueba se realiza para visualizar el desempeño de la red en el ambiente propuesto y en donde se puede notar que hubo desconexiones de un corto tiempo ya sea esta por algún factor externo o porque el protocolo OLSR encontró un mejor enlace de conexión.

En la figura 58 se muestra un análisis de potencia de la red MANET para el escenario 1:

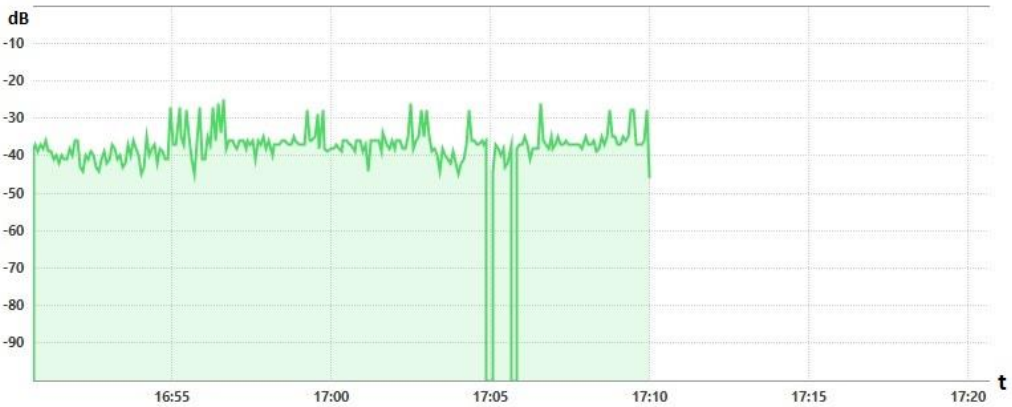


Figura 58. Análisis de potencia de red MANET.

La tabla 9 presenta un resumen con la distancia entre nodos y el retardo de video promedio de toda la red entre los nodos de la red y la computadora de control.

Tabla 9.

Resumen Escenario de Pruebas 1

Escenario 1	
Resumen	
Distancia entre Nodo 1 y Nodo 2	5 m
Distancia entre Nodo 1 y Nodo 3	1.5 m
Distancia entre Nodo 2 y Nodo 3	5.3 m
Retardo de video promedio	1s

3.2.2 Escenario 2

A continuación, se muestra el diagrama del escenario 2 con las respectivas distancias entre los nodos de la red MANET. Dicha prueba se realizó en los exteriores de la Universidad de las Américas Campus Queri.

En la figura 59 y 60 se muestra un esquema de prueba realizada en el escenario 2:

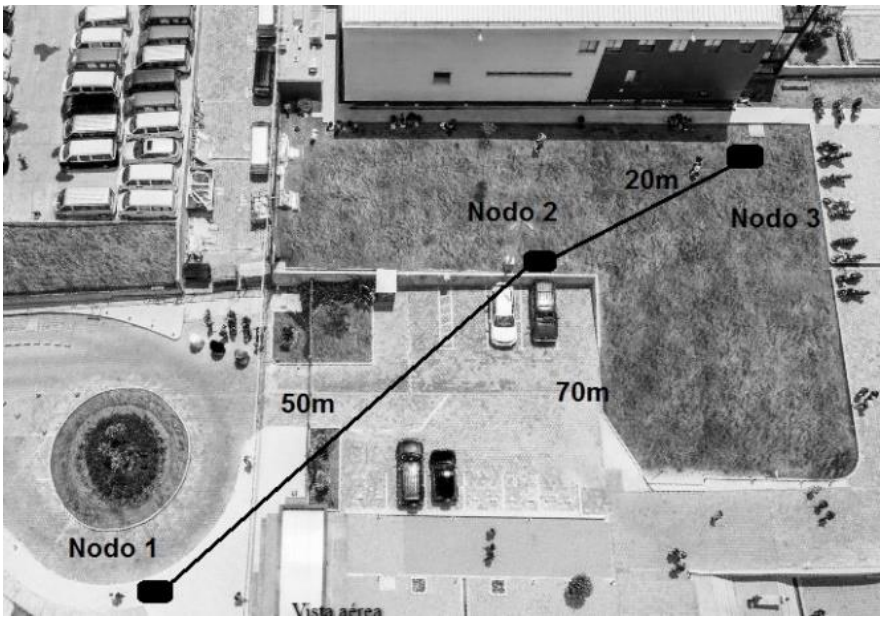


Figura 59. Red MANET Escenario 2.

Figura 60. Red MANET Escenario 2.

Se realizó la prueba de transmisión de video en tiempo real de cada uno de los nodos que forman la red MANET.

En la figura 61 se muestra la transmisión de video en tiempo real de la prueba en escenario 2:

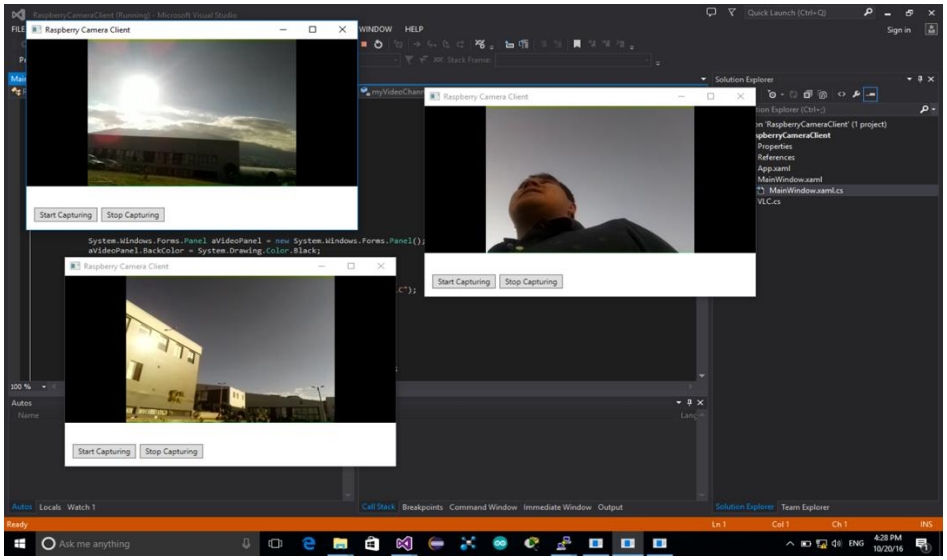


Figura 61. Prueba transmisión de video en tiempo real.

De igual manera se realizó una medición de calidad del enlace usando la interfaz gráfica de HSMM-PI respecto a cada nodo de la red.

En la figura 62 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.1, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres. Para el escenario 2 se observa ya una degradación en la calidad del enlace mientras más distancia existe entre el nodo 1 y 3 la calidad disminuye a un 84%.

En la figura 62, 63, 64 se muestra la calidad del enlace de los 3 nodos medidos en el escenario 2 respectivamente:

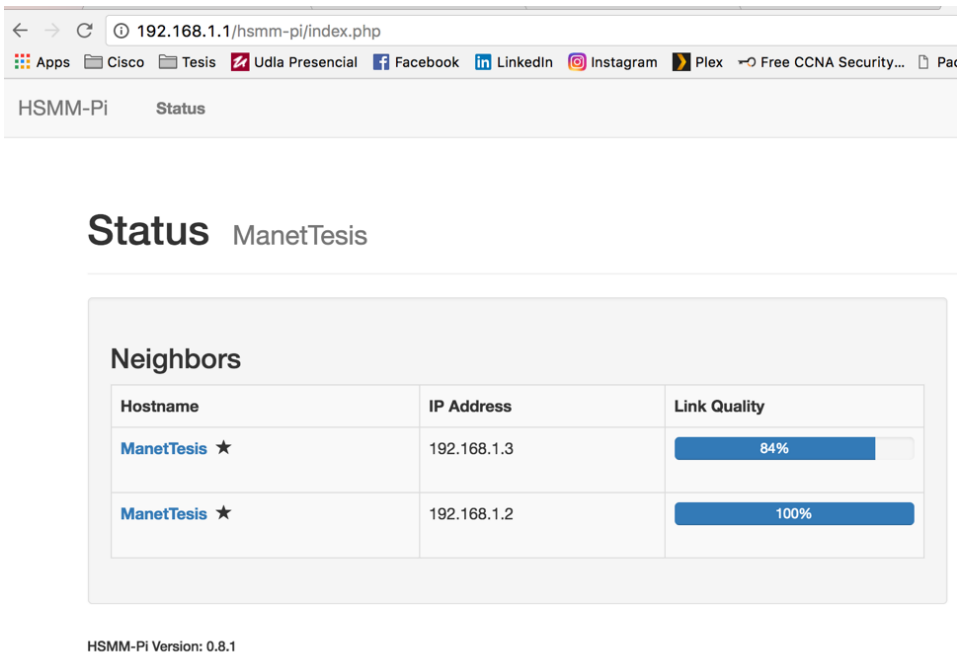


Figura 62. Prueba enlace Nodo 1.

