



UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA
La Universidad Católica de Loja

ÁREA TÉCNICA

**TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y
COMPUTACIÓN**

Evaluación de parámetros de QoS de VoIP en Redes MANET

TRABAJO DE TITULACIÓN

AUTOR: Nodine Wyatt, David Anthony

DIRECTORA: Enciso Quispe, Liliana Elvira

LOJA- ECUADOR

2019



Esta versión digital, ha sido acreditada bajo la licencia Creative Commons 4.0, CC BY-NY-SA: Reconocimiento-No comercial-Compartir igual; la cual permite copiar, distribuir y comunicar públicamente la obra, mientras se reconozca la autoría original, no se utilice con fines comerciales y se permiten obras derivadas, siempre que mantenga la misma licencia al ser divulgada. <http://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

2019

APROBACIÓN DE LA DIRECTORA DEL TRABAJO DE TITULACIÓN

Doctora.

Liliana Elvira Enciso Quispe

DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo de titulación: **Evaluación de parámetros de QoS de VoIP en Redes MANET**, realizado por **Nodine Wyatt David Anthony**, ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, octubre de 2019

f)

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

“Yo, **Nodine Wyatt David Anthony**, declaro ser autor del presente trabajo de titulación: “Evaluación de parámetros de QoS de VoIP en Redes MANET”, de la Titulación de Sistemas Informáticos y Computación, siendo la Dr. Liliana Elvira Enciso Quispe directora del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 88 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado o trabajos de titulación que se realicen con el apoyo financiero, académico o institucional (operativo) de la Universidad”

f)

Autor: Nodine Wyatt David Anthony

Cedula: 1103578272

DEDICATORIA

Dedico este trabajo principalmente a mis padres, Sarah Louise Wyatt y Charles Walden Nodine, quienes son el pilar fundamental de mi vida y quienes me han apoyado durante toda mi carrera universitaria.

A mi hermana Natasha Carla Nodine Wyatt, la cual me ha apoyado e instruido en momentos difíciles de mi vida y mis estudios.

A mi novia Heide Valeria Sandra Saft Toledo, la cual me ha apoyado en todo momento desde el inicio de mi carrera alentándome siempre a mejorar y superarme a mí mismo, asegurándose que siempre de lo mejor de mí.

AGRADECIMIENTO

Quiero agradecer a la Universidad Técnica Particular de Loja por brindarme un lugar adecuado para poder realizar mis estudios de la mejor manera y así convertirme en un excelente profesional ético y moral.

Quiero agradecer de manera especial a mi Madre por brindarme su apoyo a lo largo de toda mi carrera estudiantil tanto económicamente como moral y por siempre guiarme por el camino correcto.

Quiero agradecer a mi Directora de Tesis, Dra. Liliana Enciso, quien me ha apoyado y guiado incondicionalmente no solo en mi trabajo de titulación si no durante mi carrera universitaria, la cual considero más que una maestra una amiga, siendo ella la persona dentro de la universidad que más me ha apoyado y guiado durante este camino para llegar a mi meta la cual es graduarme.

Quiero agradecer a la ingeniera Audrey Romero por todo el apoyo y disposición de resolver cualquier inquietud o problema presentado durante el desarrollo del presente trabajo.

Quiero agradecer a mis amigos y compañeros que me han acompañado brindándome su amistad y apoyo académico.

ÍNDICE DE CONTENIDOS

APROBACIÓN DE LA DIRECTORA DEL TRABAJO DE TITULACIÓN	ii
DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS.....	iii
DEDICATORIA.....	iv
AGRADECIMIENTO.....	v
RESUMEN.....	1
ABSTRACT.....	2
ÍNDICE DE FIGURAS.....	3
ÍNDICE DE TABLAS.....	5
ÍNDICE DE ECUACIONES.....	7
INTRODUCCIÓN.....	8
CAPÍTULO I. PROBLEMÁTICA.....	10
1.1. Planteamiento del problema.....	11
1.2. Objetivos.....	11
1.2.1. Objetivo General.....	11
1.2.2 Objetivos Específicos.....	11
1.3. Alcance del Proyecto.....	11
1.4. Justificación.....	12
CAPÍTULO II. MARCO TEÓRICO.....	13
2.1. Redes de comunicación.....	14
2.1.1. Tipos de redes.....	14
2.1.1.1. Redes WLAN. IEEE 802.11.....	14
2.1.1.2. Redes Ad-Hoc.....	17
2.1.1.2.1. Redes MESH.....	17
2.1.1.2.2. Redes VANET (Vehicular Ad-Hoc Network).....	18
2.2 Redes MANET.....	20
2.2.1. Características de las redes MANET.....	21
2.2.2. Aplicaciones de las redes MANET.....	22
2.3. Protocolos de enrutamiento Ad-Hoc.....	24
2.3.1. Protocolos de Enrutamiento Proactivo.....	26
2.3.1.1. DSDV.....	27
2.3.1.2. OLSR.....	28

