



FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DISEÑO DE UN SISTEMA DE COMUNICACIÓN ACOPLADO EN
DRONES UTILIZANDO DISPOSITIVOS RASPBERRY PI

AUTORES

Bolívar Enrique Dávalos Duque
julio Antonio Arias Casillas

AÑO

2017



FACULTAD DE INGENIERÍAS Y CIENCIAS AGROPECUARIAS

DISEÑO DE UN SISTEMA DE COMUNICACIÓN ACOPLADO EN DRONES
UTILIZANDO DISPOSITIVOS RASPBERRY PI

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

Profesor Guía
Msc. Milton Neptalí Román Cañizares

Autores
Bolívar Enrique Dávalos Duque
Julio Antonio Arias Casillas

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 escogido y dando cumplimiento con todas las disposiciones vigentes que regulan los Trabajos de Titulación”

Milton Neptalí Román Cañizares
Magister en Gerencia de Redes y Telecomunicaciones
CI: 0502163447

DECLARACIÓN PROFESOR CORRECTOR

Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

Iván Ricardo Sánchez Salazar

Magister en Calidad, Seguridad y Ambiente

CI: 1803456142

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”

Bolívar Enrique Dávalos Duque
C.I.: 1713721841

Julio Antonio Arias Casillas
C.I.: 0603023888

AGRADECIMIENTO

Agradezco a Dios y a mis Padres por el trabajo duro y por brindarme la oportunidad de alcanzar esta meta.

Agradezco a mi Hermano, Cristina Luna, Julio Arias, y todo aquel que nos brindó ayuda para culminar satisfactoriamente esta Tesis.

Agradezco a la Universidad de las Américas UDLA, sus autoridades, personal académico y administrativo quienes supieron transmitir la filosofía de la Universidad para la formación de profesionales completos, en especial al Ing. Milton Román quien supo dirigir esta tesis aportando su valioso conocimiento y consejos.

Enrique Dávalos

AGRADECIMIENTO

A Dios por brindarme salud, sabiduría, fortaleza día a día y una vida llena de bendiciones.

A mis padres María y Julio, mis hermanos y mi enamorada, por ser mi soporte y por enseñarme a luchar hasta conseguir mis objetivos, por permitirme contar siempre con ellos en los buenos y malos momentos.

A mi amigo Enrique y sus padres quienes me abrieron las puertas de su hogar, brindaron su confianza y apoyo.

Julio Arias

DEDICATORIA

Dedico este logro a mis padres Bolívar y Nancy quienes son los mejores seres humanos que conozco, pues han sido mis ángeles, inculcando en mí su ejemplo de honestidad y dedicación sin que ningún problema sea una excusa para no encontrar una solución.

A mi hermano Francisco quien me enseñó que nada es imposible, mientras nuestras alas posean el valor de volar alto, no existe cielo que no se pueda conquistar.

A Cristina por su apoyo incondicional en todo momento.

Enrique Dávalos

DEDICATORIA

Dedico este proyecto a mi familia.
A mis padres María y Julio, por estar siempre a mi lado y por sentar en mí, las bases de responsabilidad y deseos de superación personal, por su lucha diaria y sacrificios realizados con el único propósito de ayudarme a culminar mis estudios.

A mi hermano Luis y mi enamorada Katherine por estar siempre conmigo brindándome su confianza, motivándome a continuar en la lucha diaria hasta cumplir mis objetivos.

Julio Arias

RESUMEN

Hoy en día el hombre explota a su máxima expresión los sistemas de telecomunicaciones para el control de objetos electrónicos a través de las diferentes tecnologías inalámbricas existentes. Esto propone un desafío para la generación de una red que permita acoplar elementos que sean dinámicos, es decir que puedan cambiar de lugar, que puedan salir o ingresar del área de cobertura; de esta manera y según el análisis generado para este tipo de comportamiento es posible lograr una solución mediante la generación de una red MANET, la cual permite solventar las necesidades actuales de los dispositivos y usuarios de manera inalámbrica; las características de una red MANET determina que es un sistema autónomo el cual se encuentra constituido por nodos y por ser una red que no está limitada a cableado físico o al movimiento de los dispositivos que se encuentren sobre su área de cobertura. Es por ello que para aprovechar las propiedades que nos brindan las redes red MANET, se desarrolla este proyecto con la finalidad de integrar placas Raspberry Pi3 que disponen de una antena Wi-Fi, la cual permite tener movilidad en la transmisión y recepción de video, de esta manera al acoplar las placas a Drones se puede realizar la captura de video de lugares con acceso limitado ya sea por características geográficas del lugar o por agentes externos que impiden el acceso por vía terrestre. Al realizar las configuraciones necesarias se da paso a la comunicación directa entre un nodo y la estación base o entre nodos distantes y la estación base mediante el enrutamiento de la información que se transmite, a través de todos los dispositivos integrantes de la red, con la finalidad de poder cubrir grandes distancias en la transmisión sin perder conexión.

ABSTRACT

Nowadays man exploited to their maximum expression of telecommunications systems for the control of electronic objects through the different existing wireless technologies. This poses a challenge for the generation of a network that allows attaching elements that are dynamic, i.e. to be able to change of place, which can leave or enter the coverage area; in this way and according to the analysis generated for this type of behavior is possible to achieve a solution through the generation of a MANET, which allows you to meet the current needs of users and devices wirelessly, the characteristics of a MANET determines that it is a stand-alone system which is made up of nodes and for being a network that is not limited to physical wiring or the movement of the devices that are on your coverage area. It is for this reason that to take advantage of the properties we provide network MANET, develops this project with the aim of integrating Raspberry Pi3 plates that have a Wi-Fi antenna, which allows you to be mobile in the transmission and reception of video, in this way when attaching the plates to Drones can perform video capture of places with limited access either by geographical features of the place or by external agents that prevent access by land. To carry out the necessary configurations gives way to the direct communication between a node and the base station or between distant nodes and the base station using the routing information that is transmitted through all devices of the network members, with the purpose of being able to cover large distances in the transmission without losing connection.

ÍNDICE

INTRODUCCIÓN.....	1
Alcance.....	2
Justificación.....	3
Objetivos	4
Objetivo general	4
Objetivos específicos.....	5
1. MARCO TEÓRICO.....	5
1.1. Introducción	5
1.2. Sistemas de radiocomunicación	6
1.2.1. Elementos para Transmisión	7
1.2.2. Canal.....	7
1.2.3. Espectro Electromagnético.....	8
1.2.4. Radio frecuencias.....	10
1.2.5. Flujo de la Transmisión para Comunicación	11
1.3. Antenas	11
1.3.1. Características de las Antenas	13
1.3.2. Parámetros de las Atenas	13
1.3.3. Tipos de antenas.....	14
1.3.3.1. Antenas Direccionales	14
1.3.3.2. Antenas Omnidireccionales.....	15
1.4. Redes inalámbricas	16
1.4.1. Ventajas de las redes Inalámbricas	17
1.4.2. Historia de las redes Inalámbricas	17
1.4.3. Estándares de las redes inalámbricas	18
1.4.4. Clasificación de las redes Inalámbricas	19
1.4.4.1. Por su topología.....	19
1.4.4.2. Por su cobertura.....	20
1.4.4.3. Por tipo de conexión	22
1.4.4.4. Por su tecnología	22

1.4.4.5.	Por su tecnología de acceso	24
1.4.4.6.	Por su infraestructura inalámbrica	24
1.4.4.6.1.	Con Infraestructura	25
1.4.4.6.2.	Redes AD-HOC o MANET	26
1.4.4.6.3.	Redes MESH	44
1.4.5.	Sistemas mallados de primera, segunda y tercera generación	47
1.4.6.	Protocolos	50
1.4.7.	Métricas	51
1.5.	Seguridad	53
1.5.1.	Tipos de Seguridad	53
1.6.	Computadores de placa reducida	54
1.6.1.	Tipos de placas reducidas	54
1.6.2.	Raspberry PI	56
1.6.2.1.	Modelos	57
1.7.	Sistemas operativos	57
1.7.1.	Tipos de SO para Raspberry PI	58
1.7.1.1.	Raspbian	58
1.7.1.2.	Windows 10 IoT	58
1.7.1.3.	NOOBS	58
1.8.	Sistemas Aéreos no Tripulados	59
1.8.1.	Tipos	59
1.8.2.	Aplicaciones	60
2.	PROPUESTA DISEÑO DE HARDWARE	62
2.1.	Introducción	62
2.2.	Equipos y Materiales	64
2.2.1.	Raspberry PI3	64
2.2.2.	Antena WIFI RPI3	65
2.2.3.	Cámara RPI3	66
2.2.4.	Memoria micro SD	68
2.2.4.1.	Clase de Tarjeta SD	69
2.2.5.	Dron ARRIS	70

2.2.6.	Estación Base.....	71
2.2.7.	Fuentes de Energía	72
3.	PROPUESTA DISEÑO DE SOFTWARE Y CONFIGURACIÓN	73
3.1.	Introducción	73
3.2.	Red manet	74
3.2.1.	Direccionamiento IP y Puertos.....	74
3.2.2.	Raspberry PI3.....	75
3.2.2.1.	Rasbian Jessy With Pixel	76
3.2.2.2.	Pantalla de presentación	77
3.2.2.3.	Instalación de Raspbian en las placas Raspberry Pi 3	77
3.2.3.	Proceso para Activar Cámara y Puerto SSH	82
3.2.3.1.	Pruebas de funcionamiento de la cámara en Raspberry Pi ...	84
3.2.4.	Aplicacion hsmm-pi en la configuracion de red manet	84
3.2.4.1.	Definición	84
3.2.4.2.	Requisitos básicos para HSMM-PI.....	86
3.2.4.3.	Modos de HSMM-PI	86
3.2.4.3.1.	Modo Puerta de Enlace o Gateway	87
3.2.4.3.2.	Modo Malla Interna.....	87
3.2.4.4.	Instalación de HSMM-PI 0.8.1	88
3.2.5.	Protocolo OSLR.....	92
3.2.6.	Configuración de Nodos	93
3.2.6.1.	Network.....	95
3.2.6.1.1.	WiFi	96
3.2.6.1.2.	Wired.....	97
3.2.6.1.3.	Mesh	97
3.2.7.	Instalación de Netcat y Mplayer en Raspberry 3.....	98
3.3.	Esquema de nodos y estación Base	100
3.4.	Estación Base	101
3.4.1.	Direccionamiento IP y Puertos.....	101
3.4.2.	Sistema Operativo	102

3.4.2.1.	Windows 7	102
3.4.2.2.	Características	102
3.4.2.3.	Versiones de Windows 7	103
3.4.2.4.	Requisitos básicos para Windows 7	103
3.4.3.	Activación de Políticas (Friwall) en Windows 7	104
3.4.4.	Configuración Red AdHoc – MANET	105
3.4.4.1.	Conexión a Red MANET	106
3.4.4.1.1.	Parámetros de la Red.....	107
3.5.	Servicio de Video.....	108
3.5.1.	Netcat.....	108
3.5.1.1.	Principales características de Netcat.....	110
3.5.2.	Mplayer.....	110
3.5.2.1.	Principales formatos soportados de Mplayer	111
3.5.2.2.	Principales CODECS de video soportados por Mplayer	111
3.5.2.2.1.	Video	111
3.5.2.2.2.	Audio	112
3.5.3.	Conectividad entre Raspberry a la Estación Base	113
3.5.4.	Reproducción de Video entre Raspberry y Estación Base	114
3.5.5.	Diagrama Estación Base Gestión para Video	116
4.	PRUEBAS Y ANÁLISIS DE RESULTADO	116
4.1.	Primer escenario	117
4.1.1.	Ambiente Conjunto Shalom Ala Este	117
4.1.2.	Ambiente Conjunto Shalom Ala Sur.....	118
4.1.3.	Ambiente Campus UDLA-QUERI	123
4.2.	Segundo y Tercer escenario	126
4.2.1.	Ambiente Conjunto Shalom Ala Este	128
4.2.2.	Ambiente Conjunto Shalom Ala Sur.....	129
4.2.3.	Ambiente Campus UDLA-QUERI	132
4.3.	Cuarto escenario	133
4.3.1.	Ambiente Conjunto Shalom Ala Sur.....	134
4.3.2.	Ambiente Campus UDLA-QUERI	137

4.4. Prueba Fina	138
4.5. Consolidado.....	140
4.6. Análisis de Nivel de Potencia	141
5. CONCLUSIONES Y RECOMENDACIONES	143
5.1. Conclusiones.....	143
5.2. Recomendaciones	147
REFERENCIAS	150
ANEXOS	153

ÍNDICE DE FIGURAS

Figura 1 Diagrama de flujo	2
Figura 2 Sistema de Telecomunicación.....	6
Figura 3 Canales de Radio y Propagación	8
Figura 4 Espectro Electromagnético	9
Figura 5 Radio Frecuencias para Comunicación.....	10
Figura 6 Diagrama de Bloques del Sistema de Transmisión	11
Figura 7 Polarización Horizontal y Vertical de las Antenas.....	13
Figura 8 Lóbulo de Antena Direccional	15
Figura 9 Lóbulo de Antena Omnidireccional.....	16
Figura 10 Topologías de Redes Inalámbricas	20
Figura 11 Clasificación de las Redes Inalámbricas	20
Figura 12 Canales de Frecuencia 2.4 GHz	24
Figura 13 Red con Infraestructura.....	25
Figura 14 Redes Ad Hoc MANET.....	26
Figura 15 Red Ad Hoc MANET y sus elementos.....	28
Figura 16 Clasificación de Protocolos Ad Hoc.....	30
Figura 17 Transmisión Broadcast de RREQ	32
Figura 18 Transmisión Unicast de RREP	32
Figura 19 Multipoint Relay para N Estaciones.....	37
Figura 20 Ejemplo de Redes Ad Hoc en Tácticas Militares	40
Figura 21 Ejemplos de Redes en Situaciones de catástrofes.....	40
Figura 22 Red de MESH	44
Figura 23 Red Mesh Primera Generación	47
Figura 24 Redes Mesh Segunda Generación	48
Figura 25 Redes Mesh Tercera Generación	49
Figura 26 Tipos de Aeronaves no Tripuladas.....	60
Figura 27. Aplicaciones de UAV.....	61
Figura 28 Diagrama Físico de Red (Nodos y Estación Base).....	62
Figura 29. Características Placa Raspberry Pi.....	64
Figura 30 Diagrama de componentes Raspberry Pi 3 modelo B	65

Figura 31. Características de Antena WiFi Raspberry Pi.....	66
Figura 32. Características de Pi Cámara P5V04C	68
Figura 33 Características de Micro SD.....	70
Figura 34. Características del DRON	71
Figura 35 Características de Estación Base.....	72
Figura 36. Características de los Bancos de Poder.....	73
Figura 37 Diagrama de Red AdHoc - MANET RASPBERRY-UDLA.....	74
Figura 38 Imagen de Raspbian Jessie With Pixel	77
Figura 39 Pantalla de inicio de Raspbian	77
Figura 40 Imagen Booteable en Tarjeta SD	78
Figura 41. Configuración de adaptares cableados e inalámbricos	79
Figura 42 Terminal Raspberry.....	80
Figura 43 Menú de Configuración Raspberry	81
Figura 44 Ventana de expansión del sistema operativo	81
Figura 45 Reinicio de sistema operativo.....	82
Figura 46 Menú de Configuración del Raspberry Pi	83
Figura 47 Habilitación de la cámara en Raspberry Pi.....	83
Figura 48. Red MANET RASPBERRY-UDLA.....	86
Figura 49. Modos de funcionamiento de HSMM-PI	87
Figura 50 Verificación de GIT en el SO	89
Figura 51. Ejecución del Comando git clone	89
Figura 52. Ingreso a la carpeta de HSMM-PI y ejecución del instalador.....	90
Figura 53. Proceso de instalación, configuración y ejecución de OSLR	90
Figura 54. Instalación de componentes y librerías	91
Figura 55 Mensaje de instalación de HSMM-PI.....	92
Figura 56. Diagrama de Flujo de Datos de OSLR	93
Figura 57. Ingreso a HSMM-PI mediante browser.....	94
Figura 58. Longin de HSMM-PI.....	94
Figura 59. Menú de Administrador HSMM-PI	95
Figura 60. Cambio de contraseña HSMM-PI.....	95
Figura 61. Ventana de Configuración WLAN.....	96
Figura 62. Ventana de Configuración de Wired.....	97

Figura 63. Ventana de Configuración Mesh	98
Figura 64. Instalación de Mplayer y Netcat en el Rapberry	99
Figura 65. Esquema nodo Raspberry PI 3	100
Figura 66. Esquema Estación Base	100
Figura 67. Esquema general del sistema	101
Figura 68. Políticas y reglas de entrada Firewall de Windows.....	105
Figura 69. Hosted Network Support	106
Figura 70. Conexión a la red Manet desde Estación Base	107
Figura 71. Conexión de red MANet.....	108
Figura 72. Presentación de nodos en la red.....	113
Figura 73. Transmisión de video desde Raspberry a Estación Base.....	115
Figura 74. Diagrama Gestión para Video desde Nodo a Estación Base.....	116
Figura 75. Primer Escenario (primeros 76 mts)	117
Figura 76. Ambiente Conjunto Shalom Ala Este (Escenario 1).....	118
Figura 77. Potencia de red MANET RASPBERRY-UDLA (Distancia 1mt).....	119
Figura 78. Intensidad de señal red MANET RASPBERRY-UDLA (Distancia 1mt).....	119
Figura 79. Calidad del Enlace desde RPI-I (Distancia 1mt)	120
Figura 80. Calidad del Enlace desde RPI-II (Distancia 1mt)	120
Figura 81. Calidad del Enlace desde RPI-III (Distancia 1mt)	120
Figura 82. Captura de Tráfico y Video (Distancia 1 mt)	121
Figura 83. Potencia de red MANET RASPBERRY-UDLA (Distancia 76 mts)	121
Figura 84. Intensidad de señal red MANET RASPBERRY-UDLA (Distancia 76 mts).....	122
Figura 85. Calidad del Enlace desde RPI-I (Distancia 76 mts)	122
Figura 86. Captura de Tráfico y Video (Distancia 76 mts)	123
Figura 87. Ambiente Conjunto Shalom Ala Sur (Escenario 1)	123
Figura 88. Uso de Canales Banda WiFi Conjunto Shalom	124
Figura 89. Uso de Canales Banda WiFi UDLA-Queri	125
Figura 90. Ambiente UDLA-Queri (Escenario 1).....	126
Figura 91. Segundo Escenario (152 mts)	127

Figura 92. Tercer Escenario (152 mts)	127
Figura 93. Ambiente Conjunto Shalom Ala Este (Escenario 2).....	128
Figura 94. Ambiente Conjunto Shalom Ala Sur (Escenario 3)	129
Figura 95. Potencia de red MANET RASPBERRY-UDLA (Distancia 152 mts).....	130
Figura 96. Intensidad de señal red MANET RASPBERRY-UDLA (Distancia 152 mts)	130
Figura 97. Calidad del Enlace desde RPI-I (Distancia 152 mts)	131
Figura 98. Calidad del Enlace desde RPI-II (Distancia 152 mts)	131
Figura 99. Calidad del Enlace desde RPI-III (Distancia 152 mts)	131
Figura 100. Captura de Tráfico y Video (Distancia 152 mts)	132
Figura 101. Ambiente UDLA-Queri (Escenario 3).....	133
Figura 102. Cuarto Escenario (228 mts).....	134
Figura 103. Ambiente Conjunto Shalom Ala Sur (Escenario 4)	135
Figura 104. Potencia de red MANET RASPBERRY-UDLA (Distancia 228 mts).....	135
Figura 105. Intensidad de señal red MANET RASPBERRY-UDLA (Distancia 228 mts)	136
Figura 106. Captura de Tráfico y Video (Distancia 228 mts)	136
Figura 107. Calidad del Enlace desde RPI-II (Distancia 228 mts)	137
Figura 108. Ambiente UDLA-Queri (Escenario 4).....	138
Figura 109. Dron con RPI3 en vuelo	139
Figura 110. Estación base y nodos acoplados en Dron y carro a control remoto.....	139
Figura 111. Transmisión de video desde dos nodos en movimiento	140
Figura 112. Grafico Potencia Vs Distancia para Tx	142

ÍNDICE DE TABLAS

Tabla 1. Estándares 802.11 IEEE	23
Tabla 2. Cuadro Comparativo de Placas de Tamaño Reducido	55
Tabla 3. Tabla de Direccionamiento IP y Puertos en cada nodo.	75
Tabla 4 Tabla de Direccionamiento IP y puerto en estación base	102
Tabla 5. Ejecución de video desde Estación Base UDP y TCP	114
Tabla 6. Ejecución de video desde Raspberry UDP y TCP	114
Tabla 7. Toma de Datos.....	142

INTRODUCCIÓN

El proyecto propuesto trata del diseño de un sistema de comunicación, este incluye la utilización de los dispositivos Raspberry pi 3, el cual es una placa de procesamiento portátil que en el tiempo actual está siendo muy utilizada puesto que proporciona altas prestaciones para desarrollar diversas aplicaciones a un bajo coste, además de su tamaño compacto peso ligero es una gran opción para realizar el acople de la placa a los Drones para realizar la transmisión de video en tiempo real dentro de la red MANET que se propone en esta memoria.

De acuerdo a lo anteriormente citado el proyecto se estructura de cuatro secciones en las que se desglosa:

La primera sección de carácter teórico donde un bloque descriptivo explica los orígenes de la Raspberry pi, los modelos existentes, los sistemas operativos y los lenguajes de programación con el propósito de introducir conocimientos básicos en la configuración de la placa.

En la segunda sección se detalla toda la propuesta en cuanto a hardware que será utilizado en la propuesta de diseño, dando a conocer cada uno de los componentes, dispositivos y materiales que dan la posibilidad de implementar y conectar elementos al área de cobertura Wi-Fi de las placas y la estación base. La tercera sección donde se explica el desarrollo de la selección en cuanto a las aplicaciones en la propuesta de software que será utilizado en la configuración de nuestro sistema de comunicación entre los dispositivos abriendo paso a la interconexión de los nodos para con ayuda de los protocolos ya desarrollados sea posible la ejecución, transmisión y reproducción de video desde los nodos hacia la estación base.

Y por último el cuarto bloque de carácter analítico en donde se exponen las pruebas y análisis de los resultados en la configuración, implementación, ejecución y resultados en cuanto a la transmisión de video desde las placas Raspberry dando una solución en cuanto a la infraestructura de la red MANET a la conectividad y enrutamiento de los nodos en la implementación, dando como

resultado el análisis de las pruebas para el cumplimiento de los objetivos, seguida de las conclusiones y recomendaciones del sistema propuesto.

Alcance

El alcance de este proyecto consiste en el diseño de un sistema de comunicación acoplado en drones, con tres dispositivos Raspberry PI, uno en cada dron; los cuales tendrán una estación base que será un computador en el cual se recibirá y almacenará la información obtenida de los tres nodos con drones en vuelo, ya sea de manera directa o atreves de los otros dos nodos Raspberry PI, en este caso aplicando la definición de una red MESH y el enrutamiento aplicado a los nodos.

Para llegar a realizar lo mencionado anteriormente, se considerará la programación del Raspberry PI, y se aplicaran los fundamentos de comunicación inalámbrica.

A continuación, se expone un diagrama de flujo en el cual se procede a explicar el funcionamiento del sistema de comunicación a diseñar y los equipos que hacen parte del mismo.

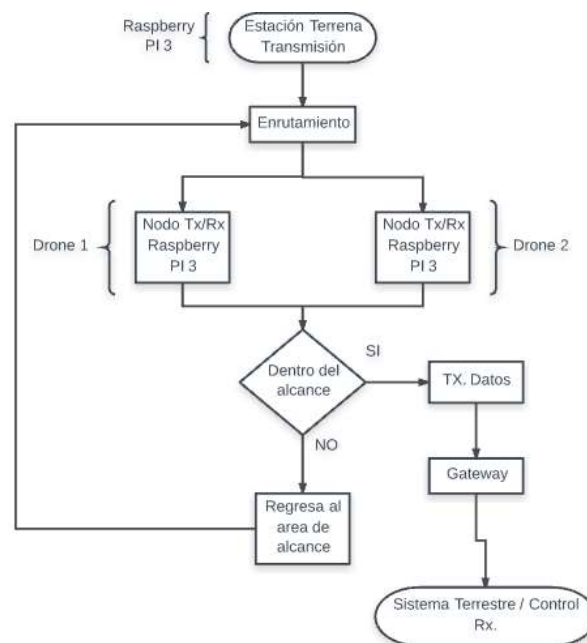


Figura 1. Diagrama de flujo

Debido a que la transmisión de información se va a realizar con los dispositivos Raspberry cuando estén en vuelo es necesario tener en cuenta que se debe mitigar los problemas de latencia e interferencia ocasionados por los drones y el medio de transmisión (AIRE).

Para cumplir con este alcance se va a poner en práctica lo aprendido en las materias de tecnologías inalámbricas, aplicaciones móviles, teoría de comunicaciones, sistemas operativos, inter-redes locales, teoría de circuitos, electrónica digital y microcontroladores.

Justificación

El desarrollo de la tecnología en la construcción de (UAV) vehículos aéreos no tripulados, crean la necesidad de explotar al máximo características que presentan estos dispositivos en este caso *Drones*. Dado que un Dron normalmente no está equipado con tantos dispositivos que permitan la comunicación entre más de uno de estos dispositivos en los Drones (UAV).

Al ser un dron una herramienta de vanguardia y de altas prestaciones tecnológicas debe ir de la mano con todos los dispositivos que permitan en este caso explotar su capacidad; creando así más alternativas de implementación y desarrollo para adicionar características y herramientas que permitan realizar tareas específicas para el beneficio humano y de la sociedad.

De esta manera es posible realizar un sistema de comunicación entre los dispositivos que me permita realizar la cobertura de un área geográfica entregando datos y video en tiempo real sin necesidad de que el ser humano o el administrador se desplace; es decir el dispositivo cumple con las funciones de desplazamiento propuesto mientras que el administrador desde la estación terrena analiza los datos y video recogidos por los nodos. Además, permite ampliar y mejorar el área de cobertura con la adición de nodos (Drones) al sistema. Por mencionar ejemplos de aplicación en este caso sería utilizado un sistema de comunicación para rastreo de personas en parques o reservas

forestales, así como también en circuitos cerrados en cuanto a vigilancia y seguridad de perímetros, análisis de plantaciones e invernaderos para conjuntamente la activación de sensores que mediante la información receptada se proceda activar bombas de fumigación, eventos sociales donde se necesite cubrir diferentes nodos que transmitan videos y datos dentro de un escenario dando un control total del evento para identificar problemas en el transcurso; en fin las aplicaciones son tan bastas en cuanto a la aplicación de este proyecto propuesto se refiere.

Otro beneficio importante de este proyecto está orientado a la Universidad de las Américas, y consiste en permitir que otros estudiantes puedan continuar con el estudio de este sistema de comunicación y la implementación de herramientas tecnológicas que entregue un valor agregado como dar utilidades específicas como las anteriormente mencionadas a los drones identificando nichos y propuestas de negocio, tomando en cuenta que este campo aún no está explotado o desarrollado en su totalidad. También este proyecto está orientado a la línea de investigación propuesta por la Carrera, que trata de generar sistemas de telecomunicaciones para el desarrollo de los sectores estratégicos de forma particular orientados a la creación de prototipos de sistemas de percepción remota.

Objetivos

Objetivo General

Diseñar un sistema de comunicación mediante el uso de dispositivos Raspberry PI como nodos, ubicados en drones para la transmisión y recepción de datos y video en tiempo real.

Objetivos Especificos

- Establecer la comunicación entre 3 nodos móviles (UAV) equipados con un dispositivo Raspberry PI cada uno; mediante el uso de protocolos y algoritmos ya desarrollados.
- Probar la cobertura Wi-Fi del Raspberry PI 3 para transmisión y recepción de datos en los 3 nodos.
- Definir una estación base para la recepción de datos tomados por los nodos.
- Analizar los resultados sobre latencia y pérdida de datos en la transmisión en el sistema propuesto.

1. MARCO TEÓRICO

1.1. Introducción

Estructuralmente en el proyecto de diseño realizado se expone muchas definiciones necesarias para el entendimiento y familiarización con el desarrollo del mismo, al abarcar el tema de las comunicaciones inalámbricas con una placa que utiliza su antena de dispositivo Wi-Fi para comunicarse dentro de la red creada, debemos incluir todo el marco teórico relacionado a las comunicaciones inalámbricas hasta llegar al tipo de red que fue escogido para realizar la estructura de comunicación que son las redes MANET. Así como también la utilización de los dispositivos ya antes mencionados como son la placa de procesamiento Raspberry pi y el uso de Drones, los cuales simulan el movimiento dinámico de las placas dando así paso a las pruebas que serán analizadas en cuanto al comportamiento de la transmisión de video desde cada una de las 3 placas en el aire.

1.2. Sistemas de radiocomunicación

Los sistemas de Radiocomunicación son un conjunto de elementos que tienen la finalidad de realizar la telecomunicación, la cual se realiza a través de ondas de radio denominadas ondas hertzianas, las cuales a su vez están caracterizadas por el movimiento de los campos eléctricos y magnéticos. La comunicación vía radio es posible gracias al espectro radioeléctrico cuyas propiedades son diversas en cuanto a la variedad de bandas de frecuencias que podemos encontrar como son baja frecuencia, alta frecuencia, ultra frecuencia, etc.

El proceso llamado transmisión como se muestra en la figura 2, es el más importante en cuanto a las radiocomunicaciones, lo cual es conocido como el proceso de enviar o transportar información desde la fuente que es el punto de partida hacia el destino que es el punto final, utilizando un medio o canal que permita esta acción.



Figura 2. Sistema de Telecomunicación

Tomado de (Ramírez, 2015)

De esta manera el sistema de radiocomunicación comprende elementos básicos que conforman un sistema de telecomunicaciones como son los medios de transmisión, los protocolos, las interfaces y la señalización. El concepto de Telecomunicaciones se define como el conjunto de recursos en espectro, espacio, tiempo y equipos necesarios para realizar una comunicación. (Ramírez, 2015)

1.2.1. Elementos para Transmisión

Los elementos que permiten generar este traspaso de datos entre los puntos de transmisión y recepción son:

- El transmisor que tiene la función de acondicionamiento de las señales, determinando un ancho de banda y potencia para que esta información sea aportada al medio de transporte.
- El receptor tiene la función de capturar las señales que se están enviando mediante el medio de transmisión, estas al ser recibidas deben pasar por procesos como la amplificación y el acondicionamiento de la señal para que esta sea entendida por el usuario final en este caso el receptor el cual puede ser cualquier ser u objeto.
- El medio de transporte es el campo físico por el cual se transmite la señal que se envía desde el transmisor al receptor, este puede ser el aire, un cable, el agua, fibra óptica, etc.

1.2.2. Canal

Cuando hablamos de radio-canal como se muestra en la figura 3, se hace referencia a que se está utilizando el aire como medio de propagación de nuestras ondas en el transmisor lo cual depende de la energía electromagnética generada por el transmisor.



Figura 3. Canales de Radio y Propagación

Tomado de (Ramírez, 2015)

1.2.3. Espectro Electromagnético

El espectro Radioeléctrico no es más que la combinación oscilante de los campos magnéticos y los campos eléctricos en el espacio de tal manera que se produzca la transportación de energía entre dos o más lugares, entre esta gama de ondas que se encuentran dentro del espectro podemos citar algunas como son la luz visible, la radio, la televisión, los rayos x, los rayo gama, etc. En donde todos ellos consisten en una radiación electromagnética las cuales se manifiestan en diferentes rangos de frecuencia y es por ello que es posible clasificarlas, así como también en por sus diferentes longitudes de onda, siendo este último el más práctico y común para clasificar este espectro. Es por ello que al calificarlos mediante la frecuencia y longitud de onda recibe el nombre de espectro electromagnético.

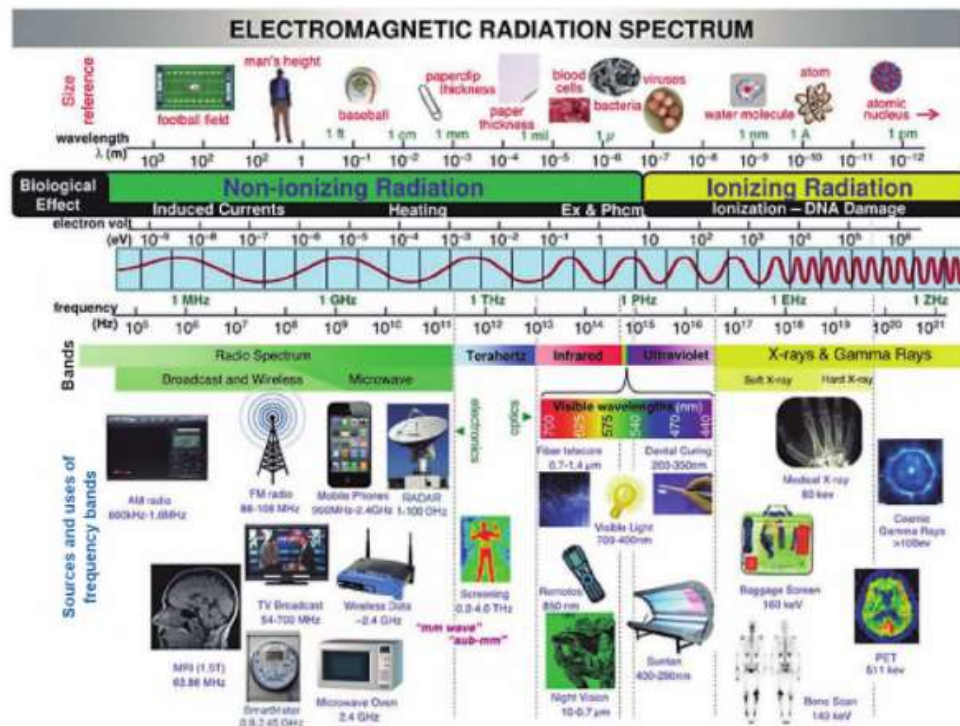


Figura 4. Espectro Electromagnético

Tomado de (Ramírez, 2015)

Como se observa en la figura 4, las bandas de frecuencia que se encuentran disponibles para ser aplicadas en los sistemas de telecomunicación se encuentran medidas por unidades de hertzios Hz, que abarca un conjunto de frecuencias inferiores a 1kHz hasta alrededor de 300 GHz. Esta pequeña parte que en otras palabras se denomina la banda de radiofrecuencia agrupa estas frecuencias que son utilizadas en comunicaciones de radio y canales de comunicación. Es por ello que en la figura 5 podemos observar la distribución de las frecuencias.

1.2.4. Radio frecuencias

Banda ITU	Nombre Nombre inglés	Símbolos (en inglés)	Gama de frecuencias Longitud de onda	Ejemplos de uso
	Frecuencia tremendamente baja Tremendously low frequency	TLF	< 3 Hz > 100 000 km	Ruido natural o provocado por el hombre
	Frecuencia extremadamente baja Extremely low frequency	ELF	3-30 Hz 100 000-10 000 km	Comunicación con submarinos
	Súper baja frecuencia Super low frequency	SLF	30-300 Hz 10 000-1000 km	Radar. Enlace de radio
	Ultra baja frecuencia Ultra low frequency	ULF	0,3 a 3 kHz 1000 a 100 km	Enlaces de radio. Ayuda a navegación aérea. Comunicaciones en minas a través de la tierra
4	Muy baja frecuencia Very-low frequency	VLF	3 a 30 kHz 100 a 10 km	Radioayuda, señales de tiempo, comunicación submarina, pulsómetros inalámbricos, geofísica
5	Media frecuencia Low frequency	LF	30 a 300 kHz 10 a 1 km	Radiodifusión en AM (onda larga) (Europa y partes de Asia), RFID, radioafición
6	Media frecuencia Medium frequency	MF	300 a 3000 kHz 1000 a 100 m	Radiodifusión en AM (onda media), radioafición, balizamiento de aludes
7	Alta frecuencia High frequency	HF	3 a 30 MHz 100 a 10 m	RFID, radar, comunicaciones ALE, comunicación cuasi-vertical (NWS), telefonía móvil y marina
8	Muy alta frecuencia Very-high frequency	VHF	30 a 300 MHz 10 a 1 m	FM, televisión, comunicaciones con aviones a la vista entre tierra-avión y avión-avión, telefonía móvil marítima y terrestre
9	Ultra alta frecuencia Ultra-high frequency	UHF	300 a 3000 MHz 1 m a 10 cm	Comunicaciones por microondas, radioastronomía, redes inalámbricas, <i>bluetooth</i> , GPS
10	Súper alta frecuencia Super-high frequency	SHF	3 a 30 GHz 10 a 1 cm	Comunicaciones por satélite, televisión por satélite, DBS
11	Frecuencia extremadamente alta Extra-high frequency	EHF	30 a 300 GHz 10 a 1 mm	Radioastronomía, transmisión por microondas de alta frecuencia, teledetección
12	Terahercios o frecuencia tremendamente alta Terahertz or tremendously high frequency	THz o THF	> 300 GHz < 1 mm	Radiografía de terahercios, espectroscopia mediante terahercios, comunicaciones/computación mediante terahercios

Figura 5. Radio Frecuencias para Comunicación

Tomado de (Ramírez, 2015)

En la figura 5 se observa la distribución de frecuencias establecida por el CCIR consejo consultivo internacional de las comunicaciones de radio el cual fue elaborado desde el año 1953 y se mantiene hasta el día de hoy como referente.

1.2.5. Flujo de la Transmisión para Comunicación

Es por ello por lo que en la figura 6, se muestra el significado de la transmisión de manera general con el propósito de las mismas, la distribución, su uso y aplicaciones.

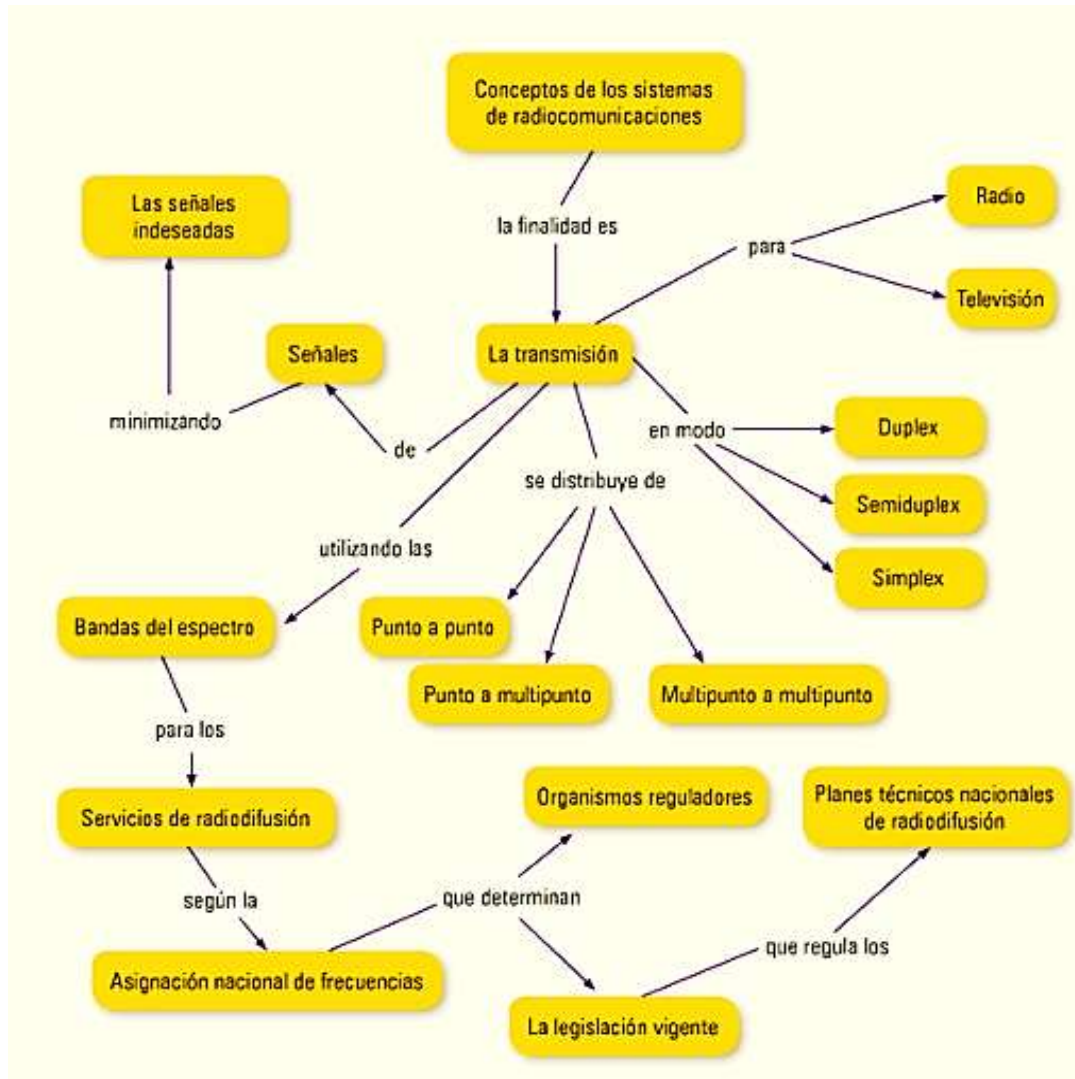


Figura 6. Diagrama de Bloques del Sistema de Transmisión
Tomado de (Ramírez, 2015)

1.3. Antenas

Las antenas son un elemento muy indispensable para que las comunicaciones inalámbricas logren su propósito, ya que como se menciona que carecen de la

dependencia de cables para realizar la comunicación entre los dispositivos pues usan antenas que se encargan de radiar las señales en forma de ondas a través del aire logrando así un área de radiación de ondas llamada cobertura.