De igual manera se realizó una medición de calidad del enlace usando la interfaz gráfica de HSMM-PI respecto a cada nodo de la red.

En la figura 63 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.2, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres. Para el escenario 2 se observa ya una degradación en la calidad del enlace mientras más distancia existe entre el nodo 2 y 3 la calidad disminuye a un 37%. Y la distancia entre los nodos 2 y 1 aumenta, la calidad del enlace muestra un 56%.

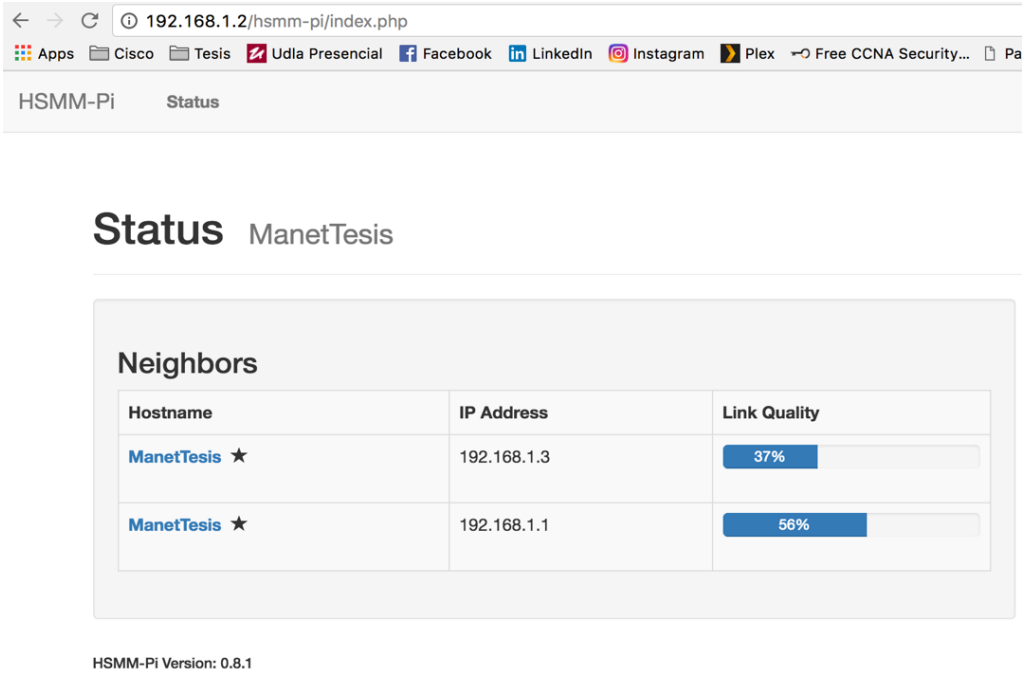


Figura 63. Prueba enlace Nodo 2.

Al realizar la medición de calidad del enlace usando la interfaz gráfica de HSMM-PI respecto a cada nodo de la red.

En la figura 64 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.3, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres. Para el escenario 2 se observa ya una degradación en la calidad del enlace mientras más distancia existe entre el nodo 3 y 2 la calidad disminuye a un 48%. Y la distancia entre los nodos 3 y 1 aumenta, la calidad del enlace muestra un 97%.

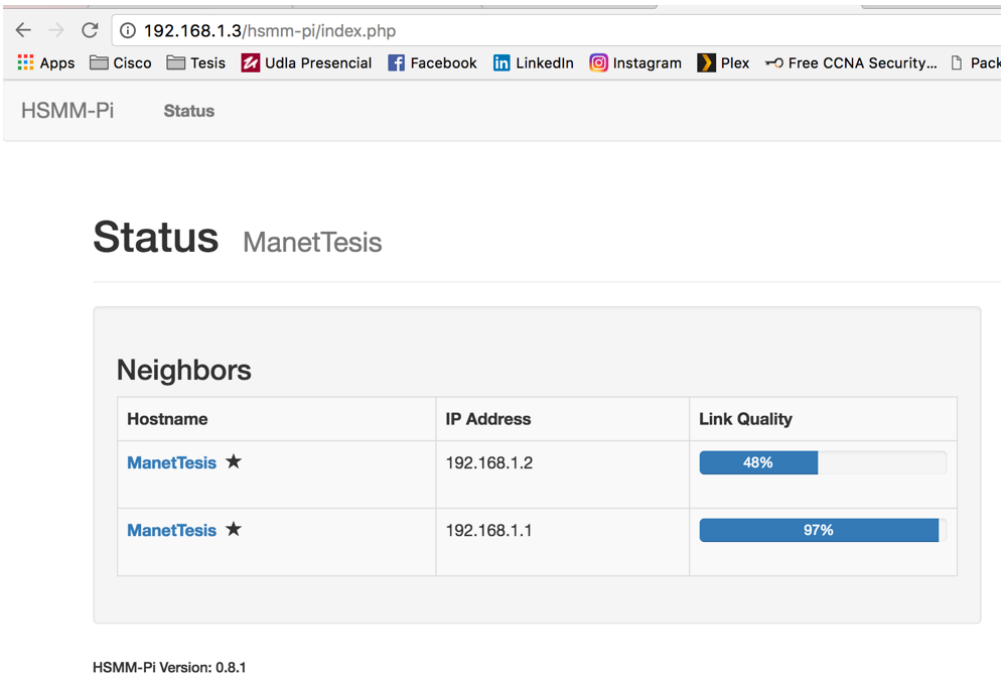


Figura 64. Prueba enlace Nodo 3

Finalizando las pruebas en el escenario 2 se realizó el análisis de potencia de la red MANET dando los siguientes resultados.

Primero se realiza un estudio con el software de gestión de redes NETSPOT para Windows 10 en donde, como se observa en la figura 70 esta solo muestra un solo canal usado por la red debido a que uno de los nodos se encontraba junto al computador de pruebas. El software analiza los 3 nodos de la red MANET como uno solo los cuales trabajan en el mismo rango de frecuencia y tienen una potencia de -40dB.

En la figura 65 se muestra la frecuencia y canal de funcionamiento de la red MANET para el escenario 2:

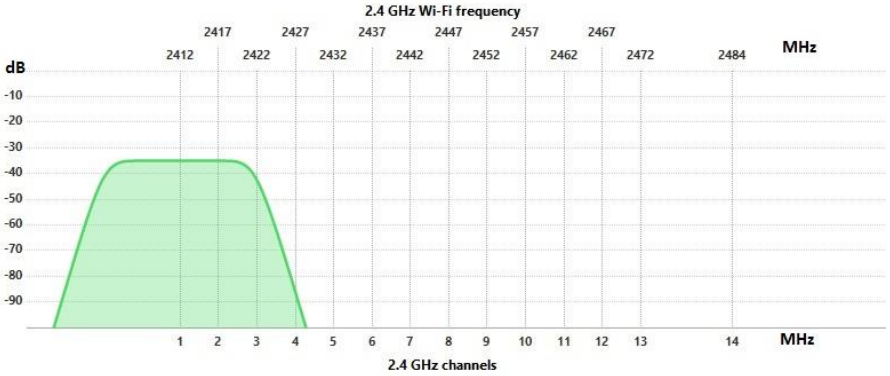


Figura 65. Frecuencia y canal de funcionamiento de red MANET.