2.3.2. Protocolos de Enrutamiento Reactivo.....	29
2.3.2.1. AODV.....	31
2.3.3. Protocolos de Enrutamiento Híbrido.....	31
CAPÍTULO III. VOZ SOBRE IP	33
3.1. VoIP.....	34
3.1.1. Funcionamiento de VoIP.....	34
3.1.2. Calidad de la voz.....	34
3.1.3. Ventajas de VoIP.....	36
3.1.4. Características de VoIP.....	36
3.2. Voz sobre IP en Redes MANET.....	37
CAPÍTULO IV. PARÁMETROS DE CALIDAD Y ENTORNO DE SIMULACIÓN	38
4.1. Parámetros de QoS en Redes MANET.....	39
4.2. Parámetros fundamentales que influyen en el desempeño de las aplicaciones de voz.....	41
4.2.1. Pérdida de paquetes.....	42
4.2.2. Retardo.....	42
4.2.3. Jitter.....	45
4.2.4. Codec.....	45
4.3. Requerimientos del simulador.....	47
4.4. Network Simulator (NS3).....	47
4.4.2. Clases fundamentales.....	48
4.4.2.1. <i>Application (aplicación)</i>	48
4.4.2.2. <i>Channel (canal)</i>	49
4.4.2.3. <i>Node (nodo)</i>	49
4.4.2.4. <i>NetDevice (dispositivo de red)</i>	50
4.4.3. Topologías de ayuda.....	50
4.5. Modelos de pérdidas de propagación y retardo.....	51
4.5.1. Modelo de movilidad.....	52
CAPÍTULO V. SIMULACIÓN POR TIPOS DE ESCENARIOS	54
5.1. Escenarios.....	55
5.2. Creación de escenarios en NS3.....	56
5.3. Simulaciones por escenarios.....	56
CAPÍTULO VI. RESULTADOS.....	58

6.1. Resultados de pérdida de paquetes.....	59
6.1.1. Experimento 1: Pérdida de paquetes (1 conexión).	59
6.1.2. Experimento 2: Pérdida de paquetes (5 conexiones simultáneas).....	62
6.1.3. Experimento 3: Pérdida de paquetes (10 conexiones simultáneas).....	65
6.1.4. Estadísticas de pérdida de paquetes.....	67
6.1.5. Resultados generales de pérdida de paquetes.	69
6.2. Resultados de retardo.....	70
6.2.1. Experimento 4: Retardo (1 conexión).	70
6.2.2. Experimento 5: Retardo (5 conexiones simultáneas).	72
6.2.3. Experimento 6: Retardo (10 conexiones simultáneas).	75
6.2.4. Estadísticas de retardo.	77
6.2.5. Resultados generales de retardo.	78
6.3. Resultados de jitter.	78
6.3.1. Experimento 7: Jitter (1 conexión).	79
6.3.2. Experimento 8: Jitter (5 conexiones simultáneas).....	82
6.3.3. Experimento 9: Jitter (10 conexiones simultáneas).....	85
6.3.4. Estadísticas de jitter.....	87
6.3.5. Resultados generales de jitter.....	89
CONCLUSIONES.....	90
RECOMENDACIONES.....	92
BIBLIOGRAFÍA.....	93
ANEXOS	96
Anexo 1. Modelo de Gilbert-Elliot	97
Anexo 2. Instalación de NS3.....	98
Anexo 3. Creación de tráfico VoIP en la red MANET	100
Anexo 4. Inserción nodos, tiempo de simulación y protocolo al simular por teclado	103
Anexo 5. Estadísticas media y varianza.	104

RESUMEN

El propósito de este trabajo es analizar los factores que influyen en la calidad de servicios (QoS) de voz sobre IP (VoIP) en redes Ad-Hoc móvil (MANET), ya que este tipo de redes ofrecen una arquitectura totalmente descentralizada, la cual es una alternativa muy factible para propósitos móviles y perfecta para escenarios donde no se puede desplegar una infraestructura de red física. Las grandes ventajas que ofrece la tecnología de VoIP, como el reducido costo de llamadas y la movilidad, son algunas de las ventajas que tiene esta tecnología. Por otro lado, tenemos la naturaleza dinámica de las redes MANET lo cual ocasiona que algunos parámetros importantes para medir QoS sean afectados: el retardo, la pérdida de paquetes y la variación del retardo. Con los resultados obtenidos se ha podido comprobar los parámetros óptimos, así como protocolos, tiempos de simulación y número de nodos, para montar una red MANET cuando sobre esta trabaje VoIP, dando de esta manera un manual de mejores prácticas para aquellas personas que deseen implementar una red de este tipo.

PALABRAS CLAVES: QoS, MANET, parámetros de calidad, NS3, protocolos de enrutamiento, VoIP.