Las antenas no son más que dispositivos que permiten el proceso de transmitir o de recibir la información por medio de las ondas de electromagnéticas. El principio de la antena es realizar la transformación de energía eléctrica en las ondas electromagnéticas que son radiadas al espacio libre y estas sean transmitidas a otra antena que las reciba y realice a función inversa. Las tres propiedades más importantes de la antena son la ganancia, la dirección y la polarización. Donde la ganancia es la el aumento de potencia que se da a la señal para que esta pueda ser transmitida o propagada mientras que la dirección determina el patrón de la transmisión de la onda o la señal por lo que una antena se encarga de redirigir la potencia de la señal a una dirección específica a la cual se intenta radiar, es por ello que tenemos una proporcionalidad inversa entre estos dos parámetros ya que si la ganancia de una antena aumenta significa que el ángulo de radiación disminuye; esto nos da como resultado una mayor distancia en cuanto a la cobertura mientras que el área de cobertura se reduce. Finalmente es necesario tomar en cuenta que al radiar la señal esta puede ser aplicada a todos los planos ya sea de manera vertical u horizontal es por ello que la polarización nos ayuda a seleccionar el plano para la radiación de la señal como se aprecia en la figura 7.

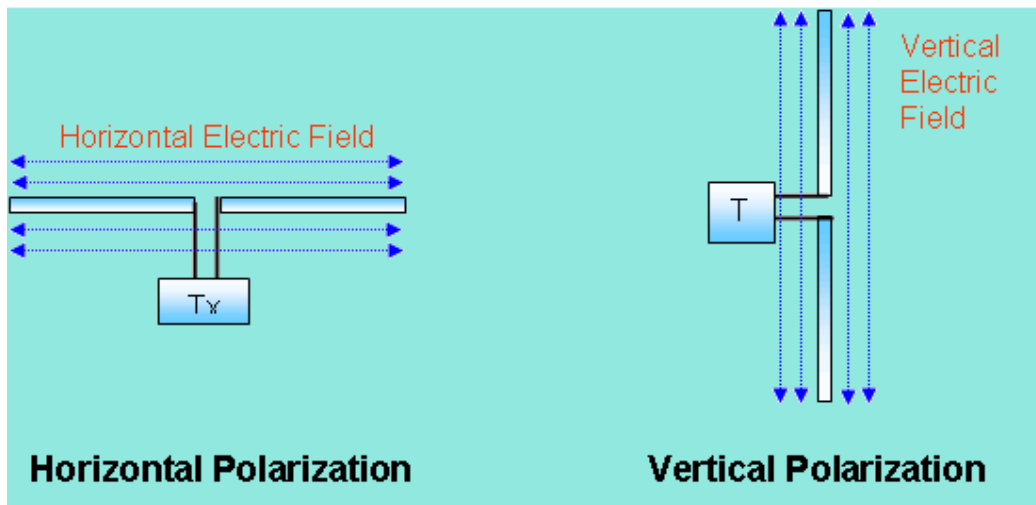


Figura 7. Polarización Horizontal y Vertical de las Antenas

Tomado de (Cisco, 2008)

1.3.1. Características de las Antenas

Las antenas y sus características dependen de la dimensión de su estructura y de la longitud de onda de la señal que emite, es por este parámetro de la longitud de onda que se puede decir que si las dimensiones de la estructura de la antena son mucho más pequeñas que la longitud de onda de la misma, se llaman a estas antenas elementales, mientras que si las dimensiones llegan a media longitud de onda, se llaman antenas resonantes y si el tamaño de la longitud de onda es mucho menor a las dimensiones de la antena se conoce como directivas.

1.3.2. Parámetros de las Antenas

Los parámetros que existen para una antena son:

- Radiación de Lóbulo
- Ancho de Banda
- Directividad de la Antena
- Ganancia de la Antena

- Eficiencia de la antena
- Impedancia de la Antena
- Apertura del haz de la Antena
- Polarización de la Antena

1.3.3. Tipos de antenas

Las antenas existentes se pueden clasificar en direccionales y omnidireccionales, también las podemos clasificar por su funcionalidad y componentes.

1.3.3.1. Antenas Direccionales

Son aquellas también llamadas unidireccionales o directivas, son capaces de la concentración de energía de RF, lo cual ayuda a cubrir grandes distancias, pero el costo es que el ancho de haz efectivo disminuye.

Como se puede apreciar en la figura 8, el lóbulo donde se puede ver la mayor ganancia que son 21dbi es donde se encuentra direccionada la señal por la antena de esta manera se puede asociar a un foco de luz incandescente de una linterna que tiene el haz de luz que se emite de forma intensa en una sola dirección para dar más alcance de visibilidad. Como ejemplos de este tipo de antenas tenemos las antenas parabólicas, antenas yagis y planares.

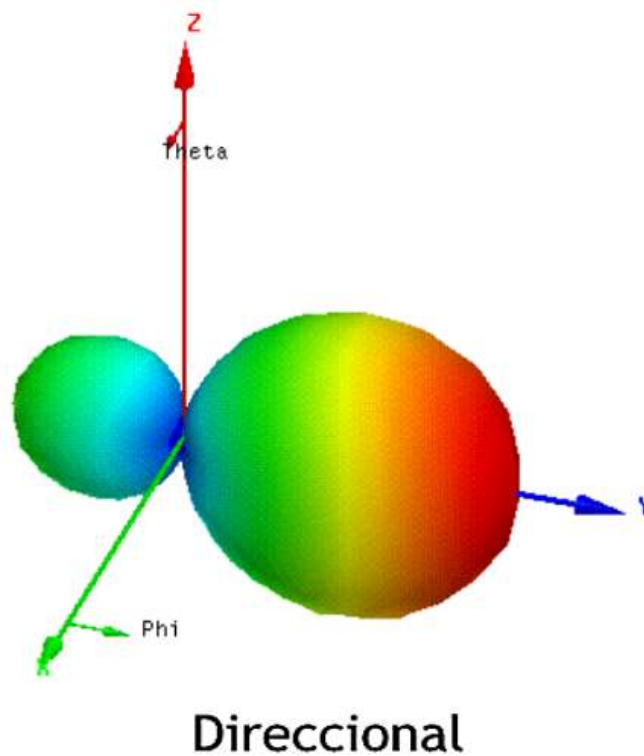
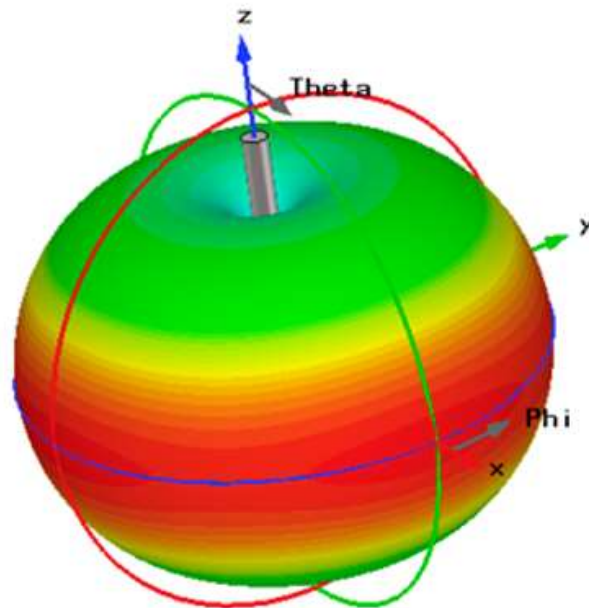


Figura 8. Lóbulo de Antena Direccional

Tomado de (Martín, 2015)

1.3.3.2. Antenas Omnidireccionales

Este tipo de antenas son capaces de difundir la señal en todas las direcciones no se enfocan en una dirección específica, de esta manera el haz es amplio al momento de radiar la señal, pero por ser un parámetro inversamente proporcional al parámetro de alcance este disminuye. Teóricamente las antenas omnidireccionales irradian la señal a los 360 grados, pero tienen un costo de alcance ya que estas no permiten tener un alcance mayor como las antenas direccionales. Como podemos apreciar en la figura 9, la señal de estas antenas se da hacia todos los ángulos ya sea de manera horizontal o vertical. Como por ejemplo las antenas de los puntos de acceso para conexiones inalámbricas.



Omnidireccional

Figura 9. Lóbulo de Antena Omnidireccional

Tomado de (Martín, 2015)

1.4. Redes inalámbricas

El término redes inalámbricas se utiliza para describir la conexión entre dos o más elementos, la cual es posible a través de ondas electromagnéticas que se propagan en el aire como medio de transporte y propagación. A cada elemento que se encuentra conectado a la red se lo denomina nodo y las redes inalámbricas son capaces de incorporar o desconectar nodos dentro de su red permitiendo la compartición de información entre ellos sin un medio físico cableado que limite la movilidad de cada dispositivo, permitiendo a estos actuar como puertos para la transmisión y recepción de datos, todo esto es posible a través de antenas.

1.4.1. Ventajas de las redes Inalámbricas

Las redes inalámbricas dan ciertas ventajas que son flexibilidad dentro de la zona de cobertura, ya que se pueden ubicar los nodos a gusto del usuario y sin tener que modificar o deshabilitar de conexión cambiar el lugar del nodo. Otra ventaja es la poca planificación ya que al no utilizar cables físicos no es necesario un diseño estructural para la colocación de los mismos, lo que implica la reducción de costos en cuanto a modificaciones del entorno para el paso del cableado a través de la estructura de cobertura. También podemos tomar ventaja en cuanto al diseño ya que al ser una red inalámbrica los dispositivos receptores son pequeños, no ocupan mayor espacio que hasta pueden ser considerados como dispositivos de bolsillo. Los parámetros de robustez y escalabilidad del sistema son una gran ventaja ya que la conexión a cada nodo por usuario es determinada por el equipo o el dispositivo, por lo que no se puede realizar una estructura de red donde es muy sencillo agregar más usuarios o quitarlos de la red sin interferencias o interrupciones al resto de nodos o usuarios conectados a la red.

1.4.2. Historia de las redes Inalámbricas

En la historia de las redes inalámbricas pues viene a ser una tecnología muy reciente con no más de 15 a 20 años de aplicación, actualmente el campo de las comunicaciones inalámbricas es uno de los segmentos con crecimiento apresurado en la industria de las telecomunicaciones. Los sistemas de comunicación inalámbrica como el celular o los teléfonos satelitales, así como también las redes de área local WLANs, se han convertido en herramientas esenciales en el día a día de las personas ya sea en el ámbito personal o profesional. Las ventajas más importantes que hacen a las comunicaciones inalámbricas tan necesarias en estos días son las facilidades que entregan al usuario en lo que refiere a movilidad y bajo costo.

Las redes inalámbricas pueden rastrearse a la Universidad de Hawái ALOHANET, a un proyecto de investigación en los años 1970's. La llave de los eventos que dieron inicio a las redes inalámbricas con un rápido crecimiento a las tecnologías del siglo 21 fue ratificada en el estándar IEEE 802.11 en 1997, y subsecuentemente desarrolladas por la certificación de la alianza Wi-Fi (WECA). Desde los 70's hacia los 90's, el crecimiento de la demanda de las conexiones inalámbricas solo podía ser lograda por un hardware costos, basado en tecnologías propietarias, las cuales no ofrecían interoperabilidad de los equipos entre las diferentes marcas, es decir eran únicamente compatibles con equipos de las mismas marcas manufacturadas, también carecían de mecanismos de seguridad y el rendimiento ofrecido era menor al estándar que ofrece Ethernet cableado de 10Mbps.

1.4.3. Estándares de las redes inalámbricas

El estándar 802.11 fue el inicio determinante para la investigación de redes inalámbricas en donde nació una de la más grande y reconocible marca como es Wi-Fi. Las diversidades en las tecnologías de redes inalámbricas ahora operan en orden sobre las 4 magnitudes en un rango de data como *ZigBee* a 20kbps que va hacia un USB inalámbrico que están sobre los 500Mbps, y sobre el orden de 6 magnitudes en un rango como NFC a 5 cm a WiMAX, así como también Wi-Fi que opera sobre de 50 km.

Es por ello que las redes inalámbricas son aceptadas y con una gran demanda a nivel mundial, entre las ventajas a corto y largo plazo tenemos la accesibilidad, en nuestro entorno es muy fácil encontrar dispositivos que tienen incorporados antenas para el acceso a las diferentes redes inalámbricas que rigen el día a día de la población, como por ejemplo los celulares que permiten al usuario la comunicación o el acceso a los recurso de la red dentro del área de cobertura, se destaca que por ser fácil de instalar es muy fácil realizar la ampliación o reducción de la misma sin afectaciones al resto de usuarios que se encuentran conectados a ella. También podemos hablar de movilidad, los usuarios pueden

mantenerse conectados mientras ellos se encuentren en cualquier ubicación dentro del área de cobertura e incluso mientras se encuentran en movimiento dentro de ella, dando acceso a los usuarios. Otro punto importante a tratar es la fácil implementación ya que al no tener que estar limitada a un cableado físico esta puede ser implementada en cualquier área, sin tener que hacer cambios al entorno donde se coloquen los dispositivos que brindan el acceso a los dispositivos. Como punto a favor de las redes inalámbricas podemos hablar de seguridad y escalabilidad, al necesitar una mayor número de dispositivos conectados no es necesario instalar más equipos ya que la red inalámbrica es muy dinámica para permitir más conexiones al contrario de una red cableada donde necesariamente se debe utilizar más recursos como cableado para añadir más dispositivos a la red y claro mediante los protocolos y claves de acceso es posible limitar gestionando la incorporación de dispositivos ajenos a la red.

1.4.4. Clasificación de las redes Inalámbricas

Las redes inalámbricas o redes sin cables se pueden clasificar por varios tipos, pero para facilitar el entendimiento las propiedades que brindan y las necesidades que se necesitan cubrir son las siguientes:

1.4.4.1. Por su topología

La clasificación de las redes inalámbricas tomando en cuenta la topología se divide en las diferentes formas mostradas en la figura 10:

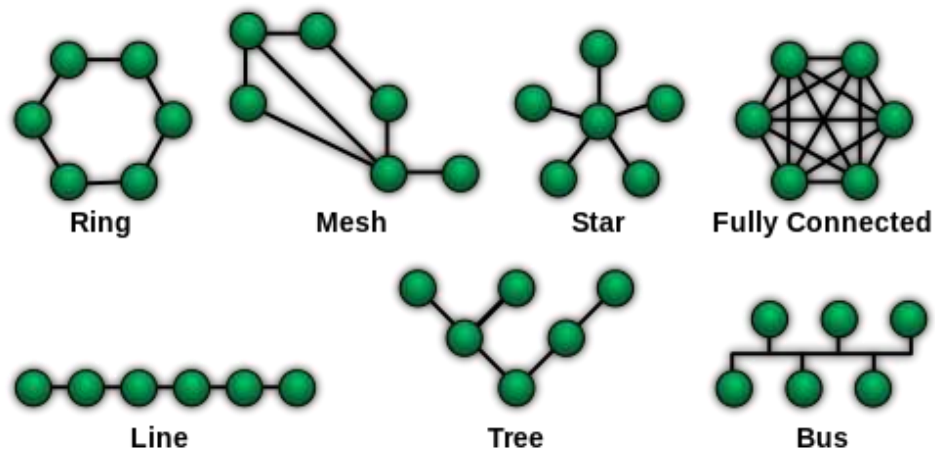


Figura 10. Topologías de Redes Inalámbricas

Tomado de (Alcibar, 2010)

1.4.4.2. Por su cobertura

Gracias a la figura 11 tenemos que por su cobertura las redes inalámbricas se clasifican:

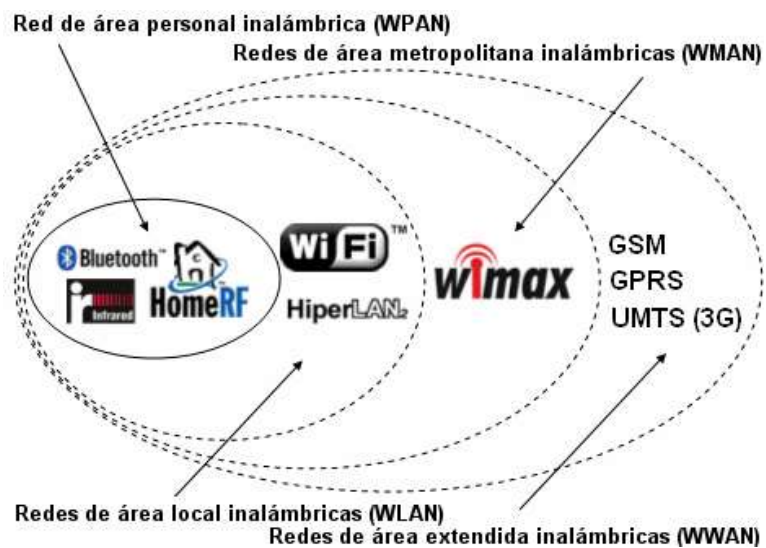


Figura 11. Clasificación de las Redes Inalámbricas

Tomado de (Kioskea, 2014)

a) Redes WPAN

Redes de área personal, son un tipo de redes que tienen una capacidad de cobertura muy reducida no sobrepasan los cinco metros como máximo, dando así la conexión entre dos dispositivos cercanos por ejemplo Bluetooth, Infrarrojo, etc.

b) Redes WLAN

Redes de área local, estas se caracterizan por estar formadas por pocos dispositivos que comparten recursos de la red, el área de cobertura depende mucho de la capacidad de la antena de los puntos de acceso WAP que son los que permiten la conexión de los dispositivos entre sí a través de ondas de radiación de señal, para esto todos los dispositivos que contienen el logo Wi-Fi, estándar de fidelidad inalámbrica, son aquellos que indican la compatibilidad de sus tarjetas de red o puntos de accesos para la incorporación en las redes sin problemas.

c) Redes WMAN

Redes de área metropolitana, son aquellas que permiten la conectividad de dispositivos u otras redes dentro de un área metropolitana, por ejemplo, entre varios edificios u oficinas dentro de una ciudad.

Esta se basa en el uso de estándar de comunicación *WiMax* que es modo de acceso *Worldwide Interoperability* mediante microondas que como resultado son redes más veloces y de gran alcance, estas son muy utilizadas para entornos de tráfico multimedia usadas para unir sucursales bancarias, etc.

d) Redes WAN

Redes de área amplia, *World Area Network* son aquellas que pueden cubrir unas áreas de gran extensión incluso a nivel geográfico amplio, se componen de varias antenas que se colocan generalmente en lugares elevados, esta utiliza tecnologías de comunicaciones móviles como la de celular, por ejemplo:

WiMAX, GPRS, CDMA2000, GSM, 3G, 4G para realizar la transferencia de los datos entre los equipos de la red.

1.4.4.3. Por tipo de conexión

Al ser una red de tipo inalámbrica podemos clasificar a los distintos de tipos de conexión mediante medios no guiados como son:

a) Red por radio

Es la que conectada a las diferentes estaciones de red a través del uso de la radiofrecuencia.

b) Red por infrarrojos

La red por medio de dispositivos infrarrojos se da gracias a los leds infrarrojos que permiten la comunicación entre dos dispositivos o nodos que tengas estos leds tanto el emisor como el receptor, el uso de esta es muy escaso ya que es indispensable la visibilidad entre ellos y su alcance es muy reducida.

c) Red por microondas

Las microondas son utilizadas por un tipo de redes inalámbricas que están regidas por protocolos que determinan la frecuencia de transmisión siendo esta en dos rangos importantes que son de 2.4GHz IEEE 802.11b, 5.4 GHz IEEE 802.11a y 5.7 GHz IEEE 802.11n, los cuales son los más comunes en este tipo de red.

1.4.4.4. Por su tecnología

Al hablar de la Tecnologías que ocupan las redes inalámbricas nos referimos a los estándares que se utilizan para su funcionamiento las cuales dotan de parámetros como la velocidad de transmisión, la frecuencia de funcionamiento, el ancho de banda y el alcance, todos estos están basados en las regulaciones

IEEE del estándar 802 es por ello por lo que clasificamos en los tipos más conocidos hasta el último publicado.

Tabla 1.

Estándares 802.11 IEEE

Resumen de Estándar 802 IEEE para Redes Inalámbricas						
Tipo	Velocidad (teórica)	Velocidad (práctica)	Frecuencia	Ancho de banda	Alcance	Año de implementación
802.11	2 Mbit/s	1 Mbit/s	2,4 Ghz	22 MHz	330 metros	1997
802.11a	54 Mbit/s	22 Mbit/s	5,4 Ghz	20 MHz	390 metros	1999
802.11b	11 Mbit/s	6 Mbit/s	2,4 Ghz	22 MHz	460 metros	1999
802.11g	54 Mbit/s	22 Mbit/s	2,4 Ghz	20 MHz	460 metros	2003
802.11n	600 Mbit/s	100 Mbit/s	2,4 Ghz y 5,4 Ghz	20/40 MHz	820 metros	2009
802.11ad	7.13 Gbit/s	6 Gbit/s	60 Ghz	2 MHz	300 metros	2012
802.11ac	6.93 Gbps	100 Mbit/s	5,4 Ghz	80 - 160 MHz	400 metros	2013
802.11ah	Wi-Fi HaLow		0.9 Ghz	2 MHz	1000 metros	2016

Como se muestra en la tabla 1 los estándares son relativamente nuevos y se encuentran en constante desarrollo para aumentar la velocidad de transmisión y el alcance. Se destaca que algunos de los estándares citados no son compatibles entre ellos como es el caso del estándar 802.11a el cual no puede trabajar con el estándar 802.11b esto depende mucho de la velocidad y los canales que poseen cada uno de los estándares. Es por eso que en la figura 12 se presentan los canales que se utilizan en la comunicación Wi-Fi que corresponden al estándar 802.11, el cual nos muestra la capacidad de los canales y su separación.

1.4.4.5. Por su tecnología de acceso

Las redes inalámbricas según la tecnología de acceso se pueden clasificar en cuanto a l uso de la frecuencia en el espectro como:

- GSM
- TDMA
- CDMA
- Wi-Fi
- Hiperlan2
- Bluetooth
- Infrarrojas

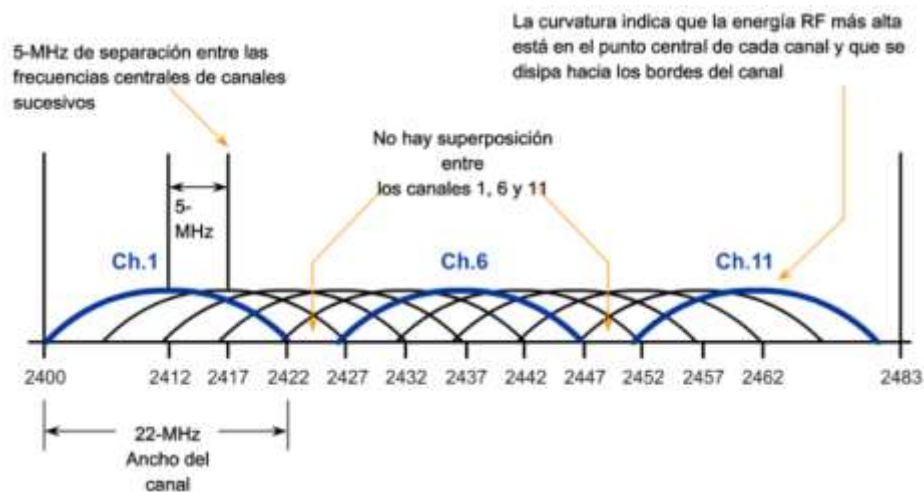


Figura 12. Canales de Frecuencia 2.4 GHz

Tomado de (House of Technology, 2011)

Mediante esta clasificación podemos apreciar el uso actual en la sociedad de las tecnologías inalámbricas.

1.4.4.6. Por su infraestructura inalámbrica

Se pueden clasificar en:

- Con Infraestructura
- AdHoc o MANET
- Mesh

1.4.4.6.1. Con Infraestructura

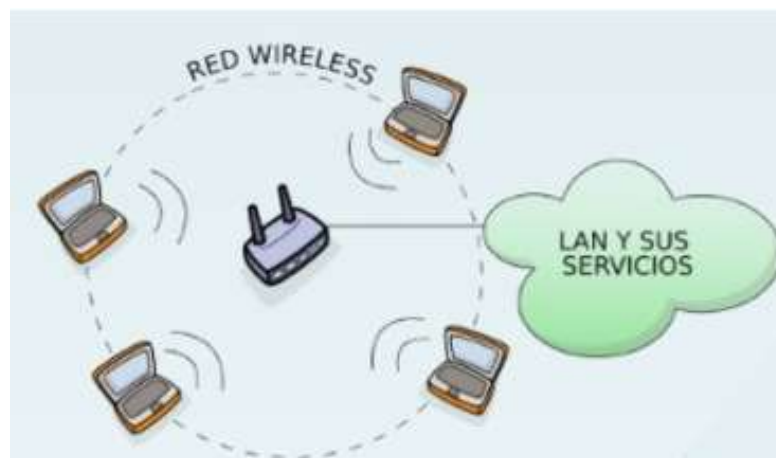


Figura 13. Red con Infraestructura

Tomado de (Dobald, 2009)

Como su nombre lo indica esta red necesita de 3 componentes esenciales para su funcionamiento, el elemento transmisor, el elemento receptor y un punto de acceso es el equipo intermedio que permite la comunicación a través de los equipos para poder realizar una comunicación o transferencia de archivos como podemos observar en la figura 2.

De esta manera no es necesario que los equipos se encuentren en un rango de alcance entre sí, mientras se encuentre conectados al mismo punto de acceso pueden establecer comunicación con todos los equipos que se encuentren en la red, a este medio se lo conoce como un sistema de red centralizado, ya que todo el tráfico debe pasar por el punto de acceso para de este, salir al receptor que se encuentra en el área de alcance. Por ejemplo, tenemos las redes WLAN, sistemas satelitales, etc.

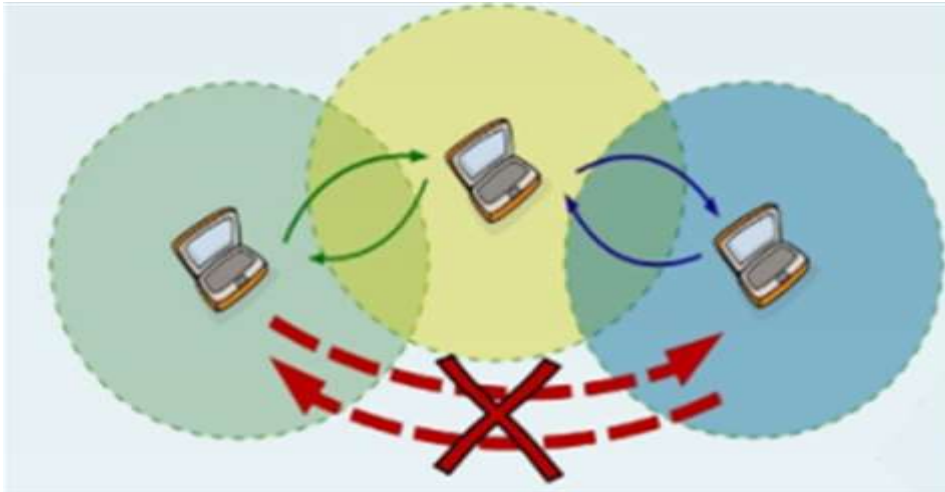


Figura 14. Redes Ad Hoc MANET

Tomado de (Dobald, 2009)

1.4.4.6.2. Redes AD-HOC o MANET

Las redes móviles *AdHoc* (Mobile Ad hoc Network - *MANET*) son aquellas que usan la propagación de mensajes o información mediante múltiples saltos. *AdHoc* hace referencia al hecho de que este tipo de redes no posee una infraestructura de comunicación única o predefinida. La comunicación de las redes *MANET* se da de una manera no planificada que responde a la distribución de los dispositivos o nodos que la conforman en un momento determinado. Estas redes no poseen elementos que realicen la gestión de las tareas de comunicación, el proceso de envío de mensajes o información es la prioridad y es la tarea distribuida entre todos los participantes de la red. Cada uno de los nodos o dispositivos que se encuentran dentro de la red son los que llevan a cabo todos los procesos relacionados con la comunicación. (Aguilera Irazabal, 2013, pp. 11-12)

Estas redes son de tipo temporales y auto-configurables basadas en múltiples saltos entre los dispositivos que la conforman; como son origen, destino o puente. Esto gracias a los nodos móviles o fijos como se aprecia en la figura 14, este tipo de red no depende de una infraestructura definida es decir como la red

por infraestructura como se aprecia en la figura 14, esta red es descentralizada, esto puede ser explicado ya que los múltiples dispositivos pueden comunicarse entre sí como una conexión punto a punto entre los dispositivos y reenviar los paquetes de datos de la fuente al destino utilizando los dispositivos intermedios como *routers*.

Las redes *AdHoc* se identifican por usar topologías dinámicas, cada nodo o dispositivo independiente, puede moverse libremente en tiempos impredecibles, esto limita a este tipo de redes ya que puede ocasionar congestión por su limitado ancho de banda en consecuencia a la capacidad variable de los enlaces inalámbricos. El encaminamiento puede utilizar un *flooding* (inundación de red) para lograr el reenvío de los datos hacia el destino. En cuanto más saltos se generan a través de los dispositivos, el tiempo de latencia crece y los datos se pueden corromper en cada dispositivo por el que se pasa hasta llegar al destino.

a) Características de las redes MANET

Entre las principales características de las redes MANET tenemos:

- **Operación distribuida:** Los nodos de las redes *MANET* no dependen de los nodos de una red estática o predefinida que le proporcione la funcionalidad de encaminamiento, esta se realiza de manera distribuida por cada uno de los nodos que integran esta red. (Aguilera Irazabal, 2013, pp. 12)
- **Topología dinámica:** Los nodos o dispositivos que integran la red *MANET* se conectan y desconectan aleatoriamente, también pueden cambiar su posición dentro de la red. Es por ello que los protocolos deben realizar las varias operaciones necesarias las cuales tiene como objetivo garantizar que la conectividad entre los nodos pueda ser mantenida mediante los protocolos que sean usados. (Aguilera Irazabal, 2013, pp. 12)
- **Variaciones en la capacidad de enlace:** Las variaciones de las redes *MANET* se producen por el uso del medio inalámbrico y los saltos a través de la malla pues los errores introducidos por los enlaces son muy

frecuentes. Los protocolos creados para las redes *MANET* deben ayudar a controlar y minimizar los errores que puedan aparecer dentro de ella. (Aguilera Irazabal, 2013, pp. 12)

- **Requisitos de baja energía:** Los dispositivos de las redes *MANET* por ser móviles usan baterías para su funcionamiento, lo cual también limita al uso de todos los recursos del dispositivo (CPU, periféricos, memoria, etc.). Es por esta razón que los protocolos de comunicación desarrollados para estas redes tienen diseños que reducen el consumo de energía y optimizan la energía que usan los dispositivos en la red. (Aguilera Irazabal, 2013, pp. 12)

b) Conceptos fundamentales

Para generar un orden en el uso de los elementos dentro de la red *MANET* que se exponen en este proyecto; ciertos términos usuales que conforman las redes Ad Hoc como se muestra en la figura 15, se describen a continuación:

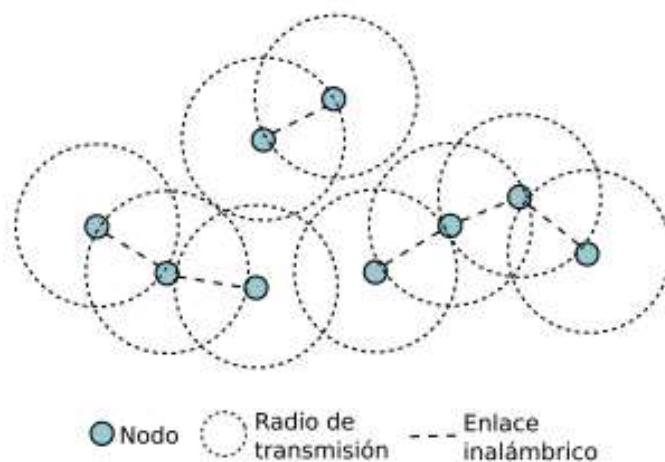


Figura 15. Red Ad Hoc *MANET* y sus elementos

Tomado de (Aguilera Irazabal, 2013)

- **Nodo:** Se denomina como nodo a cada uno de los dispositivos con capacidades de procesamiento que participan en una *MANET*. Estos dispositivos pueden tener características variadas, pero cada uno de ellos debe poseer la misma tecnología de comunicación inalámbrica

caso contrario no podrán comunicarse entre ellos ni tener acceso a la red.

- **Enlace:** La capacidad de intercomunicación entre dos o más nodos que se encuentran a una distancia que permita su comunicación, esto depende de las características de la tecnología inalámbrica utilizada por todos los nodos dentro de la red.
- **Vecino:** Se denomina con este término a aquellos nodos que se encuentran en rango de comunicación directa dentro de la red.
- **Distancia:** Esta se mide en saltos para las redes *AdHoc* y hace referencia al número de enlaces de comunicación que la información tiene que realizar para llegar a cierto nodo destino.
- **Mensaje:** Es el conjunto de información la cual se transmite entre los nodos por medio del enlace de comunicación. Este mensaje para las redes *MANET* está determinado de las características de la tecnología inalámbrica utilizada por la red y cada uno de los dispositivos.
- **Encaminamiento:** Se llama así al proceso en el que dos o más nodos de la red *AdHoc* para comunicarse entre ellos mediante el paso o salto entre uno o más mensajes a través de diferentes enlaces y nodos intermedios de la red. Las rutas o los caminos que pueden existir entre dos nodos forman enlaces consecutivos, pueden variar durante la movilidad y de la calidad del enlace de cada uno de ellos. (Aguilera Irazabal, 2013, pp. 13-14)

c) **Protocolos de enrutamiento en las redes Wireless ad-hoc**

Este tipo de redes donde no se encuentran dotadas de infraestructura definida, necesitan de algoritmos de enrutamiento adecuados en los que hay que tener en cuenta la característica dinámica de los nodos dentro de la red ya que cada nodo puede moverse modificando la topología de la red mallada. Por otro lado, cada uno de los nodos debe tener la capacidad de ser un *router*.

Los algoritmos de encaminamiento y direccionamiento existentes para las redes Wireless *AdHoc* pueden clasificarse en tres categorías: Proactivos, Reactivos e Híbridos, como viene representado en la figura 16:

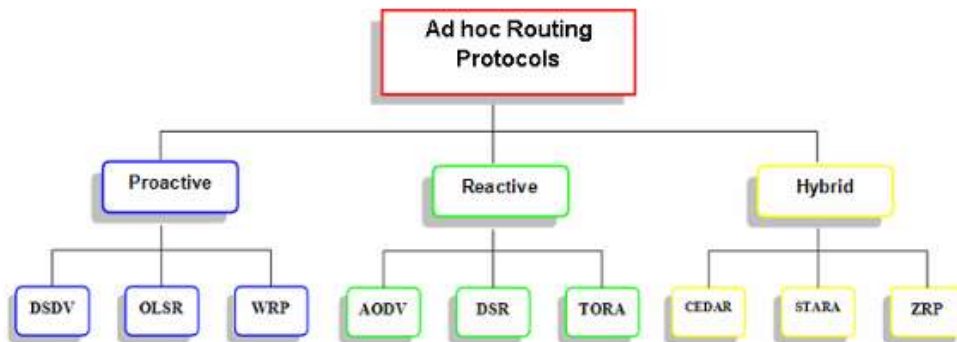


Figura 16. Clasificación de Protocolos Ad Hoc

Tomado de (Rocabado, 2013)

- **PROACTIVO:** Los protocolos de este tipo se mantienen constantemente actualizados, es decir la información de direccionamiento a través de intercambios de paquetes a intervalos temporales fijos se dan a conocer dentro de la red en todo momento, lo que permite tener un direccionamiento disponible a cada petición de enrutamiento para el encaminamiento de los paquetes, por otro lado se produce tráfico de señalización cuando se transmite así como también cuando no se transmite ningún paquete de datos y provoca sobrecarga en la red.
- **REACTIVO:** Los protocolos de este tipo invocan el procedimiento para determinar el correcto direccionamiento al momento y solo en el momento de transmitir el paquete o la información, lo que reduce el tráfico de señalización y aumenta los tiempos de entrega en los paquetes.
- **HIBRIDO:** Los protocolos de este tipo unen las ventajas de los protocolos reactivos y proactivos, limitando la aplicación de algoritmos proactivos sólo a los nodos adyacentes del que quiere transmitir dentro de la red.

A continuación, se exponen los algoritmos más utilizados en este tipo de redes:

- *AODV (Ad-hoc On-Demand Vector)*
- *DSDV (Destination Sequenced Distance Vector)*
- *DSR (Dynamic Source Routing)*
- *TORA (Temporally Ordered Routing Algorithm)*
- *OSLR (Optimized Link-State Routing Protocol)* (Rocabado, 2013, pp. 39-50)

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

Es un protocolo de enrutamiento de tipo reactivo el cual se basa en el algoritmo *Distance Vector*. Los nodos destino de una ruta, antes de proporcionar información de direccionamiento, crean un número de secuencia de destino (*destination sequence number*), lo que proporciona a los nodos un instrumento para evaluar cuanto se ha actualizado un determinado recorrido evitando la formación de lazos (*loop*) en el camino de enrutamiento. Un terminal que deba elegir entre varios caminos hacia un cierto destino, elegirá aquel caracterizado por el número de secuencia mayor, correspondiente a una información de *routing* más reciente. Además, el protocolo soporta el enrutamiento multidifusión (*multicast*). Mediante el protocolo UDP este protocolo usa mensajes particulares llamados *RREQ (Route Request)*, *RREP (Route Replies)* y *RERR (Route Errors)* que son enviados y recibidos para determinar los vecinos y establecer la confirmación de las rutas. (Rocabado, 2013, pp. 39-50)

- **Proceso de Encaminamiento**

Modo de selección de camino de un nodo hacia otro:

- 1) Se realiza el envío *broadcast* de un mensaje tipo *RREQ* figura 17.
- 2) Se atiende a una respuesta del destinatario o de otro nodo el cual posee un camino de enrutamiento bastante reciente hacia aquel destino. Esta respuesta llegará con un mensaje de tipo *RREP* figura 18, confirmando que el camino buscado está disponible. (Rocabado, 2013, pp. 39-50)

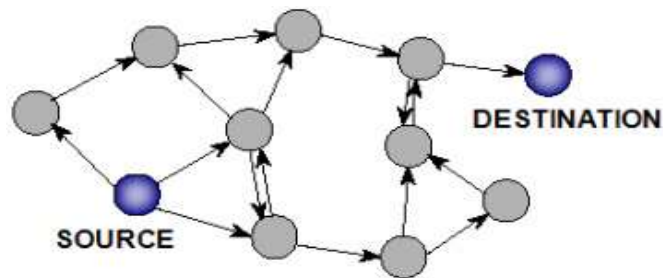


Figura 17. Transmisión Broadcast de RREQ

Tomado de (Rocabado, 2013)

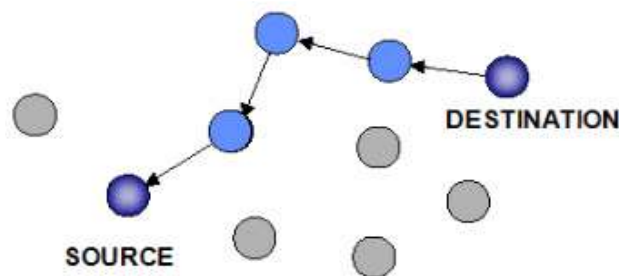


Figura 18. Transmisión Unicast de RREP

Tomado de (Rocabado, 2013)

Cada nodo que posea un camino de direccionamiento lo más reciente es aquel nodo que conozca una ruta asociada a un número de secuencia de destino que sea grande, al menos, como aquel contenido en el mensaje RREQ. Además, los nodos de la red que pertenecen o se incluyen en trayectos activos pueden transmitir periódicamente mensajes especiales de RREP, llamados mensajes "Hello", a sus nodos más cercanos. La falta de mensajes "Hello" de los nodos vecinos es interpretada como pérdida de la conexión con ese nodo, esto produce que el nodo que debería haber recibido tal mensaje proceda a corregir su tabla de enrutamiento, eliminando aquella ruta. Al llegar a la fase de extracción en donde se toma la tabla de enrutamiento de una puerta de acceso a un nodo vecino, debido a que este ya no es visto o alcanzado, el nodo envía un mensaje RERR a los nodos cercanos que usaban el trayecto, informando y actualizando el acontecimiento. Mientras todos los nodos permanezcan activos dentro de la red todo sucede sin dificultad en cuanto a que cada nodo conserva una lista de los nodos cercanos. El procedimiento del mensaje RERR viene repetido por los

nodos intermedios determinando así la actualización de las tablas de direccionamiento de todos los nodos de la red. (Rocabado, 2013, pp. 39-50)

- **DSDV (Destination Sequenced Distance Vector)**

El DSDV es un protocolo de direccionamiento de tipo proactivo que pertenece a la familia de los algoritmos *Distance Vector*. Cada nodo perteneciente a la red tiene una tabla de enrutamiento que indica para cada destino cuantos saltos (hop) hacen falta atravesar y cuál es el sucesivo. Derivando del *Distance Vector*, las actualizaciones de las tablas de enrutamiento se producen mediante el intercambio de información entre nodos cercanos y reaplicando los algoritmos de camino mínimo a menor costo. Cada ruta viene etiquetada con un número de secuencia (*sequence number*), que da una indicación temporal sobre la validez de la ruta, a aquellos números de secuencia con los valores altos son considerados como rutas más fiables. Cuando dos rutas tienen el mismo número de secuencia se elige a la que tiene el menor costo (por ejemplo, el que menor número de saltos tenga hasta llegar al destino). En caso de que un nodo registre que una ruta hacia un destino no se encuentra en funcionamiento, se asigna al número de salto un valor alto (que significa infinito) y al número de secuencia un número impar. Un número de secuencia identificado con un número impar indica que aquella ruta es inalcanzable mientras que si el número de secuencia es un número par indica que el destino sí es alcanzable. (Rocabado, 2013, pp. 39-50)

- **DSR (Dynamic Source Routing)**

Este protocolo es de tipo reactivo y se caracteriza por el uso del *Source Routing* y del mecanismo de tipo “*On-Demand*”. En el sistema el *source routing* hace que los nodos fuente conozcan “paso a paso” (*hop by hop*) el camino que deben efectuar para alcanzar al destinatario. Esto se logra gracias a una memoria de enrutamiento (*route cache*) que tiene la tarea de memorizar todos los caminos a realizar. El nodo transmisor que quiere enviar un paquete informativo empieza realizando un proceso de *Routing Discovery*. Este proceso consiste en el envío desde el nodo transmisor, de mensajes RREQ en *Flooding* sobre la red, mensajes que

todos los otros nodos receptores enviarán a su vez en *Flooding*. Mientras que en el nodo destinatario tienen en su propia memoria de enrutamiento, una ruta válida, se procede a responder al mensaje RREQ, transmitiendo al nodo solicitante un paquete RREP. Generalmente, el nodo receptor sigue un camino inverso respecto al del RREQ y almacenará toda la información de direccionamiento que se memorizará desde el nodo solicitante.