Posteriormente en la figura 66 se utiliza es mismo programa y se realiza un análisis de potencia, pero esta vez respecto al tiempo. Esta prueba se realiza para visualizar el desempeño de la red en el ambiente propuesto y en donde se puede notar que hubo desconexiones de un corto tiempo ya sea esta por algún factor externo o porque el protocolo OLSR encontró un mejor enlace de conexión.

En la figura 66 se muestra un análisis de potencia de la red MANET para el escenario 2:

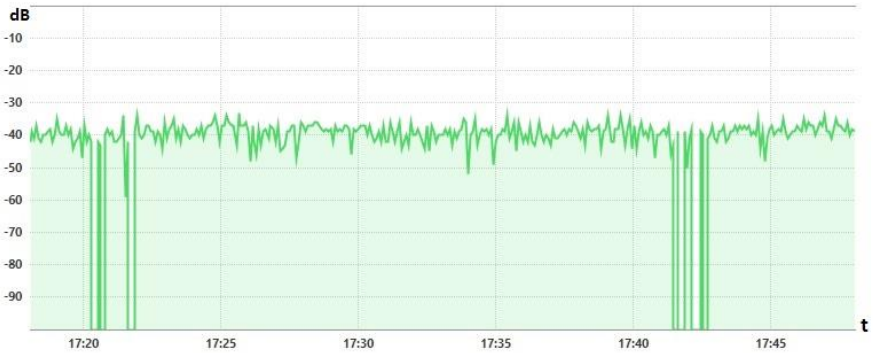


Figura 66. Análisis de potencia de red MANET.

La tabla 10 presenta un resumen con la distancia entre nodos y el retardo de video promedio de toda la red entre los nodos de la red y la computadora de control.

Tabla 10.

Resumen escenario de pruebas 2.

Escenario 2	
Resumen	
Distancia entre Nodo 1 y Nodo 2	50m
Distancia entre Nodo 1 y Nodo 3	70m
Distancia entre Nodo 2 y Nodo 3	20m
Retardo de Video	Nodo 3: 1s Nodo 2: 3s Nodo 1: 10s

En la tabla 10 se muestra que el retardo de video en el nodo 3 es de 1 segundo, esto se debe a que dicho nodo se encuentra cerca del computador de pruebas es por esta razón que en las figuras 70 y 71 se pueden observar resultados parecidos a los del primer escenario, aunque los nodos se encuentren a distancias considerables.

3.2.3 Escenario 3

A continuación, se muestra el diagrama del escenario 3 con las respectivas distancias entre los nodos de la red MANET. Dicha prueba se realizó en la cancha de básquet del conjunto habitacional granados.

En la figura 67 y 68 se muestra un esquema de prueba realizada en el escenario 3:

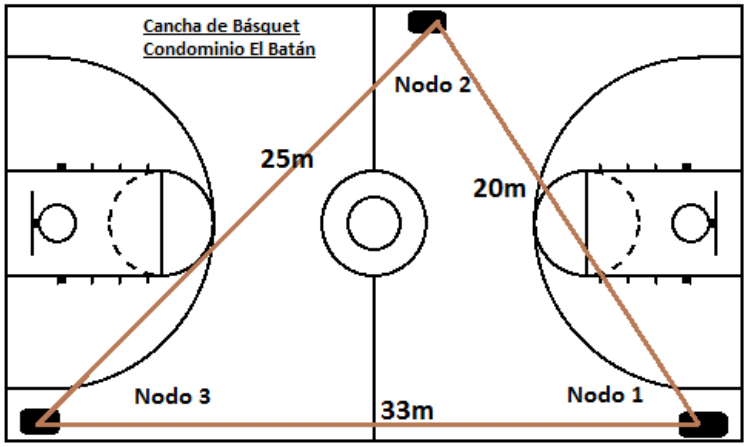


Figura 67. Red MANET Escenario 3

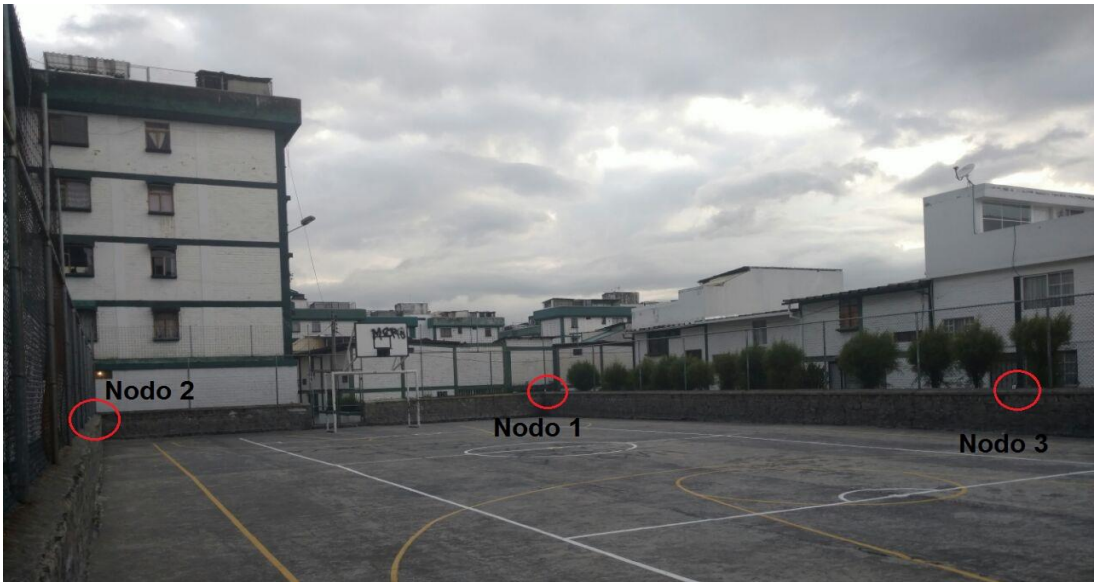


Figura 68. Red MANET prueba 3.

Se realizó la prueba de transmisión de video en tiempo real de cada uno de los nodos que forman la red MANET.

En la figura 69 se muestra la transmisión de video en tiempo real de la prueba en escenario 3:

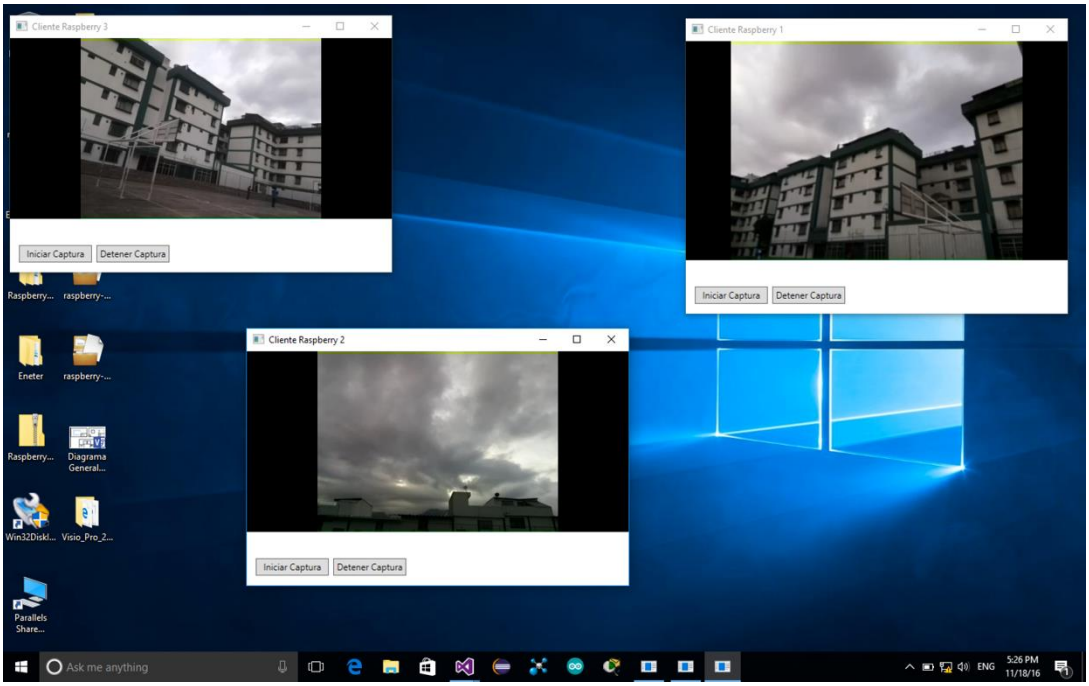


Figura 69. Prueba transmisión de video en tiempo real.