ABSTRACT

The purpose of this paper is to analyze the factors that influence in the quality of service (QoS) of voice over IP (VoIP) in MANET networks, since this type of networks offers a totally decentralized architecture, which is a very feasible alternative for mobile purposes and perfect for scenarios where a physical network infrastructure cannot be deployed. On the other hand, there is no doubt about the growth of multimedia services such as VoIP, which has become something of the daily life of Internet users. The great advantages offered by VoIP technology, such as the low cost of calling anywhere, regardless of the geographic location and mobility thanks to the fact that users can take their same number anywhere, are just some of the advantages of this technology. But on the other hand, we have the dynamic nature of MANET networks which causes some important parameters to measure quality to be affected such as packet loss, delay and variation of the delay. In order to perform this, we define which parameters directly influence the quality perceived by the user, this is done through the design of evaluation experiments for VoIP applications in certain scenarios considering the specified parameters. With the obtained results it has been possible to verify the optimal parameters to mount a MANET network when working with VoIP, as well as protocols, simulation times and number of nodes, thus giving a manual of best practices for those who wish to implement a network of these characteristics.

KEYWORDS: QoS, MANET, quality parameters, NS3, routing protocols, VoIP.

ÍNDICE DE FIGURAS

Fuente: (Anguis, 2008).	15
Elaborado por: (Anguis, 2008).	15
Figura 2. Red WLAN en modo infraestructura.....	15
Figura 3. Modo infraestructura extendido	16
Figura 4. Red WLAN en modo Ad-Hoc.....	17
Figura 5. Arquitectura inalámbrica MESH.	18
Figura 6 Red VANET.	19
Figura 7 Comunicación en una red MANET.	21
Figura 9 Aplicación de búsqueda y rescate de MANET.....	23
Figura 10 Red PAN.....	24
Figura 11 Protocolos de enrutamiento.	26
Figura 12: Protocolo de enrutamiento proactivo Ad-Hoc.	27
Figura 13: Protocolo de enrutamiento reactivo Ad-Hoc.	30
Figura 15: Distintos componentes del retardo.	43
Figura 16: Distintos componentes del retardo.	44
Figura 17: Sistema VoIP.	46
Figura 18: Patrón de desplazamiento de un nodo móvil utilizando el modelo de movilidad RandomWaypoint.	52
Figura 19: Visualización de la simulación de 30 nodos con un tiempo de 150 s utilizando el protocolo AODV y modelo de movilidad RandomWaypoint.....	57
Figura 20: Ingreso de número de nodos, tiempo de simulación y protocolo a simular por teclado.....	57
Figura 21: Resultados de pérdida de paquetes 1 conexión.....	59
Fuente: Autor.....	59
Fuente: Autor.....	60
Fuente: Autor.....	61
Figura 22: Resultados de pérdida paquetes 5 conexiones simultáneas.	62
Figura 23: Resultados de pérdida paquetes 10 conexiones simultáneas.	65
Figura 24: Resultados de retardo 1 conexión.....	70
Figura 25: Resultados de retardo 5 conexiones simultáneas.	72
Figura 26: Resultados de retardo 10 conexiones simultáneas.	75
Figura 27: Resultados de jitter 1 conexión.	79

Figura 28: Resultados de jitter 5 conexiones simultáneas.....	82
Figura 29: Resultados de jitter 10 conexiones simultáneas.....	85
Figura 31: Archivos para generar tráfico VoIP agregados a la carpeta helper.....	100
Figura 32: Archivos para generar tráfico VoIP agregados a la carpeta model.....	100
Figura 33: Entradas para archivos agregados al script waf (wscript).....	101
Figura 34: Agregación del tráfico VoIP al script.....	102
Figura 35: Variables creadas para ingreso de datos.....	103
Figura 36: Presentación de los valores a ingresar por teclado y almacenamiento del valor ingresado en las variables	103
Figura 37: Asignación de los valores ingresados por teclado a variables correspondientes del script.....	103