El paso final consiste en que, si la conexión se interrumpe, se notifican a todos los nodos mediante una serie de paquetes RERR de modo tal que todos los dispositivos se actualicen y almacenen en la memoria de direccionamiento toda la información actualizada y no usen más ese enlace para transmitir. El protocolo DSR hace un uso intenso de la memoria de direccionamiento y de la fuente de direccionamiento para evitar los lazos (*loop*). (Rocabado, 2013, pp. 39-50)

- **TORA (Temporally Ordered Routing Algorithm)**

El protocolo TORA, de tipo reactivo, se caracteriza por proporcionar anodo remitente, no sólo uno, sino múltiples trayectos para hacerle llegar al destino. El procedimiento es el siguiente: cada nodo realiza una copia de TORA para cada destino y el protocolo crea, mantiene y cancela los trayectos de enrutamiento. El TORA asocia un peso a cada nodo de la red respecto a un destino, y los mensajes se desplazan desde un nodo con mayor peso hacia uno con peso menor; mientras los caminos descubiertos con paquetes de tipo *QRY (Query)* vienen actualizados con aquellos de tipo *UPD (Update)*. Si un nodo necesita conocer un trayecto hacia un destino manda en difusión (broadcast) un paquete QRY que se propaga, hasta que no alcanza el nodo destinatario o a un nodo que posea un trayecto válido hacia el destino. El nodo que responda se servirá a su vez de un paquete UPD que agregará también su peso. Los paquetes UPD se enviarán en difusión de modo que permitan a todos los nodos intermedios modificar su peso convenientemente. Se deriva, por tanto, que los nodos que quieran alcanzar destinos lejanos o directamente inalcanzables aumentan su peso local hasta el máximo valor consentido,

mientras que el nodo que encuentre un nodo cercano con un peso que tienda a infinito, cambiará el trayecto. El paquete de tipo CLR (Clear) interviene en algunos casos para resetear todos los estados de direccionamiento de una porción de red cuando el destino sea completamente inalcanzable. El protocolo TORA se apoya en el protocolo para redes MANET llamado *IMEP (Internet MANET Encapsulation Protocol)* que proporciona un servicio de expedición fiable para protocolos de enrutamiento. La agregación en un único bloque de los mensajes IMEP y TORA reduce el *overhead* de la red y prueban el estado de los nodos vecinos. Para obtener tal agregación se utiliza periódicamente un intercambio de mensajes llamados *BEACON* y *HELLO*. (Rocabado, 2013, pp. 39-50)

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

OLSR es un protocolo de encaminamiento o direccionamiento de ruta proactivo específicamente diseñado para redes *Ad-Hoc* móviles (*MANETs*), el cual se basa en la definición y uso de estaciones dedicadas, llamadas *multipoint relays (MPRs)*. Los MPRs son los responsables de reenviar los paquetes de broadcast durante el proceso de *flooding*. Esta técnica permite reducir la sobrecarga de paquetes ya que en el que cada estación se retransmite el paquete, cuando recibe la primera copia suya. En relación a su contrario que es el algoritmo clásico del estado del enlace, OLSR apenas se distribuye información parcial del estado del enlace a la red MANET. OLSR tiene como un principio básico heredar su estabilidad de los algoritmos de estado del enlace. Puesto que es de naturaleza proactiva, este ofrece una ventaja de que las rutas disponibles pueden ser usadas inmediatamente. Los algoritmos de estado del enlace se declaran y luego se propagan a la lista de vecinos de cada uno de los nodos o de las estaciones en la red. Este protocolo pretende mejorar esta solución usando diferentes técnicas al reducir el tamaño de los paquetes de control que se intentan transmitir ya que éstos no son declarados a los nodos vecinos, sólo un pequeño grupo de ellos llamados *Multipoint Relay Selectors*. Una estación *Multipoint Relay* es la encargada de retransmitir

sus mensajes en modo de broadcast. El uso de MPRs sirve para minimizar la cantidad de las retransmisiones de mensajes de un evento de broadcast o de *flooding*. Los mensajes de control siempre son periódicos en la red, ya que este protocolo no genera tráfico de control adicional para responder a fallos o la presencia de nuevos nodos o estaciones. OSLR es capaz de mantener rutas hacia todos los destinos en la red, lo cual resulta muy útil cuando las situaciones en las que un gran número de estaciones de la MANET se están comunicando entre sí, especialmente cuando la fuente y el destino se encuentran en constante cambio; es por ello que se lo utiliza para redes con varios integrantes y llegan a tener una densidad amplia. Siendo un protocolo que opera en modo distribuido, las mejoras en las optimizaciones alcanzadas introduciendo *Multipoint Relays* generan importantes beneficios al no depender de una entidad central, la transmisión no es fiable de sus mensajes de control ya que cada estación envía periódicamente mensajes de control, es decir no tiene algún proceso que integre calidad de servicios o de corrección de errores siendo tolerante a pérdidas esporádicas de paquetes de control. OLSR también usa el reenvío de paquetes *per-node*, es decir que cada estación usa su información guardada más reciente para enrutar un paquete en la red. La capacidad para seguir a una estación y verificar la ruta para el destino puede ser ajustada al configurar el intervalo entre mensajes de control consecutivos. (Pastor, 2008, pp. 20-23)

Multipoint Relay se encarga de minimizar el *flooding* que se origina por tráfico de broadcast y trata de eliminar todas las transmisiones duplicadas de una misma región o área de enrutamiento. Cada estación de la red selecciona un subconjunto de estaciones de su entorno de vecinos para realizar el proceso de retransmitirles paquetes y estas estaciones siempre tendrán activo la retransmisión de paquetes ya que pertenecen a este subconjunto son los nodos *Multipoint Relays (MPRs)* mientras que los nodos vecinos que no se encuentran dentro de este subconjunto de MPRs del total de nodos de la red continúan con la recepción de paquetes, pero no serán retransmitidos en estos nodos. Se

mantendrá siempre una tabla con las estaciones que han sido seleccionadas como MPR. Cada estación selecciona su propio conjunto de MPRs entre sus vecinos con un criterio donde se aseguran y verifican que todas las estaciones que están a dos saltos de una estación dada pueden alcanzarse con un número mínimo de MPRs. La Figura 19 ilustra este concepto. (Pastor, 2008, pp. 20-23)

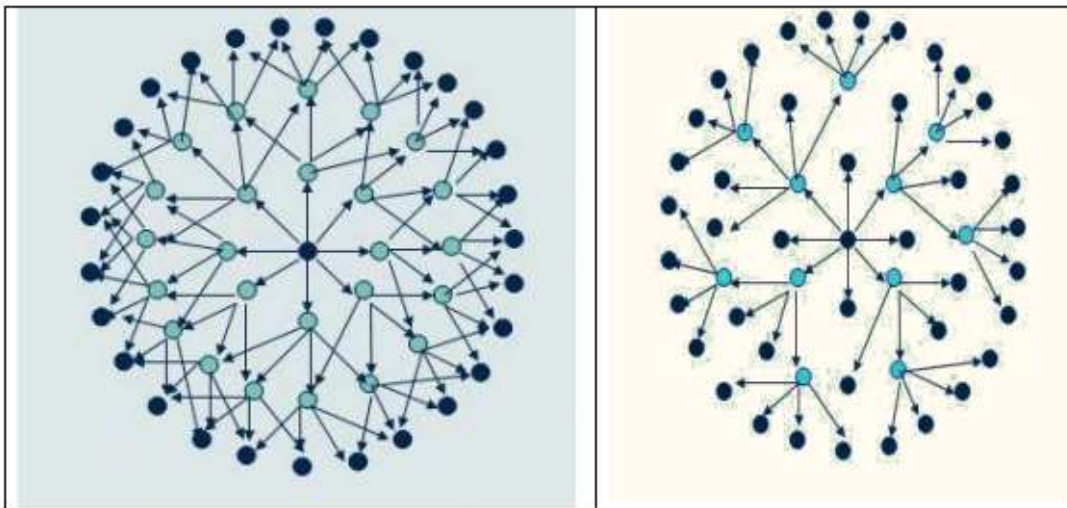


Figura 19. Multipoint Relay para N Estaciones

Tomado de (Hidalgo, 2008)

OLSR manifiesta la confianza en la selección de MPRs para calcular rutas a todos los destinos tomando estas rutas de las estaciones intermedias. Esta solución requiere que cada estación envíe por broadcast periódicamente su lista de estaciones vecinas elegidas como sus MPRs. Cuando se recibe esta información, cada vecino actualiza las rutas hacia sus estaciones conocidas en la red. (Pastor, 2008, pp. 20-23)

- **Búsqueda y Detección de nodos vecinos**

Cada nodo o estación procede a detectar las estaciones o nodos vecinos que tienen una comunicación bidireccional. Esto gracias a que cada estación emite periódicamente un mensaje de presencia por *broadcast*, el mensaje de HELLO el cual contiene información sobre sus todos los vecinos con el estado en el que se encuentran cada uno de ellos y del canal hacia ellos. Todos estos mensajes los reciben entre todas las

estaciones vecinas, pero no se retransmiten. Cada estación mantiene una tabla con una lista de todas las estaciones que se pueden reconocer de manera directa o indirectamente. Los enlaces a vecinos que están a un salto entre sí, se marcan como unidireccionales, bidireccionales o MPR, estas pueden ser las únicas tres marcas. Cada entrada de la tabla tiene un número de secuencia distinto que lo identifica a cada una y un valor de *timeout* asociados a cada ruta, por lo que las entradas obsoletas pueden eliminarse sin causar problemas a la red. (Pastor, 2008, pp. 20-23)

- **Selección Multipoint Relay**

Cada estación o nodo de la red escoge su grupo de MPRs. Para mantener una lista de vecinos constante los cuales están a dos saltos entre sí, tiene que analizar los mensajes *HELLO* recibidos y filtrar todos aquellos enlaces unidireccionales. El conjunto MPR sólo es modificado cuando se detectan dentro de la red cuando se produce un cambio en términos de los vecinos que se encuentran a un salto o a dos saltos (sólo conexiones bidireccionales). (Pastor, 2008, pp. 20-23)

- **Información de Broadcasting de grupos y MPR**

En cada una de las estaciones se debe enviar mensajes de control de topología (TC) para que entre todas las estaciones se mantengan sus bases de datos actualizadas. Estos mensajes son enviados mediante broadcast usando la técnica similar a la usada en los protocolos de enrutamiento de estado del enlace, la única diferencia es que emplea esta técnica para que el grupo de MPRs mejore la escalabilidad. Un mensaje TC se envía periódicamente a cada nodo u estación de la red de tal manera que declare su conjunto de selectores MPR. Esto quiere decir que el mensaje contiene toda una lista con los vecinos directos que lo han seleccionado como su MPR. La lista siempre tiene un número de secuencia asociado. (Pastor, 2008, pp. 20-23)

- **Cálculo de la Tabla de Encaminamiento**

Las estaciones se mantienen en una tabla de enrutamiento con información de cómo acceder a otras estaciones o nodos de la red. Cuando las estaciones reciben un mensaje TC se almacenan conjuntos de dos direcciones las cuales indican el último salto antes de alcanzar una estación destino, hasta la propia estación destino. Con esto es capaz de encontrar dentro de la red cual es el próximo salto para llegar a una estación destino. Se debe tener en cuenta el criterio de la llamada distancia mínima, de esta manera se restringe las opciones de búsqueda. Dichas entradas de la tabla de enrutamiento están compuestas de un destino, el siguiente salto y la distancia estimada a la estación destino. La tabla siempre debe ser actualizada y es llenada con la información de la red. (Pastor, 2008, pp. 20-23)

Ejemplo de aplicaciones

Por ser una red de fácil configuración y despliegue son muy utilizadas en cuanto a problemas en desastres naturales donde no existen centrales para la comunicación o en conflictos armados donde es necesario el envío de información rápida sin infraestructura determinada o preexistente.

- **Redes Militares**

En la figura 20 se expone un ejemplo de aplicaciones de las redes Ad Hoc para la comunicación en tácticas militares de ataque, reconocimiento de terreno o inspección de objetivos.

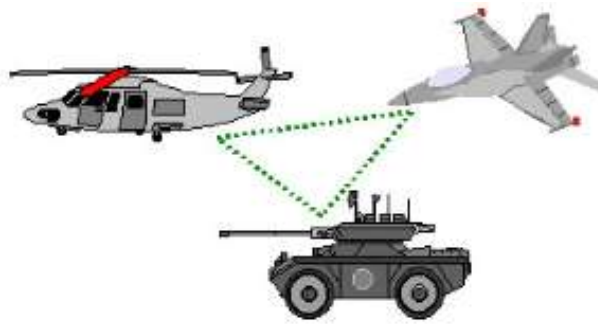


Figura 20. Ejemplo de Redes Ad Hoc en Tácticas Militares

Tomado de (Domingo, 2015)

- **Redes Desastres Naturales**

En la figura 21 se expone un ejemplo de aplicaciones de las redes Ad Hoc para la comunicación de equipos de rescate cuando se presentan catástrofes ya sean naturales o producidas por el hombre, con esta aplicación se logra un despliegue de recursos para la ayuda e intervención inmediata en ayuda a las víctimas.

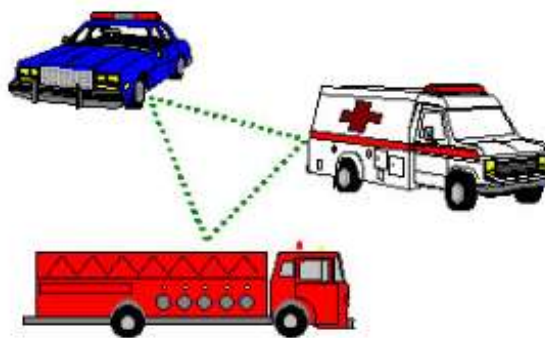


Figura 21. Ejemplos de Redes en Situaciones de catástrofes

Tomado de (Domingo, 2015)

Mecanismos de seguridad

Para dar seguridad a las redes *AdHoc* existen variadas propuestas de seguridad las cuales se centran en aspectos concretos del problema; de ellas se pueden identificar varios aspectos que deben ser cubiertos por las políticas de seguridad.

- La Criptografía (simétrica, asimétrica, de umbral).

- Autenticación de los nodos.
- Mecanismos de cooperación para detectar y reducir comportamientos egoístas en los nodos.
- Sistemas de gestión de claves.
- Seguridad física de los nodos.
- Seguridad de los protocolos de encaminamiento.
- Sistemas de detección de intrusiones (IDS).
- Sistemas de respuesta a intrusiones (IRS).
- Sistemas de tolerancia a intrusiones (ITS).
- Anonimato y privacidad. (Rocabado, 2013, pp. 18)

Atributos de la seguridad en redes móviles ad hoc:

- **Confidencialidad**

En las redes MANET se debe mantener el cifrado de los datos intercambiados para que se garantice que la información que sea enviada no pueda ser revelada o interceptada por usuarios intrusos. Estos intrusos o usuarios no autorizados no deben tener conocimiento de la existencia de los datos protegidos ni de su naturaleza de cifrado. Estas redes del tipo inalámbrico son las que utilizan el aire como medio o canal de transmisión lo que hace que todos los nodos que se encuentran dentro del rango de transmisión puedan obtener los datos los datos transmitidos si se unen a la red radiada y es por ello que se hace necesario prevenir que nodos intermedios y no confiables no logren tener acceso o puedan interpretar los mensajes o la información contenida en los paquetes que se están transmitiendo. (Rocabado, SEDICI Repositorio Institucional de la UNLP, 2013, pp. 16)

- **Autenticación**

En cuanto a la autenticación de los nodos, es importante mantener una confirmación de que las partes que se encuentran dentro de la red comunicándose entre sí sean genuinas y no imitaciones o intentos de conexión no deseados, por lo que es necesario que los nodos puedan demostrar su identidad. Sin el proceso de autenticación, un intruso

puede enmascarar un de los nodos de la red y tener acceso a información sensible y clasificada o bien podría interferir con el funcionamiento de la red. En las *MANETs* que son independientes ya que no tiene o constan de infraestructura es mucho más complicado autenticar una entidad y se hace necesario utilizar arquitecturas descentralizadas que se basan en otorgar un ID, un Web of Trust, etc.

Se pueden clasificar en cuatro tipos los procedimientos de autenticación:

- Por la entidad
 - Por la geolocalización
 - Por atributos
 - Por tipo de cifrado de datos (Rocabado, 2013, pp. 17)
-
- **Integridad**

Al hablar de integridad hace referencia a que los datos transmitidos entre los nodos de la red sean recibidos sin que puedan sufrir modificaciones o cambios por parte de terceros o ajenos a la red. Lo que se recibe debe ser lo que originalmente se ha enviado, puesto que los datos son enviados a través de medios inalámbricos también se ven afectados debido a razones no maliciosas como el ruido, las interferencias o atenuación de la señal o un ataque de terceros. (Rocabado, 2013, pp. 17)
 - **Disponibilidad y Supervivencia**

Cada una de las redes MANET es capaz de mantener accesibles cada uno de los servicios, aun cuando exista la presencia de fallos o incidentes maliciosos dentro de ella. La supervivencia indica la capacidad de las redes MANET para que se puedan normalizar los servicios luego de producirse un fallo o incidente. Por ello se puede destacar la resistencia de la red al repeler los ataques como son algunos mecanismos utilizados como son la autenticación de usuario, el uso de *firewalls* y criptografía de los datos, también el reconocimiento de intrusos mediante los IDs de

cada dispositivo o nodo SID y la recuperación de la red dentro de los límites de tiempo tolerable. (Rocabado, 2013, pp. 17-18)

Cuando se habla del anonimato se plantean los siguientes puntos a considerar para mantenerse privados y fuera del alcance de entidades no autorizadas.

Los tipos de anonimato se describen a continuación:

- **Privacidad de la identidad.** El proceso para transmitir información entre nodos hace que ningún nodo intermedio pueda obtener información acerca del origen y el destino por lo que solo los nodos de origen y de destino pueden identificarse entre sí. Para esto se utilizan identificadores de dispositivo (ID) o de red (Dirección MAC o IP), siempre se cuida que no sea posible establecer ninguna asociación entre el identificador de nodo o dispositivo y la identidad que se le asigna a cada uno de ellos.
- **Privacidad en la ruta de transmisión.** El predecir el camino o las rutas no está soportado o permitido a ninguno de los nodos intermedios entre el origen y el destino. Aquí también se destaca que ningún nodo móvil puede obtener ninguna pista o parámetro que ayude a rastrear al nodo de origen a partir del contenido de un paquete capturado.
- **Privacidad de la localización.** No está permitido que un nodo intermedio pueda obtener alguna información sobre la localización del nodo transmisor, ya sea en términos de distancia física a la que se encuentra como geolocalización o el número de saltos de la ruta origen-destino. Esta información únicamente es conocida por el nodo origen, sus vecinos inmediatos y el nodo destino. (Rocabado, 2013, pp. 18)

1.4.4.6.3. Redes MESH

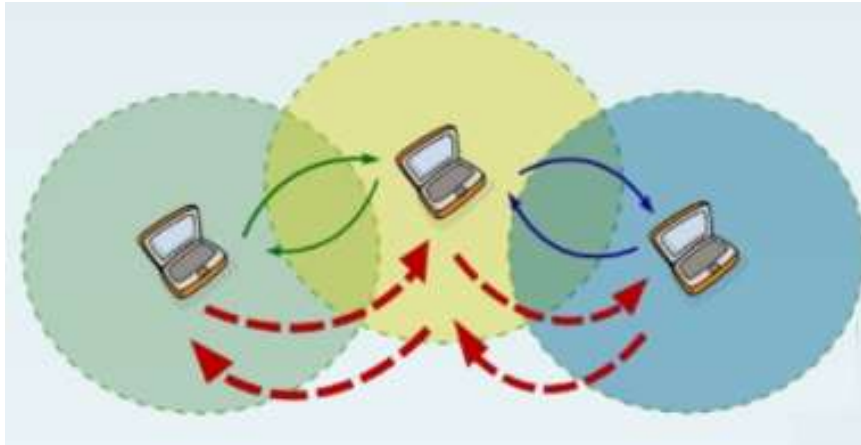


Figura 22. Red de MESH
Tomado de (Dobald, 2009)

Las redes del tipo *MESH* son de tipo malla que se derivan de la unión de las redes de infraestructura y las *AdHoc*, lo que da solución a la necesidad de redes en ambientes densamente poblados. Una gran ventaja de este tipo de redes es que al usar una potencia menor al momento de transmitir entre los nodos da cabida a mayores velocidades para la transmisión, también es mucho más práctico la distribución de acceso a internet entre los nodos de la red mallada como se muestra en la figura 22.

a) Elementos de enrutamiento MESH

- **Descubrimiento de nodos:** Identificar cada nodo en una topología que puede cambiar sobre debido a la movilidad de los dispositivos que la conforman.
- **Descubrimiento de la frontera:** Denotar los límites o bordes entre cada uno de los dispositivos de una red, por lo general son aquellos sitios donde se conecta a Internet.
- **Cálculo de rutas:** Identificar la mejor ruta o tramo, el cual se basa en algún criterio de la calidad entre los enlaces existentes dentro de la red.

- **Manejo de direcciones IP:** El control y la asignación de direcciones IP se manejan mediante la red troncal (*uplink,backhaul*), la cual realiza el manejo de conexiones a redes externas, como los enlaces a Internet. (Pérez y Granados, 2011, pp. 28)

b) Ventajas y desventajas de las redes MESH

Existen aún muchos pendientes para resolver dentro de las redes *Mesh*, en su mayoría están relacionados con las restricciones en cuanto a la velocidad de transmisión, la escalabilidad y las dificultades para garantizar calidad de servicio y la seguridad entre los enlaces. Es importante destacar que dependen de la calidad de la tecnología de los dispositivos y las diferentes frecuencias y potencias que pueden variar dependiendo de los países en cuanto al uso del espectro y distribución de frecuencias.

- **Ventajas**
 - **Menor coste:** cada uno de los nodos puede tener el papel de cliente, así como también de repetidor en la red, de esta manera se suple la necesidad de infraestructura centralizada.
 - **Robustez:** por ser una red mallada, si uno de los nodos pierde servicio, se reduce drásticamente la afectación al resto de la red, ya que existe redundancia los caminos a un nodo destino.
 - **Instalación:** No existe mayor complejidad en una red *Mesh* ya que al disponer de rutas dinámicas, solo es necesario encender el nodo para insertarlo a la red, cuando este nodo reciba la información y encuentre a un nodo vecino, estaría listo para entrar en servicio.
 - **Alimentación:** Los nodos de la red *Mesh* tienen estructuras y arquitecturas específicas que reducen el consumo de recursos de energía y ya que deben ser móviles poseen baterías.

- **Desventajas**

- **Latencia:** Si el salto entre las rutas para enviar mensajes consta de muchos saltos por la densidad de dispositivos dentro de la red esto origina que la latencia sea identificada ya que los saltos son traducidos como retardo.
- **Compartiendo el medio:** Este tipo de redes utiliza un limitado número de frecuencias donde funcionan las redes WLAN actuales, es por ello que existen interferencias entre usuarios que compartan una misma área de cobertura física y dependiendo de la potencia de la red interfiere o anula a las redes con menor potencia. La asignación automática de direccionamiento IP privadas por medio de DHCP (*Dynamic Host Configuration Protocol*) no representa problemas en las redes *Mesh* por lo que es posible la interacción con redes vecinas a cualquier momento y es por ello que se puede obtener problemas de direcciones duplicadas causando conflictos de red.
- **Seguridad:** Este tipo de redes necesitan hablar con sus clientes antes de que estos sean autenticados lo que constituye un gran problema para la seguridad ya que son muy vulnerables a los ataques y la captación de datos.
- **Rendimiento:** Todas las redes que utilizan multisalto son afectadas en cuanto al rendimiento (*throughput*) disminuye con el número de saltos que se utilice o se identifique para llegar al nodo destino. Para redes inalámbricas basadas en 802.11 los límites de rendimiento son determinados por el tipo de comunicación como *half duplex* de los radios. Mientras que las redes *Mesh* es posible aplicar otros estándares y se ha implementado exitosamente como por ejemplo en las redes inalámbricas Wi-Fi en equipos con estándares 802.11 con dos radios, en la banda de 2,4 y otro en banda de 5 GHz. Sin afectar o disminuir el rendimiento con el número de saltos puesto que el dispositivo puede recibir en una banda y transmitir en otra banda de manera simultánea. (Pérez, y Granados, 2011, pp. 29)

1.4.5. Sistemas mallados de primera, segunda y tercera generación

Los sistemas mallados por el desarrollo específico de tecnologías en diferentes campos y empresas han generado una clasificación de estas redes las cuales se exponen continuación. (Pérez & Granados, 2011, pp. 29)

a) Primera generación

La primera generación posee un sólo radio para hacer la interconexión entre nodos y dar servicio. Todos los datos son retransmitidos entre cada nodo *store-and-forward*, de tal manera que un nodo en inicio recibe los datos para luego retransmitirlos. Este sistema no es capaz de transmitir y recibir datos simultáneamente por un sólo canal de radio ya que esto provocaría interferencia, congestión y contención en cada uno de los nodos como se muestra en la figura 23. (Pérez & Granados, 2011, pp. 30)

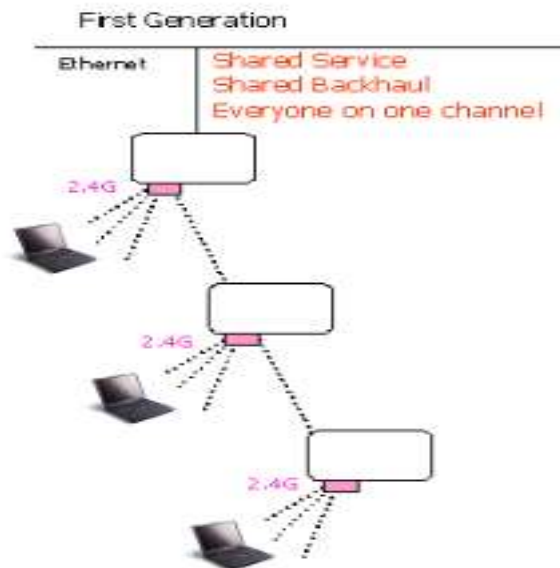


Figura 23. Red Mesh Primera Generación

Tomado de (Pérez & Granados, 2011)

b) Segunda generación

En la segunda generación se perciben grandes mejoras ya que se combina dos radios, uno para dar servicio con el estándar 802.11b/g y el otro para interconectar los nodos con el estándar 802.11a. De esta manera se logra eliminar la interferencia en los nodos al trabajar con diversas bandas de frecuencia (entre 2.4GHz y 5.8GHz) para dar servicio a los usuarios e interconectar nodos, pero al aumentar la demanda del servicio solicitada por el usuario se presentan contenciones y congestiones en la banda que se usa para la interconexión de los nodos como se muestra en la figura 24. (Pérez & Granados, 2011, pp. 31)

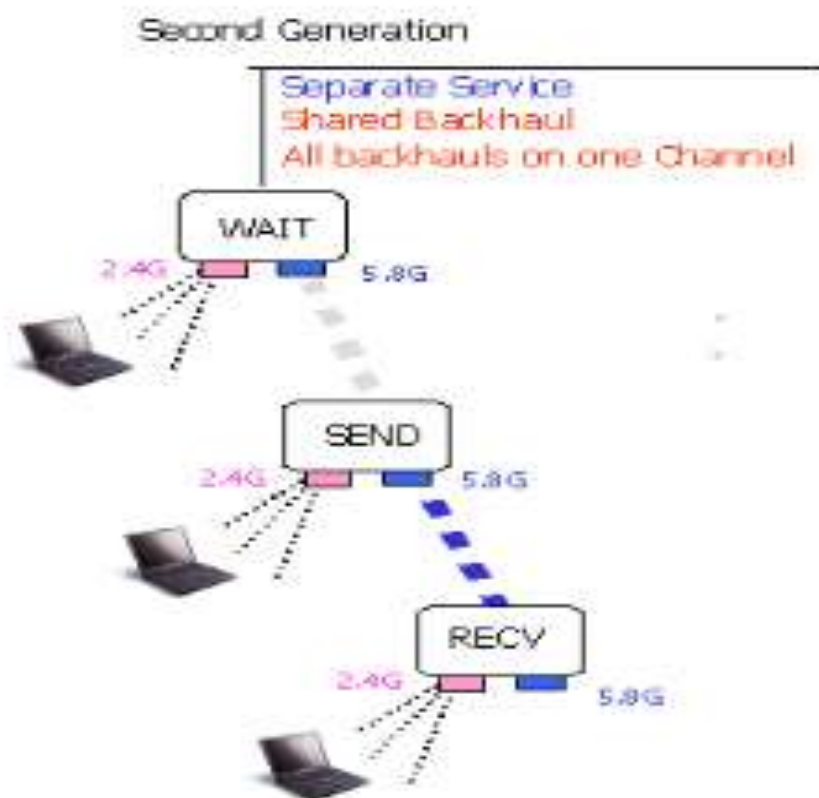


Figura 24. Redes Mesh Segunda Generación

Tomado de (Pérez & Granados, 2011)

c) Tercera generación

La tercera generación complementa los problemas en las generaciones anteriormente mencionadas ya que usan equipos inteligentes por utilizar una tecnología moderna. Cada uno de los nodos de la red puede enviar y recibir datos de sus nodos vecinos, así como también que los canales disponibles se pueden reutilizar, haciendo que el espectro disponible sea más amplio generando que el funcionamiento de la red aumente 50 o más veces su tamaño. El desarrollo de estos equipos se basa en el uso de multi-radios que soportan múltiples configuraciones de la red. Un radio de los equipos de tercera generación se usa para crear un enlace hacia su nodo *upstream* (nodo más cerca al *gateway*) y otro radio se utiliza para un enlace *downstream* al nodo vecino siguiente. (Pérez y Granados, 2011, pp. 32)

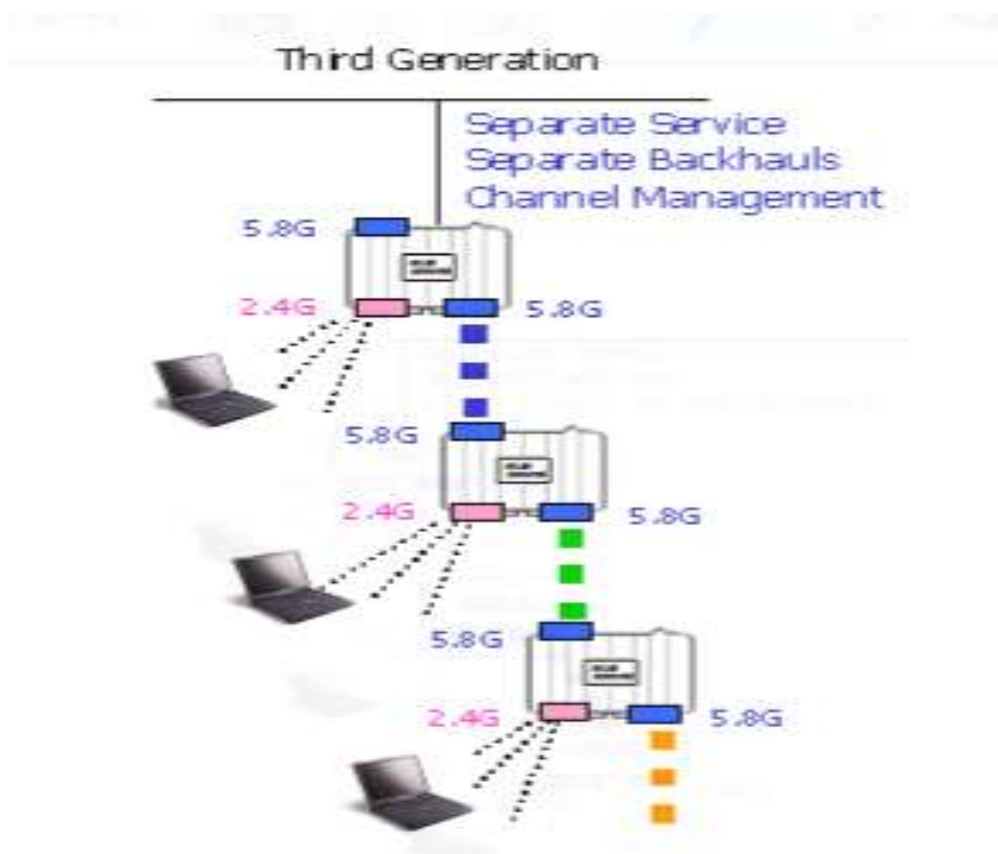


Figura 25. Redes Mesh Tercera Generación

Tomado de (Pérez & Granados, 2011)

1.4.6. Protocolos

- **MMRP (Mobile Mesh)**

Contiene tres protocolos independientes, cada uno de ellos dedicado a una función específica:

- Descubridor de enlace llamado Link Discovery
- Enrutamiento y verificación de enlace llamado Routing Link
- Identificador de Borde y túneles llamado Border Discovery Enables
(Pérez y Granados, 2011, pp. 33)

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

El protocolo OSLR diseñado para redes *AdHoc*, es un protocolo estable siendo la base de la mayoría de las redes *Mesh* en el continente europeo. Por ser un protocolo proactivo el cual envía de forma distribuida mensajes de “*Hello*” para dar a conocer a los nodos que se encuentran a su alcance dentro de la red y una vez conocidos los nodos se identifican las rutas para el envío mensajes de TC (*Topology Control*) a un subconjunto de estos nodos MPR para establecer conexiones.

- **OSPF (Open Shortest Path First)**

Este protocolo se aplica sobre la ruta más corta, fue desarrollado por un grupo trabajador de la IETF Interior llamado *Gateway Protocol* (IGP), y toma su base del algoritmo SPF:

- Envía llamadas, verifica el estado de los enlaces y se lo notifica a todos los enrutadores de la misma área de jerarquía.
- Funciona como un LSAs (Link – state advertsement) y avisa las interfaces presentes, informando el tipo de medición utilizada, así como otras variables.
- Los enrutadores son capaces de almacenar información para usar el algoritmo SPF y de esta manera calcular el camino más corto al destino.

- Compite con los protocolos RIP e IGRP, los cuales pertenecen a los protocolos de enrutamiento vectores de distancia.

OSPF envía todas las tablas de enrutamiento a todos los enrutadores o nodos vecinos para de esta manera se mantenga actualizada la información. (y Granados, 2011, pp. 34)

1.4.7. Métricas

Se denomina de esta manera al marcador que identifica la mejor ruta entre dos o más rutas distintas dentro de la red mallada para llegar al mismo destino. De esta manera es posible evaluar la mejor ruta basándose en uno o varios parámetros. Cada protocolo existente de enrutamiento utiliza su propia métrica. En general la métrica más usada ha es la del mínimo número de saltos hacia el nodo destino. Pero en el caso de las redes inalámbricas, la métrica también depende de la calidad del enlace y puede que la ruta con el camino más corto no sea la más adecuada. (Pérez y Granados, 2011, pp. 36)

a) Hop Counting (Conteo de saltos)

Los saltos son definidos como el paso entre dos nodos o dispositivos adyacentes. Ese tipo de métrica se basa en la distancia, por lo que mide por medio de los saltos la distancia existente entre el nodo origen y el nodo destino. Se escoge el camino más corto para llegar al destino lo que significa que se escoge el menos número de saltos para llegar al destino. Por la existencia de los saltos entre los nodos en las redes inalámbricas, la pérdida de los paquetes se presenta muy frecuente y en general puede ser muy variable, esto depende directamente de la potencia del enlace entre los nodos de la red. Es por ello que este tipo de métrica es el más adecuado para estas redes siempre y cuando no se tome en cuenta la calidad del enlace entre los nodos. (Pérez y Granados, 2011, pp. 36)

b) ETX (Expected Transimission Count)

Este tipo de métrica complementa los problemas del conteo de saltos ya que las redes en malla mediante el ETX (*Expected Transmisi3n Count*) el conteo de los errores de transmisi3n esperados se considera en el tramo entre los nodos. Esta t3cnica se aplica a los diferentes protocolos de enrutamiento existentes en las redes malladas ya que permite tomar en cuenta las caracter3sticas de transmisi3n de cada enlace que se expresan con un “peso” el cual es un identificador adicional, por lo que al encontrar un enlace con mayores p3rdidas se le asigna un peso con un valor mayor y de esta manera se utiliza para evaluar si la métrica de la trayectoria total es de calidad y 3ptima. El problema es que no toma en cuenta el ancho de banda de los enlaces que existen y pueden significar una mejor ruta.

El uso de este tipo tiene un gran impacto al momento de considerar tramos que incluyan diferentes pasarelas a Internet y que pueden variar considerablemente en ancho de banda por ejemplo cuando se tiene tramos que utilizan 802.11 b combinados con tramos que utilizan 802.11 a o g. (P3rez y Granados, 2011, pp. 36)

c) ETT (Expected Transimission Time)

Se trata de una métrica surgida a partir de la conocida ETT, como consecuencia de que 3sta no tiene en cuenta el ancho de banda de los enlaces entre nodos. (P3rez y Granados, 2011, pp. 36)

d) PDR

El PDR es un tipo de métrica que intenta maximizar el *path delivery ratio*, es decir el radio de entrega de enlace de la ruta. Para la obtenci3n de este parámetro es necesario que se realice una predicci3n del *Link Delivery Ratio (LDR)* a cada salto de la ruta. La principal caracter3stica de esta métrica es que se elige los caminos de mayor calidad para la comunicaci3n entre los nodos, lo que resulta con una mayor tasa de transmisi3n de entrega y un menor n3mero de cortes en

dichos enlaces respecto a la métrica por saltos. (Pérez y Granados, 2011, pp. 37)

1.5. Seguridad

Al mencionar seguridad, los inconvenientes de las redes inalámbricas a comparación de las redes cableadas son más vulnerables en cuanto a la seguridad y accesos a las mismas, es por ellos que este tema es importante de tratar en cuanto a las redes inalámbricas. La seguridad se manifiesta en diferentes puntos de las conexiones como son las claves de acceso, el cifrado del tráfico entre otras.

WEP es uno de los tipos de cifrado más básicos en cuanto a cifrado de datos existe. Este tipo de cifrado de dos tipos que son a 64 bits o 128 bits que es cadenas de 5 a 13 dígitos o cadenas de 10 a 26 dígitos alfanuméricos, esto se logra creando una clave del cifrado de los datos antes de que sea lanzado o transmitido al medio, mientras más extensa sea la clave colocada más fuerte es el cifrado, esto hace que si el dispositivo de destino no conoce la clave no pueda realizar el proceso inverso y ver la información recibida.

1.5.1. Tipos de Seguridad

los tipos de seguridad más usados hoy en día en las conexiones inalámbricas son:

- **WPA**

Es un modo en el cual se maneja con un cifrado dinámico de la clave, a diferencia de WEP donde la clave es estática, en WAP esta clave siempre está cambiando lo que dificulta el acceso o la irrupción de algún ataque, esto es posible gracias a que este tipo de seguridad inserta claves sin restringir la longitud de los dígitos

alfanuméricos, es recomendable la utilización de caracteres especiales, mayúsculas y minúsculas que dificulten la codificación de las claves.

- **WPA2**

Es la mejora en cuanto a WAP, este es el más usado y encontrado en la mayoría de dispositivos de acceso inalámbrico hoy en día. La diferencia con su antecesor es la complejidad en cuanto al cifrado, el mismo que fue evolucionado para su existencia y distribución. Es muy importante en el caso de resguardar nuestra información y el acceso a la red inalámbrica la posibilidad de combinar el cifrado más complejo con una aplicación que también incluya la seguridad por filtros MAC. En las redes WiFi se puede también tener seguridad mediante parámetros como el SSID que ese el identificador de red, donde en cada uno de los dispositivos colocamos este parámetro para conocer y detectar la red a la cual podemos acceder, esto también es regulado por un control de acceso en nuestro punto de acceso conocido como ACL.

1.6. Computadores de placa reducida

Son placas suficientemente potentes en las cuales se puede correr un sistema operativo, a pesar de tener características muy similares a un computador tradicional la relación costo beneficio es bastante significativo, fueron diseñadas con fines educativos y de investigación científica permitiendo de esta manera que muchos estudiantes y programadores con conocimientos básicos en electrónica puedan desarrollar varios proyectos. (González & Gordillo W., 2014)

1.6.1. Tipos de placas reducidas

Existen varios tipos de placas reducidas utilizadas en proyectos de electrónica, como se muestra en la tabla 2 en la cual se menciona algunos tipos de placas que pueden ser encontradas en el mercado, las mismas que difieren entre si ya sea por costos, características físicas de las mismas como capacidades de

almacenamiento, velocidades de procesamiento o tipos de conectividad que permiten cada una, depende mucho del tipo de proyecto que se pretende realizar para su correcta elección.

Tabla 2.

Cuadro Comparativo de Placas de Tamaño Reducido

MINI ORDENADORES	PROCESADOR	MEMORIA INTERNA	MEMORIA RAM	CONECTIVIDAD
Raspberry Pi 3	Quad-core ARM V8	8 GB	1 GB	USB, Bluetooth, Ethernet, WiFi
Jaguar One	Intel Atom Z3735G	16 GB	1 GB DDR3	USB 2.0, HDMI 1.4, Ethernet
Orange Pi	H3 Quad-core Cortex-A7	FT card máx. 64 GB	1 GB DDR3	USB 2.0, HDMI, Ethernet, WiFi
ODroid-C2	Quad-core Cortex A53	FT card máx. 64 GB	2 GB DDR3	USB 2.0, HDMI 2.0, Ethernet, Serial
Hummingboard	ARM A9 hasta Dual Core	8 GB	512 MB DDR3	USB 2.0, HDMI 2.0, Ethernet, Bluetooth
Beaglebone Black	ARM A8 1GHz (TI Sitara AM3358)	4 GB	512 MB DDR3	USB 2.0, HDMI 2.0, Ethernet
Cubieboard 5	ARM A7 8 núcleos	8 GB + SATA	2 GB DDR3	USB, HDMI, Display port, audio digital, WiFi, BT 4.2
PcDuino 4	ARM A7 4 núcleos (Allwinner H3)	8 GB	1 GB DDR3	USB 2.0, HDMI 2.0, Ethernet

Entre los distintos microcomputadores que se encuentran listados en la tabla 2, en cuanto al desarrollo del presente proyecto fue seleccionado el Raspberry Pi en su modelo 3, puesto que este dispositivo lidera la lista en referencia a sus cualidades como son su sistema operativo que permite una mayor compatibilidad con dispositivos por su interfaz basada en Linux.