De igual manera se realizó una medición de calidad del enlace usando la interfaz gráfica de HSMM-PI respecto a cada nodo de la red.

En la figura 70 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.1, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres. Para el escenario 3 se observa ya una degradación en la calidad del enlace mientras más distancia existe entre el nodo 1 y 3 la calidad disminuye a un 80%. A su vez la distancia entre los nodos 1 y 2 la calidad del enlace es de 91%.

En la figura 70, 71, 72 se muestra la calidad del enlace de los 3 nodos medidos en el escenario 3 respectivamente:

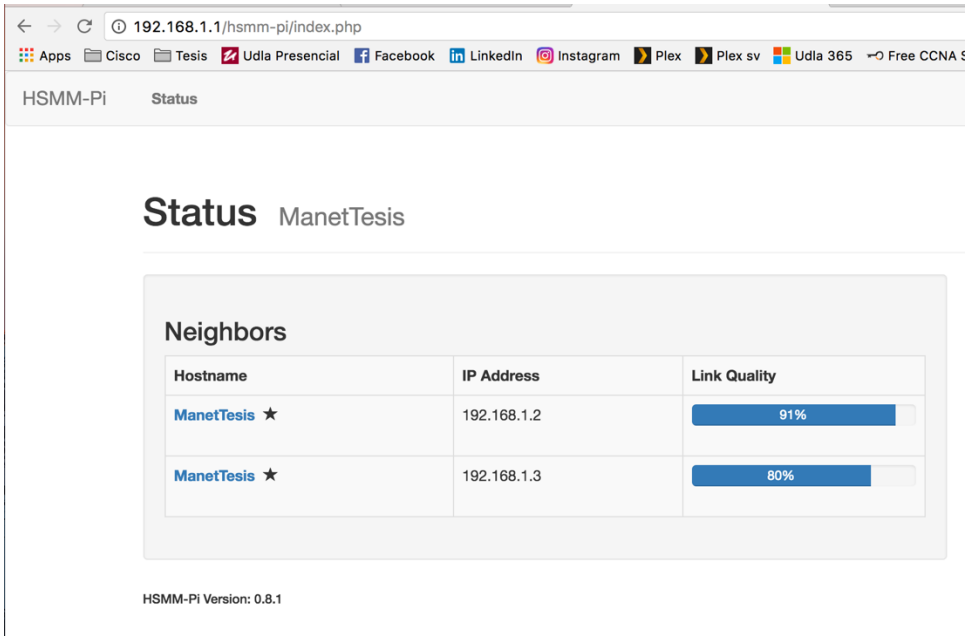


Figura 70. Prueba enlace Nodo 1.

En la figura 71 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.2, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres. Para el escenario 3 se observa ya una degradación en la calidad del enlace mientras más distancia existe entre el nodo 2 y 3 la calidad disminuye a un 56%. A su vez la distancia entre los nodos 2 y 1 la calidad del enlace es de 95%.

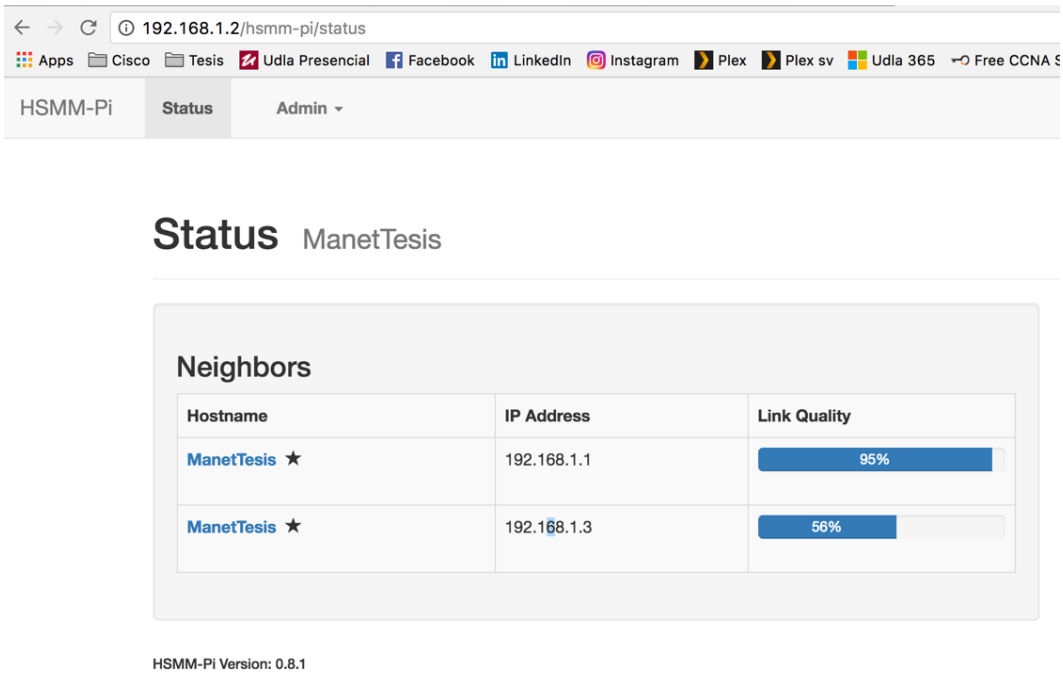


Figura 71. Prueba enlace Nodo 2.

En la figura 72 se puede observar que se ingresa a través del buscador Google Chrome a la dirección 192.168.1.3, la cual corresponde al nodo uno de la red MANET. La página principal muestra el nombre de los vecinos, la dirección IP y la calidad de enlace de los nodos dos y tres. Para el escenario 3 se observa ya una degradación en la calidad del enlace mientras más distancia existe entre el nodo 3 y 1 la calidad disminuye a un 56%. A su vez la distancia entre los nodos 3 y 2 la calidad del enlace es de 65%.

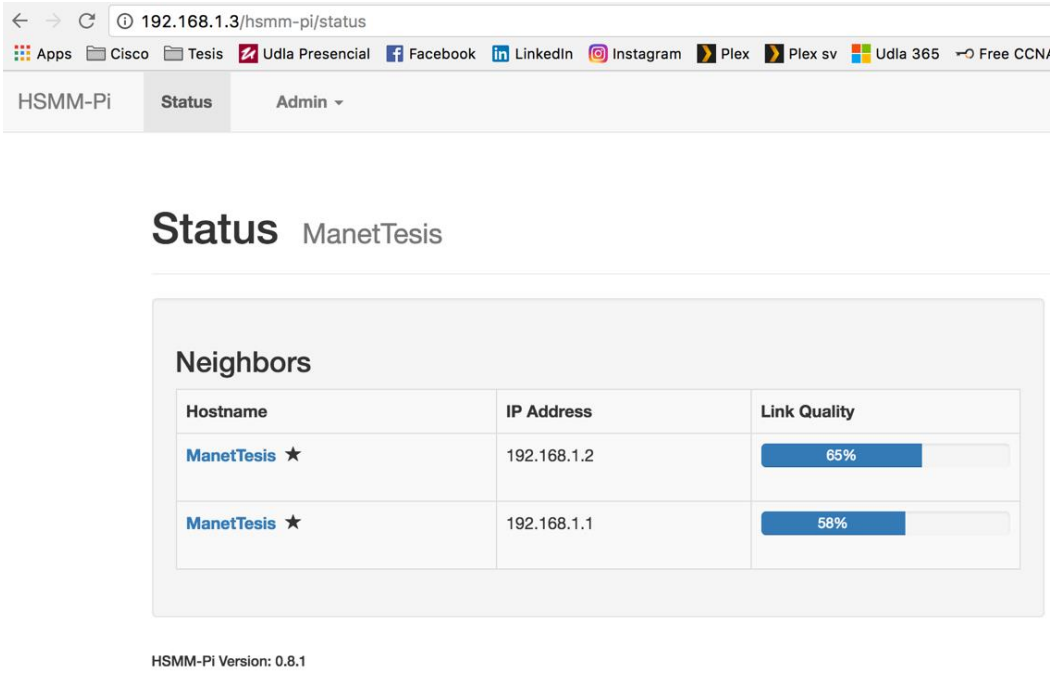


Figura 72. Prueba enlace Nodo 3

Finalizando las pruebas en el escenario 3 se realizó el análisis de potencia de la red MANET dando los siguientes resultados.