ÍNDICE DE TABLAS

Tabla 1: Comparación de características de protocolos proactivos, reactivos e híbridos.	25
Tabla 2: Atributos de los deferentes codecs de VoIP.....	46
Tabla 3. Parámetros para escenarios con un tiempo de 150 y 300 segundos.....	55
Tabla 4. Escenarios con 1 conexión.	55
Tabla 5. Pérdida de paquetes con tiempo de simulación 150 s y 1 conexión.....	60
Tabla 6. Pérdida de paquetes con tiempo de simulación 300 s y 1 conexión.....	61
Tabla 7. Escenarios con valores aceptables de pérdida de paquetes con 1 conexión.	61
Tabla 8. Pérdida de paquetes con tiempo de simulación 150 s y 5 conexiones simultáneas. ...	63
Tabla 9. Pérdida de paquetes con tiempo de simulación 300 s y 5 conexiones simultáneas. ...	63
Tabla 10. Escenarios con valores aceptables de pérdida de paquetes con 5 conexiones simultáneas.	64
Tabla 11. Pérdida de paquetes con tiempo de simulación 150 s y 10 conexiones simultáneas. 66	
Tabla 12. Pérdida de paquetes con tiempo de simulación 300 s y 10 conexiones simultáneas. 66	
Tabla 13. Escenarios con valores aceptables de pérdida de paquetes con 10 conexiones simultáneas.	67
Tabla 14. Estadísticas de pérdida de paquetes 150 s.....	68
Tabla 15. Estadísticas de pérdidas de paquetes 300 s.	68
Tabla 16. Estadísticas de pérdida de paquetes por número de conexiones.....	69
Tabla 17. Estadísticas de pérdida de paquetes por número de conexiones simultáneas con valores aceptables.....	69
Tabla 18. Retardo con tiempo de simulación 150 s y 1 conexión.....	71
Tabla 19. Retardo con tiempo de simulación 300 s y 1 conexión.....	72
Tabla 20. Retardo con tiempo de simulación 150 s y 5 conexiones simultáneas.	73
Tabla 21. Retardo con tiempo de simulación 300 s y 5 conexiones simultáneas.	74
Tabla 22. Retardo con tiempo de simulación 150 s y 10 conexiones simultáneas.	76
Tabla 23. Retardo con tiempo de simulación 300 s y 10 conexiones simultáneas.	76
Tabla 24. Estadísticas retardo 150 s.....	77
Tabla 25. Estadísticas retardo 300 s.....	77
Tabla 26. Estadísticas retardo por número de conexiones simultáneas.....	78
Tabla 27. Estadísticas retardo por número de conexiones simultáneas con valores aceptables	78
Tabla 28. Jitter con tiempo de simulación 150 s y 1 conexión.....	80
Tabla 29. Jitter con tiempo de simulación 300 s y 1 conexión.....	80

Tabla 30. Escenarios con valores aceptables de jitter con 1 conexión.	81
Tabla 31. Jitter con tiempo de simulación 150 s y 5 conexiones simultáneas.	83
Tabla 32. Jitter con tiempo de simulación 300 s y 5 conexiones simultáneas.	83
Tabla 33. Escenarios con valores aceptables de jitter con 5 conexiones simultáneas.	84
Tabla 34. Jitter con tiempo de simulación 150 s y 10 conexiones simultáneas.	86
Tabla 35. Jitter con tiempo de simulación 300 s y 10 conexiones simultáneas.	86
Tabla 36. Escenarios con valores aceptables de jitter con 10 conexiones simultáneas.	87
Tabla 37. Estadísticas de jitter 150 s.	87
Tabla 38. Estadísticas de jitter 300 s.	88
Tabla 39. Estadísticas de jitter por número de conexiones simultáneas.....	88
Tabla 40. Estadísticas de jitter por número de conexiones simultáneas con niveles aceptables	88
Tabla 41. Conjunto de datos de la población.	104
Tabla 42. Resultados de $x - \mu$	106
Tabla 43. Resultados de $(x - \mu)^2$	107

ÍNDICE DE ECUACIONES

Ecuación 1: Pérdida de paquetes.	42
Ecuación 2: Retardo.	44
Ecuación 3: Jitter.	45
Ecuación 4: Pérdida de propagación.	51
Ecuación 5: Media.	104
Ecuación 6: Varianza.	105

INTRODUCCIÓN

Hoy en día con el auge de las tecnologías inalámbricas, las redes Ad-Hoc han tomado un lugar fundamental en el área investigativa debido a su capacidad de ofrecer una arquitectura totalmente descentralizada, lo cual es ideal para aplicaciones móviles o donde no se pueda extender una infraestructura, tal como pueden ser situaciones de emergencia, desastres naturales, en el ámbito militar. Las redes MANET (Mobile Ad-Hoc Network) se pueden utilizar en cualquier lugar y en cualquier momento debido a su característica de no necesitar una infraestructura, proporcionando conectividad entre los usuarios y proveyendo a los mismos de servicios.

A razón de su naturaleza dinámica, una red MANET, debe ser capaz de crear una red auto configurable en el cual todos los nodos cumplan una función colaborando con las tareas de enrutamiento, por lo cual, cada nodo puede desempeñarse como hosts y como enrutadores, usando protocolos específicos y adecuados para las redes MANET.

Por otro lado con el creciente número de usuarios de las redes de comunicación, estas se están convirtiendo en un servicio básico a nivel mundial, con lo cual la cantidad de multimedia que se transmite por este medio está en aumento, siendo uno de estos contenidos el tráfico de voz sobre Protocolo de Internet (VoIP), el cual hoy en día tiene un auge entre los usuarios del Internet, esto gracias a sus bajos costos y los niveles de calidad que esta ha alcanzado, además de la posibilidad de conectarse desde cualquier punto geográfico.

La transmisión de VoIP en redes MANET enfrenta muchos más inconvenientes que en las redes convencionales. En las redes MANET el aspecto de calidad es más crítico debido a su característica dinámica ya que esto puede afectar de manera directa el retardo, jitter (variación del retardo) y la pérdida de paquetes, entre otros, debido a que sus enlaces están expuestos a diferentes efectos de propagación y condiciones del entorno.