Este dispositivo a diferencia de sus equivalentes en las diferentes marcas expuestas logra mantener un tamaño ideal con una serie de componentes de última tecnología que permiten entregar un mayor alcance para la conexión de los dispositivos entre sí; es por esto por lo que sus componentes al realizar una conexión inalámbrica superan a sus competidores por su antena que no limita su gran capacidad de cobertura.

La configuración de la red Manet se vuelve posible ya que la aplicación del protocolo escogido HSMM-Pi la cual permite crear la red y difundirla entre todos los dispositivos se basa en una instancia de Raspbian con una aplicación WEB que indica y monitorea la calidad del enlace entre los dispositivos, utilizando OSLR para verificar el salto más corto entre los nodos para llegar a su destino a través de la red Mesh.

Es por esta razón que este dispositivo es más comercial y económico al momento de seleccionar una placa de procesamiento para el desarrollo de aplicaciones, a diferencia de las otras placas el Raspberry Pi cuenta con una gran variedad de drivers, librerías y aplicativos desarrollados gratuitamente para el público en general, lo que permite la fácil configuración y utilización de este dispositivo; es decir existen más desarrollo de herramientas de software y hardware para este dispositivo que para el resto de placas.

1.6.2. Raspberry PI

El Raspberry Pi es una computadora de tamaño reducido a la que se puede conectar un monitor, un mouse y un teclado, capaz de ser utilizado en proyectos de electrónica y para muchas cosas más como las puede realizar un ordenador o PC de escritorio, ejemplos de esto son la capacidad de poder realizar cálculos, procesamiento de textos, navegación por internet y juegos.

También al poseer un puerto HDMI puede reproducir video de alta definición.

1.6.2.1. Modelos

Los modelos de la Raspberry Pi que se encuentran actualmente disponibles en el mercado son:

- **Raspberry Pi 3 Modelo B**

La Raspberry Pi 3 modelo B lanzada en febrero de 2016, utiliza un CPU ARM Cortex-A53 de cuatro núcleos de 64 bits, tiene 1 GB de RAM, 802.11n LAN inalámbrica integrada y Bluetooth 4.1.

- **Raspberry Pi 2 Modelo B**

El modelo de la Raspberry Pi 2 comparte muchas especificaciones con su antecesora la Raspberry Pi 1 B+, pero utiliza un procesador *quad-core* ARM Cortex-A7 de 900 MHz y tiene 1 GB de RAM.

- **Raspberry Pi Zero**

El Pi Zero tiene la mitad del tamaño de una Raspberry modelo A+, con un CPU de un solo núcleo de 1Ghz y 512MB de RAM, puertos mini-HDMI y USB.

- **Raspberry Pi 1 Modelo B+**

La Raspberry modelo B+ cumple con las siguientes características 512MB de RAM, cuatro puertos USB, 40 pines GPIO y un puerto Ethernet, en febrero de 2015 fue reemplazado por el Raspberry Pi 2 modelo B.

- **Raspberry Pi 1 Modelo A+**

El modelo de la Raspberry Pi A+ es una de las placas de bajo costo, tiene 512MB de RAM a partir de agosto de 2016 (modelos anteriores tenían 256MB), un puerto USB, 40 pines GPIO y ningún puerto Ethernet. (Raspberrypi, 2017)

1.7. Sistemas operativos

Es complicado el precisar con exactitud el significado de un sistema operativo, pues parte de este problema es que los sistemas operativos logran desempeñar

básicamente funciones independientes, como lo son extender la máquina o administrar recursos.

El sistema operativo tiene como finalidad administrar todos los elementos de un sistema complejo y de esta forma permitir que el usuario final pueda interactuar con una interfaz gráfica.

1.7.1. Tipos de SO para Raspberry PI

Entre los sistemas operativos que pueden correr si ningún problema sobre una Raspberry PI se puede mencionar los siguientes:

- Raspbian
- Windows 10 IoT
- NOOBS

1.7.1.1. Raspbian

Es el sistema operativo oficial de la fundación Raspberry, este sistema operativo viene preinstalado con una variedad de software enfocado a la educación, programación y para uso general, contiene Python, Scratch, Sonic Pi, Java, Mathematica y más.

1.7.1.2. Windows 10 IoT

Es una versión de Windows 10 creada para dispositivos más pequeños que pueden o no disponer pantalla, puede ser ejecutado en dispositivos ARM como en dispositivos X86 y X64, Windows 10 IoT utiliza la extensa plataforma universal de Windows para poder crear grandes soluciones.

1.7.1.3. NOOBS

Es un instalador de sistema operativo fácil que contiene Raspbian, muy útil para que los principiantes puedan empezar a trabajar con las placas Raspberry,

adicional a esto también permite la opción de seleccionar sistemas operativos alternos que pueden ser descargados de internet e instalarlos. (Raspberrypi, 2017)

1.8. Sistemas Aéreos no Tripulados

Existe en la actualidad una gran variedad de aeronaves con un determinado grado de autonomía, dichos sistemas fueron denominados como ROA (*Remotely Piloted Aircraft*) o UA (*Unmanned Aircraft o Uninhabited Aircraft*), actualmente se utilizan términos como UAV (*Unmanned Aerial Vehicle*) o UAS (*Unmanned Aircraft System*), todas las denominaciones anteriores hacen referencia a la falta de tripulación en la aeronave para que este pueda operar, lo que es sinónimo de autonomía.

El cambio de vehículo a sistema trata no solo de una aeronave instrumentada de forma adecuada, sino también de una estación terrena con la cual se complementa el sistema para su operatividad. (Barrientos, y otros, 2007)

1.8.1. Tipos

Se puede establecer un tipo de clasificación de los UAV como pueden ser aquellos de despegue vertical de las que no son, encontrando dentro de las de despegue vertical las de ala rotativa o hélice como son los helicópteros y *quad-rotors*, los de ala flexible como parapentes y alas delta, por otro lado, los auto-sustentados como dirigibles y globos. Dentro de los UAV de despegue no vertical podemos encontrar los de ala fija como aeroplanos, la figura 26 muestra lo anteriormente descrito. (Barrientos, y otros, 2007)

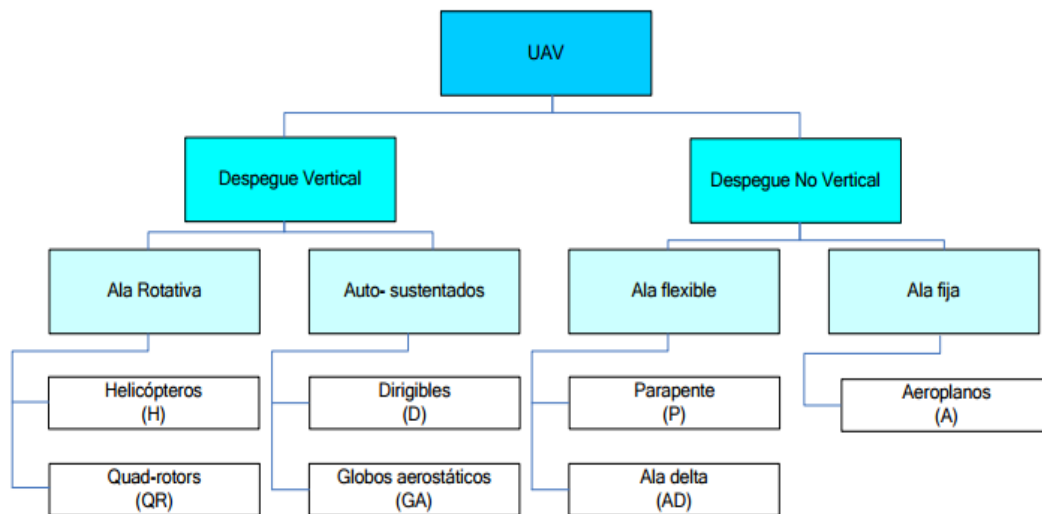


Figura 26. Tipos de Aeronaves no Tripuladas

Tomado de (Barrientos, 2007)

1.8.1.1. Aplicaciones

Inicialmente los drones fueron implementados para uso militar, el uso de estas aeronaves no tripuladas en el ámbito civil va tomando fuerza siendo, permitiendo así explotar varios campos como por ejemplo helicópteros con telecontrol para tareas de fumigación, a diferencia de un helicóptero convencional elimina riesgos del piloto, permite tener vuelos a baja velocidad y menor altura, incluso en tema de costos es mucho más favorable.

Aplicación	Ejemplo	Tipo de aeronave más frecuente
Inspección de infraestructuras	Líneas eléctricas Oleoductos y Gaseoductos	H
Inspección de obra civil	Puentes, viaductos, presas	
Vigilancia de Fronteras	Inmigración ilegal Contrabando	H,A
Supervisión de Tráfico		H
Patrulla marítima	Inmigración ilegal Contrabando	A
Filmografía	Cine Reportaje fotográfico	H,A
Reconocimiento y toma de datos en desastres naturales	Huracanes Riadas Volcanes	H,A
Levantamiento de mapas	Topografía	A
Climatología	Toma de muestras y monitorización de partículas en Aerosol Monitorización de contaminación atmosférica	H,A,D
Agricultura	Aplicación de fumigantes Análisis del estrés hídrico Agricultura de precisión	H
Intervención en desastres no naturales	Radioactivos Vertidos contaminantes (Petróleo) Incendios forestales	H,A
Enlace de comunicaciones		A,H
Localización de recursos naturales	Pesca Minería	A,H
Transporte de paquetería		A
Búsqueda y rescate	Nafragios Accidentes en montaña o zonas de difícil acceso	H

Figura 27. Aplicaciones de UAV

Tomado de (Barrientos, 2007)

Otro gran uso de estos helicópteros y que está tomando mucha fuerza es la filmografía, en este caso esta aeronave se encuentra dotado de un equipo necesario para poder capturar y transmitir imágenes o videos a una estación base ubicada en tierra, estos sistemas permiten abordar tareas como inspección, vigilancia, rodajes cinematográficos o conciertos.

Como se muestra en la figura 27 en la cual se puede encontrar una lista no exclusiva de varias aplicaciones civiles de los UAV.

2. CAPITULO III. PROPUESTA DISEÑO DE HARDWARE

2.1. Introducción

De acuerdo con el alcance del proyecto propuesto, la solución a plantearse consiste en un sistema de comunicación acoplado en drones utilizando dispositivos Raspberry PI en el que se especifican de antemano algunos de sus componentes, y los demás son seleccionados durante el desarrollo, considerando criterios técnicos y económicos:

En este capítulo se describe todos los elementos y hardware que han sido seleccionados para realizar el sistema de comunicación entre tres nodos móviles (*Drones*) que tienen implementadas las placas Raspberry PI y una estación base que está compuesta por una PC portátil, como se puede ver en la figura 28.



Figura 28. Diagrama Físico de Red (Nodos y Estación Base)

El funcionamiento básicamente consiste en la transmisión de video desde los nodos móviles (*Drones*) hacia la estación base antes citados, depende de la ubicación geográfica que cada nodo tome para poder describir el escenario de

transmisión en el que se encuentren, esto será desarrollado más adelante en el capítulo cuatro, correspondiente a pruebas y análisis de resultados, pero en si lo que se busca es implementar un protocolo de transmisión con el cual se pueda establecer comunicación de una manera rápida entre los nodos, para de esta manera en el momento que un nodo decida transmitir video a la estación base y este a su vez se encuentre completamente alejado de la misma, pueda detectar el camino más óptimo a atravesar la información que se trasmite por los nodos vecinos hasta que pueda llegar a su destino.

Existe una gran variedad de posibilidades donde puede ser aplicado este sistema, dependiendo del interés de cada usuario, entre los existentes se pueden mencionar los siguientes:

- **Ingreso a lugares de difícil acceso:** Esto es factible debido a que la comunicación que se establece entre los nodos es de manera inalámbrica y al encontrarse las placas Raspberry acopladas a drones permite hacer uso del espacio aéreo en el cual no existe obstáculos como en un espacio terrestre, ejemplos de esto pueden ser: captura de video en incendios forestales, manifestaciones públicas entre otros.
- **Lugares de entretenimiento público:** En este caso se puede realizar la cobertura de eventos públicos como: partidos de futbol, conciertos, obras de teatro entre otros, pues muchas veces para cubrir un espectáculo publico la infraestructura necesaria para la misma consiste de equipos muy grandes y los lugares donde se localizan muchas veces se encuentran copados por los asistentes.

Como se puede ver en los ejemplos citados se menciona mucho el tema público, esto debido a que el espacio aéreo no puede ser violado, por ejemplo, no se puede hacer uso de estas herramientas para realizar la transmisión de video dentro del espacio de una vivienda, ya que es privada y por ende el acceso es restringido, a no ser que se cuente con un permiso del propietario.

2.2. Equipos y Materiales

Todos los equipos y materiales utilizados en el desarrollo de este proyecto van a ser detallados a continuación.

2.2.1. Raspberry PI3

Como podemos observar en la figura 29, la placa Raspberry PI3 es la tercera generación de la Raspberry PI, este módulo reemplazó a la Raspberry Pi2 modelo B en febrero del 2016, en comparación con esta Raspberry, se presenta las siguientes características.

RASPERRY PI 3	
CPU	A 1.2 GHz 64-bit ARMv8 quad-core
RAM	1 GB
STORAGE	Micro SD card slot
PORTS	4 USB, HDMI, Ethernet
GPIO	40 PINES
WIRELESS	802.11n, Bluetooth 4.1
INTERFACES	Cámara, Display

Figura 29. Características Placa Raspberry Pi

Tomado de (Raspberrypi, 2017)

Se decidió trabajar con esta placa debido a las facilidades por el tipo de tecnología que brinda, pues ya cuenta con una antena para Wi-Fi incorporada como se puede ver en la figura 30, lo que significa un ahorro económico, ya que no es necesario adquirir la misma por separado, por otra parte el espacio físico que

ocupa una antena externa es mayor a la ya incorporada, facilidad a la hora de adquirir en el mercado tecnológico en comparación a sus similares con un costo de \$60,00 dólares americanos el *starter kit*.

Adicional a las características descritas para esta placa Raspberry, en el primer capítulo se detallan las características de sus similares en otras marcas, incluso entre las placas existentes de la misma marca, con lo cual se puede notar porque se escogió esta placa para el proyecto.

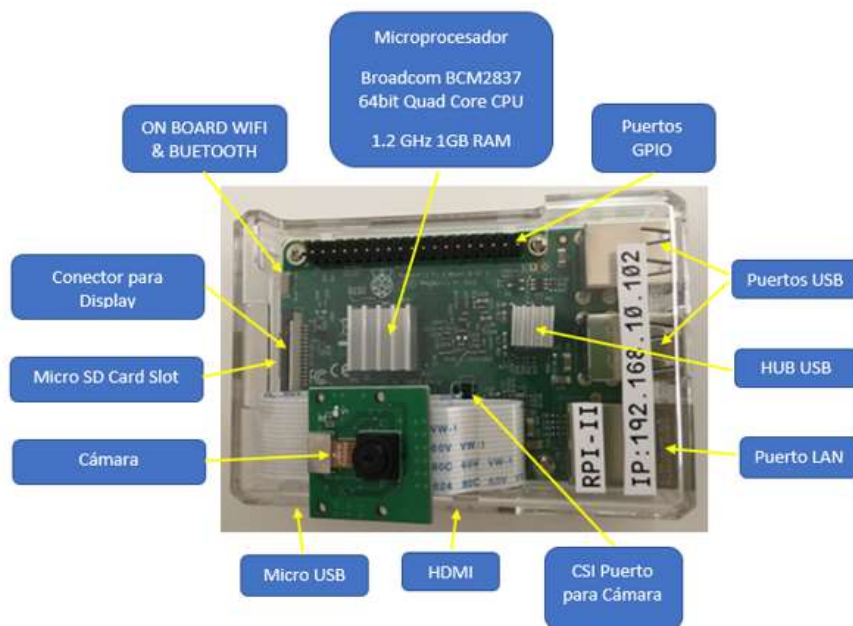


Figura 30. Diagrama de componentes Raspberry Pi 3 modelo B

Entre los componentes señalados en la figura 30, durante el desarrollo del capítulo 2 se realiza un análisis más profundo de los principales componentes.

2.2.2. Antena WIFI RPI3

Las placas Raspberry PI 3 tienen incorporado el chip de banda ancha BCM43438, el cual proporciona redes inalámbricas 802.11n de 2.4GHz, *Bluetooth Low Energy* y *Bluetooth 4.1 Classic*, la incorporación del chip se da con el fin de mantener los costos bajos, al ser una antena incorporada en la placa

se puede ver en la figura 31 el tamaño reducido que tiene la misma. Sus radios están conectados a esta antena chip soldada directamente a la placa, con el fin de mantener el tamaño del dispositivo a un mínimo. A pesar de su reducida estatura, esta antena debe ser capaz de captar las señales inalámbricas LAN y Bluetooth incluso a través de las paredes.



Figura 31. Características de Antena WiFi Raspberry Pi

Tomado de (The Magpi Magazine, 2016)

2.2.3. Cámara RPI3

La cámara utilizada es la Pi camera P5V04C de Raspberry versión 1.3, la cual posee una cinta de cables de 15 pines que es conectada directamente al conector CSI de la placa Raspberry PI3, puede entregar una imagen con una resolución de 5MP cristalina o 1080p de grabación de vídeo HD a 30fps., cuenta con un sensor *Omnivision 5647* de 5MP (2592 × 1944 píxeles) en un módulo de enfoque fijo, la cámara se conecta al slot dedicado de 15 polos MIPI camera serial interface (CSI), que fue diseñado especialmente para la interfaz de las

cámaras. El bus CSI tiene la capacidad de transmitir velocidades de datos extremadamente altas y lleva exclusivamente datos de píxeles al procesador BCM2835.

Las dimensiones de la placa base de la cámara son 25 mm x 20 mm x 9 mm, y pesa un poco más de 3 gr. En términos de imágenes fijas, la cámara es capaz de generar imágenes fijas de 2592 x 1944 píxeles y soporta 1080p @ 30fps, 720p @ 60fps y 640x480p 60/90 grabación de vídeo. El costo de esta mini cámara bordea los \$15,00 dólares americanos.

Se seleccionó esta cámara debido a su compatibilidad con la última versión de *Raspbian*, al ser la prioridad de este proyecto la transmisión de video, las características de esta cámara especialmente desarrollada para la placa Raspberry Pi, la convierte en una herramienta capaz de captar video para ser transmitido mediante la red a través de los nodos que la componen. Al ser una cámara desarrollada especialmente para esta placa, contiene ya un bus de datos con los pines para el slot de la placa a diferencia del resto de cámaras que necesitan ser adaptadas para que se puedan conectar a la placa esto depende del tamaño de la ranura del socket en la placa, así como también la compatibilidad en cuanto a la tecnología y características de la cámara ya que esta placa por su procesamiento no permite un tipo de cámara con características mayores a los 12 Megapíxeles. La capacidad de la cámara es transmitir utilizando el ancho de banda que se genera en la red creada entre los dispositivos por lo que para no saturar el canal se usa 1 Megapíxel, es por ello que el sistema operativo que se está usando en la elaboración de este proyecto permite de manera fluida mediante sus librerías y drivers el uso de este dispositivo, así como al ser una cámara desarrollada para este tipo de placas, las características de la cámara que se utiliza en el proyecto esta detallada en la siguiente figura 32.

PI Camera P5V04C	
	
COMPATIBILIDAD	Raspberry Modelo A y B
MODULO	5MP Omnivisión 5647
IMAGEN	2592 x 1944
VIDEO	1080p @ 30fps 720p @ 60fps 640 x 480p 60/90
TAMAÑO	20 x 25 x 9 mm
PESO	3 gr.

Figura 32. Características de Pi Cámara P5V04C

Tomado de (Pi Supply, 2017)

2.2.4. Memoria micro SD

Las placas Raspberry PI están aptas para trabajar con cualquier tarjeta SD mientras esta sea compatible, pero debe cumplir con algunas directrices. Entre los detalles de las características de Raspberry, básicamente se recomienda que para la instalación de Sistema Operativo Raspbian es necesario 4GB, mientras que es un dispositivo que almacena información se recomienda obtener un adicional de mínimo 2GB ya que dependiendo de la configuración de la placa esta es capaz de almacenar datos como por ejemplo el almacenamiento de video, audio e imágenes dentro de la memoria. Es por ello que en el Kit de compra de Raspberry se encuentra recomendado e incluido una tarjeta Micro SD de mínimo 8GB.

La capacidad de la tarjeta mínima requerida para la instalación de NOOBS es de 8 GB, para la instalación de imágenes se recomienda como mínimo 4 GB.

2.2.4.1. Clase de Tarjeta SD

La clase de la tarjeta determina la velocidad de escritura que es soportada para cada una así podemos mencionar las siguientes:

- Clase 4 capaz de escribir a 4 MBps
- Clase 10 capaz de escribir a 10 MBps

Mientras mayor es la clase no quiere decir que es superior al resto de tarjetas SD, puesto que a menudo las velocidades de escritura se logran a costa de la velocidad de lectura y el aumento en los tiempos de búsqueda, la tarjeta con la que se va a trabajar es una clase 8 se utiliza esta tarjeta ya que al momento de la adquisición de la placa esta vino en el paquete y al ser suficiente por su capacidad para el proyecto, no se realizó cambio alguno, los costos en el mercado varían dependiendo la capacidad, se pueden encontrar tarjetas de 8GB que bordean los \$ 9,50 dólares americanos.

Entre sus características se puede destacar la existencia de dos tamaños físicos de las tarjetas SD, los modelos de Raspberry Pi A y B requieren tarjetas SD de tamaño completo, mientras que los modelos de Raspberry Pi A+, 2B, zero y 3B requieren tarjetas micro SD, las características de la micro SD que se utiliza en este proyecto esta descrito en la siguiente figura 33. (RASPBerry PI FOUNDATION, 2017)

ADAPTADOR y MICRO CD	
	
CAPACIDAD	8 GB
CLASE	8
VELOCIDAD DE ESCRITURA	8 MBps

Figura 33. Características de Micro SD

Tomado de (Raspberrypi, 2017)

2.2.5. Dron ARRIS

Arris M700 entre sus características se destaca la funcionalidad fácil de plegar, tan solo necesita dos pasos para doblar un brazo, entre los diseños de las partes centrales, la placa central adopta el diseño de gran tamaño, proporcionando suficientes espacios para adaptar todo tipo de equipos electrónicos. Adicional a esto se suma el diseño de amortiguación de la tarjeta del controlador de vuelo, es muy importante pues la vibración tiene influencia en el controlador de vuelo normal por lo que puede resultar en un vuelo inestable, en la figura 34 se puede ver el diseño que tienen los drones a utilizar. (Hobbie-Wing, 2017)

Se decidió trabajar con este modelo debido a que para fines prácticos se cuenta con dos drones pertenecientes a la universidad de las Américas y son prácticas pues entre sus características cuenta con la capacidad de carga suficiente para elevar el prototipo. El valor comercial aproximado del mismo es de \$700.00 dólares americanos.



Figura 34. Características del DRON

Tomado de (HobbieWing, s.f.)

2.2.6. Estación Base

La estación base en el proyecto consta de una portátil en la cual se realizan las configuraciones necesarias para poder conectar la estación base a la red *Manet* "Raspberry-UDLA", también se crea una carpeta que va a contener los archivos correspondientes a *Netcat* y *Mplayer*, los cuales serán descritos en el siguiente capítulo correspondiente a software.

Las características de la estación base se puede ver descritas en la siguiente figura 35, en la cual se encuentran las características principales con las que debe cumplir el equipo, las partes que no se mencionan como por ejemplo capacidad de disco duro no es importante pues no es necesario mayor capacidad, más que la básica requerida para la instalación del sistema operativo.



Figura 35 Características de Estación Base

2.2.7. Fuentes de Energía

Las placas Raspberry tienen su propia fuente de alimentación para su funcionamiento, en este proyecto no se hace uso de la fuente de energía del *Drone*, puesto que la carga que la misma recepta es la necesaria para mantener al dron durante 15 minutos en vuelo.

Para mantener con energía durante el vuelo a las placas Raspberry se realizó la adquisición de bancos de poder los cuales suministran la energía necesaria a las placas según las características descritas en la figura 36. El costo de estos bancos de prueba bordea el \$20.00 dólares americanos.

En cuanto al consumo energético de la placa se obtiene los siguientes rangos:

- En reposo: 230 mA -> 1.2 W
- A pleno rendimiento: 350 mA -> 1.8 W

Es por ello que al seleccionar un banco de energía para esta placa fue necesario escoger en los estándares de consumo masivo que permitan el uso extendido de los dispositivos más de 5 horas para realizar pruebas de captación de video,

conexión inalámbrica mediante WiFi a la red, transmisión de contenido y datos. Es por ello que el banco seleccionado tiene las características seleccionadas para suplir la demanda de energía que requieren las placas para funcionar sin problema durante 5 horas continuas.

BANCOS DE PODER	
PESO	0.63 gr.
ESPEJOR	0.5 pulgadas
TAMAÑO	6.1 X 3.1 pulgadas
PUERTO CARGA	5v - 1A
2 PUERTOS USB	5v - 2A
CAPACIDAD	12000 mAh

Figura 36. Características de los Bancos de Poder

Tomado de (Dulla, 2017)

3. CAPITULO IV. PROPUESTA DISEÑO DE SOFTWARE Y CONFIGURACIÓN

3.1. Introducción

En este capítulo se describe una propuesta de diseño y configuración de un sistema de comunicación acoplado en drones utilizando dispositivos Raspberry PI, para lo cual se hace una caracterización de todas las aplicaciones de software que son seleccionadas y se usan para conseguir la transmisión de video desde la red MANET hacia la estación base, describiendo el funcionamiento de cada una de ellas enfocado en la implementación del mismo. Además, presenta una breve descripción de su configuración.

En la figura 37, se describe la red MANET que componen la Red RASPBerry-UDLA diseñada para este proyecto.

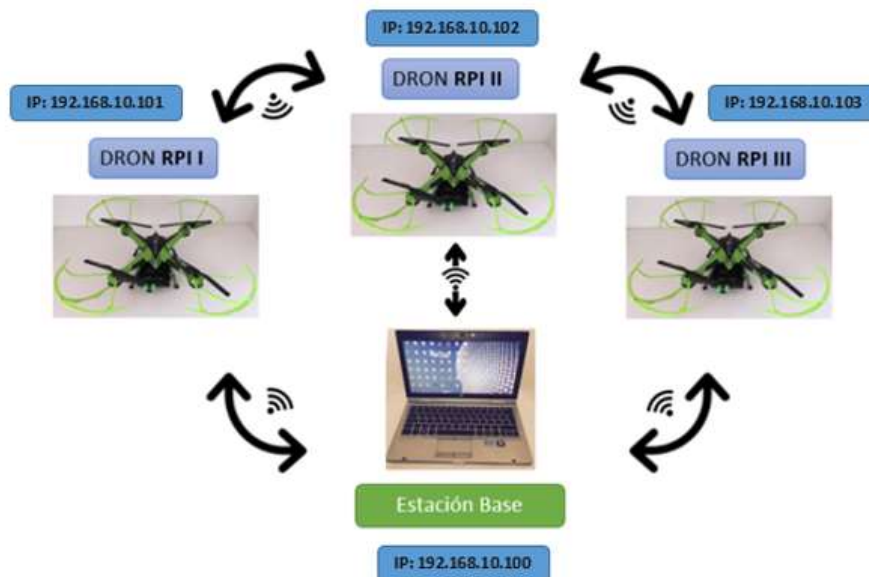


Figura 37. Diagrama de Red AdHoc - MANET RASPBerry-UDLA

Para el desarrollo del capítulo se dividirá el trabajo en tres componentes:

- Red MANET
- Estación Base
- Servicios de video

3.2. RED MANET

En esta sección se va a tratar todos los temas referentes a la conformación de la red MANET como son direccionamiento IP de todos los dispositivos que intervienen en la misma, protocolo de enrutamiento implementado, configuración de cada nodo (placa Raspberry).

3.2.1. Direccionamiento IP y Puertos

En la tabla 3 se citan las direcciones IP que fueron configuradas en cada uno de los dispositivos para el funcionamiento dentro de la red MANET "RASPBerry-

UDLA” y el puerto utilizado tanto para la transmisión y la recepción de los datos de video de cada nodo implementado, el puerto puede ser distinto en cada *Dron*, depende del escenario en que se encuentre cada nodo.

Tabla 3.

Tabla de Direccionamiento IP y Puertos en cada nodo.

Dispositivo	Nombre Del Dispositivo	Dirección IP del Dispositivo	Puerto Tx / Rx de Dispositivo
Raspberry Pi 3	RPI-I	192.168.10.101	5001
Raspberry Pi 3	RPI-II	192.168.10.102	5001
Raspberry Pi 3	RPI-III	192.168.10.103	5001

3.2.2. Raspberry PI3

Según lo propuesto en el proyecto, los dispositivos Raspberry PI son quienes conforman la red MANET, cumplen la función de nodos intermediarios para que la señal de información viaje desde un origen hacia su destino en el caso de requerir enrutamiento, para esto es necesario realizar la configuración de los mismos, se inicia cargando el sistema operativo.

El sistema operativo a utilizar es *Rasbian Jessy Whith Pixel*, entre la gran variedad de sistemas operativos compatibles con la placa que existen.

A continuación, se describen algunas características referentes al sistema operativo seleccionado y la instalación respectiva del mismo en la placa Raspberry.

3.2.2.1. Rasbian Jessy With Pixel

Para el sistema operativo de la placa de alto procesamiento Raspberry se eligen entre las diferentes distribuciones Linux, las cuales son compatibles con Raspberry y su arquitectura ARM, de estas versiones, la versión propia desarrollada por Raspberry se la conoce como *Raspbian*, esta es la más óptima en cuanto al desarrollo del proyecto, ya que es la más completa en cuanto a las librerías y componentes necesarios para a configuración e implementación de nuestra red inalámbrica conjuntamente el manejo de todos los componentes de la placa. La configuración para uso de la cámara y la ejecución de la aplicación HSMM-PI son parámetros que nos guiaron la elección de *Raspbian Jessy with Pixel 4.4* que es la última versión del sistema operativo desarrollada para el dispositivo saliendo en mayo del año 2017; esta nos permite la creación y despliegue de la red MANET con los nodos integrantes de la misma puesto que la aplicación HSMM-PI solo se encuentra probada en *Raspbian* y *NOBOS*. La fácil activación y configuración de la cámara que viene desarrollada para el bus de conexión de la placa Raspberry Pi 3 constituye un desempeño eficiente del componente al momento de la transmisión de video por medio del uso de la librería *raspivid* que se encuentra precargada en el sistema operativo *Raspbian*.

La base de *Raspbian* utiliza sistema operativo Debian por lo que su uso integra varias características de funcionamiento para aprovechar al máximo el uso de la placa y todos sus componentes. *Raspbian Jessy* al ser el sistema operativo robusto y el oficial para este mini-computador en este nuevo año 2017 lanzo la última versión llamada *RASPIAN JESSY WITH PIXEL (Pi Improved Xwindows Environment Lightweight)*, que es la nueva versión del sistema operativo de Raspberry y trae consigo mejoras al entorno grafico del sistema operativo de la placa donde se aprecian cambios en cuanto a la interacción grafica con el usuario volviéndola más atractiva y de fácil operación, esta puede ser descargada de la página oficial de la organización Raspberry, y se encuentra como en la figura 38 la versión de este sistema operativo es la última lanzada en abril del 2017 en su versión 4.4.

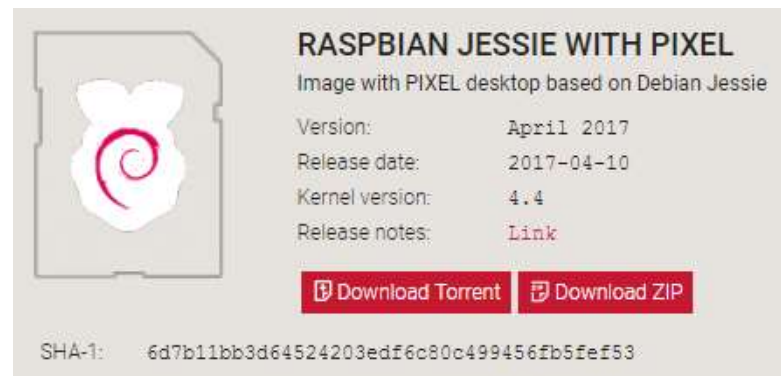


Figura 38. Imagen de Raspbian Jessie With Pixel

Tomado de (Raspberrypi, 2017)

3.2.2.2. Pantalla de presentación

En esta nueva versión tenemos una pantalla de bienvenida al inicio del sistema como se puede ver en la figura 39.

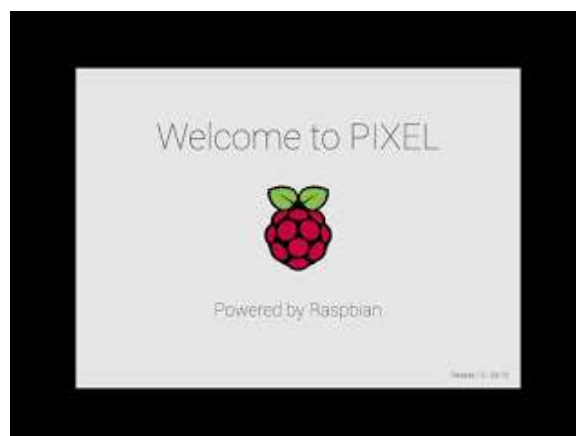


Figura 39. Pantalla de inicio de Raspbian

En el Anexo 01 se encuentran descritas algunas de las funcionalidades que se puede utilizar por medio de la interfaz gráfica de Raspbian.

3.2.2.3. Instalación de Raspbian en las placas Raspberry Pi 3

Para la instalación del sistema operativo es necesario descargar la versión de la página oficial de Raspberry en el siguiente link:

<https://www.raspberrypi.org/downloads/raspbian/>

En esta dirección podemos encontrar los dos tipos que se encuentran disponibles para descargar que son la versión completa y la versión ligera.

- Una vez descargado el instalador del sistema operativo, es necesario conectar al dispositivo los siguientes equipos que son necesarios para visualizar y ejecutar la instalación:
 - Teclado
 - Mouse
 - Pantalla
 - Tarjeta Micro SD
 - Batería
- Con estos dispositivos es posible iniciar con la instalación, el instalador debe ser copiado en la tarjeta de memoria a manera de imagen *bootable*, para esto existen una variedad de programas que ayudan a realizar esta operación como Win32 Disk Imager, Iso manager, etc., esto es necesario ya que, al encender el dispositivo, es decir al ser conectado a la batería por medio del cable de alimentación, este empezará automáticamente la instalación de *Raspbian* como se muestra en la figura 40.

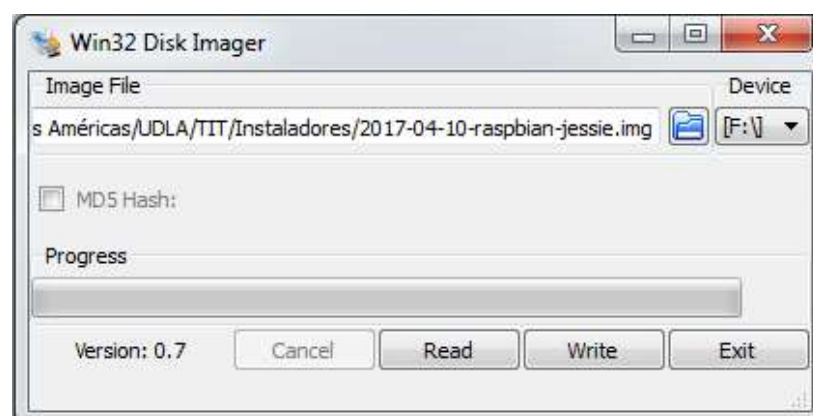


Figura 40. Imagen Booteable en Tarjeta SD

- Una vez que termina esta operación es necesario verificar que el dispositivo se encuentre funcionando, por lo que con la ayuda de los periféricos podemos navegar en el escritorio del Raspbian, y a la vez también es necesario verificar si la conexión Wi-Fi está en funcionamiento al conectar el dispositivo a una red disponible en la lista como se muestra en la figura 41.



Figura 41. Configuración de adaptadores cableados e inalámbricos

- Es posible realizar la adición de una IP estática al dispositivo mediante la ventana de configuraciones de red como lo muestra la figura 41, y de esta manera es posible ingresar mediante conexión SSH utilizando cualquier programa que permita abrir esta conexión como por ejemplo *Putty* a través de la IP colocada, al abrir esta terminal se puede acceder mediante el usuario y clave por defecto de *Raspbian*, este usuario con atributos de administrador nos permite realizar cambios de la configuración del dispositivo como el nombre del equipo, cambio o creación de usuarios y contraseñas.
- El siguiente paso es realizar la expansión de la tarjeta de memoria que se está utilizando, esto se debe a que al instalar el sistema operativo utiliza la cantidad básica necesaria del espacio total, es decir utiliza una

partición del total de la tarjeta de memoria, es por ello que para poder aprovechar al máximo de la tarjeta de memoria que está en la ranura del Raspberry y poder hacer completo uso del espacio para descargar archivos, guardar imágenes, videos, etc. El procedimiento para realizar esta operación es abrir la terminal de Raspberry, dando un clic en el icono de terminal en la barra superior del escritorio como lo muestra la figura 42.

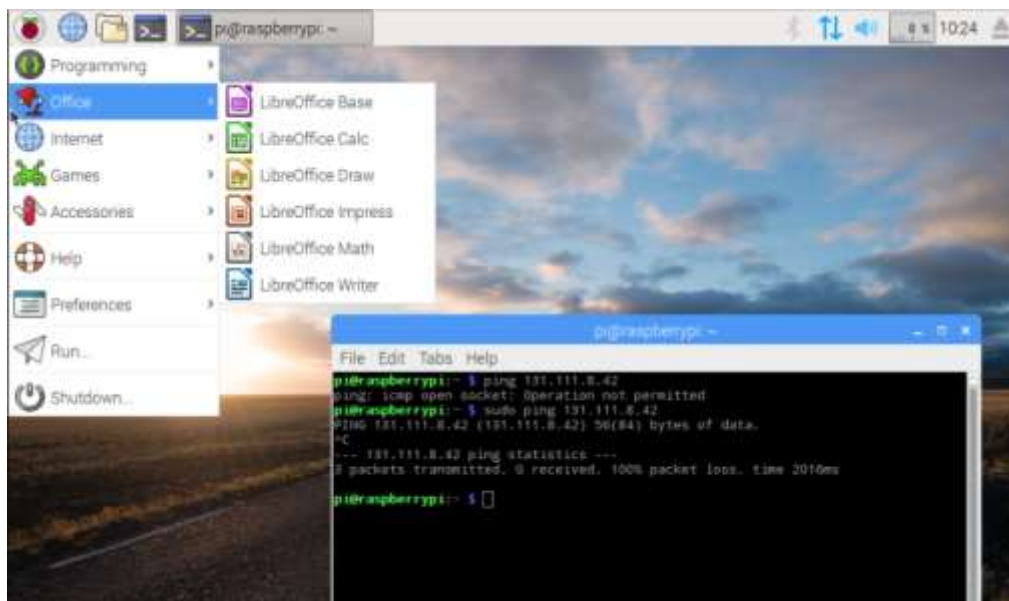


Figura 42. Terminal Raspberry

- Una vez abierto la ventana de la terminal, se escribe el comando: *sudo raspi-config*, este comando abre el programa de configuración de Raspberry donde se encuentran varias opciones referentes a la configuración del dispositivo, se debe seleccionar la opción *Advance Options* con un *enter* mediante el teclado, se coloca *select* para aceptar esta opción como se muestra en la figura 43.



Figura 46. Menú de Configuración del Raspberry Pi

Al entrar a la opción de configuración se despliega una ventana donde se encuentra la gran variedad de parámetros del Raspberry donde se selecciona la opción de ENABLE CAMERA como se muestra en la figura 47, para luego de aceptar la habilitación de la cámara, se cierra la ventana y se recomienda realizar un reinicio del sistema para aplicar la configuración realizada, de igual manera podemos activar SSH desde esta misma ventana.

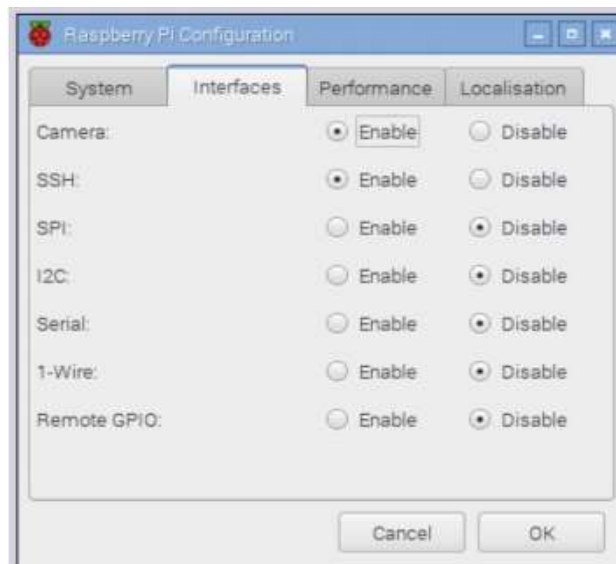


Figura 47. Habilitación de la cámara en Raspberry Pi

3.2.3.1. Pruebas de funcionamiento de la cámara en Raspberry Pi

De esta manera la cámara que se ha colocado en la ranura de la placa se activa para ser utilizada por el usuario, para su uso existen dos aplicativos que me permiten explotar los recursos de la cámara que son mediante la terminal del Raspberry usando comandos de Linux y el programa Python. En este caso mediante la ventana del terminal del equipo, se realizan pruebas de funcionamiento mediante los comandos:

- a) `raspistill -v -o test.jpg`
- b) `raspivid -o pruebavideo.h264 -t 10000`
- c) `MP4Box -fps 30 -add nombre_del_video.h264 mvideo.mp4`

Con estos comandos podemos lograr capturar una imagen de muestra que será mostrada momentáneamente en la pantalla del escritorio del dispositivo, también es posible la captura de video que de igual manera será mostrado momentáneamente en la pantalla del escritorio del Raspberry y finalmente el tercer comando nos permite guardar un archivo codificado con el códec h264 en nuestro equipo para que se pueda reproducir mediante un reproductor compatible con este formato.