Primero se realiza un estudio con el software de gestión de redes NETSPOT para Windows 10 en donde, como se observa en la figura 80 esta solo muestra un solo canal usado por la red debido a que el software analiza los 3 nodos de la red MANET como uno solo los cuales trabajan en el mismo rango de frecuencia y tienen una potencia de -40dB.

En la figura 73 se muestra la frecuencia y canal de funcionamiento de la red MANET para el escenario 3:

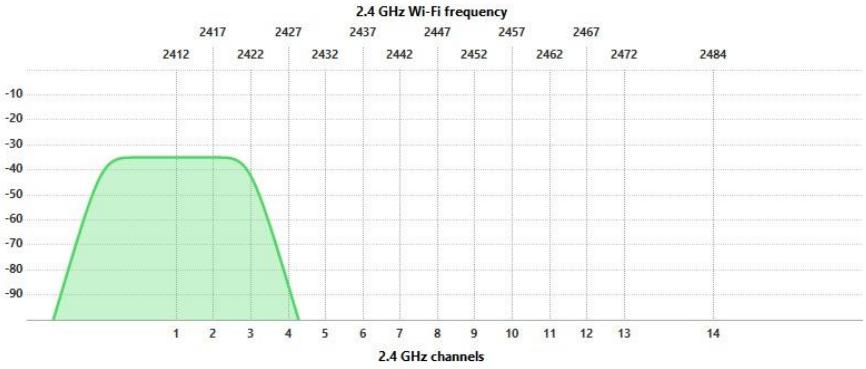


Figura 73. Frecuencia y canal de funcionamiento de red MANET.

Posteriormente en la figura 74 se utiliza es mismo programa y se realiza un análisis de potencia, pero esta vez respecto al tiempo. Esta prueba se realiza para visualizar el desempeño de la red en el ambiente propuesto y en donde se puede notar que hubo desconexiones de un corto tiempo ya sea esta por algún factor externo o porque el protocolo OLSR encontró un mejor enlace de conexión.

En la figura 77 se muestra un análisis de potencia de la red MANET para el escenario 3:

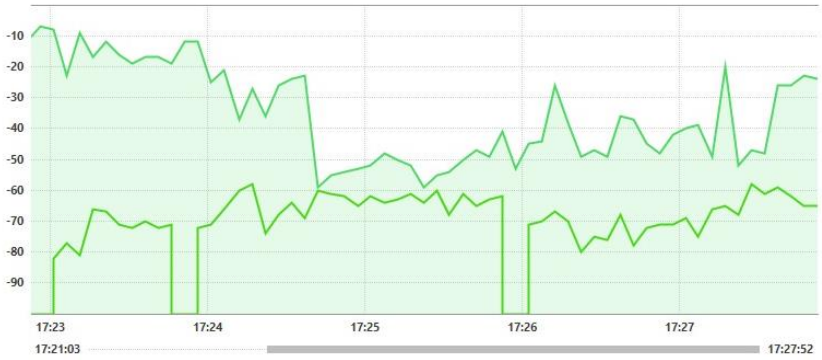


Figura 74. Análisis de potencia de red MANET.

En la figura 74 se puede ver que no existe solo la señal de la red MANET analizada, se puede visualizar otra señal que se encuentra en el rango de los -10dB la cual aparece como una señal que interfiere con el funcionamiento de la

red MANET. Esta interferencia se realiza ya que las 2 señales están trabajando en el mismo canal, es decir, 2.4 GHz.

En la tabla 11 se presenta un resumen con la distancia entre nodos y el retardo de video promedio de toda la red entre los nodos de la red y la computadora de control.

Tabla 11.
Resumen escenario de pruebas 3

Escenario 3	
Resumen	
Distancia entre Nodo 1 y Nodo 2	20m
Distancia entre Nodo 1 y Nodo 3	33m
Distancia entre Nodo 2 y Nodo 3	25m
Retardo de video	Nodo 1: 2s Nodo 2: 2.5s Nodo 3: 3s

3.3 Resultados Finales

Al concluir los tres escenarios de pruebas se pudo comprobar el funcionamiento del protocolo OLSR, y del correcto funcionamiento de la red MANET durante la transmisión de video en tiempo real, usando los componentes que se han mencionado en capítulos anteriores, además, tomando aspectos como distancias entre nodos y línea de vista que afectan la transmisión con pérdida de paquetes de video y provocando retrasos que se observan al ser recibidos por el aplicativo.

Durante una de las pruebas en este caso el número 2 se evidenció que el principal problema para la transmisión era la falta de línea de vista ya que uno de los nodos, como parte de la prueba, se lo colocó junto a un poste de concreto el cual afectaba claramente la transmisión hacia otro de los nodos, aumentando el retraso de la recepción de video a 10 segundos.

Analizado el inconveniente en el escenario 2, se procede a realizar una tercera prueba esta vez procurando que todos los nodos tengan línea de vista entre sí dando como resultado un retraso no mayor a 3 segundos.

A continuación, la tabla 12 muestra un resumen de las pruebas realizadas con la red MANET.

Tabla 12.

Tabla Comparativa de Resultados.

Tabla de Resultados			
	Escenario 1	**Escenario 2**	**Escenario 3**
Distancia entre Nodos	Nodo 1 y Nodo 2: 5m. Nodo 1 y Nodo 3: 1.5m. Nodo 2 y Nodo 3: 5.3m.	Nodo 1 y Nodo 2: 50m. Nodo 1 y Nodo 3: 70m. Nodo 2 y Nodo 3: 20m.	Nodo 1 y Nodo 2: 20m. Nodo 1 y Nodo 3: 33m. Nodo 2 y Nodo 3: 25m.
Potencia	-40dB	-38db	-55dB
Retardo	Nodo 1: 1s. Nodo 2: 1s. Nodo 3: 1s.	Nodo 1: 10s. Nodo 2: 3s. Nodo 3: 1s	Nodo 1: 2s. Nodo 2: 2,5s. Nodo 3: 3s.
Resolución	640x380p	640x380p	640x380p

4. Conclusiones y Recomendaciones

4.1 Conclusiones

Una vez desarrollado y concluido este proyecto de una manera óptima se logró satisfacer satisfactoriamente con todos los objetivos planteados al inicio del proyecto, obteniendo así los resultados esperados, ya que, tanto el diseño de la red MANET como sus componentes funcionan sin ningún inconveniente.

Tras haber realizado un estudio comparativo de antenas y dispositivos que se podrían usar para realizar la red MANET necesaria para cubrir el principal objetivo de este proyecto, se pudo seleccionar el dispositivo correcto, en este caso el Raspberry Pi 3 y su antena Broadcom BCM43438; los cuales permiten enviar video en tiempo real de una manera óptima ya que el ancho de banda necesario para poder lograrlo es cubierto sin ningún problema por los dispositivos antes mencionados.

Para la transferencia de información se usó un Servidor FTP, con la finalidad de enviar un script de transmisión de video para que pueda ser ejecutado dentro de cada nodo de la red MANET, solucionando así el problema del traspaso de archivos entre sistemas operativos en este caso MAC OS X y Raspbian. Cabe recalcar que se le dio un uso extra a la red MANET establecida, ya no solo para la transmisión de video, sino también para el intercambio de información entre nodos y dispositivos de control.