Una de las características fundamentales de las redes MANET son los protocolos de enrutamiento que utiliza, los cuales hacen que estas redes sean un punto de investigación y desarrollo, siendo necesario que estos protocolos sean eficientes para satisfacer la alta calidad de servicio requerida por una transmisión de voz, en una red altamente dinámica como son las redes MANET.

El desempeño de servicio de VoIP en redes dinámicas como MANET no ha sido investigado con la misma intensidad que en las redes de infraestructura, por lo cual se espera que este estudio pueda dar una idea más clara de cuáles son los parámetros más apropiados para el uso de servicios VoIP en una red MANET.

Este trabajo de titulación (TT) se encuentra organizado en seis capítulos: Capítulo I, corresponde a la presentación de la problemática, así como los objetivos, las limitaciones que presenta el TT, el alcance y la justificación. En el Capítulo II, se presenta el marco teórico, se define los distintos tipos de redes y los protocolos de las redes Ad-Hoc. En el Capítulo III, se presenta todo lo referente a VoIP, definiciones, funcionamiento, características. En el Capítulo IV, se describe QoS en las redes MANET, los parámetros que influyen en la calidad de voz, el simulador que se utilizará para las simulaciones y sus características. En el Capítulo V, se presentan los escenarios y los procesos de simulación. En el Capítulo VI, se presentan los resultados obtenidos de las simulaciones por cada escenario.

CAPÍTULO I. PROBLEMÁTICA

1.1. Planteamiento del problema.

Actualmente, un tema de interés en el área de redes de comunicación son las redes móviles, que están diseñadas para brindar comunicaciones rápidas y eficientes sin la existencia de una infraestructura de red, debido a que se basa en una topología distribuida, esto es muy útil en situaciones donde no se puede desplegar una red de infraestructura por motivos geográficos, situaciones de emergencia como desastres naturales o entornos militares.

En este Trabajo de Titulación (TT) se analiza la calidad de servicio (QoS) de las redes MANET (Mobile Ad-Hoc Network) que presentan una alternativa para soluciones de voz sobre protocolo de Internet (VoIP) en escenarios con movilidad de los nodos sin infraestructura. Sin embargo, el soporte de servicios de voz enfrenta más desafíos en redes MANET que en otras redes. En el presente TT se pretende analizar el desempeño de los parámetros como: el retardo, la pérdida de paquetes y el jitter; y, como estos se ven afectados por el cambio de la topología debido a la movilidad de los nodos obteniendo datos que permitan crear redes de este tipo, que funcionen de la manera más eficiente posible.

1.2. Objetivos.

1.2.1. Objetivo General.

Evaluar parámetros de calidad de servicio para aplicaciones de VoIP en redes MANET.

1.2.2 Objetivos Específicos.

- Elaborar el estado del arte sobre redes MANET y VoIP
- Determinar los parámetros de QoS de VoIP, el número de protocolos, escenario y modelo de movilidad para el proceso de simulación.
- Medir los parámetros de QoS de VoIP en el simulador escogido.
- Analizar los resultados obtenidos de acuerdo con los parámetros establecidos.

1.3. Alcance del Proyecto.

El presente TT pretende analizar los factores que influyen en QoS de VoIP en Redes MANET, luego crear experimentos que permitan medir los distintos factores identificados en distintos escenarios, realizar la implementación de estos experimentos en un entorno de simulación y

finalmente, analizar los resultados obtenidos de acuerdo con los parámetros de QoS establecidos.

1.4. Justificación.

Hoy en día, el tema de proporcionar QoS en todos los ámbitos es de gran importancia, sobre todo en VoIP; por esta razón es que se están realizando innumerables investigaciones en esta área.

Los componentes creados para redes comunes (con una infraestructura) no son aplicables de modo directo a las redes MANET debido a las disconformidades entre estas tecnologías. Por esta razón, uno de los retos más importantes de la actualidad es, dotar de QoS a las redes MANET cuando sobre estas funcione VoIP.

CAPÍTULO II. MARCO TEÓRICO

2.1. Redes de comunicación.

Una red de comunicaciones es un conjunto de equipos informáticos autónomos, que permiten la comunicación sin importar la localización geográfica y esto sirve para transmitir múltiples tipos de información (audios, videos, voz, etc.) por ondas electromagnéticas, a través de diversos medios (cable, aire, cable de fibra óptica, cable coaxial, etc.) (Armendáriz, 2009).

Hoy en día, las redes de comunicación juegan un papel fundamental dentro de la sociedad debido que se usan en todos los ámbitos como bancos, redes sociales, en el ejército, situaciones de desastre, etc. Y por esta misma razón es que se han convertido en un tema que llama mucho la atención de los investigadores para mejorar y crear nuevas maneras de comunicación.

2.1.1. Tipos de redes.

2.1.1.1. *Redes WLAN. IEEE 802.11.*

Una red de área local inalámbrica (WLAN, Wireless Local Area Network) se encuentra regida por el estándar IEEE 802.11. Estas redes tienden a tener el alcance de una oficina, un edificio o una empresa.