3.2.4. Aplicacion HSMM-PI en la configuracion de red manet

En esta sección del proyecto se procede a describir la aplicación HSMM-PI y el protocolo que utiliza, las características necesarias con las que deben cumplir las placas Raspberry para que pueda correr la aplicación en cada una, también se indicará los pasos a seguir para la configuración.

3.2.4.1. Definición

Se puede definir al HSMM-PI como una herramienta que contiene varios aplicativos los cuales permiten la configuración del dispositivo Raspberry Pi en

maña dentro de una red inalámbrica como un nodo multimedia de alta velocidad para el uso de banda ancha BBHN y AREDN. El HSMM-Pi hace posible el uso de este dispositivo para radioaficionados ya que el uso no requiere la adquisición de una licencia para el uso de frecuencias dentro de las redes inalámbricas del estándar 802.11 b/g, de esta manera la herramienta que fue desarrollada específicamente para esta placa Raspberry entrega al usuario una interfaz para la implementación de esta característica que es la más importante para el desarrollo de este proyecto, ya que sin él no es posible establecer la red inalámbrica MESH entre los nodos y la estación base para la transmisión de video probando el enrutamiento que permita dar saltos entre los nodos entregando la posibilidad de visualizar video en tiempo real.

El HSMM-PI utiliza una aplicación web que puede ser habilitada y desplegada al colocar la IP del nodo en el browser, de esta manera se despliega la aplicación web PHP, la cual permite la configuración y supervisión de los parámetros necesarios para el modo de maña en la red MESH.

El uso de esta aplicación es el más adecuado para este proyecto puesto que permite realizar mediante saltos la conectividad de cada uno de sus nodos, de esta manera es posible transmitir video desde el nodo más lejano respecto a la estación base; esto es posible gracias al protocolo OSLR el cual es usado por la aplicación HSMM-PI. Este protocolo permite a cada uno de los nodos conocer a sus vecinos dentro de la red *AdHoc* MANET, a la cual se encuentran enlazados sin que estos nodos se encuentren sobre el área de cobertura de la Estación Base, es decir estos pueden estar dispersos en un área extendida, mientras cada uno se pueda conectar de manera de red estos pueden transmitir desde cualquier dispositivo dentro de la maña de la red como lo muestra la figura 48. Esto permite extender el área de cobertura para la red y se comprueba con el envío de video desde el último nodo hacia la estación base. Por ser una red que transmite datos es afectada por la distancia entre los nodos, las interferencias de otras redes presentes, el canal utilizado para realizar la comunicación, elementos físicos que se interponen entre los nodos, la velocidad del viento, los fenómenos

naturales y físicos del ambiente donde se realiza la comunicación, las vibraciones, el ruido electromagnético, etc., un sinnúmero de afectaciones al momento de transmitir video.

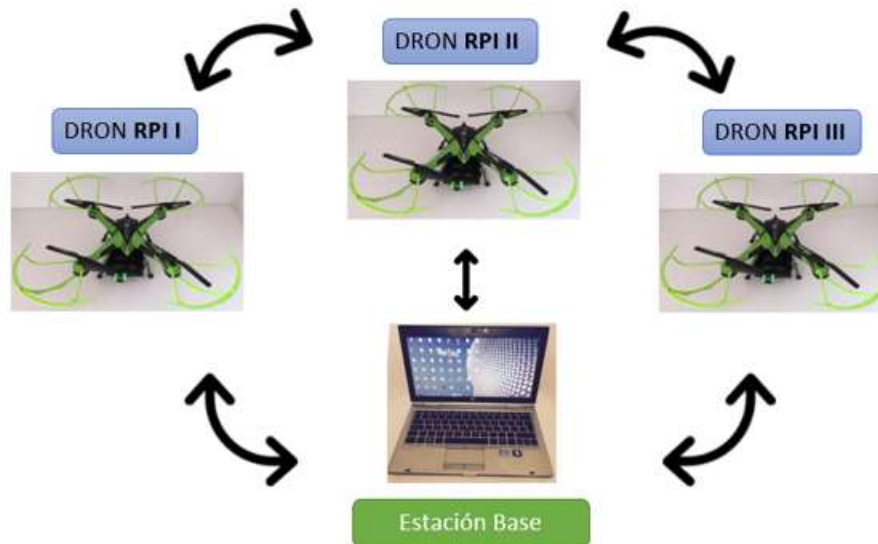


Figura 48. Red MANET RASPBERRY-UDLA

La posibilidad de enrutar a través de saltos el enlace entre los nodos hasta llegar a la Estación Base y permitir la comunicación para la transmisión de video solventa los objetivos de este proyecto.

3.2.4.2. Requisitos básicos para HSMM-PI

Por lo anterior mencionado es necesario tener en cuenta los requisitos básicos necesarios para la instalación de esta herramienta que son:

- Raspberry PI
- Adaptador WiFi
- Tarjeta de memoria SD 4Gb

3.2.4.3. Modos de HSMM-PI

Los tipos de configuración que nos entrega esta herramienta son dos:

3.2.4.3.1. Modo Puerta de Enlace o Gateway

Este modo permite el uso de la red MESH a través de su conexión inalámbrica por medio de su adaptador WiFi existente en cada nodo Raspberry y como puerta de enlace a internet a través de su puerto cableado ethernet. De esta manera la puerta de enlace obtiene DHCP por medio de la interface cableada dando aviso de conexión a los nodos de la red MESH utilizando OSLR (*Optimized Link State Routing Protocol*).

3.2.4.3.2. Modo Malla Interna

El tráfico de la red MESH se distribuye por rutas a cualquier host conectado a la red ya sea esta inalámbrica o cableada. El nodo en este modo permite la ejecución de un servidor DHCP a todo nodo que se encuentre en la red *MESH* así como también es capaz de ejecutar un servidor DNS que puede resolver nombres para los dos tipos de nodos y hosts en la red. En la figura 49 se muestra el funcionamiento de los dos modos de HSMM-PI.

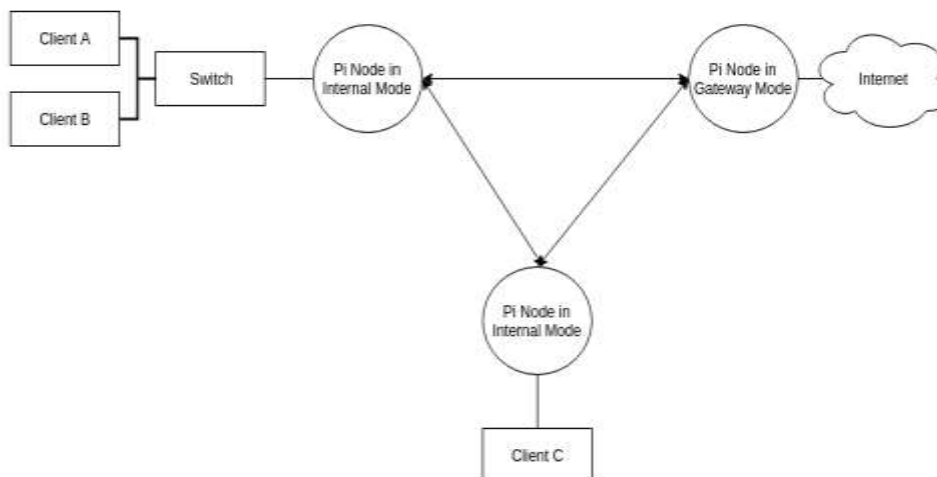


Figura 49. Modos de funcionamiento de HSMM-PI

Tomado de (Github, 2017)

3.2.4.4. Instalación de HSMM-PI 0.8.1

Para la instalación de la herramienta en la placa Raspberry se realiza el siguiente procedimiento, para lo cual es necesario que el Raspberry se encuentre encendido y conectado a una red ya sea cableada o inalámbrica por medio de sus adaptadores *Ethernet* o *Wlan*.

Se abre la ventana del terminal en el escritorio del *Raspbian* donde colocamos los siguientes comandos:

- `sudo apt-get update`
- `sudo apt-get install -y git`
- `git clone https://github.com/urlgrey/hsmm-pi.git`
- `cd hsmm-pi`
- `sh install.sh`

Es necesario la actualización de la versión de sistema operativo y todos sus ficheros para prevenir cualquier error durante la descarga e instalación de la herramienta con el primer comando. Después con el comando: *apt-get install*, se lo recomienda para verificar si se encuentra instalado el GIT en el *Raspbian* ya que las últimas versiones de *Raspbian* ya lo tienen preinstalado, de no estar instalado este comando realiza la instalación de este instalador desde repositorio GIT. El comando: *git clone*, se lo utiliza para iniciar la instalación de HSMM-PI, lo que logra es descargar desde GIT el directorio que contiene todos los archivos de la herramienta para la instalación del mismo en la placa Raspberry. Una vez que esta acción se ha realizado es necesario mediante la terminal ingresar a la carpeta dentro del sistema donde se colocó el directorio con los archivos e instaladores del HSMM-PI que se realiza por defecto con el comando: *cd hsmm-pi*, y una vez dentro de esta carpeta colocar el comando: *sh install.sh*, que permite ejecutar el instalador que se encuentra en esta carpeta, como se muestran en las figuras 50-54.

```

login as: pi
pi@192.168.1.121's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Apr 29 17:35:12 2017
pi@RPI-II:~ $
pi@RPI-II:~ $ sudo apt-get install -y git^C
pi@RPI-II:~ $ sudo apt-get install -y git
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version.
git set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.
pi@RPI-II:~ $ █

```

Figura 50. Verificación de GIT en el SO

```

login as: pi
pi@192.168.1.121's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Apr 29 17:35:12 2017
pi@RPI-II:~ $
pi@RPI-II:~ $ sudo apt-get install -y git^C
pi@RPI-II:~ $ sudo apt-get install -y git
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version.
git set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.
pi@RPI-II:~ $ git clone https://github.com/urlgrey/hmmm-pi.git
Cloning into 'hmmm-pi'...
remote: Counting objects: 2009, done.
remote: Total 2009 (delta 0), reused 0 (delta 0), pack-reused 2009
Receiving objects: 100% (2009/2009), 804.01 KiB | 473.00 KiB/s, done.
Resolving deltas: 100% (1004/1004), done.
Checking connectivity... done.
pi@RPI-II:~ $ █

```

Figura 51. Ejecución del Comando git clone

```

pi@RPI-II:~ $ cd hsmm-pi
pi@RPI-II:~/hsmm-pi $ sh install.sh
Hit http://mirrordirector.raspbian.org jessie InRelease
Hit http://mirrordirector.raspbian.org jessie/main armhf Packages
Hit http://mirrordirector.raspbian.org jessie/contrib armhf Packages
Hit http://mirrordirector.raspbian.org jessie/non-free armhf Packages
Hit http://mirrordirector.raspbian.org jessie/rpi armhf Packages
Hit http://archive.raspberrypi.org jessie InRelease
Ign http://mirrordirector.raspbian.org jessie/contrib Translation-en
Ign http://mirrordirector.raspbian.org jessie/main Translation-en
Ign http://mirrordirector.raspbian.org jessie/non-free Translation-en
Ign http://mirrordirector.raspbian.org jessie/rpi Translation-en
Hit http://archive.raspberrypi.org jessie/main armhf Packages
Hit http://archive.raspberrypi.org jessie/ui armhf Packages
Ign http://archive.raspberrypi.org jessie/main Translation-en
Ign http://archive.raspberrypi.org jessie/ui Translation-en
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
make is already the newest version.
make set to manually installed.
ntp is already the newest version.
The following extra packages will be installed:
  apache2-bin apache2-data apache2-utils dns-root-data dnsmasq-base
  libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libb-hooks-endofscope-perl libbison-dev libclass-load-perl
  libclass-singleton-perl libcommon-sense-perl libcurses-perl
  libcurses-ui-perl libdatettime-format-w3cdf-f-perl libdatettime-locale-perl
  libdatettime-perl libdatettime-timezone-perl libfl-dev libgps-point-perl
  libgps21 libio-socket-inet6-perl libjson-xs-perl liblist-allutils-perl
  liblist-moreutils-perl liblua5.1-0 libmcrypt4 libmnl0
  libmodule-implementation-perl libmodule-runtime-perl libnamespace-clean-perl
  libnetfilter-contrack3 libonig2 libpackage-stash-perl

```

Figura 52. Ingreso a la carpeta de HSM-PI y ejecución del instalador

```

Creating config file /etc/php5/mods-available/pdo_sqlite.ini with new version
php5_invoke: Enable module pdo_sqlite for cli SAPI
php5_invoke: Enable module pdo_sqlite for apache2 SAPI
Setting up sqlite (3.8.17-1) ...
Setting up sqlite3 (3.8.17.1+deb8u2) ...
Setting up ssl-cert (1.0.35) ...
Setting up sysv-rc-conf (0.99-7) ...
Processing triggers for libc-bin (2.19-19+deb8u7) ...
Processing triggers for systemd (215-17+deb8u6) ...
Processing triggers for dbus (1.8.22-0+deb8u1) ...
Processing triggers for libapache2-mod-php5 (5.6.20+dfsg-0+deb8u1) ...
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'ifplugd' is not installed, so not removed.
0 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.
Already up-to-date.
All settings correct for using Composer
Downloading...

Composer (version 1.4.1) successfully installed to: /home/pi/hsmm-pi/src/var/www/hsmm-pi/composer.phar
Use it: php composer.phar

Loading composer repositories with package information
Installing dependencies (including require-dev) from lock file
Package operations: 1 install, 0 updates, 0 removals
  - Installing cakephp/cakephp (2.8.0): Downloading (100%)
Generating autoload files

Welcome to CakePHP v2.8.* Console
-----
App : hsmm-pi
Path: /home/pi/hsmm-pi/src/var/www/hsmm-pi/
-----
Cake Schema Shell
-----

The following table(s) will be dropped.
location_settings
network_services

```

Figura 53. Proceso de instalación, configuración y ejecución de OSLR

```

pi@RPI-II:~$ cd hsmm-pi
pi@RPI-II:~/hsmm-pi$ sh install.sh
Hit http://mirrordirector.raspbian.org jessie InRelease
Hit http://mirrordirector.raspbian.org jessie/main armhf Packages
Hit http://mirrordirector.raspbian.org jessie/contrib armhf Packages
Hit http://mirrordirector.raspbian.org jessie/non-free armhf Packages
Hit http://mirrordirector.raspbian.org jessie/rpi armhf Packages
Hit http://archive.raspberrypi.org jessie InRelease
Ign http://mirrordirector.raspbian.org jessie/contrib Translation-en
Ign http://mirrordirector.raspbian.org jessie/main Translation-en
Ign http://mirrordirector.raspbian.org jessie/non-free Translation-en
Ign http://mirrordirector.raspbian.org jessie/rpi Translation-en
Hit http://archive.raspberrypi.org jessie/main armhf Packages
Hit http://archive.raspberrypi.org jessie/ui armhf Packages
Ign http://archive.raspberrypi.org jessie/main Translation-en
Ign http://archive.raspberrypi.org jessie/ui Translation-en
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
make is already the newest version.
make set to manually installed.
ntp is already the newest version.
The following extra packages will be installed:
  apache2-bin apache2-data apache2-utils dns-root-data dnsmasq-base
  libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libb-hooks-endofscope-perl libbison-dev libclass-load-perl
  libclass-singleton-perl libcommon-sense-perl libcurses-perl
  libcurses-ui-perl libdatetime-format-w3cdf-perl libdatetime-locale-perl
  libdatetime-perl libdatetime-timezone-perl libfl-dev libgps-point-perl
  libgps21 libio-socket-inet6-perl libjson-xs-perl liblist-allutils-perl

```

Figura 54. Instalación de componentes y librerías

Una vez que se realiza la instalación completa de la herramienta HSMM-PI se muestra al final un mensaje de éxito o de lo contrario muestra un mensaje de error con su explicación de la falla como se muestra en la figura 55 una vez realizado esta instalación es recomendable reiniciar el sistema operativo ya que este instalador también ejecuta el código que permite el uso del protocolo OSLR dentro del sistema operativo y sus adaptadores de red.


```

config -n /usr/local/lib
mkdir -p "/etc/olsrd"
cp "./resources/olsrd.pud.position.conf" "/etc/olsrd"
: "/usr/local/lib/olsrd_pud.so.2.0.0"
make[1]: Leaving directory '/var/tmp/olsrd/lib/pud'
make[1]: Entering directory '/var/tmp/olsrd/lib/quagga'
: olsrd_quagga.so.0.2.2
install -D -m 755 olsrd_quagga.so.0.2.2 /usr/local/lib/olsrd_quagga.so.0.2.2; /s
bin/ldconfig -n /usr/local/lib
make[1]: Leaving directory '/var/tmp/olsrd/lib/quagga'
make[1]: Entering directory '/var/tmp/olsrd/lib/secure'
: olsrd_secure.so.0.6
install -D -m 755 olsrd_secure.so.0.6 /usr/local/lib/olsrd_secure.so.0.6; /sbin/
ldconfig -n /usr/local/lib
make[1]: Leaving directory '/var/tmp/olsrd/lib/secure'
make[1]: Entering directory '/var/tmp/olsrd/lib/sgwdynspeed'
install -D -m 755 olsrd_sgwdynspeed.so.1.0.0 /usr/local/lib/olsrd_sgwdynspeed.so
.1.0.0; /sbin/ldconfig -n /usr/local/lib
mkdir -p "/etc/olsrd"
cp "./resources/olsrd.sgw.speed.conf" "/etc/olsrd"
: "/usr/local/lib/olsrd_sgwdynspeed.so.1.0.0"
make[1]: Leaving directory '/var/tmp/olsrd/lib/sgwdynspeed'
make[1]: Entering directory '/var/tmp/olsrd/lib/txtinfo'
: olsrd_txtinfo.so.0.1
install -D -m 755 olsrd_txtinfo.so.0.1 /usr/local/lib/olsrd_txtinfo.so.0.1; /sbi
n/ldconfig -n /usr/local/lib
make[1]: Leaving directory '/var/tmp/olsrd/lib/txtinfo'
make[1]: Entering directory '/var/tmp/olsrd/lib/watchdog'
: olsrd_watchdog.so.0.1
install -D -m 755 olsrd_watchdog.so.0.1 /usr/local/lib/olsrd_watchdog.so.0.1; /s
bin/ldconfig -n /usr/local/lib
make[1]: Leaving directory '/var/tmp/olsrd/lib/watchdog'
inserv: warning: current stop runlevel(s) (empty) of script `olsrd' overrides L
SB defaults (0 1 6).

---- SUCCESS ----

Login to the web console to configure the node
pi@RPI-II:~/hsmm-pi $

```

Figura 55 Mensaje de instalación de HSM-M-PI

3.2.5. Protocolo OSLR

El protocolo OSLR es el gestor de enrutamiento que se utiliza para la optimización de la red *AdHoc* y todos los dispositivos que se encuentran dentro de esta red en su totalidad, por ser un protocolo proactivo utiliza los procedimientos de *HELLO* y *TOPOLOGY CONTROL*, los cuales son utilizados para el descubrimiento de información de estado de enlace en toda la red, así como también la difusión de la información en toda la malla de la red *AdHoc* móvil. Cada uno de los nodos individualmente usan esta información para calcular la topología de los destinos y los saltos dentro de la red, lo cual permite a cada nodo conocer los caminos más cortos para el envío de información a través de saltos como se puede apreciar en la figura 56 el flujo de datos mediante el protocolo de OSLR.

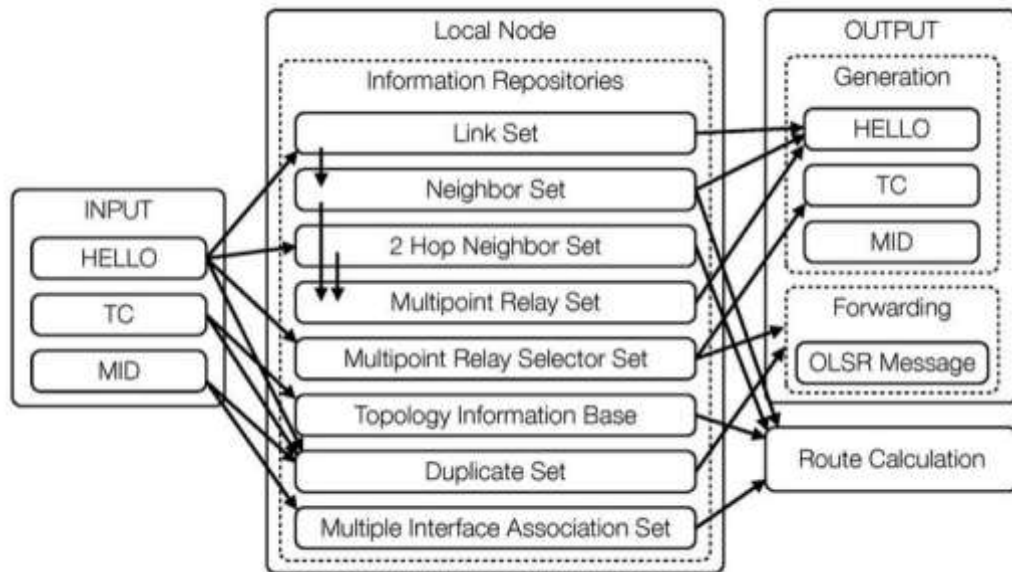


Figura 56. Diagrama de Flujo de Datos de OSLR

Tomado de (Morgado Reyes, 2009)

3.2.6. Configuración de Nodos

Cuando la herramienta HSMM-PI se encuentra instalada con éxito en todos los Raspberry y cada uno de ellos se encuentre dentro de una red inalámbrica, es posible acceder a cada uno de ellos mediante la dirección IP de cada nodo en el browser de cualquier navegador, desde cualquier dispositivo dentro de la red incluso desde los mismos Raspberry utilizando el navegador Chromium. De esta acción se despliega una ventana como se muestra en la figura 57.

Escribimos en el navegador: `http://(IP del nodo Raspberry):8080/`

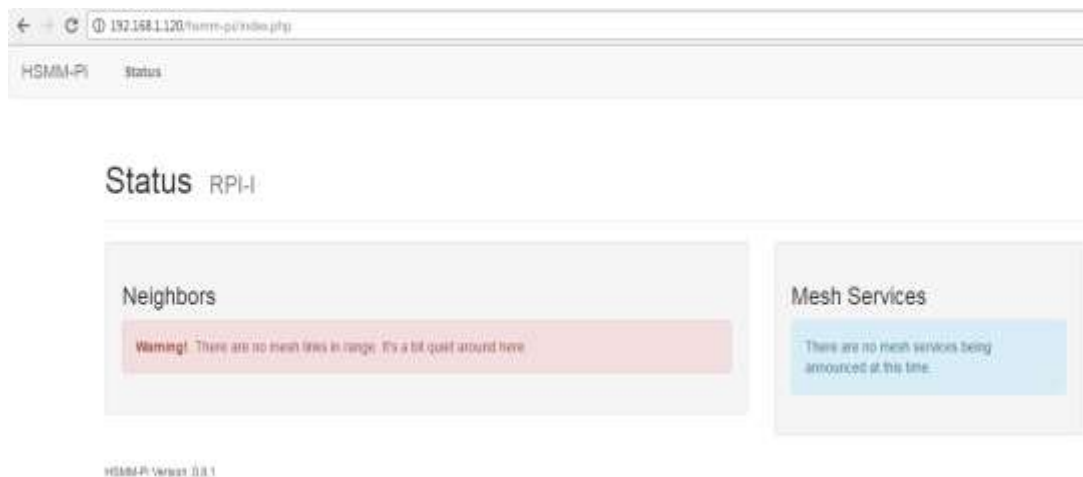


Figura 57. Ingreso a HSM-PI mediante browser

En la ventana que se despliega del nodo se ingresa a la opción de *login*, por la cual accedemos a la configuración de HSM-PI en el nodo ingresado, para lo cual es necesario colocar el usuario y contraseña como se muestra en la figura 58, estos por defecto son los siguientes:

- Usuario: admin
- Contraseña: changeme

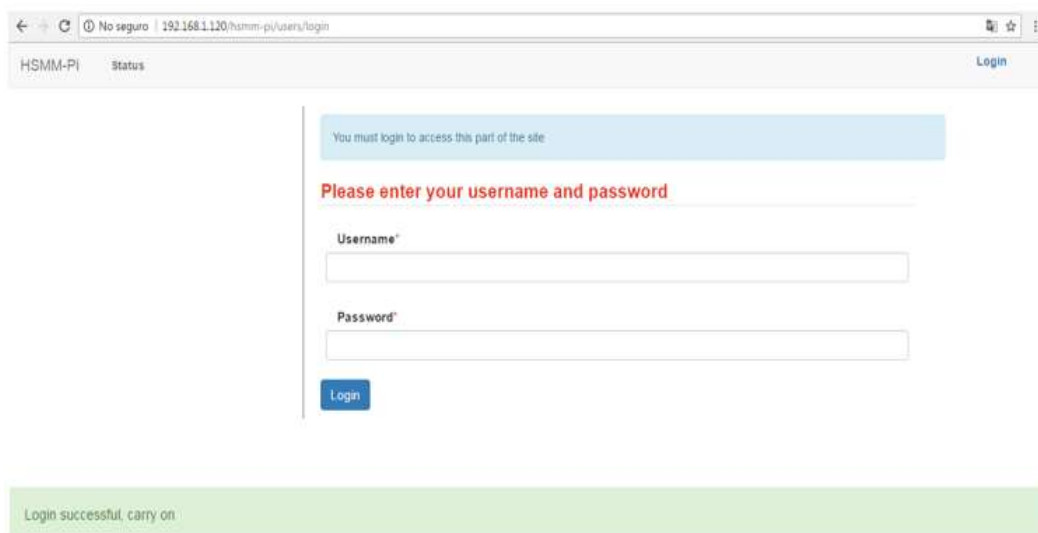


Figura 58. Longin de HSM-PI

Estos se pueden cambiar una vez dentro se selecciona la pestaña de Admin y se despliega el menú de Admin, en donde se encuentra la opción de Account como se muestra en las figuras 59, 60.

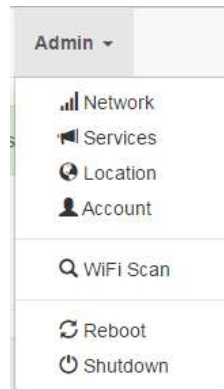


Figura 59. Menú de Administrador HSMM-PI

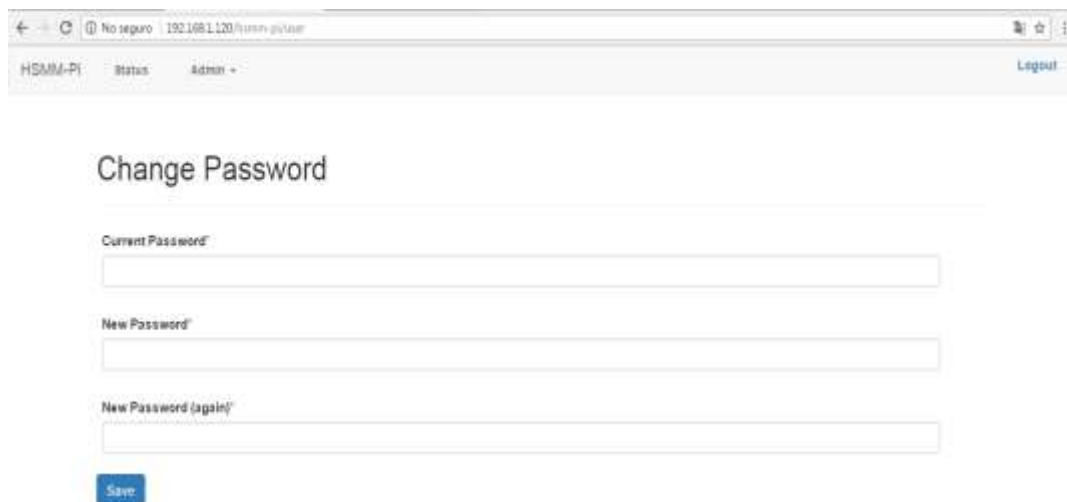


Figura 60. Cambio de contraseña HSMM-PI

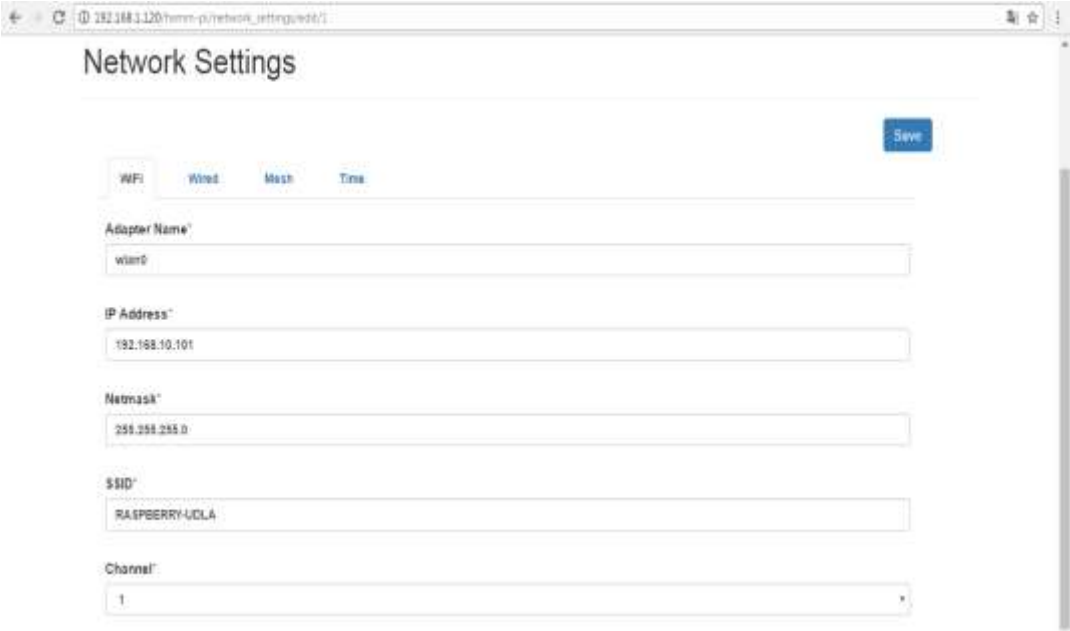
3.2.6.1. Network

En la opción de Network del menú en la pestaña de *Account* como se muestra en la figura 64, se aprecia la ventana donde se despliegan cuatro pestañas en donde es posible configurar:

- WiFi
- Wired
- Mesh
- Time

3.2.6.1.1. WiFi

En esta opción como se muestra en la figura 61 se encuentran los parámetros para la configuración del adaptador de red WLAN del dispositivo, mediante esta nos permite conectarnos de manera inalámbrica a las redes, es por ello que se debe especificar el adaptador de red que se está utilizando en este caso wlan0, la dirección IP del Raspberry, la máscara de la red y el canal para unirnos a la red deseada. El parámetro de (SSID) que es el identificador de red para cada adaptador y cada dispositivo debe ser el mismo para todos los nodos y dispositivos que se encuentren en la red, caso contrario no podrán establecer conexión en la red MESH.



The image shows a web browser window displaying the 'Network Settings' page. The browser's address bar shows the URL '192.168.1.120/home-pi/reboot_settings/1'. The page title is 'Network Settings'. There are four tabs: 'WiFi' (selected), 'Wired', 'Mesh', and 'Time'. A blue 'Save' button is located in the top right corner. The form contains the following fields:

- Adapter Name***: wlan0
- IP Address***: 192.168.10.101
- Netmask***: 255.255.255.0
- SSID***: RASPBERRY-UCLA
- Channel***: 1

Figura 61. Ventana de Configuración WLAN

3.2.6.1.2. Wired

En esta opción podemos realizar la configuración del adaptador de red cableada en este caso la interfaz Ethernet que el dispositivo utilice como se muestra en la figura 62. En este caso no se utiliza ninguna interfaz cableada por lo que todos los nodos se encuentran en los drones movilizados en el aire. Pero es aquí donde es posible configurar los modos puerta de enlace o modo *internal*.

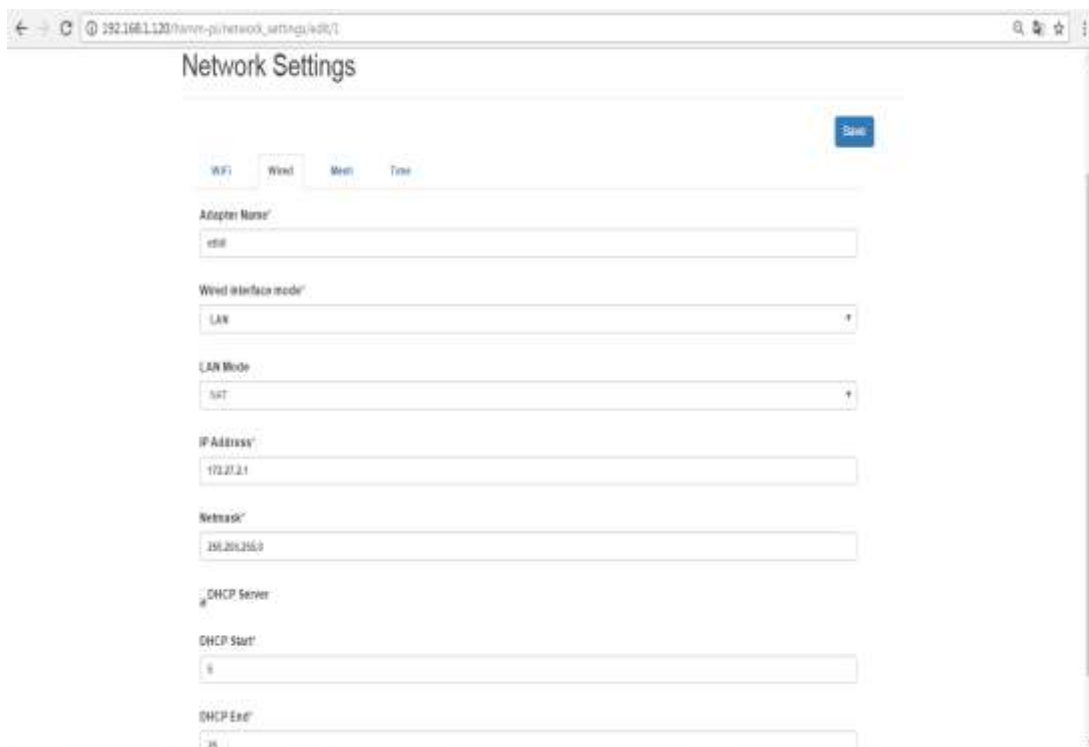


Figura 62. Ventana de Configuración de Wired

3.2.6.1.3. Mesh

En esta pestaña se encuentra la opción para la configuración de los parámetros de la red MESH como se muestra en la figura 63, por lo que es posible colocar el nombre del dispositivo como va a ser identificado en la tabla de direccionamiento para los saltos que se presenten en la red. El parámetro de OSLRD se lo desactiva ya que este parámetro aísla la conexión de los nodos entre sí.

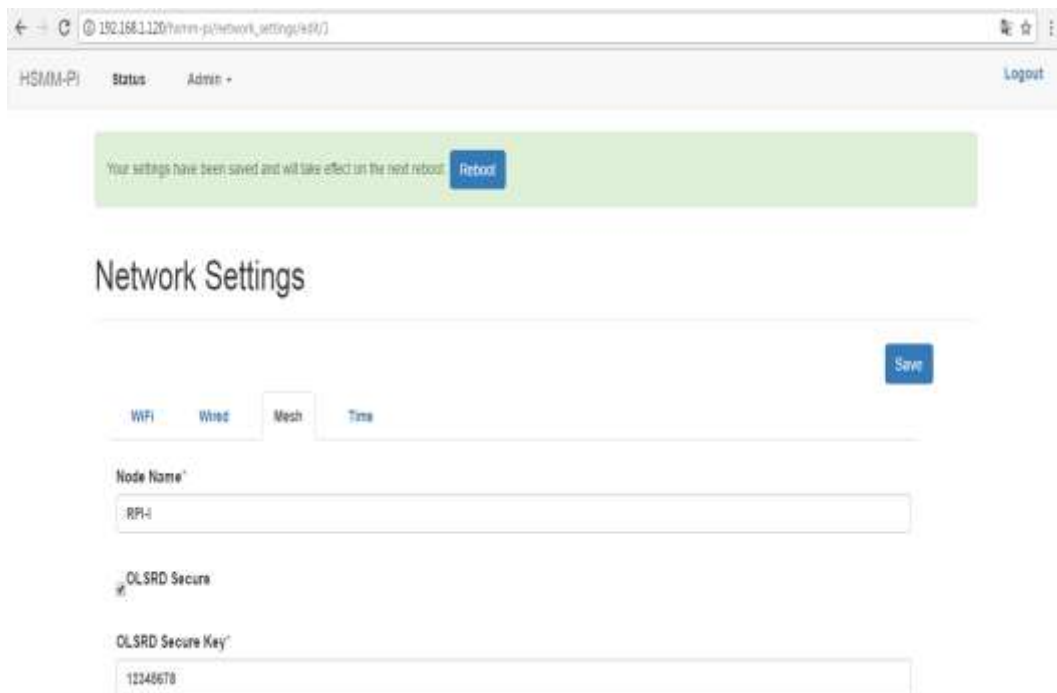


Figura 63. Ventana de Configuración Mesh

Es necesario siempre que se realiza o ejecuta algún cambio dentro de la configuración de HSM-PI reiniciar el sistema operativo, de esta manera se garantiza la aplicación de los cambios realizados. Adicionalmente en HSM-PI se encuentra una pestaña referente a servicios donde es posible colocar cualquier tipo de servicio UDP y TCP dentro de la red MESH, así como también servicios de localización y GPS mediante el aplicativo de mapas desde una cuenta Microsoft.

3.2.7. Instalación de Netcat y Mplayer en Raspberry 3

La versión que se usa en este proyecto de *Netcat* es la versión 1.11 en el cual se encuentra un archivo comprimido con las versiones tanto para 32 y 64 bits; este archivo se puede descargar del siguiente link:

<https://eternallybored.org/misc/netcat/>

Mientras que para Mplayer se utiliza la versión 1.3.0, esta versión es la última de la herramienta y se puede descargar de la página oficial en el siguiente link.

<http://www.mplayerhq.hu/design7/dload.html>

Para la computadora que es la Estación Base de este proyecto no es necesario instalar la herramienta solo se debe colocar el archivo ejecutable llamado Nc64.exe para la arquitectura de 64 bits en una carpeta dentro del equipo al igual que el archivo ejecutable de Mplayer que tiene el nombre de Mplayer.exe.

Para los Raspberry si es necesario la instalación del directorio con todos los componentes de Netcat y Mplayer, por lo que la placa debe tener conexión a internet para poder realizar la descarga y la instalación de esta herramienta.

Colocamos en la terminal del dispositivo el comando: `sudo apt-get install mplayer netcat`

Con este comando el Raspberry automáticamente descarga mediante GIT los instaladores de Netcat y Mplayer para ejecutar la instalación en el dispositivo, esta acción dura pocos segundos lo cual depende mucho de la conexión a internet que se está usando en el Raspberry como se muestra en la figura 64.

```
pi@raspberrypi ~ $ sudo apt-get install mplayer netcat
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  icelib libblas3gf liblapack3gf
Use 'apt-get autoremove' to remove them.
Suggested packages:
  mplayer-doc netselect fping
The following NEW packages will be installed:
  mplayer netcat
0 upgraded, 2 newly installed, 0 to remove and 9 not upgraded.
Need to get 0 B/2,533 kB of archives.
After this operation, 4,536 kB of additional disk space will be used.
```

Figura 64. Instalación de Mplayer y Netcat en el Rapberry

3.3. Esquema de nodos y estación Base

A continuación, se presenta los esquemas de un nodo (figura 65), estación base (figura 66) y un esquema general del sistema de comunicación a ser implementado (figura 67).

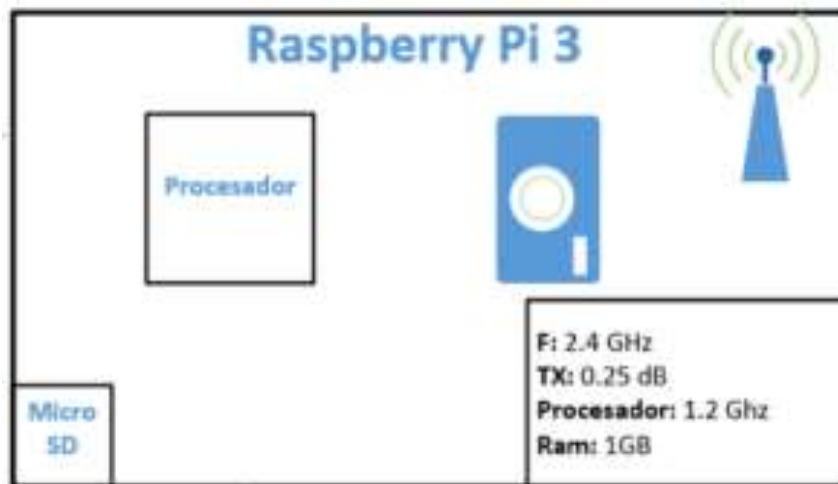


Figura 65. Esquema nodo Raspberry PI 3

Tomado de (Valencia & Risueño, 2017)



Figura 66. Esquema Estación Base

Tomado de (Valencia & Risueño, 2017)

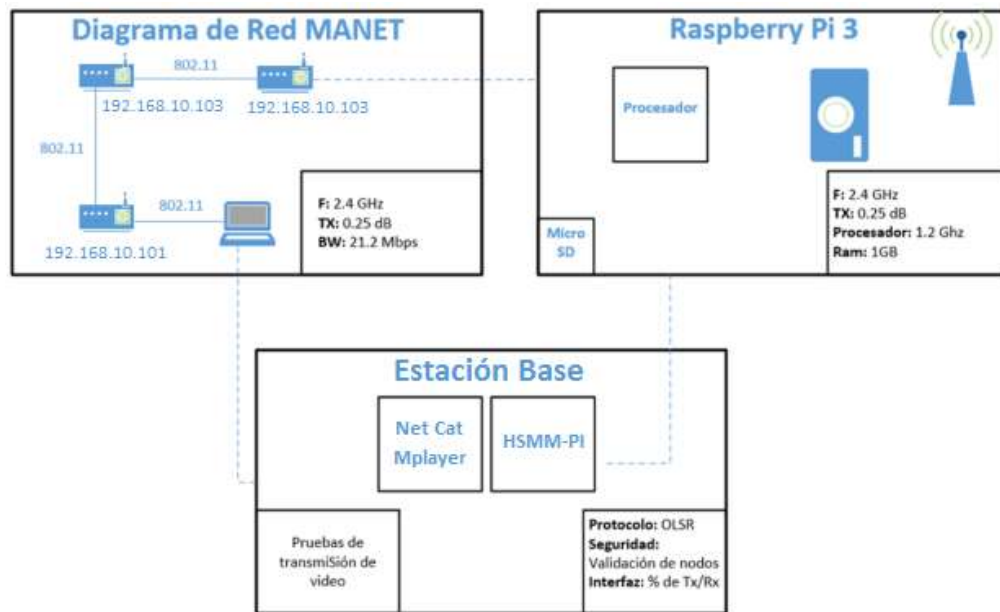


Figura 67. Esquema general del sistema

Tomado de (Valencia & Risueño, 2017)

3.4. Estación Base

Al igual que en el tema anterior en este caso se va a desarrollar todos los temas referentes a la estación base como el direccionamiento IP del equipo, características básicas con las que debe cumplir el equipo y la configuración necesaria para poder conectar el equipo a la red MANET

3.4.1. Direccionamiento IP y Puertos

En la tabla 4 se cita la dirección IP que fue configurada en la estación base para el funcionamiento dentro de la red MANET "RASPBERRY-UDLA" y el puerto utilizado tanto para la transmisión y la recepción de los datos de video de cada nodo implementado, hay que tener en cuenta que el puerto puede ser distinto en cada *Dron*, esto en el caso de que los tres drones transmitan video simultáneamente, con esto se evitará la saturación del canal, la estación base debe tener configurado el mismo puerto que tiene el *Dron*.