Inicialmente se iba a implementar el protocolo AODV para el enrutamiento de los nodos de la red MANET, pero al estar usando el software HSMM-Pi el cual no es compatible con todos los protocolos de enrutamiento (incluido AODV), se investigó cuáles de ellos eran compatibles y se escogió el protocolo de enrutamiento OLSR el cual tiene como principal ventaja sobre AODV el uso de MPR que disminuye la sobrecarga de tráfico en la red causada por la comunicación excesiva que tienen que tener los nodos entre sí para mantener una tabla de enrutamiento actualizada, además la sobrecarga de tráfico

consume ancho de banda por lo que también en OLSR se reduce este problema.

Debido al uso general del protocolo TCP/IP en el cual se establece que solo se debe usar un puerto para cada transmisión ya sea esta de video, datos o audio y tomando en cuenta que el framework Eneter necesita usar un puerto para transmitir la información, se usaron tres puertos 8093, 8094, 8095 respectivamente para cada nodo y para el aplicativo dando como resultado una transmisión de video fluida y sin interferencias.

Al estar usando la antena incorporada en el Raspberry Pi 3, la cual tiene una ganancia de 0,25 dB, se realizó las pruebas respectivas de la cámara usando cada uno de los 8 megapíxeles con los que esta cuenta, concluyendo así que mientras mayor sea la resolución que se esté usando en la cámara con la antena antes mencionada, mayor será el retraso en la recepción del video en tiempo real. Así pues, se usó en la implementación de este proyecto un valor menor a 1 megapíxel para que el retraso sea prácticamente imperceptible.

Realizada la etapa de pruebas en la cual se trabajó en 3 escenarios diferentes, en los cuales se pudo evidenciar uno de los principales factores con los que cuenta este proyecto que es la línea de vista. En el caso de la red MANET implementada es de vital importancia que exista línea de vista entre los nodos, es decir que no haya ningún obstáculo entre ellos que haga que la potencia de la transmisión se reduzca provocando pérdida de paquetes y retrasos. Cabe recalcar que esto tiene mucho que ver con la frecuencia que se esté usando, en este caso 2.4 GHz.

Por motivos de seguridad en la red MANET, se impide el uso del protocolo DHCP a través del enlace inalámbrico, por lo que, para la inclusión del dispositivo de control a la red, se optó por agregar una dirección IP estática.

Cada nodo dispone del protocolo DHCP, pero este solo es accesible a través del puerto ethernet incluido en cada Raspberry, el cual no va a ser utilizado.

HSMM-PI es un software que puede ser utilizado para creación de redes MANET o MESH, dependiendo de la necesidad, ya que, si se requiere que los nodos se mantengan en una posición previamente, aprovechando otros beneficios con los que este software cuenta, como por ejemplo la habilidad de proveer internet a los nodos y que estos los distribuyan a los respectivos usuarios.

Tras haber realizado tres pruebas de la red MANET en diferentes escenarios se puede observar que el enrutamiento OLSR que se utiliza es de gran importancia ya que, gracias a este, el alcance de TX/RX es mucho mayor, brindando gran cobertura, lo que no se puede lograr si solo existiera conexión punto a punto y sin enrutamiento.

Este proyecto es el resultado de un gran proceso tanto de investigación, desarrollo y pruebas de laboratorio, los cuales ayudaron a la culminación del mismo, siendo este una base bastante sólida para completar el objetivo macro de este proyecto el cual es la transmisión de información en tiempo real usando plataformas aéreas.

4.2 Recomendaciones

Para obtener los mejores resultados posibles, siempre es recomendable tener las versiones actualizadas del sistema operativo Raspbian, drivers, frameworks etc. De esta manera se evita posibles errores durante la instalación de los elementos necesarios para el funcionamiento de la red MANET.

Para tener un mayor alcance en la transmisión y una resolución de video más alta, se recomienda el uso de una antena compatible con Raspberry Pi y con HSMM-PI que tenga una ganancia mayor a 0,25 dB (actualmente usada), la

cual ayudará a aprovechar las características de los elementos usados en la red MANET como la cámara, en su total capacidad.

Para usar la red MANET durante un tiempo de uso si interrupciones de entre 1 a 3 horas (o superior), es recomendable el uso de una batería portátil de mínimo 4000 mAh, la cual brindará energía suficiente para que cada nodo funcione correctamente.

Antes de usar la red MANET es de gran importancia verificar que las cámaras de cada nodo estén habilitadas para evitar errores mientras se esté ejecutando el aplicativo.

Se recomienda realizar un análisis comparativo entre sistemas operativos para verificar compatibilidad de los mismos con la red MANET implementada, ya que dependiendo su uso es de gran importancia que esta sea compatible con el mayor número de dispositivos independientemente de sus sistemas operativos.

REFERENCIAS

Garzón, M., Lara, R. & Olmedo, G. (2011) Estudio del comportamiento de una red Ad-Hoc MANET metropolitana basado en los protocolos de enrutamiento.

Camp, T., Boleng, J. & Davies, V. (2002) *A Survey of Mobility Models for Ad Hoc Network Research.* Dept. of Math. and Computer Sciences Colorado School of Mines, Golden, CO, USA.

Hong, X., Gerla, M., Pei, G. & Chiang, Ch. (s.f.) *A Group Mobility Model for Ad HocWireless Networks.* Computer Science Department University of California Los Angeles, CA, USA.

Meghanathan, N. (2010) *Impact of the Gauss-Markov Mobility Model on Network Connectivity, Lifetime and Hop Count of Routes for Mobile Ad hoc Networks.* Computer Science Department Jackson State University, Jackson, MS, USA.

Basagni, S., Conti, M., Giordano, S. & Stojmenovic, I. (2012) *Mobile Ad Hoc Networking: The Cutting Edge Directions.* Hoboken, New Jersey, USA: John Wiley & Sons, INC.

Kioumourtzis, G., Gkamas, A. & Bouras, C. (s.f.) *Mobile Ad hoc networks (MANETs) for multimedia transmission.*

Loo, J., Mauri, Ll. & Ortiz, J. (2012) *Mobile Ad Hoc Networks Current Status and Future Trends.* Boca Raton, Florida, USA: Auerbach Publications.

Murthy, C. & Manoj, B. (2004) *Ad Hoc Wireless Networks Architectures and Protocols.* Upper Saddle River, New Jersey, USA: Prentice Hall Communications Engineering and Emerging Technologies Series.

Bell, Ch. (2013) *Beginning Sensor Networks with Arduino and Raspberry Pi.* New York, NY, USA: Apress Media LLC.

Donat, W. (2014) *Learn Raspberry Pi Programming with Python.* New York, NY, USA: Apress Media LLC.

Wu, Sh. & Tseng, Y. (2007) *Wireless Ad Hoc Networking.* Boca Raton, Florida, USA: Auerbach Publications.

Gómez, C (2011) Efectos de la Movilidad en la Conectividad de Redes Móviles Ad Hoc (MANET's)-Edición *Única.* Monterrey, N.L, México: Instituto Tecnológico y de Estudios Superiores de Monterrey.

Sarkar, K., Basavaraju, T. & Puttamadappa, C. (2008) *Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications.* Boca Raton, Florida, USA: Auerbach Publications.

Raniwala, A. & Chiueh, T. (s.f.) *Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network.* Computer Science Department, Stony Brook University, Stony Brook, NY, USA.

Frikha, M. (2011) *Ad Hoc Networks.* (1ª. ed.) London, United Kingdom & Hoboken, New Jersey, USA: ISTE Ltd and John Wiley & Sons, Inc.

Lian, Sh. (2009) *Multimedia Content Encryption Techniques and Applications.* Boca Raton, Florida, USA: Auerbach Publications.

Khosrow-Pour, M. (2005) *Encyclopedia of Information Science and Technology Volume I.* Hershey, PA, USA & London, United Kingdom: Idea Group Reference.

Norris, D. (2015) *The Internet of Things: Do-It-Yourself Projects with Arduino, Raspberry Pi, and BeagleBone Black.* New York, USA: McGraw-Hill Education.

Chlamtac, I., Conti, M. & Liu, J. (2003) *Mobile ad hoc networking: imperatives and challenges.* Ámsterdam, Netherlands: Elsevier B.V.

Ansari, T. & Ganesh, S. (s.f.) *Mobile Ad-Hoc Networks Its Advantages and Challenges.* A.S.M's Institute of Management & Computer Studies, Thane, India.