El estándar 802.11 es una familia de especificaciones desarrolladas por la IEEE (Institute of Electrical and Electronic Engineers) para la tecnología de redes de área local inalámbricas, y que precisa el uso de los dos niveles inferiores de la arquitectura OSI (Open Systems Interconnection) como son capa física y de enlace de datos. En este estándar se especifica una interfaz a través del aire, entre el cliente y la estación base o entre dos clientes inalámbricos. Actualmente incluye numerosas técnicas de transmisión por modulación que utilizan protocolos similares (Herrera-Ramírez, Díaz-Ramírez, & Calafate, 2007).

Anguis (2008) afirma que:

“La arquitectura 802.11 está basada en una arquitectura celular, el sistema se divide en celdas o células denominadas BSS, (Basic Service Set). Un BSS está formado por nodos, fijos o móviles, llamados estaciones”.

La Figura 1 muestra la arquitectura lógica-funcional de IEEE 802.11.



Figura 1. Arquitectura lógica-funcional de IEEE 802.11.

Fuente: (Anguis, 2008).

Elaborado por: (Anguis, 2008).

En las redes WLAN se determina modos de funcionamiento de los cuales se puede destacar:

- **El Modo de infraestructura o BSS** (Basic Service Set): permite la conexión de las estaciones inalámbricas a través de un punto de acceso que gestiona las conexiones. Las estaciones inalámbricas envían los paquetes al punto de acceso que los redirige a su destino (Pellejero, Andreu, & Lesta, 2006). La Figura 2 muestra una red WLAN en modo infraestructura.

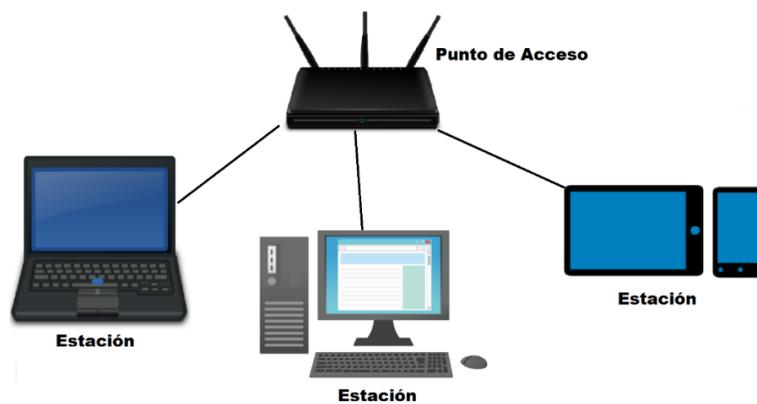


Figura 2. Red WLAN en modo infraestructura

Fuente: Autor.

Elaborado por: Autor

- **Modo Infraestructura Extendido o ESS** (Extended Service Set): es un caso específico del modo infraestructura, se basa en tener dos o más redes en modo BSS interconectados, normalmente por una red LAN (Local Area Network) convencional, de forma que cada BSS abarca una zona o celda que corresponde a su radio de alcance. Los usuarios pueden moverse libremente de una celda a otra y su conexión se establecerá automáticamente con el punto de acceso que les brinde una mejor cobertura. A esto se le llama *roaming* o itinerancia entre celdas (Anguis, 2008). La Figura 3 muestra una red en modo infraestructura extendido.