Tabla 4

Direccionamiento IP y puerto en estación base

Tipo Del Dispositivo	Nombre Del Dispositivo	Dirección IP del Dispositivo	Puerto Tx / Rx de Dispositivo
Computador HP	Estación Base	192.168.10.100	5001

3.4.2. Sistema Operativo

Para la Estación Base propuesta para este proyecto se escoge el Sistema Operativo Windows en su versión 7, aunque no se descarta el uso de otros sistemas operativos como Linux y las otras versiones de Windows. La elección de este Sistema es el más adecuado para el proyecto ya que para la configuración de la Red *AdHoc* no es necesario realizar procedimientos extra como en Windows 8 o Windows 10, también por que la interfaz gráfica de este sistema operativo es la más popular y conocida a nivel mundial, lo que hace que esta configuración y despliegue de la red sea más sencilla.

3.4.2.1. Windows 7

El Sistema Operativo Windows 7, fue desarrollado por el coloso fabricante de *software Microsoft Corporation* el 22 de octubre del 2009 y durante los 7 años en el mercado ha realizado mejoras en los diferentes *service pack* donde el más estable hasta la fecha es el de la versión 6.1, donde su predecesor es el Windows Vista y su Sucesor el Windows 8.

3.4.2.2. Características

Entre las características más relevantes ante su predecesor tenemos:

- Se realiza mejoras en desempeño, confiabilidad y seguridad, se elimina las carteleras de seguridad en los servicios la cual se controla en esta versión directamente por el usuario mediante la herramienta de Control de la Cuenta de Usuario.

- Se mejora la interfaz en cuanto al uso y compatibilidad de conexión con periféricos y reconocimiento de equipos táctiles, discos virtuales, el reconocimiento de voz y se realiza mejoras en cuanto a procesamiento multi-núcleo.
- Se mejora drásticamente en rapidez de arranque y funcionamiento del sistema.
- Se despliegan versiones del SO tanto para arquitectura de 32 bits y 64 bits.
- Se mejora su interfaz gráfica para simplificar tareas, la navegación se vuelve más amigable con el usuario para optimizar al máximo los recursos de mayor uso en la barra de tareas.
- Incorpora nuevos formatos de archivos para la reproducción de audio y video que no se encuentre con protección de fabricante.

3.4.2.3. Versiones de Windows 7

- Windows 7 Starter
- Windows 7 Home Basic
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Enterprise
- Windows 7 Ultimate

3.4.2.4. Requisitos básicos para Windows 7

- Procesador de 1 GHz.
- 2 GB de RAM en 32 bits, y 4 GB de RAM en 64 bits.
- 16 GB de disco libre en 32 bits, y 20 GB de disco libre en 64 bits.

3.4.3. Activación de Políticas (Friwall) en Windows 7

Para lograr la implementación de la red y su funcionamiento eficaz que permita el flujo de tráfico a través de la malla entre cada uno de los nodos es importante considerar ciertos parámetros que se deben configurar.

En primer lugar, se debe bajar las seguridades en el computador ya que los programas como antivirus pueden bloquear el paso del tráfico hacia el computador o fuera de este, por lo que es recomendable desactivar o eliminar este tipo de programas de la estación base. Otro punto importante es que se debe verificar que el firewall este desactivado ya que este también impide el flujo de tráfico en puertos y como es de conocimiento los nodos a través de la red *AdHoc* no presenta niveles de seguridad por lo que puede considerar como tráfico no seguro a mi dispositivo y cerrar el paso del tráfico. También se recomienda verificar las políticas de Windows ya que al utilizar diferentes puertos para el envío de tráfico de información de los dispositivos, muchos de estos pueden encontrarse restringidos para su uso es por ello que es necesario verificar mediante las herramientas y parámetros si la conexión entre los dispositivos es posible puesto que pueden darse variedad de problemas pero lo más común son la restricción de comunicación por políticas de seguridad y bloqueos en la red, en este caso fue necesario activar la política que se muestra en la figura 68.

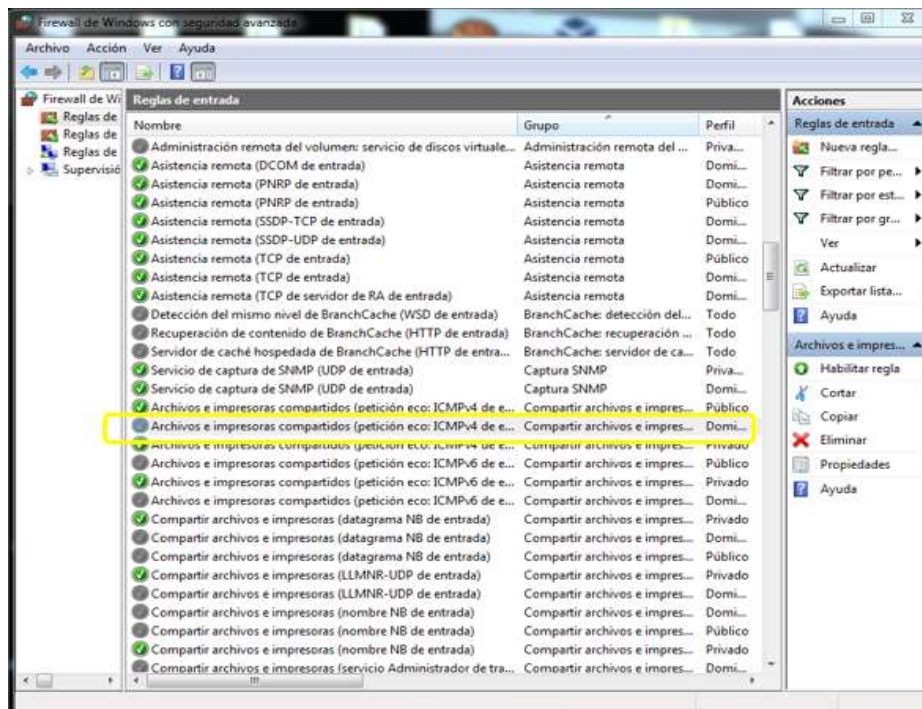
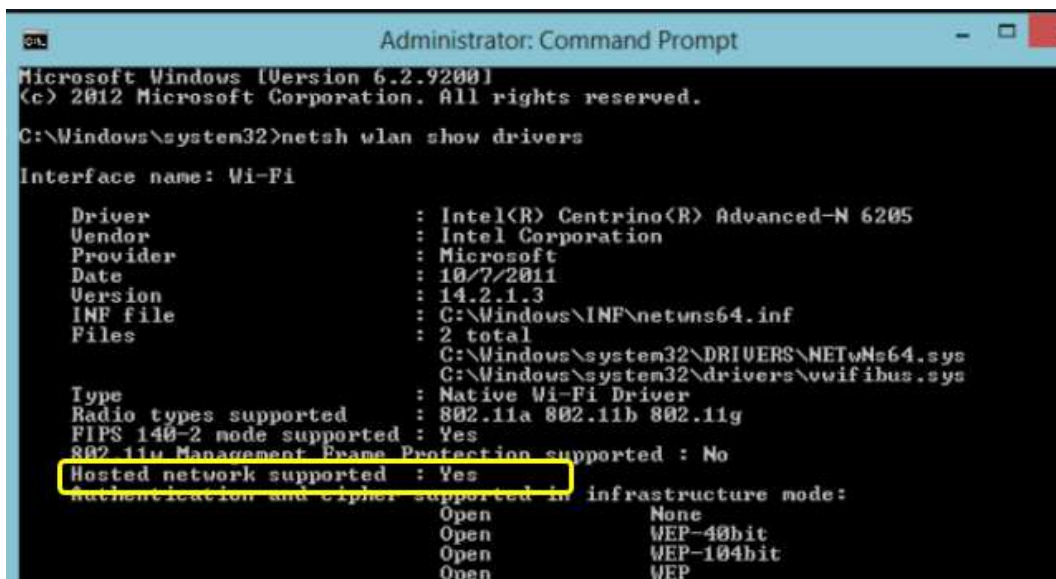


Figura 68. Políticas y reglas de entrada Firewall de Windows

3.4.4. Configuración Red AdHoc – MANET

Para la configuración de la red en la estación base que para este caso es el computador portátil HP que se describe en el capítulo 2 en cuanto a la propuesta de hardware y en el actual capítulo en la propuesta de software, es necesario comprobar que la tarjeta de red inalámbrica es la adecuada y permita la creación de la red *AdHoc – MANET*, es por ello se abre una terminal CMD en Windows ingresando el comando: `netsh wlan show drivers`

Al colocar este comando nos entrega la información de la figura 69, donde es posible verificar si esta soporta o no la red *AdHoc*.



```

Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
C:\Windows\system32>netsh wlan show drivers

Interface name: Wi-Fi

Driver                : Intel(R) Centrino(R) Advanced-N 6205
Vendor                : Intel Corporation
Provider              : Microsoft
Date                  : 10/7/2011
Version               : 14.2.1.3
INF file              : C:\Windows\INF\netwms64.inf
Files                 : 2 total
                       C:\Windows\system32\DRIVERS\NETwms64.sys
                       C:\Windows\system32\drivers\wvifibus.sys
Type                  : Native Wi-Fi Driver
Radio types supported : 802.11a 802.11b 802.11g
FIPS 140-2 mode supported : Yes
802.11u Management Frame Protection supported : No
Hosted network supported : Yes
Authentication and cipher supported in infrastructure mode:
Open                  None
Open                  WEP-40bit
Open                  WEP-104bit
Open                  WEP

```

Figura 69. Hosted Network Support

Si el equipo presenta YES en este parámetro es posible realizar la configuración de la red, caso contrario es necesario actualizar el driver del adaptador de red para poder activar esta opción automáticamente al instalar la nueva versión, esta opción de actualización no funciona en Windows 8 y Windows 10 por lo que es necesario realizar el procedimiento que se describe en la página oficial de Microsoft para las versiones de Windows 8 y 10.

3.4.4.1. Conexión a Red MANET

Para que la estación base funcione como un nodo más dentro de la malla de nodos en la red MANET, es necesario colocar una IP en la configuración de la red inalámbrica ya que como no existe un Servidor no es posible la conexión con los Raspberry si no se encuentran en el mismo segmento de red es por ello que se coloca la IP detallada en la tabla 3, y de esta manera se realiza la conexión a la Red RASPBERRY-UDLA que es captada por la tarjeta de red de la Estación Base como se muestra en la figura 70.

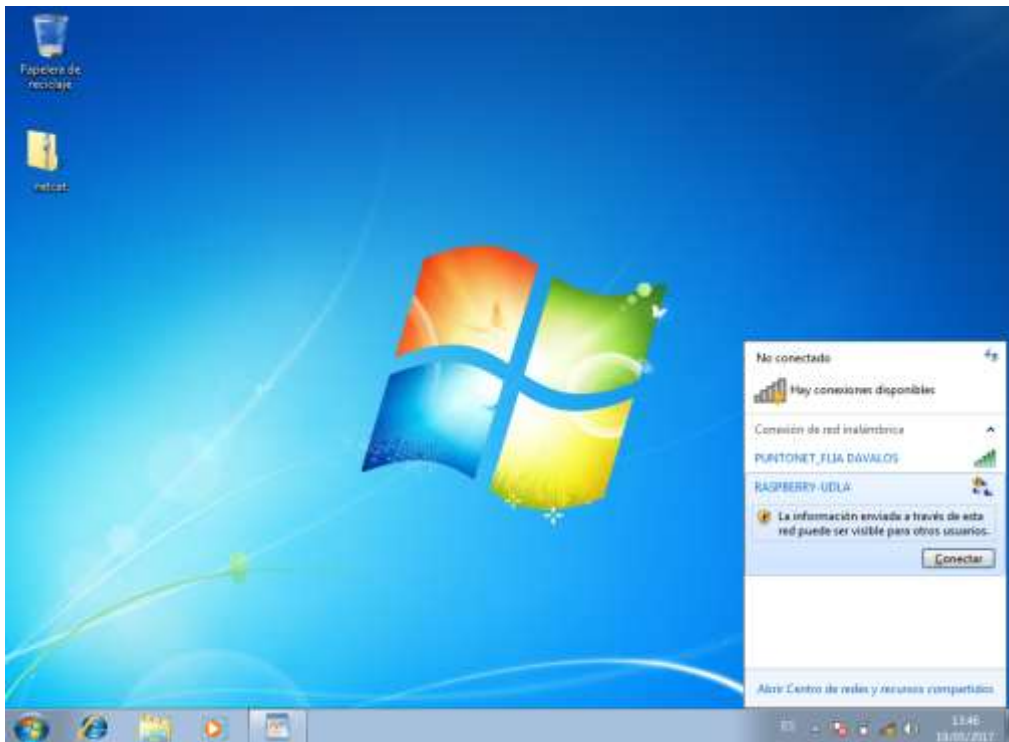


Figura 70. Conexión a la red Manet desde Estación Base

3.4.4.1.1. Parámetros de la Red

Para la red creada colocamos el nombre de la red como:

Nombre de Red: RASPBERRY-UDLA

Contraseña: 12345678

De esta manera es posible el enlace de los dispositivos Raspberry a la red mediante la conexión de su adaptador de red inalámbrica WLAN0 como se muestra en la figura 71, donde al seleccionar la red, se solicita la contraseña de acceso lo cual permite dar seguridad al ingreso de cualquier componente o dispositivo a la red desplegada.

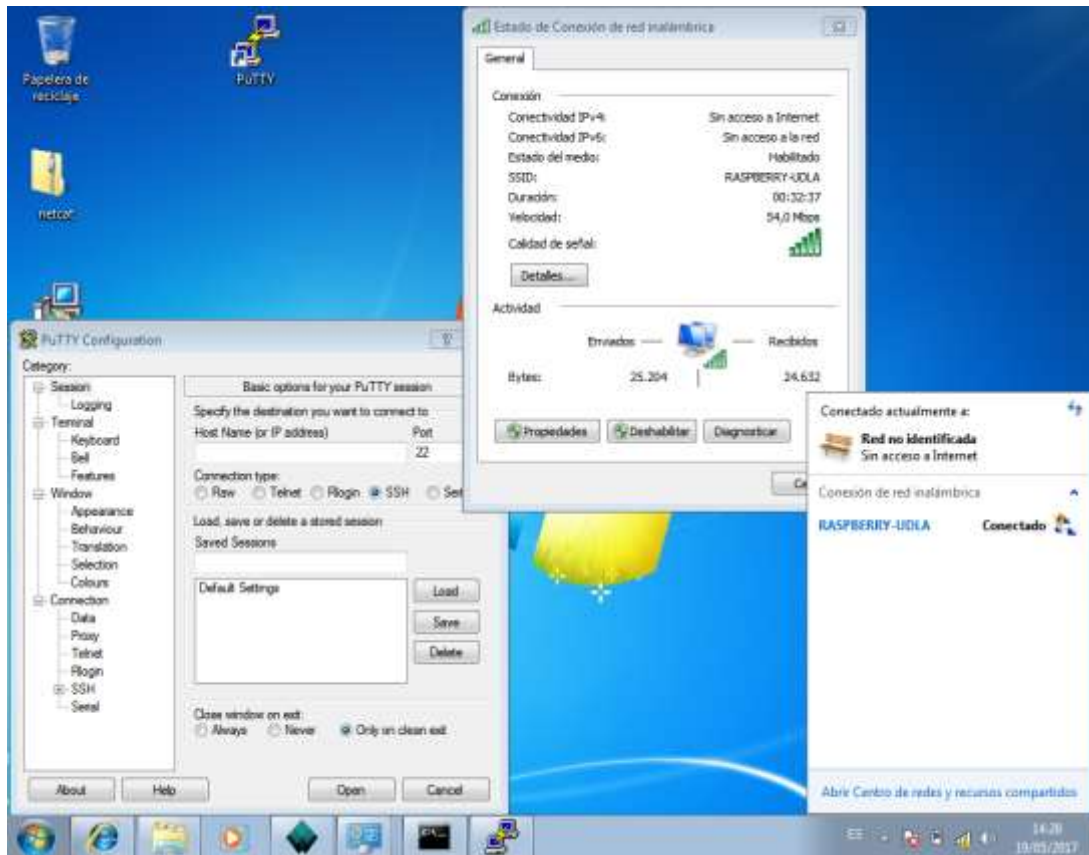


Figura 71. Conexión de red MANET

3.5. Servicio de Video

Para la activación del servicio de video es necesario establecer la configuración de cierto software, a continuación, se detalla cada uno de estos, y como se establece el servicio de video entre el nodo a transmitir y la estación Base.

3.5.1. Netcat

Esta es una herramienta fue desarrollada por HOBBIT en 1996 para más tarde ser libre con una licencia de software libre, lo que permitió desarrollarla y modificarla para que sea utilizada en Windows, MAC OS, etc. La herramienta de red basada en Unix permite la lectura y escritura de datos a través de las redes, estas pueden ser por medio de dos tipos de conexión que son TCP o UDP. Es

conocido como la navaja suiza para redes, ya que su uso permite que interprete comandos que abren puertos TCP/UDP en un dispositivo para dejarlos en escucha en el receptor y en el lado del transmisor remotamente mediante la IP del dispositivo en la red con la ruta conocida forzando conexiones TCP/UDP por ejemplo el rastreo de puertos o la transferencia de archivos entre los dos puntos TX y RX. El paso de la información se la realiza bit a bit entre los dispositivos

Existen dos modos de configuración que son el modo cliente y servidor, de esta manera el comportamiento de la herramienta es crear un socket para conectarse a un servidor o para configurarse en modo servidor, de esta manera en el puerto seleccionada abre la transmisión de flujo de información de este socket de manera binaria, mientras que en el receptor abre el socket dejando en modo escucha para recibir de manera estándar todo el flujo de datos transmitido.

Los parámetros que se configuran en Netcat son los siguientes:

- -l: Indica que Netcat abre el puerto para Escucha (Listen): Acepta una única conexión de un Cliente y se cierra.
- -p: Especifica el puerto
- -k: Fuerza a que el puerto permanezca abierto tras haber recibido una Conexión. Se usa con el parámetro -l y permite infinitas Conexiones.
- -u: El puerto abierto se abre como UDP, en vez de TCP que es la opción por default.
- -v: Muestra información de la conexión.
- -t: Las respuestas son compatibles para sesiones de Telnet.
- -q segundos: Tras haber recibido el EOF de la Entrada de datos, espera los segundos indicados para enviarla.
- -i segundos: Especifica un delay (retraso) de tiempo para el envío o recepción de las líneas de texto. (Netcat, 2013)

3.5.1.1. Principales características de Netcat

- Conexiones salientes o entrantes, TCP o UDP, hacia o desde cualquier puerto
- DNS completo avance / retroceso de cheques, con las advertencias apropiadas
- Capacidad de utilizar cualquier puerto fuente local
- Capacidad para utilizar cualquier dirección de origen de la red de configuración local
- Incorporado en las capacidades de búsqueda de puertos, la aleatoriedad
- Capacidad incorporada de fuente-enrutamiento suelta
- Puede leer los argumentos de línea de comandos desde la entrada estándar
- Slow-sent modo, una línea cada N segundos
- Volcado hexadecimal de los datos transmitidos y recibidos
- Capacidad opcional de dejar pasar otras conexiones de servicio de programas establecidos
- Telnet-opciones de respuesta opcional (Netcat, 2013)

3.5.2. Mplayer

Es una herramienta de reproducción multimedia, esta herramienta multiplataforma gratuita es capaz de reproducir en su gran mayoría los diferentes tipos de formatos existentes para audio y video como MPEG, AVI, MP4, etc. Esta herramienta multimedia se originó en el año 2000 por Hungarian Árpád Gereöffy inicialmente creado para Linux, pero luego en el 2003 fue adaptado para funcionar en el resto de SO.

3.5.2.1. Principales formatos soportados de Mplayer

- (S)VCD (Super Video CD)
- CDRwin's .bin archivos de imagen
- DVD, incluyendo DVD encriptado
- MPEG1/2 (ES/PS/PES/VOB)
- Formato de archivo RIFF AVI
- Formato ASF/WMV/WMA
- Formato QT/MOV/MP4
- Formato RealAudio/RealVideo
- Archivos OGG/OGM
- Formato VIVO
- Formato FLI
- Formato NuppelVideo
- Formato yuv4mpeg
- Formato FILM (.cpk)
- Formato RoQ
- Formato PVA
- Matroska
- NSV - Nullsoft Streaming Video
- Soporte de streaming via http, RTP, RTSP, mms, mmst, mpst, sdp
- TV (The MPlayer Project, 2017)

3.5.2.2. Principales CODECS de video soportados por Mplayer

3.5.2.2.1. Video

- MPEG1 (VCD) y video MPEG2 (SVCD/DVD/DVB)
- MPEG4 en todas las variantes incluyendo DivX ;-), OpenDivX (DivX4), DivX 5 (Pro), Xvid
- Windows Media Video 7/8 (WMV1/2)

- Windows Media Video 9 (WMV3) (usando DLL x86)
- RealVideo 1.0, 2.0 (G2)
- RealVideo 3.0 (RP8), 4.0 (RP9) (usando bibliotecas Real)
- Sorenson v1/v3 (SVQ1/SVQ3), Cinepak, RPZA y otros codecs QuickTime comunes
- DV video
- 3ivx decoder
- Intel Indeo3 (3.1, 3.2)
- Intel Indeo 4.1 y 5.0 (usando DLL x86 o codecs XAnim)
- VIVO 1.0, 2.0, I263 y otras variantes H.263(+) (usando DLL x86)
- MJPEG, AVID, VCR2, ASV2 y otros formatos hardware
- FLI/FLC
- HuffYUV
- Varios formatos simples y antiguos del tipo RLE-like (The MPlayer Project, 2017)

3.5.2.2.2. Audio

- MPEG layer 1, 2, y 3 (MP3) audio
- AC3/A52 (Dolby Digital) audio (software o SP/DIF)
- AAC (audio MPEG4)
- WMA (DivX Audio) v1, v2
- WMA 9 (WMAv3), Voxware audio, ACELP.net etc (usando x86 DLLs)
- RealAudio: COOK, SIPRO, ATRAC3, DNET (usando bibliotecas Real)
- RealAudio: DNET y codecs antiguos
- QuickTime: Qclp, Q-Design QDMC/QDM2, MACE 3/6 (usando bibliotecas QT)
- Ogg Vorbis audio
- VIVO audio (g723, Vivo Siren) (usando DLL x86)
- Alaw/ulaw, (ms)gsm, pcm, *adpcm y otros formatos de audio simples y antiguos (The MPlayer Project, 2017)

3.5.3. Conectividad entre Raspberry a la Estación Base

Una vez que se realiza la instalación de la Red AdHoc, y la instalación de Netcat y Mplayer en los dispositivos Raspberry, es necesario probar si los equipos se encuentran conectados y son vistos en la Red propuesta para este proyecto que es RASPBERRY-UDLA; para lo cual desde la Estación Base se ingresa la dirección IP de cada uno de los nodos mediante el browser. Si los nodos se encuentran dentro de la red se puede visualizar la ventana de la aplicación de HSMM-PI como se muestra en la figura 62 dentro de la malla de la red MANET.

Es aquí donde se observa que cada nodo que se encuentra en la red ya que es posible verificar el nivel de potencia medido por porcentaje sobre el 100% en las barras azules, en esta ventana también se encuentra la información de cada nodo vecino como son nombre y la dirección IP del Raspberry como se muestra en la figura 72, se ingresa la dirección IP del nodo 2 en el browser, en la ventana se observa los vecinos que existen en la Red MANET con sus nombres y direcciones IP, con las barras de conectividad hacia cada uno de ellos.

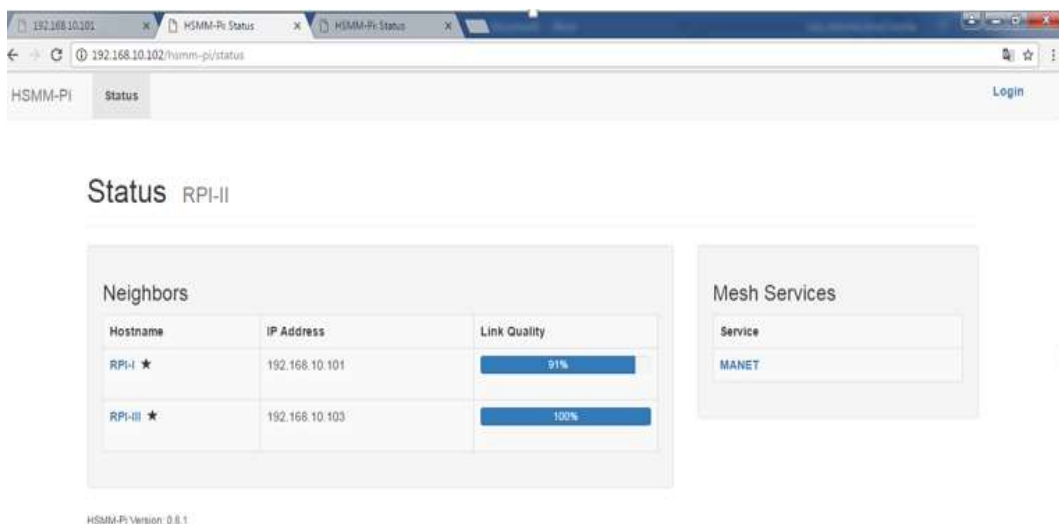


Figura 72. Presentación de nodos en la red

3.5.4. Reproducción de Video entre Raspberry y Estación Base

Para transmitir video desde el nodo Raspberry hacia la Estación Base se realizan los siguientes pasos:

- Se activa al terminal de comandos CMD.
- Se ingresa a la carpeta en donde se encuentran los archivos ejecutables de Netcat y Mplayer mediante el comando: `cd C:\Netcat y Mplayer`
- Una vez dentro de la carpeta, se debe iniciar Netcat y Mplayer, para dejar el puerto seleccionado en estado de escucha, mientras que Mplayer está listo para reproducir el tráfico que recibe por el puerto realizando el proceso de codificar para ser visualizado el video transmitido; Mplayer realiza esta operación utilizando códec H264, para esto se digita el siguiente comando:

Tabla 5.

Ejecución de video desde Estación Base UDP y TCP

Estación Base	
TCP	<code>nc64 -l -p 5001 mplayer -fps 31 -cache 1024-</code>
UDP	<code>nc64 -l -u -p 5001 mplayer -fps 31 -cache 1024-</code>

Tabla 6.

Ejecución de video desde Raspberry UDP y TCP

Raspberry	
TCP	<code>raspivid -t 0 -w 360 -h 360 -vf -hf -o - nc 192.168.10.100 5001</code>
UDP	<code>raspivid -t 0 -w 360 -h 360 -vf -hf -o - nc -u 192.168.10.100 5001</code>

- De esta manera en cuanto se recepte tráfico en el puerto de escucha, abre el Mplayer para que este tráfico sea procesado por la computadora y lo reproduzca automáticamente, este puede ser TCP como UDP, utilizando los comandos como se muestra en la Tabla 5 y Tabla 6.

El procedimiento debe ser activado en primer lugar en la estación base o en el dispositivo que recibe los datos y luego en el dispositivo que transmite los datos esto se da en este orden ya que al iniciar la transmisión el Netcat se encarga de establecer conexión para el tráfico de los datos o de la información a todos los dispositivos que tengan su puerto en estado de escucha si no encuentra ninguno este automáticamente cierra el tráfico como se muestra en la figura 73, donde se realiza la Tx de video.



Figura 73. Transmisión de video desde Raspberry a Estación Base

3.5.5. Diagrama Estación Base Gestión para Video

En la figura 74 se describe la gestión que realiza la estación base para permitir la comunicación y la transmisión de video desde uno de los nodos, la cual depende de los elementos expuestos para establecer conexión entre la base y el nodo, la ejecución tanto de los puertos seleccionados en escucha y envío de datos, la aplicación web que verifica la potencia de la señal en cuanto a la conexión y finalmente la reproducción de video mediante el Mplayer.

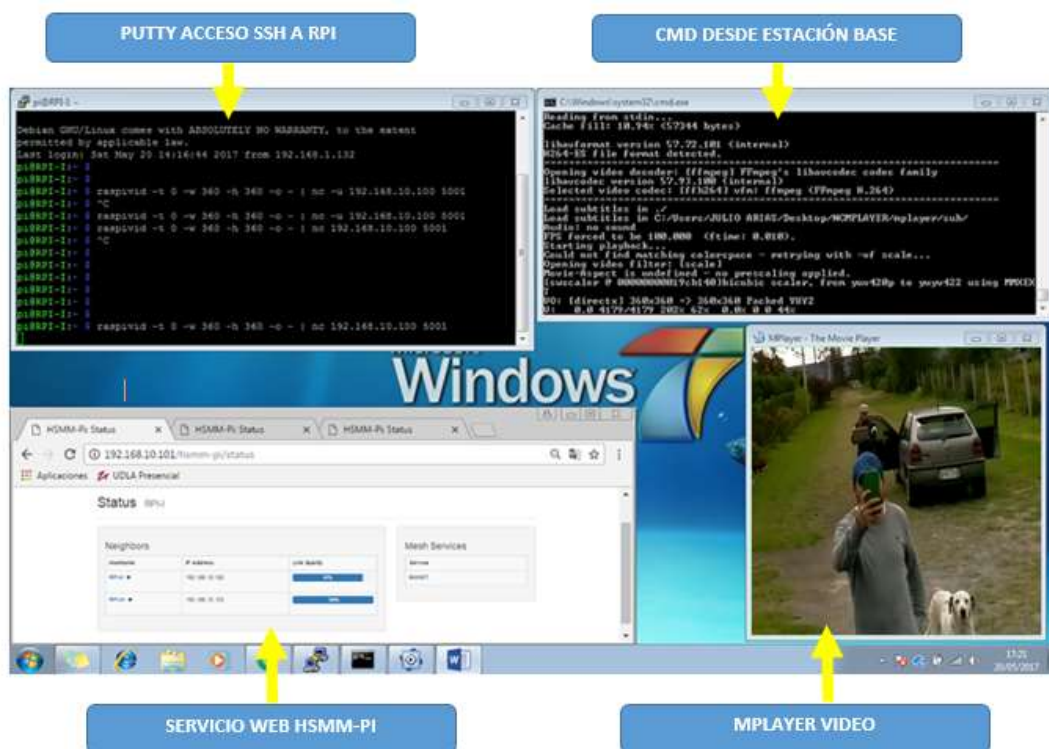


Figura 74. Diagrama Gestión para Video desde Nodo a Estación Base

4. CAPITULO V. PRUEBAS Y ANÁLISIS DE RESULTADO

En este capítulo se describen todas las pruebas realizadas con su respectivo análisis, según la ubicación geográfica que obtiene cada nodo (Raspberry Pi3), se presenta cuatro escenarios para la transmisión de video los cuales serán desarrollados a continuación, por cada escenario se tiene tres ambientes de prueba.

4.1. Primer escenario

En esta configuración todos los nodos se encuentran dentro del área de cobertura de la estación base como se muestra en la figura 75, en este escenario todos los nodos transmiten video directamente y puede ser de forma simultánea en el caso de requerirlo, ya que todos se pueden comunicar directamente con la estación base. La distancia máxima a la que los nodos se pueden alejar de la estación base es 76 metros, se debe tener en cuenta que los nodos mientras más se alejan de la estación base la potencia va disminuyendo mientras que la velocidad de transmisión aumenta considerablemente y se empieza a tener problemas en la calidad del video.

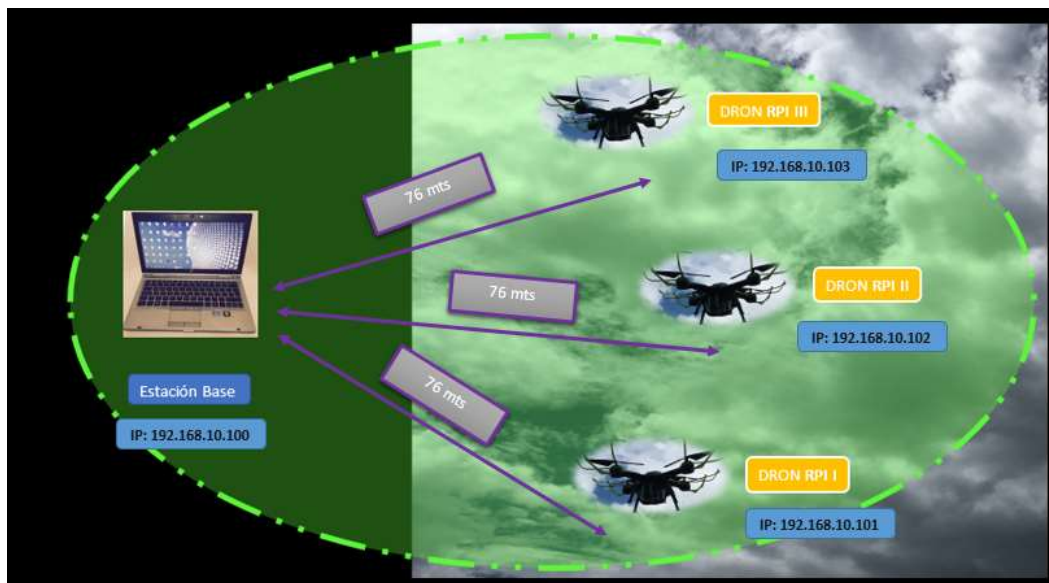


Figura 75. Primer Escenario (primeros 76 mts)

4.1.1. Ambiente Conjunto Shalom Ala Este

Estas pruebas fueron realizadas de forma terrestre con el fin de comprobar si los tres nodos establecen conexión directa con la estación base y de esta forma puedan transmitir video de forma independiente o simultánea, en la figura 76 se muestra la ubicación geográfica de cada nodo, teniendo en cuenta que cada uno de los nodos no sobrepasa los 40 metros de distancia.

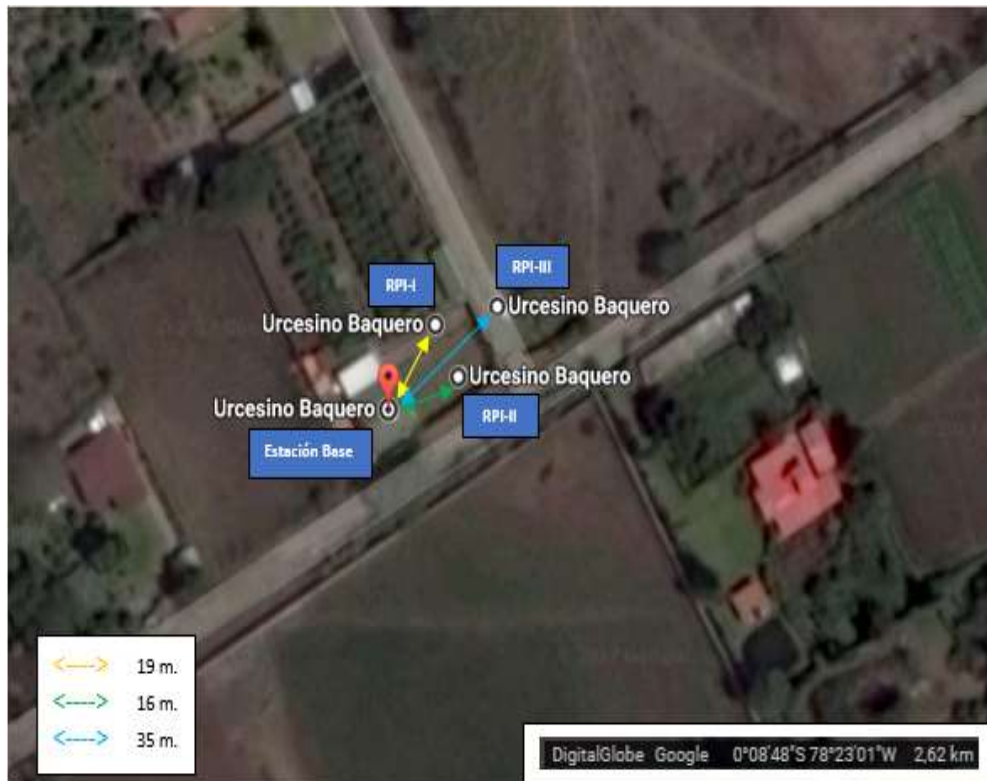


Figura 76. Ambiente Conjunto Shalom Ala Este (Escenario 1)

Adaptado de (Google Earth, 2017)

4.1.2. Ambiente Conjunto Shalom Ala Sur

En este ambiente de pruebas se pretende obtener los datos de las distancias máximas a las que se pueden encontrar cada uno de los drones con relación a la estación base, para poder obtener dichos resultados se utilizó un software para analizar las redes WiFi llamado *Acrylic_WiFi_Home* en el cual se puede ver los niveles de potencia presentes para establecer comunicación, adicional a esto, también se utilizó el software *Wireshark* en el cual se puede obtener una lectura de los protocolos que se está usando en la red, por otro lado cada uno de los nodos cuenta con una aplicación propia de la herramienta HSMM-PI con interfaz web, en la cual se puede ver la calidad del enlace que mantiene cada uno con respecto a cada uno de sus vecinos. Como se muestra en la figura 87 los nodos están ubicados exactamente a la misma distancia de la estación base

la que con los datos arrojados resulta ser la máxima distancia alcanzable para poder obtener video, el cual presenta ya problemas de latencia, debido a que mientras mayor es la distancia la potencia disminuye y la latencia es mayor. Primero se muestra las capturas de las pruebas en un estado inicial (Figuras 77-87) en el cual la distancia de los nodos a la base no supera un metro de distancia.