Ilyas, M. (2003) *The Handbook of Ad Hoc Wireless Networks.* Boca Raton, Florida, USA: CRC Press LLC.

Faludi, R. (2011) *Building Wireless Sensor Networks.* Sebastopol, CA, USA: O'Reilly Media, Inc.

Suehle, R. & Callaway, T. (2014) *Raspberry Pi Hacks.* Sebastopol, CA, USA: O'Reilly Media, Inc.

Dennis, A. (2016) *Raspberry Pi Computer Architecture Essentials.* Birmingham, United Kingdom: Packt Publishing.

Pei, G., Gerla, M. & Chen, T. (2000) *Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks.* Piscataway, New Jersey, US: IEEE.

Chalmeta, J. (2009) Estudio y análisis de prestaciones de redes móviles Ad Hoc mediante simulaciones NS-2 para validar modelos analíticos. Barcelona, Cataluña, España: Universitat Politecnica de Catalunya.

Schmidt, M. (2014) *Raspberry Pi: A Quick-Start Guide.* Dallas, Texas & Raleigh, North Carolina, USA: The Pragmatic Programmers, LLC.

Barnes, R. (s.f.) *The Official Raspberry Pi Projects Book.* Cambridge, United Kingdom: Raspberry Pi (Trading) Ltd.

Rubinstein, M., Moraes, I., Campista, M., Costa, L. & Duarte, O. (s.f.) *A Survey on Wireless Ad Hoc Networks.* Rios De Janeiro, Brazil: Universidade do Estado do Rio de Janeiro.

Scheideler, Ch. (2010) *Algorithms for Sensor Systems.* Germany: Springer-Verlag Berlin Heidelberg.

Ortiz, J. (2012) *Telecommunications Networks – Current Status and Future Trends.* Rijeka, Croatia: InTech.

Garzón, M. (2009) Estudio del comportamiento de una red ad hoc (manet) Metropolitana, basado en los protocolos de enrutamiento. Sangolquí, Ecuador: Escuela Politécnica del Ejército.

Azuaje, O. (2015) *Performance Evaluation of an IEEE 802.11 Mobile Ad-Hoc Network on the Raspberry Pi.* Porto, Portugal: Faculdade de Engenharia da Universidade do Porto.

Viswanath, K., Obraczka, K., Member., IEEE & Tsudik, G. (2006) *Exploring Mesh and Tree-Based Multicast Routing Protocols for MANETs.* Piscataway, New Jersey, US: IEEE.

Bradbury, A. & Everard, B. (2014) *Learning Python with Raspberry Pi.* West Sussex, United Kingdom: John Wiley & Sons Ltd.

Flores, E. (2012) Redes de Sensores Inalámbricas Aplicado a la Medicina. Cantabria, España: Escuela Técnica Superior de Ingenieros ndustriales y de Telecomunicación Universidad de Cantabria.

Ruiz, J. (2008) Configuración DHCP en Redes Manet Subordinadas. Madrid, España: Departamento de Ingeniería del Software e Inteligencia Artificial Facultad de Informática Universidad Complutense de Madrid.

Pérez, J. (2012) Protocolos de Encaminamiento IP en Dispositivos Móviles para Crear Redes MANETs. Granada, España: Universidad de Granada.

Rocabado, S. (2013) Caso de Estudio de Comunicaciones Seguras sobre Redes Móviles Ad Hoc. La Plata, Argentina: Facultad de Informática Universidad de La Plata.

s.n. (2014) Simulación de Protocolos de Enrutamiento para Redes Móviles Ad-Hoc mediante Herrramienta de Simulación NS-3. Málaga, España: Universidad de Málaga.

Cruz, D. (2014) Evaluación de redes de sensores inalámbricos mediante el Simulador OMNeT++. Departamento de Comunicaciones Universidad Politecnica de Valencia.

Enneya, N., Oudidi, K. & Elkoutbi, M (2009) *Enhancing Delay in MANET Using OLSR Protocol.* Rabat, Morocco: Mohammed V University.

Smith, C (s.f.) *HSMM-Pi.* Recuperado el 15 de agosto de 2016 de: https://github.com/urlgrey/hsmm-pi.

ANEXOS

Anexo A

Código fuente aplicativo Visual Studio

```
using System;
using System.IO.Pipes;
using System.Threading;
using System.Windows;
using Eneter.Messaging.MessagingSystems.MessagingSystemBase;
using Eneter.Messaging.MessagingSystems.TcpMessagingSystem;
using Eneter.Messaging.MessagingSystems.UdpMessagingSystem;
using VLC;


namespace RaspberryCameraClient
{

   public partial class MainWindow : Window
   {
      private IDuplexOutputChannel myVideoChannel;

      // creacion de variable de Pipe Streaming que sera leido por VLC
      private NamedPipeServerStream myVideoPipe;

      private VlcInstance myVlcInstance;
      private VlcMediaPlayer myPlayer;

      public MainWindow()
      {
         InitializeComponent();

         System.Windows.Forms.Panel aVideoPanel = new System.Windows.Forms.Panel();
         aVideoPanel.BackColor = System.Drawing.Color.Black;
         VideoWindow.Child = aVideoPanel;

         // Ruta de acceso a los codecs incluidos en VLC.
         myVlcInstance = new VlcInstance(@"C:\Program Files (x86)\VideoLAN\VLC");

         // Uso de mensajes TCP.
         myVideoChannel = new TcpMessagingSystemFactory()

            //direccion ip del nodo con su respectivo puerto
            .CreateDuplexOutputChannel("tcp://192.168.1.2:8094/");
         myVideoChannel.ResponseMessageReceived += OnResponseMessageReceived;
      }

      private void Window_Closed(object sender, EventArgs e)
      {
```

```
        StopCapturing();
    }

    private void OnStartCapturingButtonClick(object sender, RoutedEventArgs e)
    {
        StartCapturing();
    }

    private void OnStopCapturingButtonClick(object sender, RoutedEventArgs e)
    {
        StopCapturing();
    }

    private void StartCapturing()
    {

        string aVideoPipeName = Guid.NewGuid().ToString();

        // Se abre la transmision de video que sera analizada por VLC.
        myVideoPipe = new NamedPipeServerStream(@"\" + aVideoPipeName,
PipeDirection.Out, 1, PipeTransmissionMode.Byte, PipeOptions.Asynchronous, 0, 32764);
        ManualResetEvent aVlcConnectedPipe = new ManualResetEvent(false);
        ThreadPool.QueueUserWorkItem(x =>
        {
            myVideoPipe.WaitForConnection();


            aVlcConnectedPipe.Set();
        });

        // Inicio de la tranmision de video con VLC.
        using (VlcMedia aMedia = new VlcMedia(myVlcInstance, @"stream://\\\.\pipe\" +
aVideoPipeName))
        {
            // Procesamiento de video usando codec para H264
            aMedia.AddOption(":demux=H264");

            myPlayer = new VlcMediaPlayer(aMedia);
            myPlayer.Drawable = VideoWindow.Child.Handle;


            myPlayer.Play();
        }
```

```
            if (!aVlcConnectedPipe.WaitOne(5000))
            {
                throw new TimeoutException("VLC did not open connection with the pipe.");
            }

            // Apertura de canal de conexion con raspberry.
            myVideoChannel.OpenConnection();
        }

        private void StopCapturing()
        {
            // Cierre de canal de conexion con raspberry.
            myVideoChannel.CloseConnection();


            if (myVideoPipe != null)
            {
                myVideoPipe.Close();
                myVideoPipe = null;
            }

            // Parar VLC.
            if (myPlayer != null)
            {
                myPlayer.Dispose();
                myPlayer = null;
            }
        }

        private void OnResponseMessageReceived(object sender,
DuplexChannelMessageEventArgs e)
        {
            byte[] aVideoData = (byte[])e.Message;


            myVideoPipe.Write(aVideoData, 0, aVideoData.Length);
        }
    }
}
```