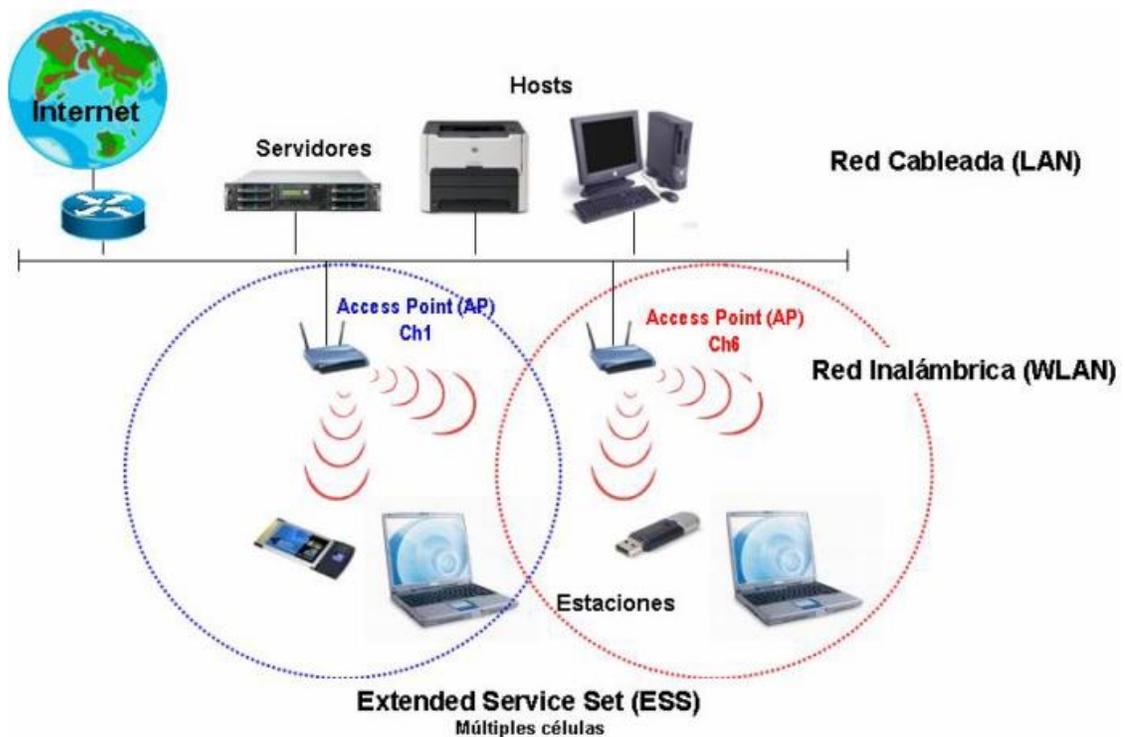


Figura 3. Modo infraestructura extendido

Fuente: (Anguis, 2008).

Elaborado por: (Anguis, 2008).

- **Modo Ad-Hoc:** permite la interconexión entre dispositivos de usuario (de igual a igual) sin necesidad de un punto de acceso. La información se envía directamente entre los equipos implicados, sin necesidad de un punto de acceso o una infraestructura, obteniéndose un aprovechamiento máximo del canal de comunicaciones (Anguis, 2008; Pellejero et al., 2006). En la Figura 4 se muestra una red WLAN en modo Ad-Hoc.

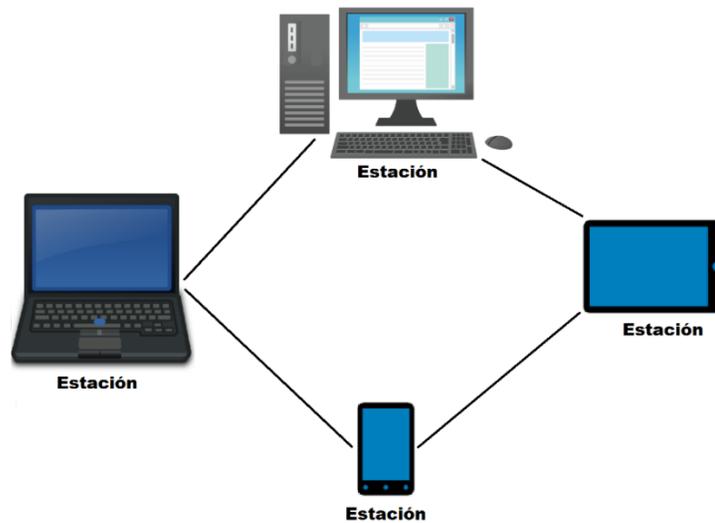


Figura 4. Red WLAN en modo Ad-Hoc

Fuente: Autor.

Elaborado por: Autor

2.1.1.2. Redes Ad-Hoc.

Como se ha mencionado anteriormente, las redes Ad-Hoc son redes que no dependen de una infraestructura fija, en estas redes las estaciones cumplen la función de emisor y receptor del tráfico, por lo cual, se necesita de protocolos específicos para el enrutamiento de información que permitan a las estaciones reenviar el tráfico de paquetes (Batiste Troyano, 2011).

Preexisten varios tipos de redes Ad-Hoc como son: malladas (MESH), vehiculares (VANET, Vehicular Ad-Hoc Network) y Móviles (MANET, Mobile Ad-Hoc Network).

2.1.1.2.1. Redes MESH.

La red MESH son una red híbrida ya que une la topología Ad-Hoc con la topología de Infraestructura.

La Figura 5 muestra una red MESH, la cual es una red Ad-Hoc con la diferencia de que los nodos MESH básicos pueden ser los encargados de enrutar el tráfico y actualizar información sobre la topología de la red. Existen algunos nodos que pueden funcionar como puntos de acceso, a los que se conectan clientes equipados con interfaces inalámbricas, además algunos nodos pueden funcionar como puente hacia otro tipo de redes (Batiste Troyano, 2011).

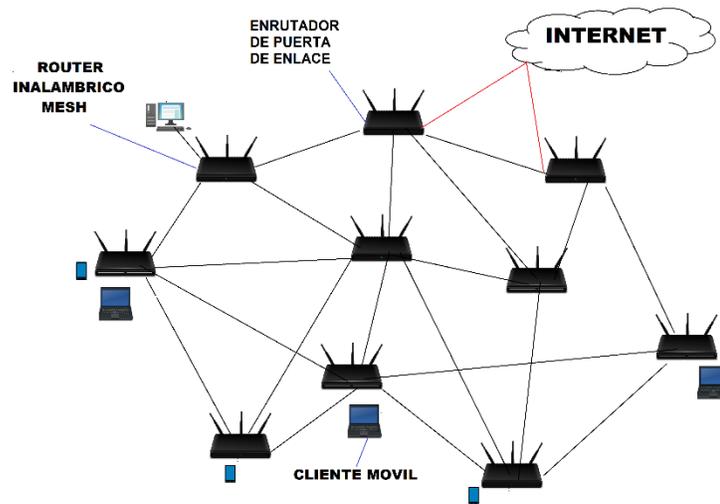


Figura 5. Arquitectura inalámbrica MESH.