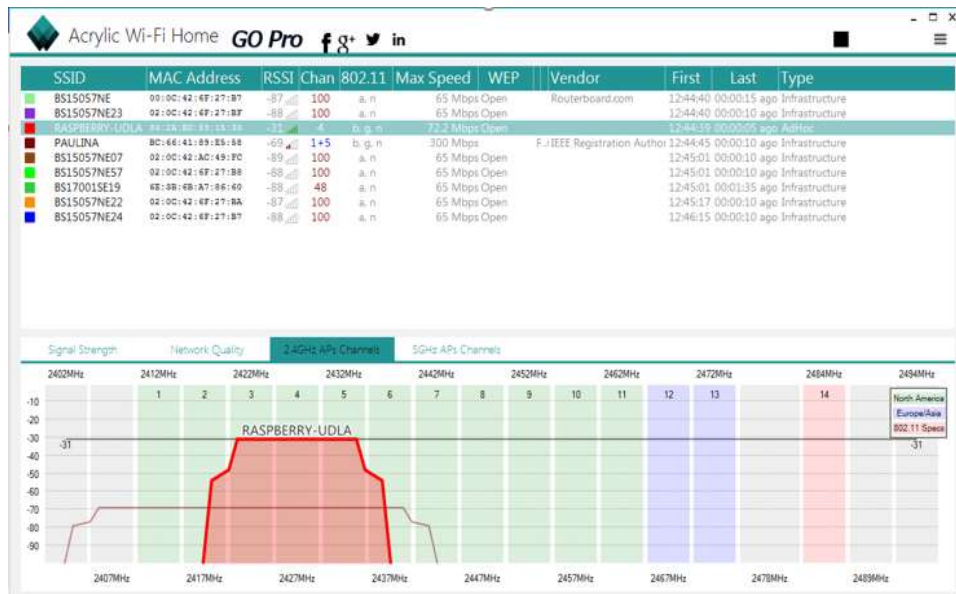


Figura 77. Potencia de red MANET RASPBERRY-UDLA (Distancia 1mt)

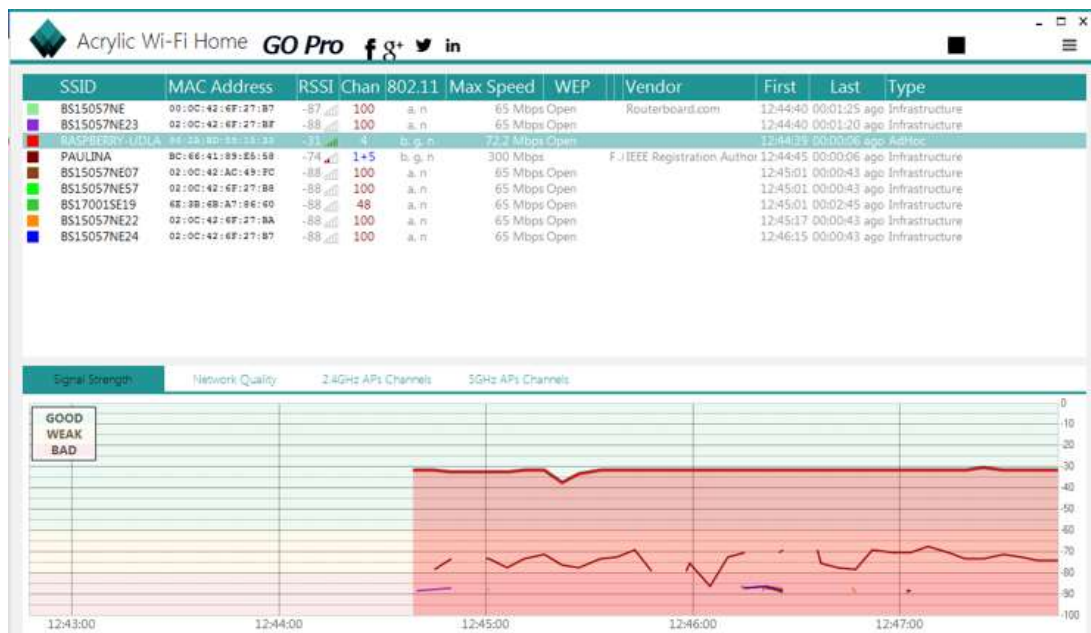


Figura 78. Intensidad de señal red MANET RASPBERRY-UDLA (Distancia 1mt)

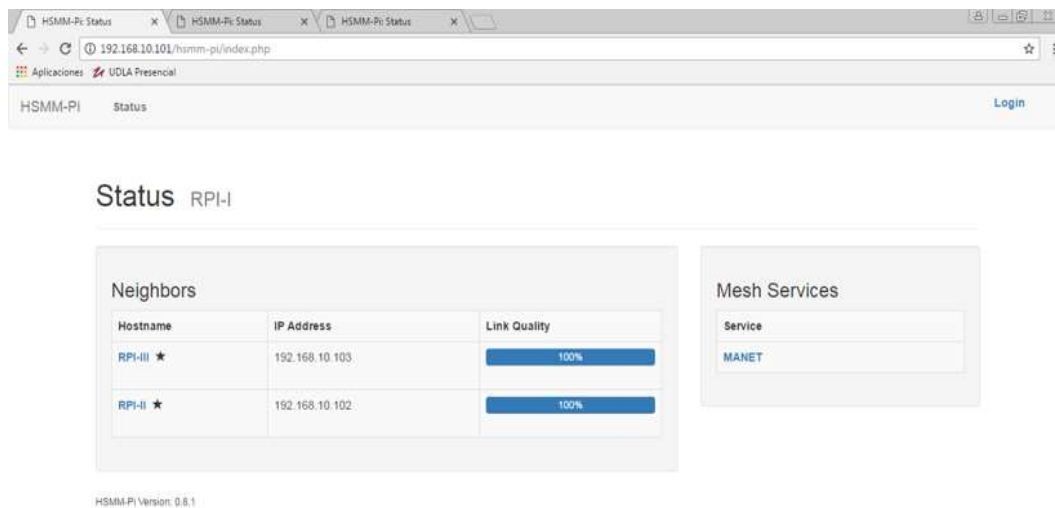


Figura 79. Calidad del Enlace desde RPI-I (Distancia 1mt)

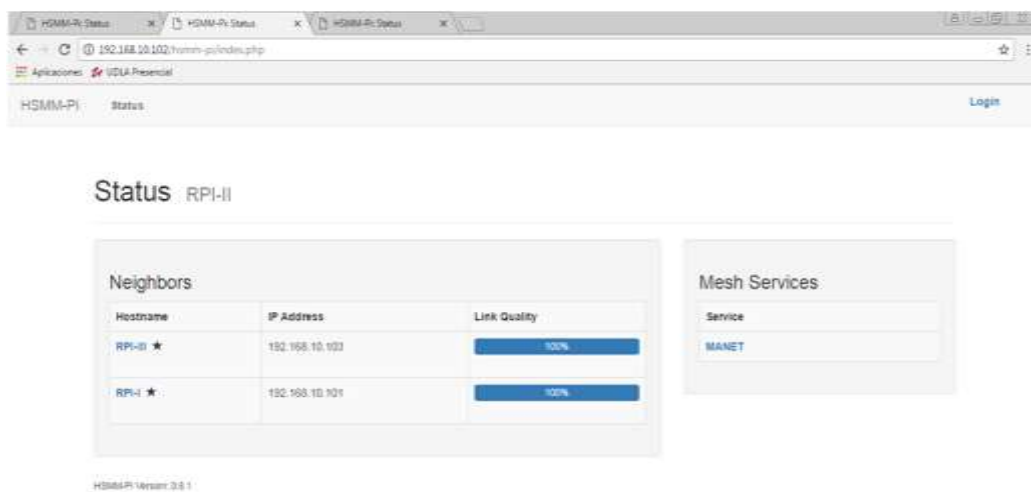


Figura 80. Calidad del Enlace desde RPI-II (Distancia 1mt)

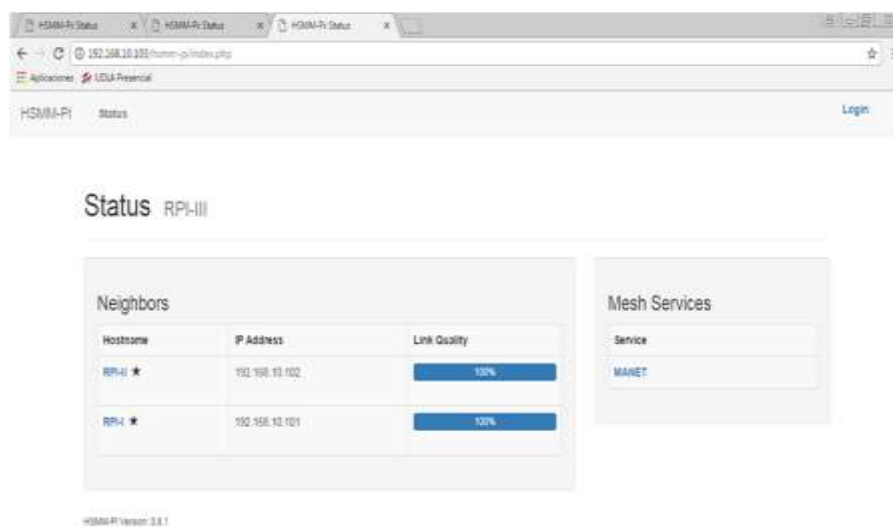


Figura 81. Calidad del Enlace desde RPI-III (Distancia 1mt)

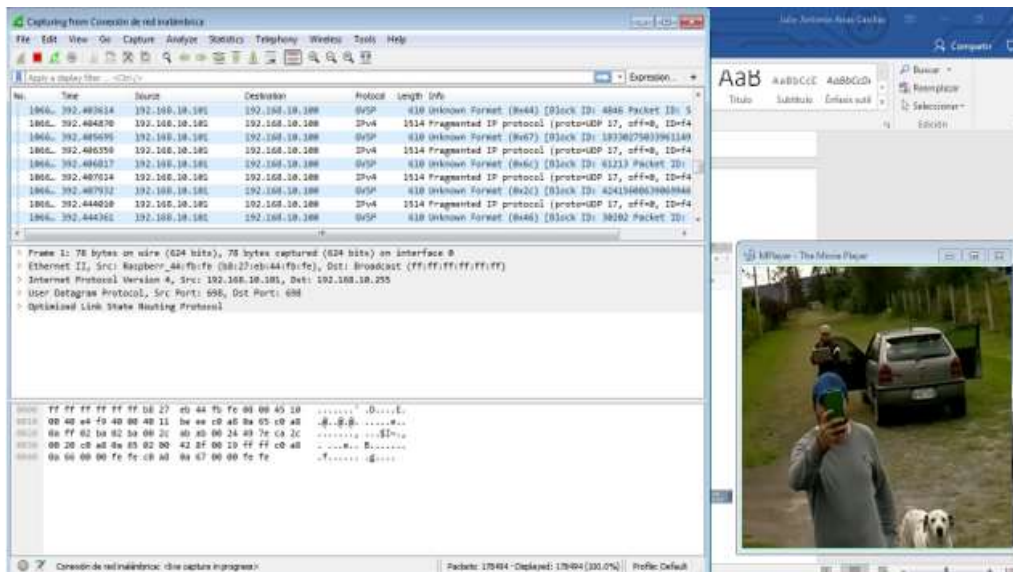


Figura 82. Captura de Tráfico y Video (Distancia 1 mt)

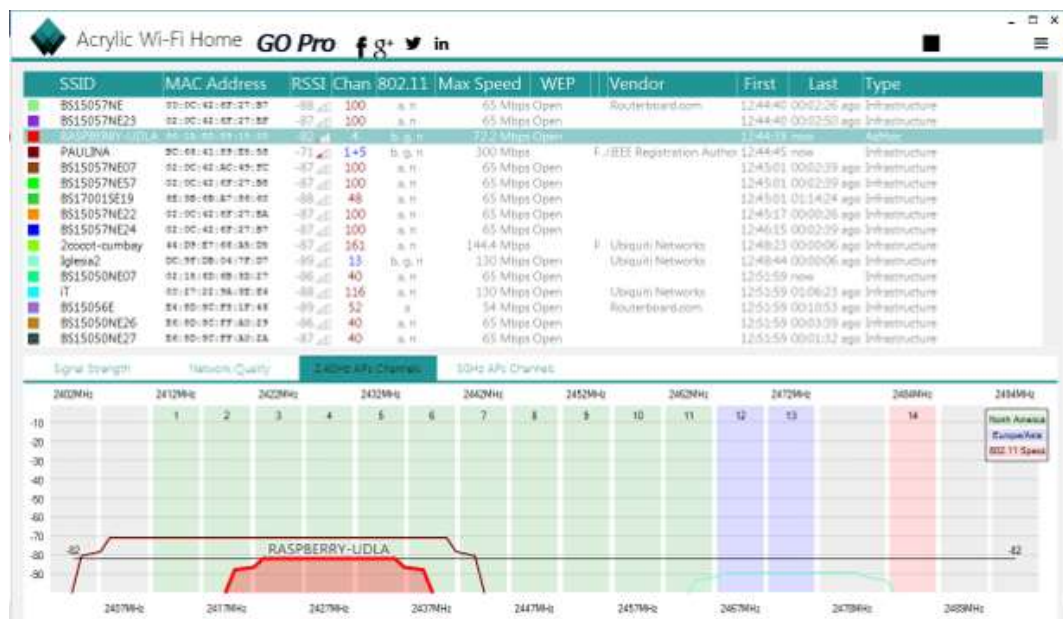


Figura 83. Potencia de red MANET RASPBERRY-UDLA (Distancia 76 mts)

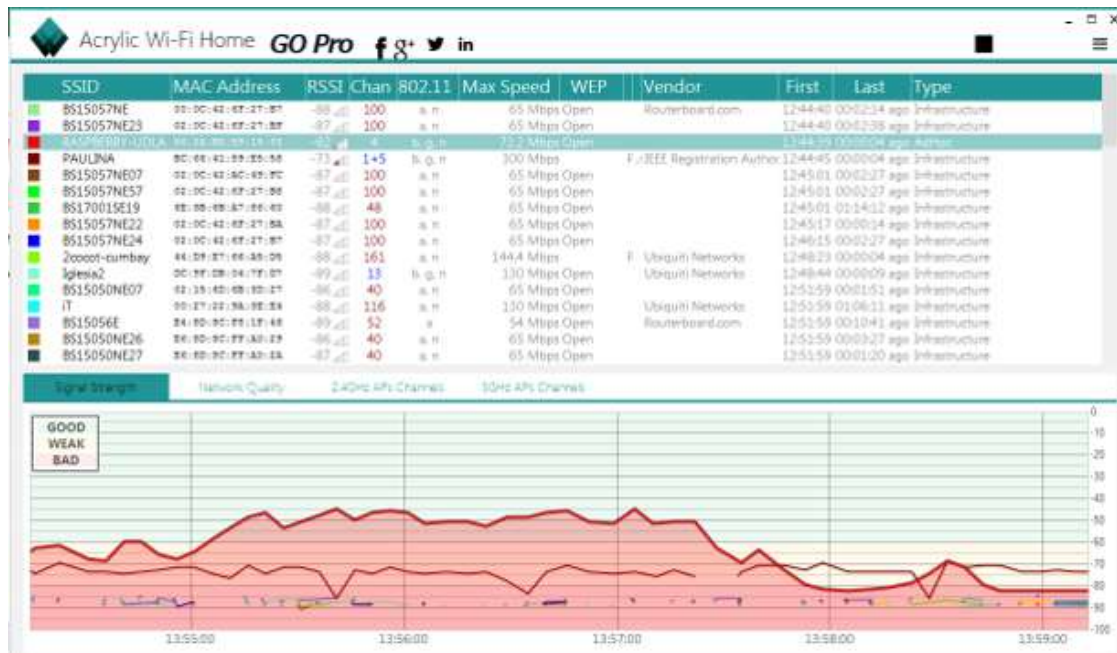


Figura 84. Intensidad de señal red MANET RASPBERRY-UDLA (Distancia 76 mts)

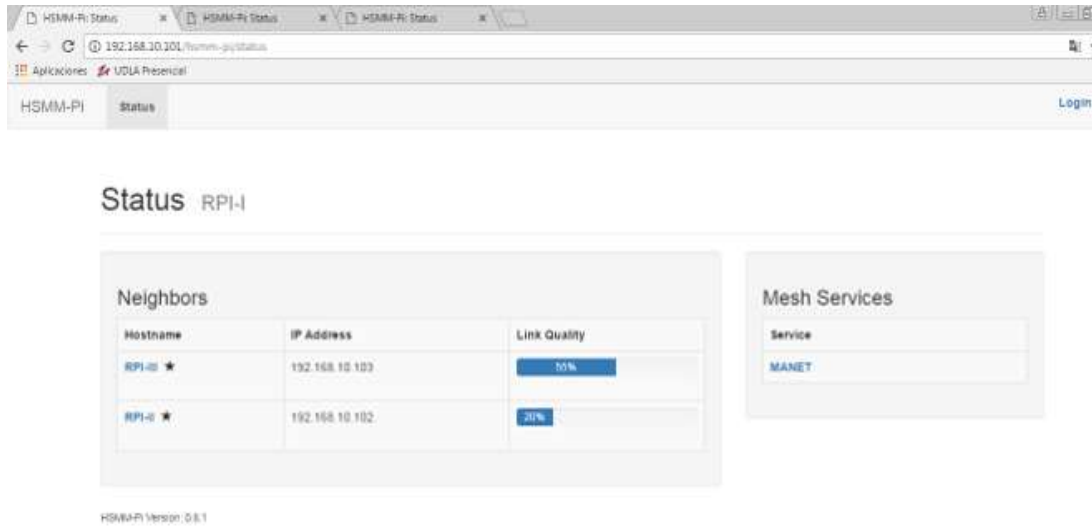


Figura 85. Calidad del Enlace desde RPI-I (Distancia 76 mts)

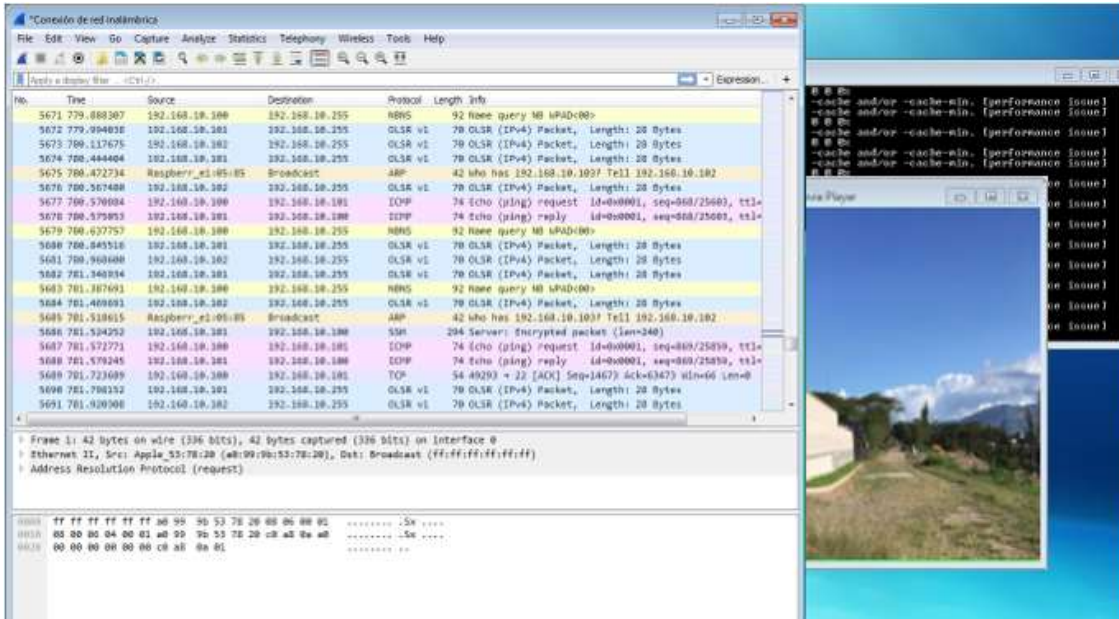


Figura 86. Captura de Tráfico y Video (Distancia 76 mts)



Figura 87. Ambiente Conjunto Shalom Ala Sur (Escenario 1)

Adaptado de (Google Earth, 2017)

4.1.3. Ambiente Campus UDLA-QUERI

Las pruebas en este ambiente fueron realizadas con el fin de validar la configuración de los cambios en la selección del canal de transmisión, dependiendo cuan congestionados se encuentran los 11 canales correspondientes a la banda de 2,4GHz de la tecnología WiFi, ya que las pruebas

realizadas en los ambientes anteriores fueron realizadas en un ambiente sin mucha congestión de señales como se puede ver en la figura 88.

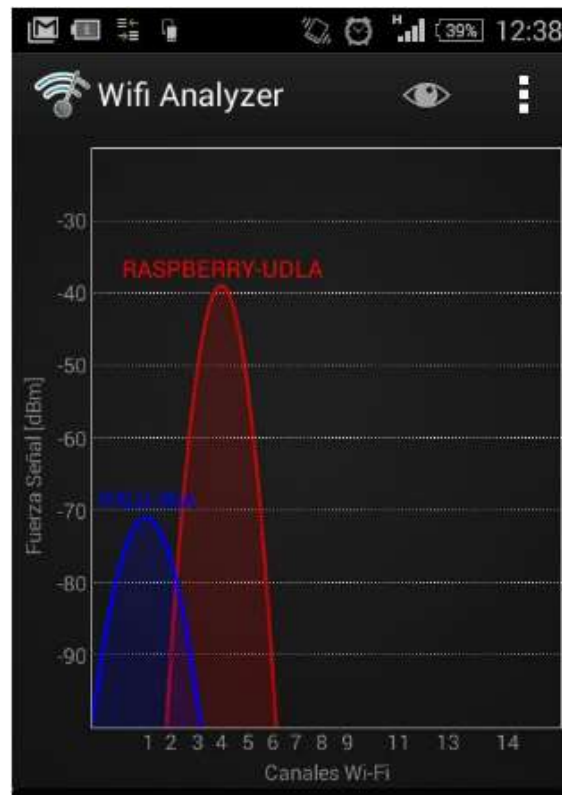


Figura 88. Uso de Canales Banda WiFi Conjunto Shalom

En la banda antes ya mencionada, cuando se realizaron pruebas en el bloque cuatro del campus UDLA Queri, al momento de transmitir video se presentaron varios problemas entre estos el más importante y considerable fue la interferencia con otras señales que se encontraban en el mismo canal de transmisión, como se muestra en la siguiente figura 89.



Figura 90. Ambiente UDLA-Queri (Escenario 1)

Adaptado de (Google Earth, 2017)

4.2. Segundo y Tercer escenario

En este escenario todos los ambientes se basarán en la misma distribución geográfica de los nodos, de esta manera el segundo escenario queda como se muestra en la figura 91, donde dos drones se mantendrían dentro del área de cobertura (primeros 76 metros) de la estación base y el tercer dron sale de esta área de cobertura e ingresa a la segunda área de cobertura (segundos 76 metros), en los cuales establece comunicación directa con cualquier nodo de los que están dentro de la primera área pero no puede establecer conexión directa con la base, de esta manera se puede extender el área de cobertura total del

sistema teniendo un alcance de 152 metros máximos entre el dron más alejado y la estación base, el tercer escenario es analizado conjuntamente con el segundo escenario debido a que las áreas de cobertura no se modifican, únicamente al poder transmitir de manera simultánea desde todos los drones en el tercer escenario salen de la primera área dos nodos y en la primera área únicamente se mantiene un nodo el cual sirve como puente para poder llegar hasta la estación base, como se muestra en la figura 92.



Figura 91. Segundo Escenario (152 mts)

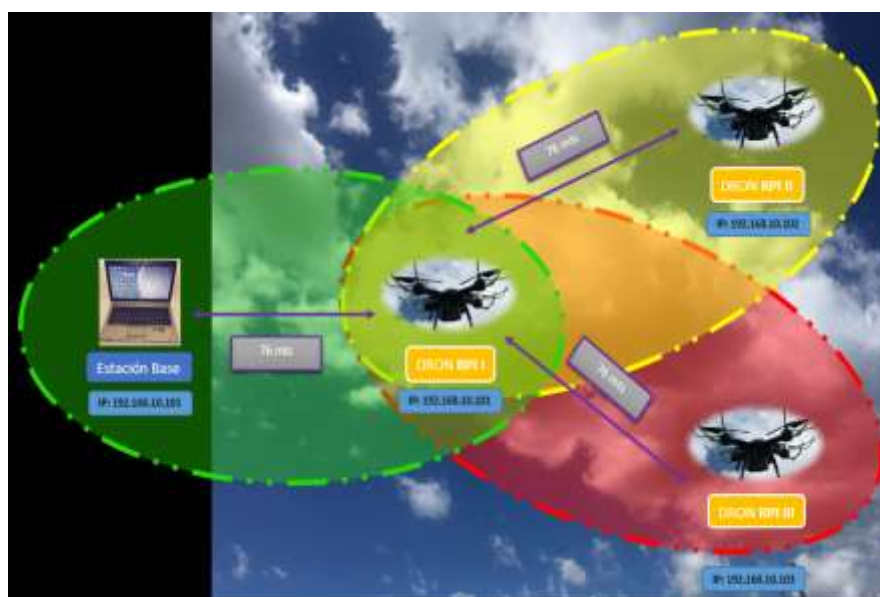


Figura 92. Tercer Escenario (152 mts)

4.2.1. Ambiente Conjunto Shalom Ala Este

En este ambiente las pruebas se basaron en comprobar la funcionalidad del protocolo OLSR, debido a que al encontrarse un nodo sin poder mantener comunicación directa con la estación base se ve obligado a buscar una nueva ruta para que el video pueda llegar a la base, con ayuda del protocolo OLSR, el nodo que se encuentra fuera de la primera área busca la mejor ruta, al tener dos opciones por donde llegar hasta el destino, dependerá cuál de los otros dos nodos le dé mejor prestación, en el caso de que uno de los dos falle, no se pierde la transmisión pues queda un último camino por donde llegar, en la figura 93 se puede ver cómo están ubicados los nodos de manera geográfica, según lo detallado antes. Para el tercer escenario se trabaja con las mismas distancias máximas de alcance, la única diferencia con el segundo escenario es que se encuentran dos nodos fuera de la primera área de alcance, limitando a un solo camino por donde se pueda transmitir video desde los dos drones externos hacia la estación base.

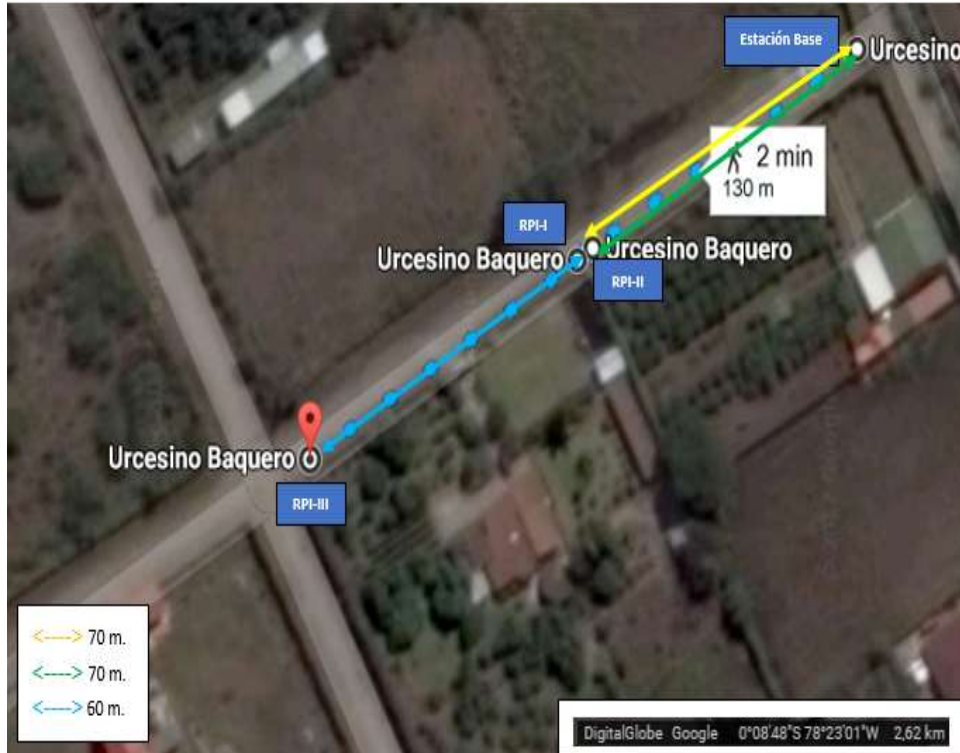


Figura 93. Ambiente Conjunto Shalom Ala Este (Escenario 2)

Adaptado de (Google Earth, 2017)

4.2.2. Ambiente Conjunto Shalom Ala Sur

Al igual que en el primer escenario las pruebas realizadas en los escenarios segundo y tercero en el ambiente ala sur se realizaron con el fin de determinar cuáles son las distancias máximas que se puede alcanzar con los drones dependiendo de su configuración.

Según el segundo y tercer escenario se determinó que la distancia máxima alcanzable es de 76 metros al igual que en la primera área como se muestra en la figura 91, pues al sobrepasar esta distancia las perdidas en la transmisión se incrementan.

Con ayuda de los mismos programas que se utilizó en el primer escenario se obtuvo las mediciones tanto de niveles de potencia como información de los protocolos que se están utilizando en la red como se muestra en las figuras 94-100.

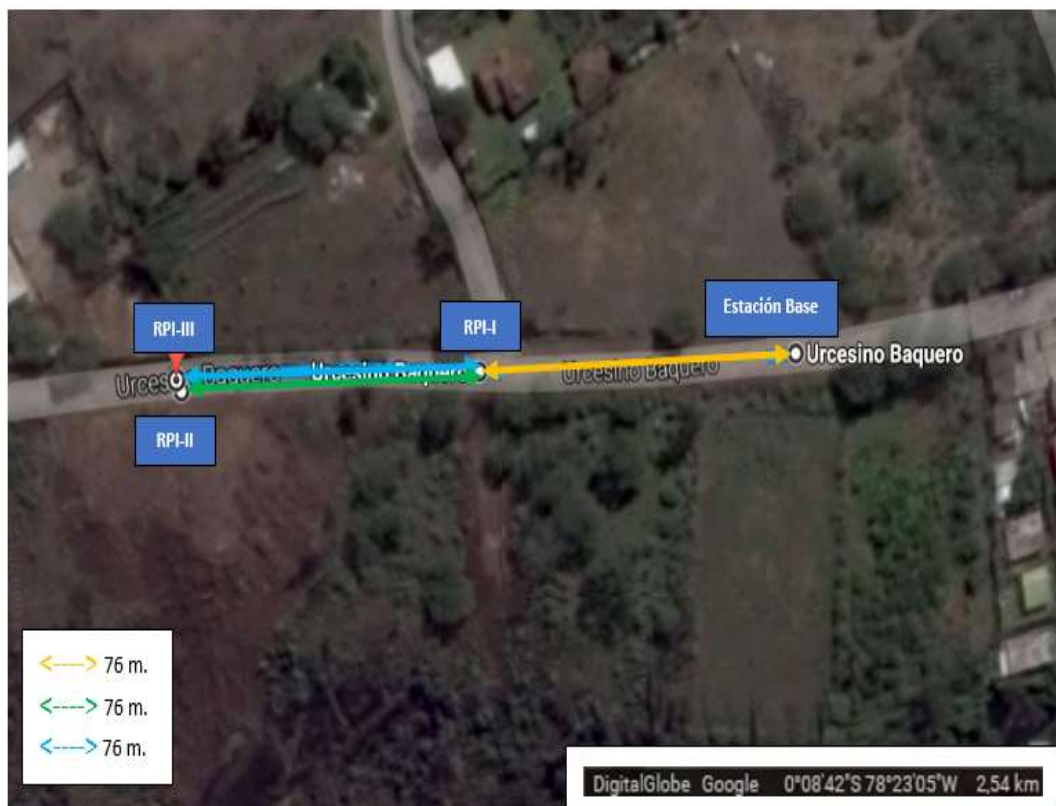


Figura 94. Ambiente Conjunto Shalom Ala Sur (Escenario 3)

Adaptado de (Google Earth, 2017)

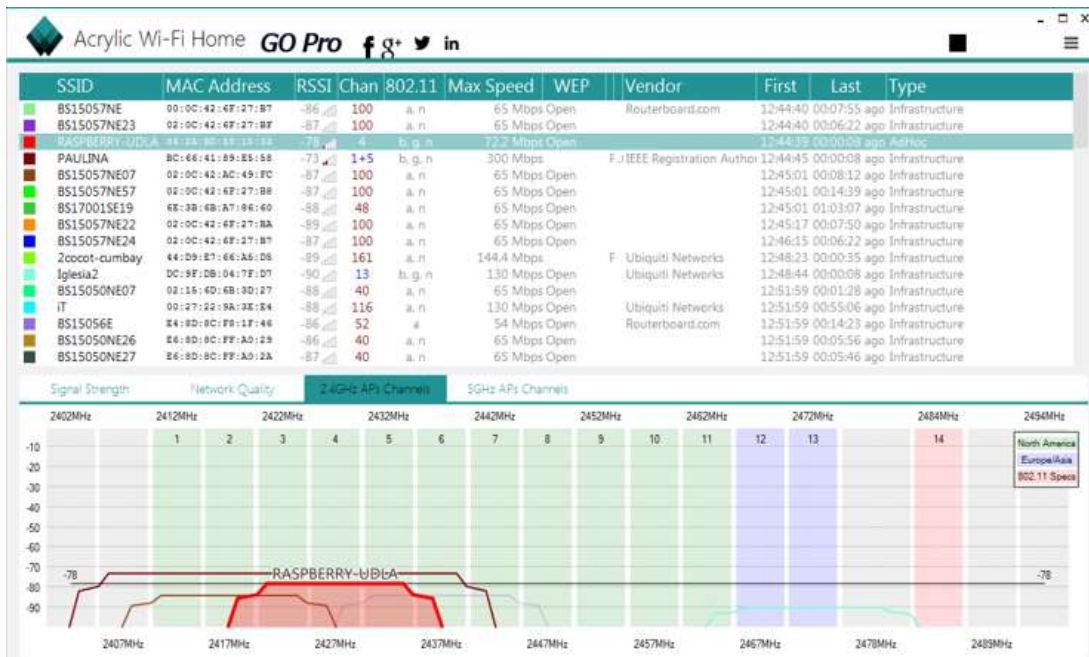


Figura 95. Potencia de red MANET RASPBERRY-UDLA (Distancia 152 mts)

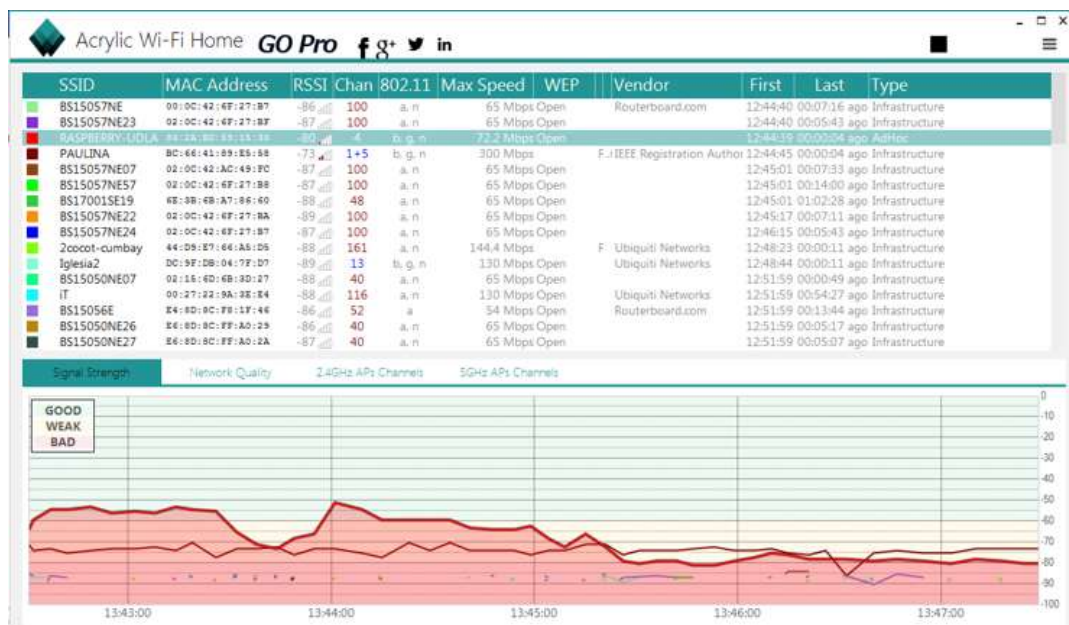


Figura 96. Intensidad de señal red MANET RASPBERRY-UDLA (Distancia 152 mts)

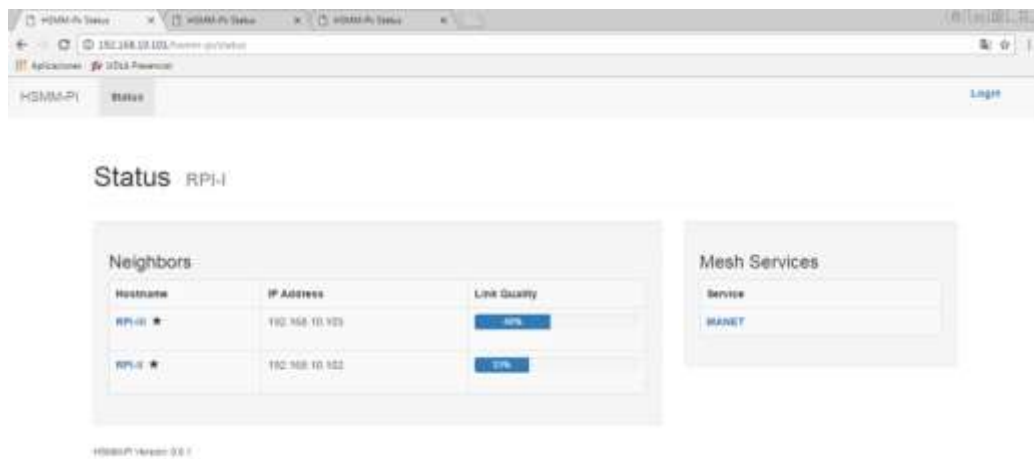


Figura 97. Calidad del Enlace desde RPI-I (Distancia 152 mts)

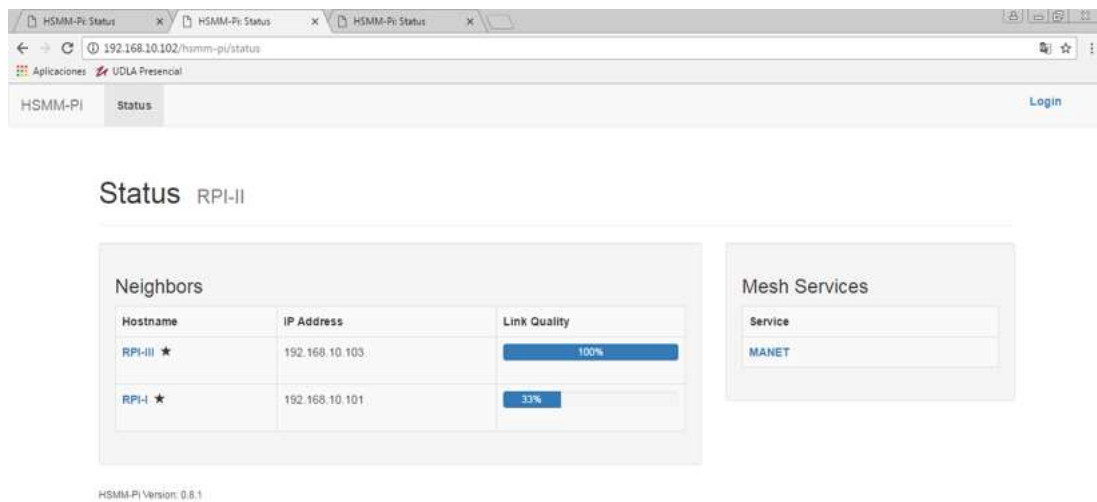


Figura 98. Calidad del Enlace desde RPI-II (Distancia 152 mts)

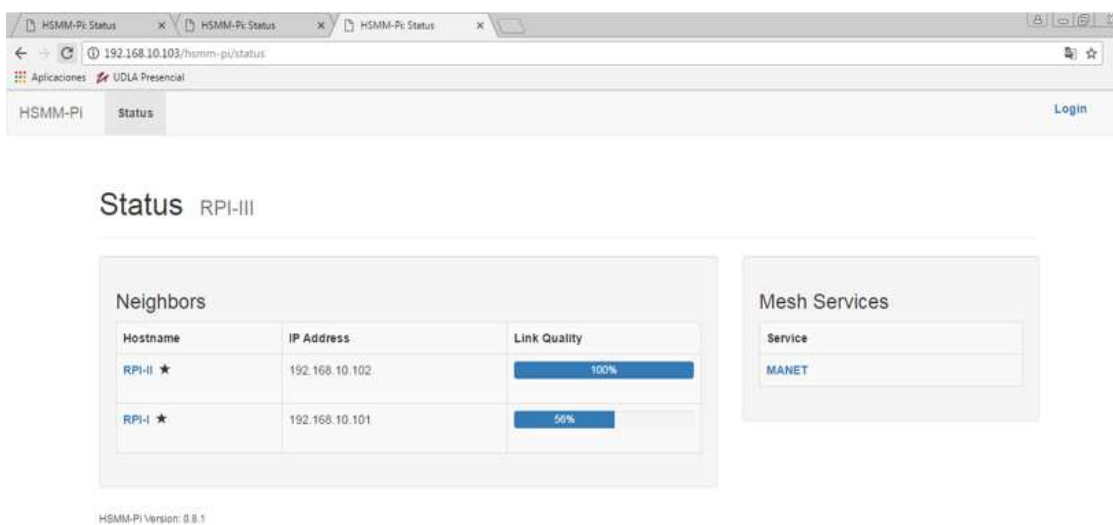


Figura 99. Calidad del Enlace desde RPI-III (Distancia 152 mts)

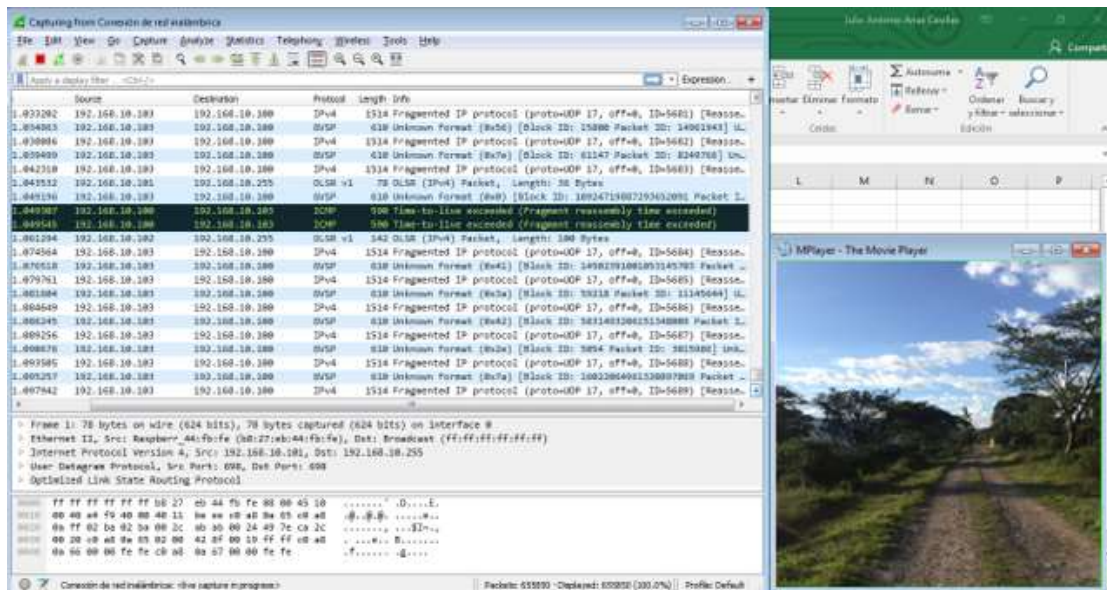


Figura 100. Captura de Tráfico y Video (Distancia 152 mts)

4.2.3. Ambiente Campus UDLA-QUERI

En la figura 101 se puede ver la ubicación geográfica de los nodos según los escenarios antes descritos, no se realiza capturas de pruebas debido a que son las mismas pruebas realizadas en el ambiente anterior, solo se comprueba que puedan transmitir los dos nodos más alejados de la base.



Figura 101. Ambiente UDLA-Queri (Escenario 3)

Adaptado de (Google Earth, 2017)

4.3. Cuarto escenario

En este escenario solo se desarrolla los ambientes Conjunto Shalom Ala Sur y Campus UDLA-QUERI, este se debe a que en el ambiente Conjunto Shalom Ala Este las pruebas son terrenas, recordar que las pruebas realizadas en este ambiente tenían como objetivo comprobar la existencia de enrutamiento, al ser terrenas no se pudo separar los nodos lo suficiente para que estos puedan tener comunicación únicamente con su vecino continuo. A continuación, en la figura 102 se explica cómo se encuentran ubicados los nodos con la finalidad de alcanzar la mayor distancia permitida por las características de los equipos y la red.