Anexo B

Código fuente script de Tx de video

```
package eneter.camera.service;

import java.io.*;

public class Program
{
   public static void main(String[] args)
   {
      try
      {
         CameraService aService = new CameraService();


         aService.startService("0.0.0.0", 8095);

         System.out.println("Servicio de Video en uso. Presiona ENTER para DETENER");
         new BufferedReader(new InputStreamReader(System.in)).readLine();

         aService.stopService();
      }
      catch (Exception err)
      {
         System.err.println("Fallo del Servicio");
         err.printStackTrace();
      }
   }

}



package eneter.camera.service;

import java.io.InputStream;
import java.util.HashSet;

import eneter.messaging.diagnostic.EneterTrace;
import eneter.messaging.messagingsystems.messagingsystembase.*;
import eneter.messaging.messagingsystems.tcpmessagingsystem.TcpMessagingSystemFactory;
import
eneter.messaging.messagingsystems.udpmessagingsystem.UdpMessagingSystemFactory;
import eneter.net.system.EventHandler;

class CameraService
```

```
  {
    synchronized (myConnectionLock)
    {
      myConnectedClients.add(e.getResponseReceiverId());
      myClientsUpdatedFlag = true;

      if (myRaspiVidProcess == null)
      {
        // Captura de video en: 640x480 pixeles, 24 frames/s
        String aToExecute = "raspivid -n -vf -hf -sh -co -br -ih -w 320 -h 240 -fps 24 -t 0 -o -";
        myRaspiVidProcess = Runtime.getRuntime().exec(aToExecute);
        myVideoStream = myRaspiVidProcess.getInputStream();

        Thread aRecordingThread = new Thread(myCaptureWorker);
        aRecordingThread.start();
      }
    }
  }
  catch (Exception err)
  {
    String anErrorMessage = "Error al iniciar la transmisión";
    EneterTrace.error(anErrorMessage, err);

    return;
  }
}

private void onClientDisconnected(Object sender, ResponseReceiverEventArgs e)
{
  EneterTrace.info("Client disconnected.");

  synchronized (myConnectionLock)
  {
    myConnectedClients.remove(e.getResponseReceiverId());
    myClientsUpdatedFlag = true;

    // If no client is connected then turn off the camera.
    if (myConnectedClients.isEmpty() && myRaspiVidProcess != null)
    {
      myRaspiVidProcess.destroy();
      myRaspiVidProcess = null;
    }
  }
}
```

```
private void doCaptureVideo()
{
   try
   {
      String[] aClients = {};
      byte[] aVideoData = new byte[4096];
      while (myVideoStream.read(aVideoData) != -1)
      {

         if (myClientsUpdatedFlag)
         {
            aClients = new String[myConnectedClients.size()];
            synchronized (myConnectionLock)
            {
               myConnectedClients.toArray(aClients);
               myClientsUpdatedFlag = false;
            }
         }

         for (String aClient : aClients)
         {
            try
            {
               // envia la informacion de video capturada al cliente.
               myVideoChannel.sendResponseMessage(aClient, aVideoData);
            }
            catch (Exception err)
            {

            }
         }
      }
   }
   catch (Exception err)
   {

   }

   EneterTrace.info("Captura de Video Terminada.");
}

private EventHandler<ResponseReceiverEventArgs> myClientConnected
   = new EventHandler<ResponseReceiverEventArgs>()
```

```
    {
        @Override
        public void onEvent(Object sender, ResponseReceiverEventArgs e)
        {
            onClientConnected(sender, e);
        }
    };

    private EventHandler<ResponseReceiverEventArgs> myClientDisconnected
        = new EventHandler<ResponseReceiverEventArgs>()
    {
        @Override
        public void onEvent(Object sender, ResponseReceiverEventArgs e)
        {
            onClientDisconnected(sender, e);
        }
    };


    private Runnable myCaptureWorker = new Runnable()
    {
        @Override
        public void run()
        {
            doCaptureVideo();
        }
    };

}
```

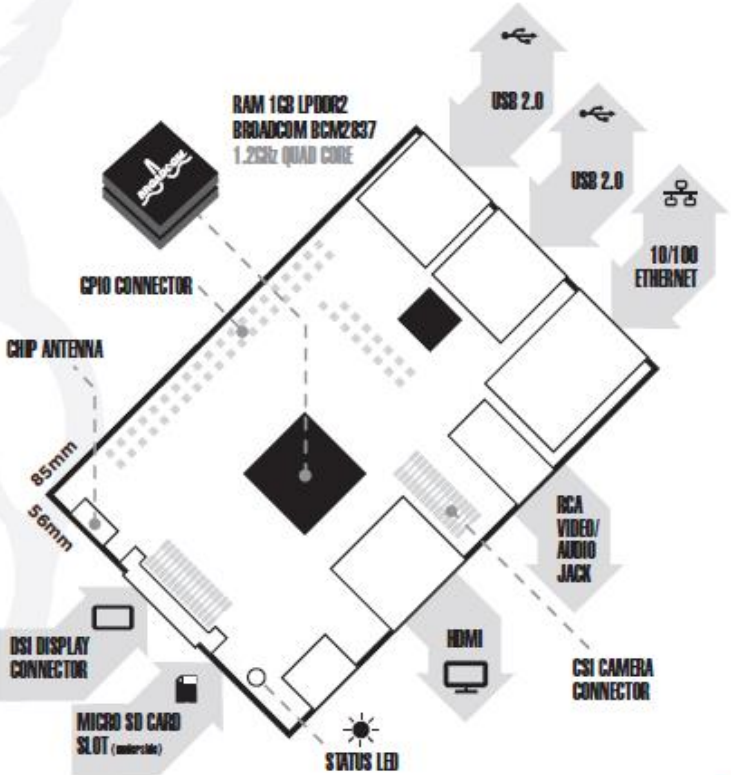
Anexo C

Datasheet Raspberry PI 3

Raspberry Pi

Raspberry Pi 3 Model B

Product Name	**Raspberry Pi 3**
Product Description	The Raspberry Pi 3 Model B is the third generation Raspberry Pi. This powerful credit-card sized single board computer can be used for many applications and supersedes the original Raspberry Pi Model B+ and Raspberry Pi 2 Model B. Whilst maintaining the popular board format the Raspberry Pi 3 Model B brings you a more powerful processer, 10x faster than the first generation Raspberry Pi. Additionally it adds wireless LAN & Bluetooth connectivity making it the ideal solution for powerful connected designs.
RS Part Number	**896-8660**



RS

Raspberry Pi

Raspberry Pi 3 Model B

Specifications

Processor	Broadcom BCM2387 chipset. 1.2GHz Quad-Core ARM Cortex-A53 802.11 b/g/n Wireless LAN and Bluetooth 4.1 (Bluetooth Classic and LE)
GPU	Dual Core VideoCore IV® Multimedia Co-Processor. Provides Open GL ES 2.0, hardware-accelerated OpenVG, and 1080p30 H.264 high-profile decode. Capable of 1Gpixel/s, 1.5Gtexel/s or 24GFLOPs with texture filtering and DMA infrastructure
Memory	1GB LPDDR2
Operating System	Boots from Micro SD card, running a version of the Linux operating system or Windows 10 IoT
Dimensions	85 x 56 x 17mm
Power	Micro USB socket 5V1, 2.5A

Connectors:

Ethernet	10/100 BaseT Ethernet socket
Video Output	HDMI (rev 1.3 & 1.4 Composite RCA (PAL and NTSC)
Audio Output	Audio Output 3.5mm jack, HDMI USB 4 x USB 2.0 Connector
GPIO Connector	40-pin 2.54 mm (100 mil) expansion header: 2x20 strip Providing 27 GPIO pins as well as +3.3 V, +5 V and GND supply lines
Camera Connector	15-pin MIPI Camera Serial Interface (CSI-2)
Display Connector	Display Serial Interface (DSI) 15 way flat flex cable connector with two data lanes and a clock lane
Memory Card Slot	Push/pull Micro SDIO

Key Benefits

- Low cost
- Consistent board format
- 10x faster processing
- Added connectivity

Key Applications

- Low cost PC/tablet/laptop
- IoT applications
- Media centre
- Robotics
- Industrial/Home automation
- Server/cloud server
- Print server
- Security monitoring
- Web camera
- Gaming
- Wireless access point
- Environmental sensing/monitoring (e.g. weather station)

RS