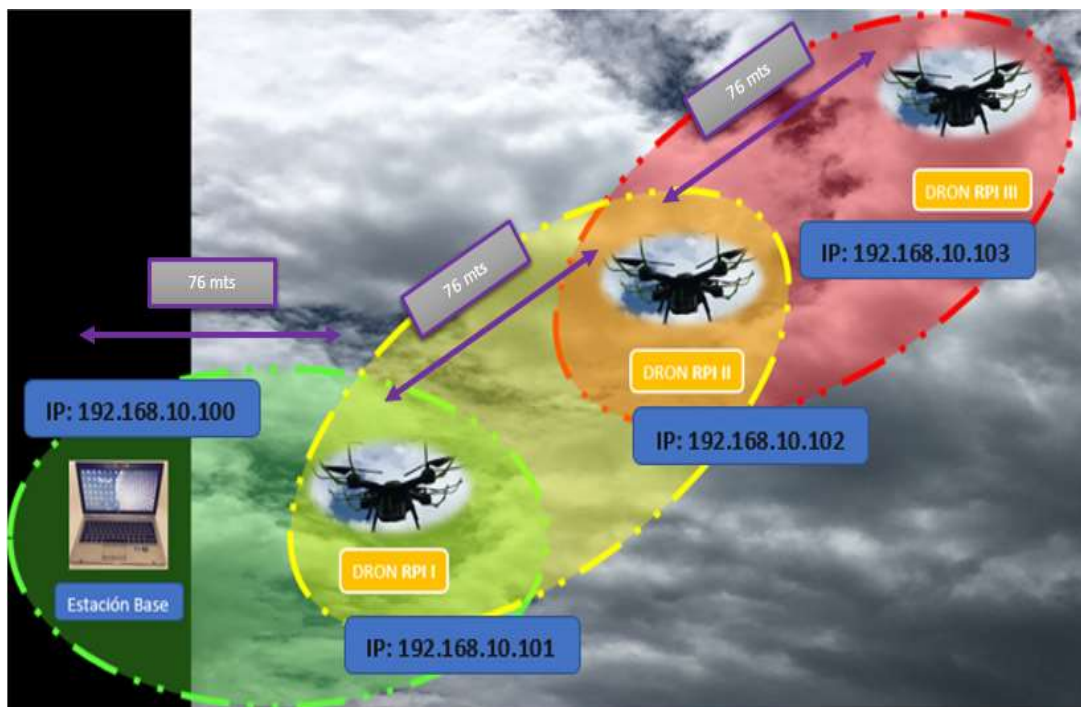


Figura 102. Cuarto Escenario (228 mts)

4.3.1. Ambiente Conjunto Shalom Ala Sur

En este ambiente es donde se puede realizar las pruebas de alcance de mejor manera en el cual se pudo determinar la distancia del alcance máximo permitido en la red MANET, el cual consta de tres áreas de 76 metros cada una dando un total de 228 metros en el área total como se muestra en la figura 103, teniendo en cuenta que mientras se encuentren en el límite pero dentro del área de cobertura los drones pueden transmitir con mayor latencia y menor potencia, si un nodo sobrepasa en su totalidad estas áreas, mientras mayor es la distancia se va a tener mayores complicaciones para la transmisión, hasta salir definitivamente del alcance y perder comunicación.



Figura 103. Ambiente Conjunto Shalom Ala Sur (Escenario 4)

Adaptado de (Google Earth, 2017)

Una vez más las distancias máximas alcanzadas se detectaron gracias al software instalado en el equipo base, con el cual se puede validar valores como potencia, protocolos usados en la red y calidad de enlace, en las siguientes figuras 104-107, se observan valores que justifican lo antes mencionado.



Figura 104. Potencia de red MANET RASPBERRY-UDLA (Distancia 228 mts)

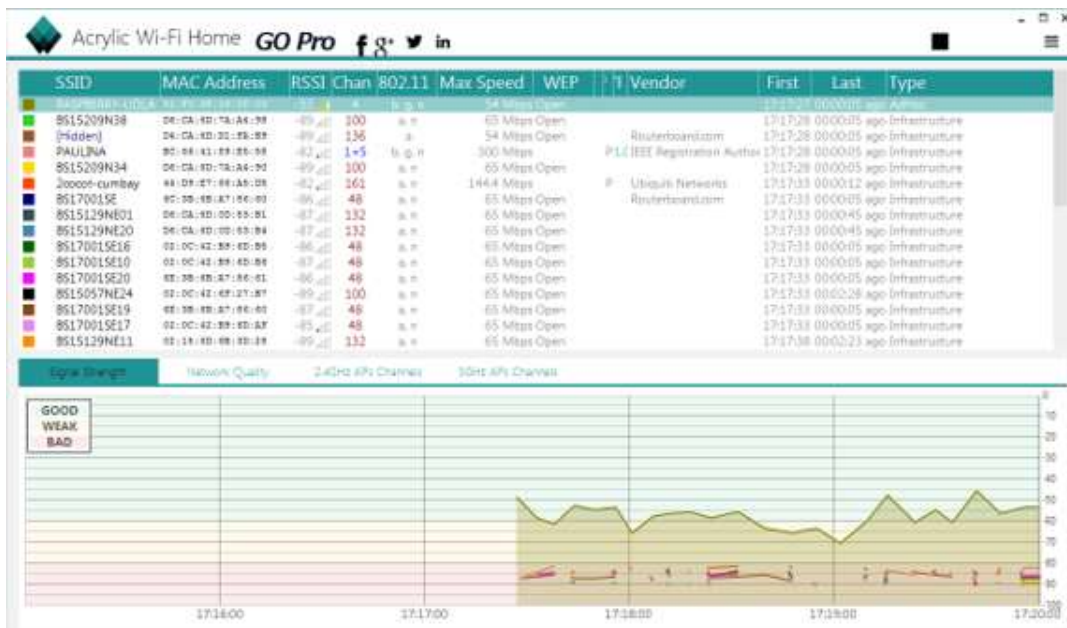


Figura 105. Intensidad de señal red MANET RASPBERRY-UDLA (Distancia 228 mts)

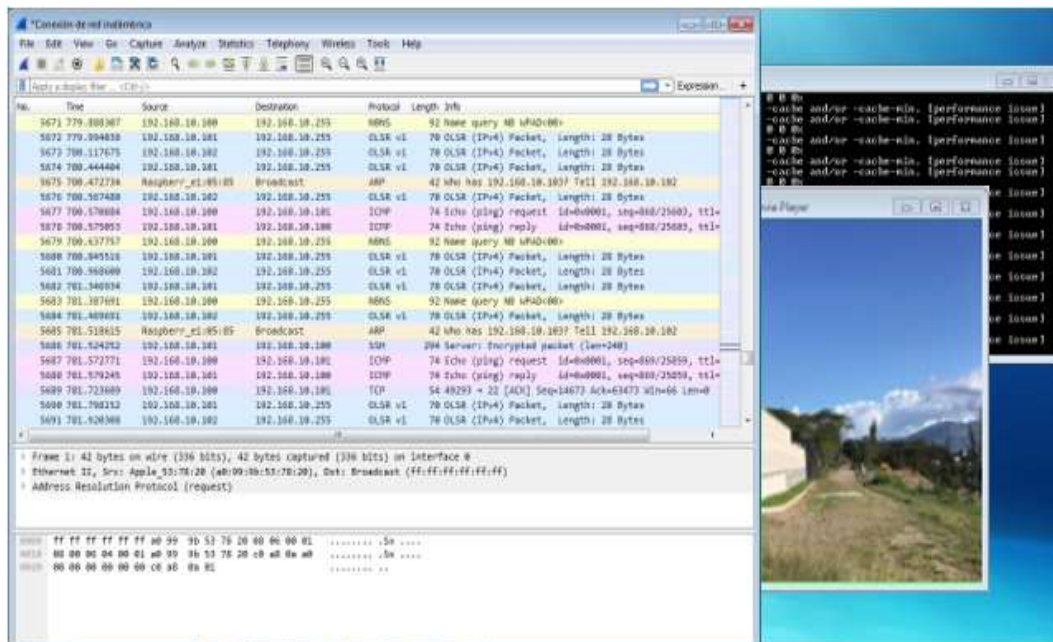


Figura 106. Captura de Tráfico y Video (Distancia 228 mts)

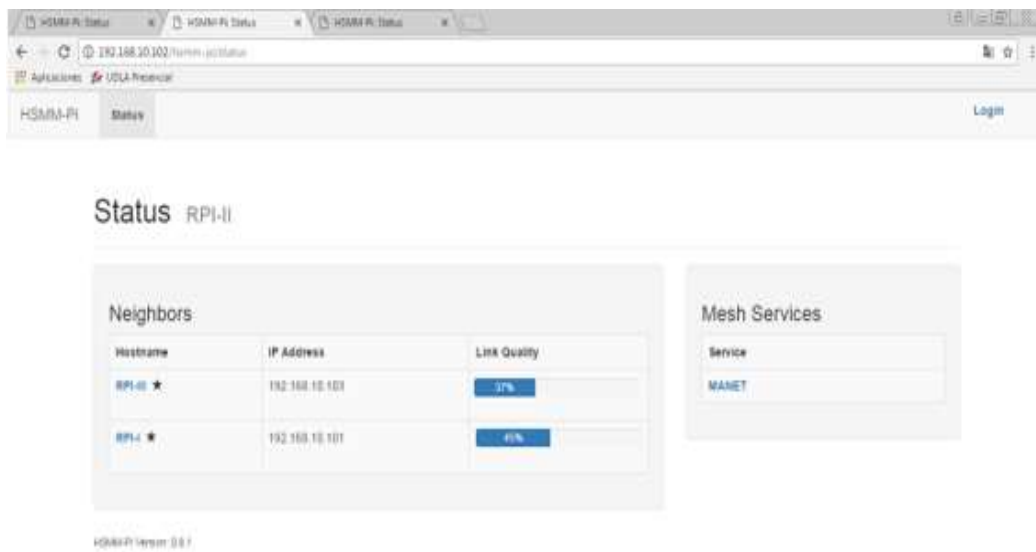


Figura 107. Calidad del Enlace desde RPI-II (Distancia 228 mts)

4.3.2. Ambiente Campus UDLA-QUERI

En el campus Queri de la universidad se realizó la misma prueba, en el cual se demuestra que el área máxima de cobertura no solo puede ser en línea recta, debido que el área de cobertura es de 360°, esta puede tomar varias direcciones mientras se mantengan en el área de cobertura como se muestra en la figura 108.



Figura 108. Ambiente UDLA-Queri (Escenario 4)

Adaptado de (Google Earth, 2017)

4.4. Prueba Fina

La prueba final fue realizada en el parque metropolitano, norte de la ciudad de Quito, en el cual se pudo comprobar el funcionamiento del prototipo en vuelo, la prueba consto en transmitir desde dos nodos en movimiento, uno acoplado al dron, el segundo en un carro a control remoto, los cuales llegan a la estación base a través del tercer nodo.

El nodo acoplado al dron fue alejado de la estación base a tal punto que la comunicación que realizaba con la estación base fue a través del nodo más cercano a la estación, luego el dron se alejaba aún más con el fin de perder la comunicación con cualquiera de los nodos restantes y la estación base llegando a perder la transmisión de video, después de esto el dron se reincorporaba al

área de cobertura de la red y se retomaba la transmisión de video de manera automática, comprobando con esto la automatización en la creación de la red MANET en cuanto a retomar un camino para llegar al destino gracias al protocolo de enrutamiento OSLR, así como al momento de irse alejando de la estación base hacía uso de los nodos adicionales para poder llegar a establecer comunicación con la estación base, en las figuras 109 – 111 se tiene registros fotográficos de la prueba antes descrita.



Figura 109. Dron con RPI3 en vuelo



Figura 110. Estación base y nodos acoplados en Dron y carro a control remoto

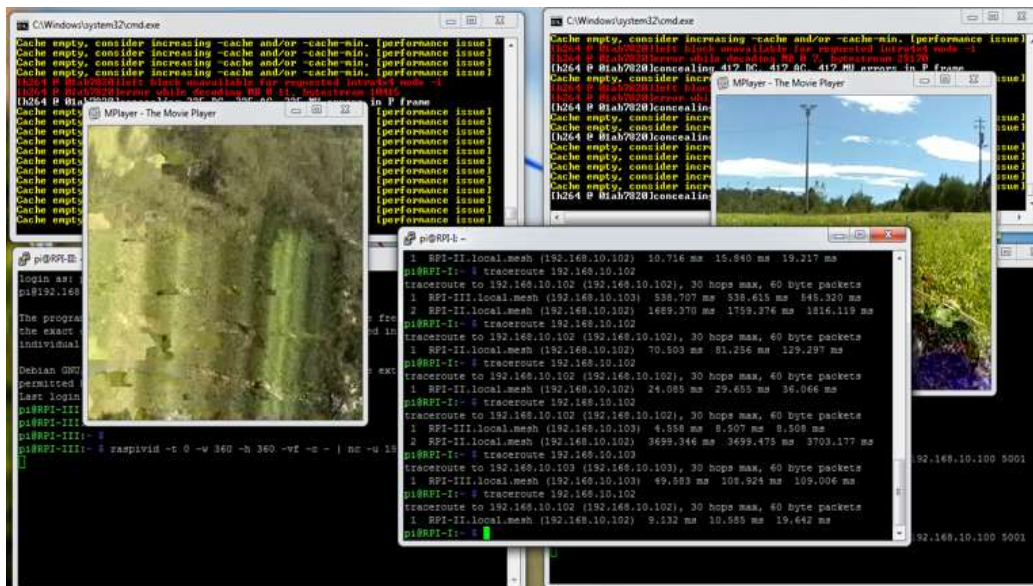


Figura 111. Transmisión de video desde dos nodos en movimiento

4.5. Consolidado

Como un consolidado de los cuatro escenarios podemos resaltar lo siguiente:

- En el primer escenario existen las siguientes opciones de transmisión, una cuando todos los nodos realizan la transmisión de video de manera simultánea, en este caso todos los nodos pueden tener configurados el mismo puerto para la transmisión y recepción, pero es recomendable se realice la configuración de puertos distintos para cada nodo, con esto se evita que el canal se sature y se presenten problemas como latencia, el segundo caso es cuando únicamente dos nodos transmiten teniendo en cuenta lo antes señalado y el tercer caso únicamente un solo nodo transmite, para los dos últimos casos antes señalados los nodos que no transmiten no cumplen ninguna función adicional, puesto que al encontrarse los nodos dentro de la primera área de cobertura transmiten de forma directa a la estación base.
- Para el segundo y tercer escenario los casos son distintos, pues en estos escenarios uno o dos drones respectivamente pueden salir del área de cobertura directa con la estación base, encontrándose entre los 76 y 152

metros, en estos escenarios la transmisión de los nodos más externos utilizan a los o el nodo respectivamente como intermediario en la red para poder alcanzar el destino que es la estación base, al diferenciar cada uno de los escenarios tenemos que en el segundo escenario únicamente un dron sale de su área de cobertura directa con la estación base, en este caso para poder llegar al destino puede enviar la información por medio de cualquiera de los dos nodos que se encuentran dentro de los 76 metros o en el tercer escenario son dos los nodos que se van a encontrar en el área entre 76 y 152 metros, se puede realizar la transmisión simultánea de los nodos o por separado, se debe tener en cuenta que en este caso solo un nodo trabajaría como intermediario para que pueda la información llegar a la estación base.

- En el cuarto escenario, por la ubicación geográfica se pudo conocer la distancia máxima en la cual se puede transmitir desde el nodo mucho más externo hasta la base teniendo en cuenta que cada nodo estaría ubicado en una de las áreas ya antes señaladas, a la hora de transmitir información los dos nodos restantes van a servir como intermediarios para que la información pueda llegar hasta su destino.

4.6. Análisis de Nivel de Potencia

Según la tabla 7 de datos obtenidos en el levantamiento de información correspondiente a las pruebas realizadas en el primer escenario, la gráfica resultante como se muestra en la figura 112, indica prácticamente lo que ya se trató en capítulos anteriores, mientras la distancia entre la estación base y los nodos se va incrementando, el nivel de potencia disminuye, esto se convierte en un problema debido a que si en el mismo canal se encuentran más señales de redes vecinas y estas a su vez tienen un mejor nivel de potencia que la señal de nuestra red, la misma se verá fuertemente afectada. No se realiza toma de datos en los demás escenarios, debido a que la imagen resultante sería prácticamente la misma, esto debido a que el análisis sería únicamente dentro de los 76 metros de cobertura.

Tabla 7.

Toma de Datos

DISTANCIA (m)	NIVEL POTENCIA (dbm)	VIDEO (latencia)
0	-30	REAL
10	-57	REAL
20	-70	REAL
30	-74	REAL
40	-77	MEDIO
50	-79	MEDIO
60	-80	MEDIO
70	-82	MALO

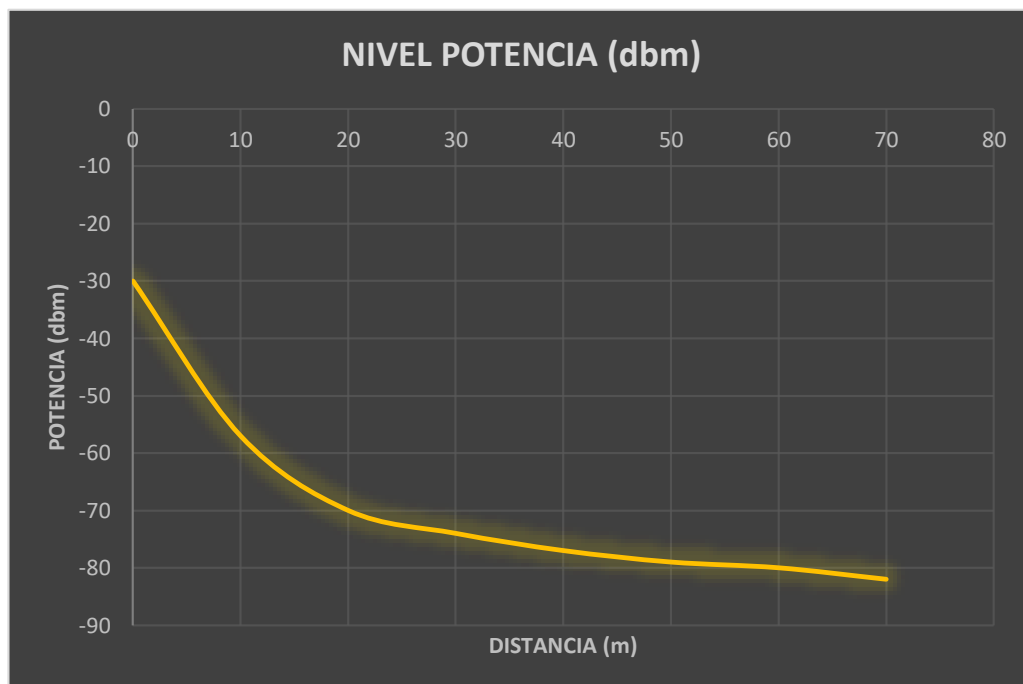


Figura 112. Grafico Potencia Vs Distancia para Tx

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El diseño del prototipo para el sistema de comunicación conformado por 3 nodos móviles y una estación base permiten se pueda establecer la transmisión de video en tiempo real; de tal manera que el video es receptado de forma simultánea desde cada uno de los nodos hacia la estación base, esto se logra mediante el uso de los dispositivos Raspberry Pi 3 en conjunto con las herramientas de software tanto libres como licenciadas para cubrir las necesidades del sistema de comunicación en la red mallada.

El protocolo OSLR de enrutamiento utilizado para el descubrimiento de nodos adyacentes dentro de la red y el uso de aplicaciones como HSMM-PI que permite la evaluación y determina la calidad del enlace entre los nodos que conforman la red mallada, son las herramientas encargadas de permitir la transmisión de video en la red; video que es enviado mediante la aplicación de Netcat y finalmente con la ayuda del software Mplayer la reproducción del mismo en la estación base.

La métrica utilizada para contabilizar y determinar la ruta más óptima que es seleccionada entre el nodo origen y destino utiliza los protocolos OSLR, MMRP y OSPF de esta manera se calcula la tabla de enrutamiento que se mantiene actualizada en todo momento y selecciona la ruta por la menor cantidad de saltos entre el nodo origen y el nodo destino, así como también toma en cuenta la calidad de la potencia del enlace entre los nodos para determinarla.

Al ser una red inalámbrica está expuesta a ser vulnerable a la interferencia de otras redes que estén utilizando el mismo canal para transmitir por lo que si la red se encuentra expuesta a la interferencia de otras redes en el mismo canal predomina la red que posea la mayor frecuencia mientras que las otras redes con menor potencia serán consideradas como ruido y no es posible efectuar la transmisión de video.

La seguridad de la red está determinada por los parámetros de seguridad expuestos en la presente tesis para las redes inalámbricas, en este caso se utiliza el identificador de nodo llamado SID el cual permite que si este parámetro no coincide con la información de la red creada este no podrá conectarse a la red y será descartado para la conexión a la misma así como también las redes MANET permiten la resistencia para repeler ataques, el reconocimiento de IDS y la recuperación de la funcionalidad de la red dentro de los límites tolerables de tiempo.

La implementación de una red adhoc que permite la fácil y muy rápida implementación de la red sin una infraestructura predefinida da cabida a la libre movilización de los nodos sin tener repercusiones o afectaciones dentro de la red, la ventaja de ser una red distribuida permite que los nodos puedan conocer la existencia de sus nodos vecinos y entregar información de las tablas de enrutamiento entre el nodo origen y el nodo destino, es por estas características que es posible abarcar una mayor cobertura utilizando los nodos disponibles de la red gracias a que cada uno de ellos irradia su propia área de cobertura.

La cobertura de este tipo de redes se determina en cuanto a la capacidad de radiación de cobertura de onda y el tipo de antena que posee cada dispositivo, en nuestro caso los dispositivos Raspberry fueron expuestos a distancias máximas de cobertura entre nodos menores a 76 metros entre nodos, se pudo comprobar que esta es la distancia máxima que permite la interconexión entre cada uno de ellos sin perder o salir de la cobertura y enlace de la red lo que nos permite desplegar los nodos para obtener una cobertura en línea recta de 228 metros.

Los problemas de latencia son perceptibles al usuario según la distancia entre los nodos va creciendo, la potencia de la transmisión disminuye al mismo tiempo que provoca mayores pérdidas de información que se pueden dar a notar en la conexión UDP del video. Un método de solventar este problema en cuanto a la funcionalidad del sistema propuesto es el uso de un protocolo de enrutamiento

que permita que el proceso de transferencia de información sea realizado en el menor número de saltos puesto que esto permite conservar la calidad en el servicio, es por ello el uso del protocolo adecuado y diseñado para redes AdHoc y MESH que es OSLR.

Se verificó que el protocolo de múltiples saltos al momento de perder a un nodo de la cobertura de la malla como se muestra en el escenario 4, en el cual se encuentran trabajando conjuntamente con la aplicación HSMM-Pi y la ejecución de Netcat; dejan la conexión abierta de la comunicación con el tercer nodo que al salir del área de cobertura pierde enlace a la red pero no la cierra, es decir la mantiene hasta que el nodo regrese al área de cobertura y automáticamente empiece a transmitir datos a la red y estos sean procesados en la Estación Base para la continuidad de la reproducción de video. Esto toma unos segundos que no pueden ser cuantificados ya que a mayor distancia aumenta el tiempo de la reconexión del nodo. Cabe recalcar que al existir o realizar esta prueba en un ambiente lleno de interferencias de señales que utilizan el mismo canal produce mayor latencia y pérdida de datos en los que muchas veces no es posible la reproducción de video.

El funcionamiento de las herramientas de software y los protocolos utilizados para este proyecto funcionan de manera satisfactoria ya que es posible salir del área de cobertura mientras se está transmitiendo video desde uno de los dispositivos más lejanos a la estación base, lo cual se logra por medio del enrutamiento a través del resto de nodos que conforman la red; al no cerrarse la conexión permite que al regresar el nodo al área de cobertura este retome la transmisión del video.

Para la transmisión de información a 2,4 GHz en WI-FI, al ser un tipo de tecnología bastante explotada la interferencia de señales es un problema que debe ser tomada en cuenta ya que debe existir una separación de 2,4 GHz entre cada frecuencia central de los canales, esto se puede lograr por ejemplo en los canales 1, 6 y 11; en el campus de la universidad se encontró que existe una

gran congestión en todos los canales posibles por utilizar, por lo cual se optó por utilizar el canal con menor interferencia, sin dejar de lado el tema de la potencia.

La aplicación HSMM-Pi con el servicio Web el cual indica el nivel de potencia de enlace entre los nodos posee un retardo al momento de mostrar los datos en las barras de porcentaje; esto se produce ya que esta solicitud viene iniciado desde la Estación Base y por medio del protocolo OSLR y la tabla e enrutamiento ARP, esta solicitud de estado de enlace debe recorrer toda la red mallada, es por ello que muchos factores afectan a esta operación como son la distancia, los obstáculos entre los nodos y la posición de los nodos por su lóbulo de radiación ya que se comprobó que al colocar los equipos Raspberry a mayores distancias en un área geográfica irregular al ser colocados los dispositivos en el suelo se pierde y absorbe la radiación de la antena y produce perdidas de enlace entre los nodos.

Cuando todos los nodos que conforman la red se encuentran dentro de la cobertura de la estación base la transmisión de información es directa entre la base y el nodo, no es necesario realizar enrutamiento dentro de esta área, pues al llegar directamente a la base esta se convierte en la mejor ruta para enviar información.

En la estación base el uso de la memoria cache es importante puesto que al activar el reproductor de video Mplayer y la recepción de la transmisión de video se produce un alto consumo de recursos entre estos el principal es el uso de memoria, con las pruebas realizadas se pudo determinar que al utilizar 600 MB de memoria por cada nodo a transmitir video es suficiente para garantizar la reproducción de video y una latencia mínima, esto permite que los 3 nodos puedan enviar video simultáneamente a la estación base sin consumir dicho recurso de una manera desproporcionada.

En la selección de las características que debe cumplir un equipo para que funcione como una estación base, lo mas importante es que tenga una cantidad

suficiente de memoria dependiendo del número de nodos que vayan a transmitir video de manera simultánea, también es importante es que el equipo debe tener la opción de conectarse a una red Ad-Hoc, mediante su tarjeta de red inalámbrica.

Como se puede ver en el capítulo existe un análisis de la potencia con relación a la distancia, en el cual mientras aumenta la distancia la potencia disminuye y de esta manera la latencia aumenta en el sistema propuesto.

Existen varios factores que afectan la transmisión de vídeo en el sistema de comunicación el más importante y conflictivo es la saturación de los canales de frecuencia para 2,4 GHz, el cual influye en la pérdida de paquetes en la transmisión puesto que si existe una señal con mayor nivel de potencia está predomina en el uso del canal, así como el número de saltos que debe atravesar la información hasta llegar a la estación base, pues mientras mayor es el número de saltos la latencia aumenta y puede existir mayor número de paquetes perdidos en el caso de trabajar con UDP, explicado en capítulos anteriores.

5.2. Recomendaciones

En caso de tener problemas con la corrupción de las tarjetas SD, pueden seguir los siguientes pasos para solucionar los errores:

Asegurarse de estar utilizando una fuente de alimentación de buena calidad, se puede comprobar la fuente de alimentación midiendo el voltaje entre TP1 y TP2 en el Raspberry Pi, si este voltaje cae por debajo de 4.75V cuando se realizan tareas complejas, es muy probable que no sea adecuado.

Asegurarse de cerrar sesión en le Raspberry Pi correctamente, escribir sudo shutdown y esperar a que la Raspberry Pi señale que está listo para ser apagado parpadeando el LED de actividad.

Muchas veces la tarjeta se queda en modo corrupto, esto sucede cuando la Raspberry es apagada de la forma incorrecta, para solucionar este problema se debe ingresar la micro SD en una portátil para realizar la reparación.

Una manera de solventar los problemas relacionados al número de usuarios que conforman o pueden integrar el sistema propuesto, es la utilización de la banda de los 5 GHz, ya que esta permite muchos más usuarios conectados ya que posee una densidad más grande de canales que la banda de los 2.4GHz.

Como recomendación para solventar problemas por saturación de uso de canales y la densidad de redes que ocupan los canales para Tx es verificar los canales en los cuales la potencia de las redes existentes no supere a la red planteada, ya que a pesar de encontrarse dentro de un ambiente con varias redes que pueden interferir la Tx; la red que irradie mayor potencia será la que predomine frente al resto y logre la Tx de los datos en nuestro caso en el ambiente de la universidad fue posible solventar el problema de interferencia colocando los nodos en el canal

Para que los nodos puedan irradiar correctamente deben ser colocados a una altura mínima de 1 metro del suelo ya que al colocarse los nodos en el suelo pierden su capacidad de irradiar su señal y esto produce que los equipos Raspberry pierdan su capacidad de comunicarse, esto se produce porque el suelo absorbe la radiación de la antena.

Para que una PC sea seleccionada para ser un nodo más de la red o pueda conectarse a la red Ad Hoc debe poseer un tarjeta y antena que permitan esta acción, por lo que es necesario verificar con el comando `netsh wlan show drivers`, donde se debe verificar que el parámetro de *Hosted Network supported*, tiene un valor de *yes* caso contrario no será posible que la PC se pueda unir a la red.

Para poder transmitir de manera simultánea teniendo en cuenta que se encuentran localizados los dispositivos Raspberry como se muestra en el

escenario uno Figura# en la sección de diagramas, se recomienda ingresar en los comandos distintos puertos para transmisión y recepción por cada uno de los Raspberry, esto ayuda a que no se sature el canal y no se incremente la latencia.

Es muy importante en el caso de resguardar nuestra información y el acceso a la red inalámbrica la posibilidad de combinar el cifrado más complejo con una aplicación que también incluya la seguridad por filtros MAC.

Al momento de transmitir es posible configurar los parámetros para la codificación de los datos y estos a su vez ser comprimidos por Mplayer para ser visualizados como video, de esta manera la calidad de imagen puede producir saturación ya que el ancho de banda es muy reducido, es por ello que se recomienda utilizar en el parámetro de FPS que son los cuadros por segundo un valor no menor a 30 ya que el video no es apreciado de manera real, el parámetro de W ancho de imagen y H la altura de la imagen se recomienda colocar para W el valor de 360 y para H el valor 300 el cual será visualizado sin problema en la pantalla de la computadora; el valor de CACHE se recomienda utilizar valores entre 500 y 2000 ya que si el valor es menor a 500 no puede procesar el número de FPS que se recomiendan para una calidad de video y si el valor es mayor debemos tomar en cuenta la capacidad del recurso en memoria del equipo que lo va a reproducir.

El proyecto permite la transmisión de video, pero no se limita únicamente a este servicio ya que es posible la configuración de muchos otros servicios como por ejemplo la transmisión de audio, texto, geo-localización de los nodos, etc., al igual que un sin número de lecturas de datos y parámetros que entregan sensores los cuales que pueden ser integrados fácilmente en los dispositivos Raspberry para ser enviados estos datos a la estación base.

REFERENCIAS

- Aguilera Irazabal, U. (2013). *Biblioteca Digital Loyola*. Recuperado el 16 de mayo de 2017, de http://paginaspersonales.deusto.es/unai.aguilera/documents/unaguil_tesis.pdf
- Alcibar, J. (2010). *Las diversas topologías que existen para la creación de redes*. Recuperado el 25 de mayo de 2017, de <http://1136120053.blogspot.com/>
- Barrientos, A., del Cerro, J., Gutiérrez, P., San Martín, R., Martínez, A., & Rossi, C. (2007). *Vehículos Aéreos no Tripulados para uso civil*. Recuperado el 24 de mayo de 2017, de Tecnología y aplicaciones: <http://webdiis.unizar.es/~neira/docs/ABarrientos-CEDI2007.pdf>
- Cisco. (2008). *Antena omnidireccional vs. antena direccional*. Recuperado el 24 de mayo de 2017, de http://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html
- Dobald, A. (2009). *Mvirtuales*. Recuperado el 12 de mayo de 2017, de <https://es.slideshare.net/alandk/topologias-inalambricas-presentation>
- Domingo, M. (2015). *UPCommons Portal de conocimiento UPC*. Recuperado el 14 de mayo de 2017, de <http://www.tesisenred.net/bitstream/handle/10803/7036/01Mcda01de01.pdf?sequence=1>
- Dulla. (2017). *DULLA M50000 Portable Power Bank 12000mAh External Battery Charger*. Recuperado el 22 de mayo de 2017, de <https://www.amazon.com/DULLA-M50000-Portable-12000mAh-External/dp/B01DHTV0Q8>
- Github. (2017). *A set of tools to easily configure the Raspberry Pi to function as a High-Speed Multimedia (HSMM) wireless node*. Recuperado el 13 de mayo de 2017, de <https://github.com/urlgrey/hsmm-pi>
- González, K., & Gordillo W. (2014). Estudio sobre Computadores de Placa Reducida Raspberry Pi Modelo B. *ENGI Revista Electrónica De La Facultad De Ingeniería*, 6-9.

- Hidalgo, F. (2008). *RuiNet Universidad Politécnica de Valencia*. Recuperado el 16 de mayo de 2017, de https://riunet.upv.es/bitstream/handle/10251/13183/TesinaMaster_FcoJavierHidalgo.pdf?sequence=1
- HobbyWing. (s.f.). *ARRIS M700 Foldable Carbon Fiber Hexacopter Frame W Retractable Landing Skid*. Recuperado mayo 27, 2017, de <http://www.hobby-wing.com/arris-m700-foldable-hexacopter-frame.html>
- Kioskea. (2014). *Redes inalámbricas*. Recuperado el 23 de mayo de 2017, de <http://es.ccm.net/contents/818-redes-inalambricas>
- Martín, D. (2015). *Un repaso al funcionamiento de las antenas, sus tipos y aplicaciones en una red Wi-Fi*. Recuperado el 30 de mayo de 2017, de <https://www.geektopia.es/es/technology/2015/10/07/articulos/antenas-conoce-como-funcionan-aprende-colocar-tu-router-repetidor-senal-wi-fi.html>
- Morgado Reyes, E. (2009). *Prestaciones de las Redes Ad Hoc*. Recuperado el 11 de mayo de 2017, de https://eficiencia.urjc.es/bitstream/handle/10115/2425/TesisDoctoral_EduardoMorgado.pdf?sequence=1
- MPlayerProject. (2017). *Informasion*. Recuperado mayo 12, 2017, de <http://www.mplayerhq.hu/design7/info.html>
- Netcat. (2013). *Sourceforge*. Recuperado from <http://nc110.sourceforge.net/>
- Pérez, T., & Granados, G. (2011). *Universidad de Almería riUAL*. Recuperado el 21 de mayo de 2017, de http://www.adminso.es/recursos/Proyectos/PFM/2010_11/PFM_mesh.pdf
- Pi Supply. (2017). *Raspberry Pi Camera Board v1.3 (5MP, 1080p)*. Recuperado el 19 de mayo de 2017, de <https://www.pi-supply.com/product/raspberry-pi-camera-board-v1-3-5mp-1080p/>
- Ramírez, R. (2015). *Sistemas de Radiocomunicaciones*. Madrid: Ediciones Paraninfo S.A.

- Raspberrypi. (2017). *FAQS* . Recuperado mayo 23, 2017, de <https://www.raspberrypi.org/help/faqs/>
- Raspberrypi. (2017). *Rasbian*. Recuperado mayo 22, 2017, de <https://www.raspberrypi.org/downloads/raspbian/>
- Raspberrypi. (2017). *SD CARDS*. Recuperado el 21 de mayo de 2017, de <https://www.raspberrypi.org/documentation/installation/sd-cards.md>
- Rocabado, S. (2013). *SEDICI Repositorio Institucional de la UNLP*. Recuperado el 10 de mayo de 2017, de <http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F08+-+Capitulo+3.pdf>
- The Magpi Magazine. (2016). RASPBERRY PI 3 IS OUT NOW! SPECS, BENCHMARKS & MORE. *The Magpi Magazine*, 8.
- Valencia, S., & Risueño, E. (2017). DISEÑO E IMPLEMENTACIÓN DE UNA RED MANET CON DISPOSITIVOS DE COMUNICACIÓN MÓVIL. Quito, Ecuador.

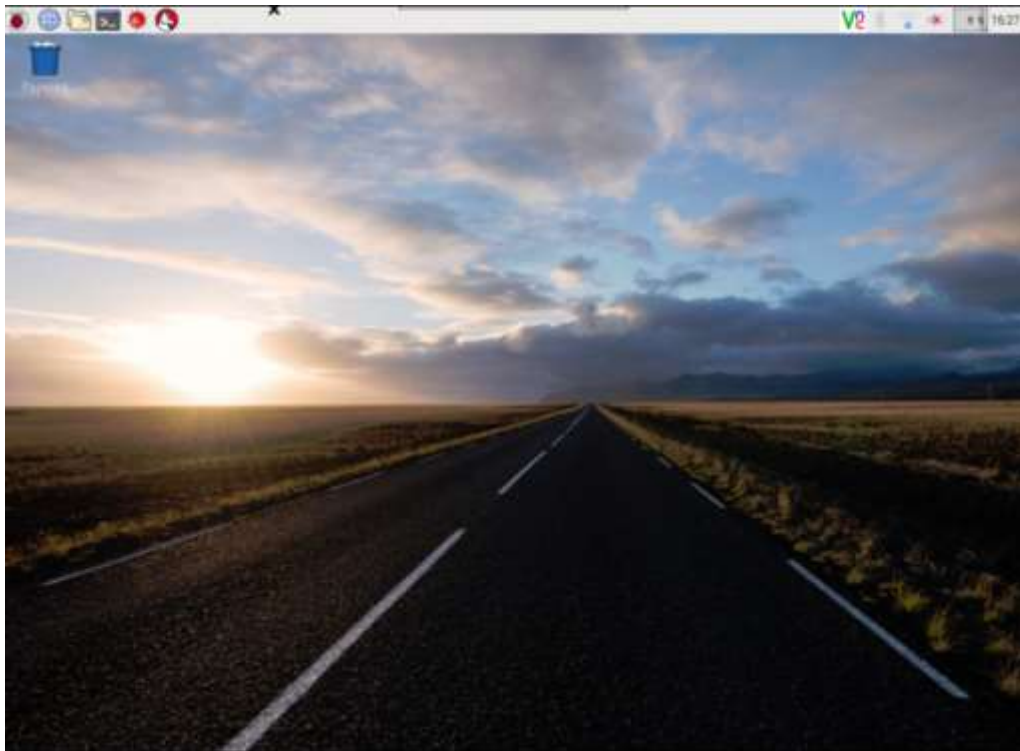
ANEXOS

Anexo 1.

Funcionalidades que se puede utilizar por medio de la interfaz gráfica de Raspbian.

1. Interfaz gráfica de Raspbian

El escritorio de esta versión es capaz de mostrar o configurar a gusto del usuario diferentes imágenes, estas las podemos encontrar en la carpeta `/usr/share/pixel-wallpaper/`, de tal manera que la presentación del nuevo escritorio gráfico de *Raspbian* se lo aprecia como en la figura 01.



Escritorio de Raspbian

2. Menú de cambios en la interfaz

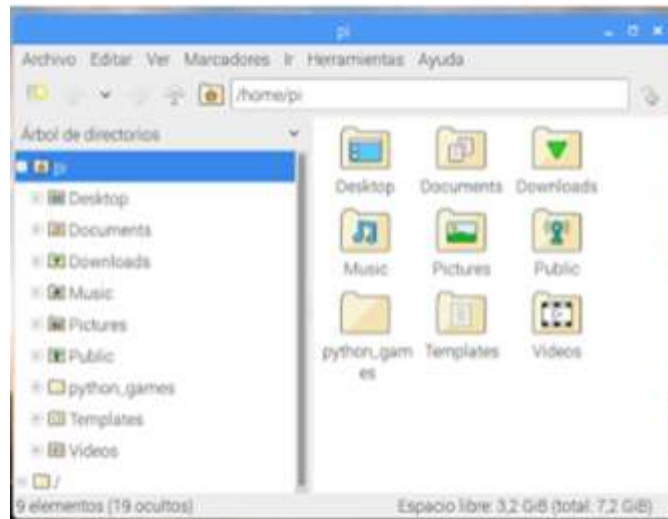
Se dan muchos cambios como los que se pueden visualizar en la figura 02, tenemos el menú para realizar cambios de fondo de pantalla, color de fondo, color del texto y varios parámetros que pueden ser configurados a gusto del usuario.



Ventana de Configuración de Apariencia

3. Ventanas de navegación

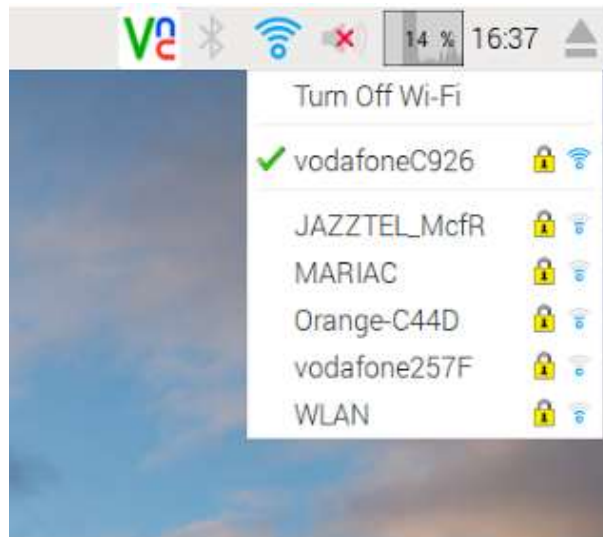
El diseño de las ventanas es otro factor que cambia en esta versión permitiendo de manera más simple la navegación dentro del equipo como se muestra en la figura 03, entregando detalles de espacio libre y total de espacio del equipo.



Ventana de Navegación de Carpetas y Contenido

4. Mejoras de conexión y variables.

Existen mejoras en la presentación de las redes de conexión que están siendo utilizadas en el equipo, permite al usuario de manera sencilla verificar la red o redes disponibles para el dispositivo como se muestra en la figura 04.



Ventana de Conexiones Inalámbricas