Fuente: (Pathak & Dutta, 2011).

Elaborado por: Autor

Este tipo de redes admiten unirse a una red de dispositivos, aunque estos se encuentren fuera del rango de cobertura de los puntos de acceso, mientras estos se encuentren dentro del rango de cobertura de alguna estación que se comunique de manera directa o indirecta con un punto de acceso que si tenga cobertura. Esto también permite que, si algún nodo abandona la red, este mediante el protocolo de enrutamiento pueda redirigir el tráfico hacia otros nodos. Todos los nodos que conforman la red se basan en el estándar IEEE 802.11, configurados en modo Ad-Hoc, lo cual les permite actuar como clientes o servidores (“Red inalámbrica Mesh - EcuRed,” 2011).

2.1.1.2.2. Redes VANET (Vehicular Ad-Hoc Network).

En las últimas décadas se ha visto la integración de las tecnologías informáticas y de comunicación, así como la integración de estos en vehículos. Uno de los avances han sido las redes VANET que usan a los vehículos como nodos móviles los cuales permiten la intercomunicación entre vehículos cercanos y equipo de carretera. Pero estas redes difieren de otras por sus características especiales específicamente, los nodos (vehículos) en las redes VANET se encuentran limitados a la topología de la carretera mientras se mueven, debido a esto, si la información de la carretera está disponible se puede, predecir la posición futura de un vehículo o informar al mismo sobre acontecimientos en la vía, además puede dar nuevas

funcionalidades tal como la transmisión multimedia, VoIP, etc. (Liang, Li, Zhang, Wang, & Bie, 2015).

Pero las redes VANET también vienen con sus propios retos como es, la posibilidad de gran escala debido a la gran cantidad de vehículos en la vía y que esta puede extenderse por toda la infraestructura vial, tienen una topología cambiante debido al constante desplazamiento de los vehículos los cuales generalmente se mueven a grandes velocidades (Liang et al., 2015).

En una red VANET, como se observa en la Figura 6, el módulo de comunicación agrupado a cada vehículo no solo cumple el papel de nodo de la red, sino también, de router y switch.

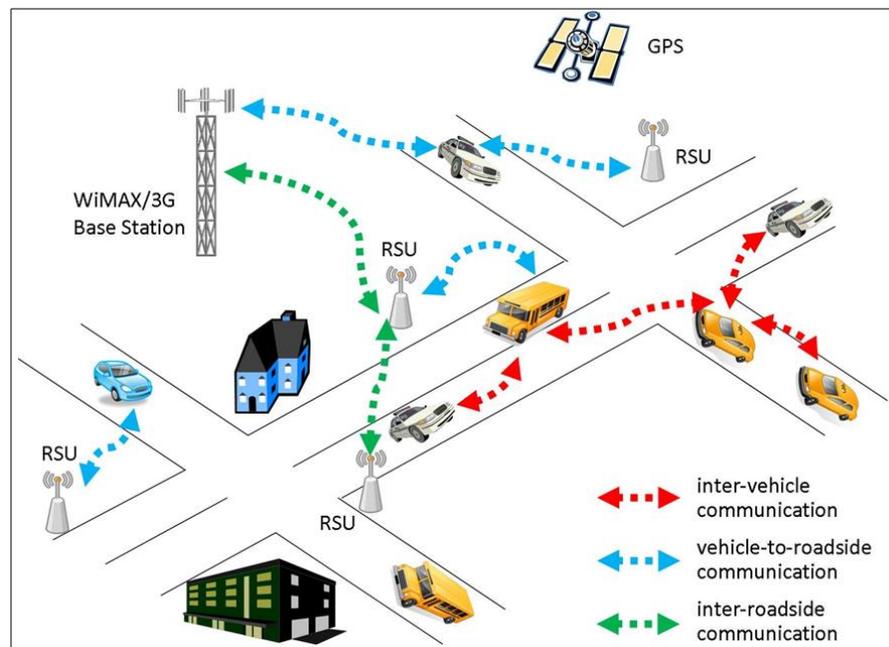


Figura 6 Red VANET.

Fuente: (jblesa, 2017).

Elaborado por: (Loo et al., 2016)

Las redes VANET se pueden explicar según el trabajo de (Al-Sultan, Al-Doori, Al-Bayatti, & Zedan, 2014). En la arquitectura de una VANET la comunicación entre vehículos, o entre vehículos y la unidad de carretera (RSU) se logra mediante un medio inalámbrico llamado WAVE. Este método de comunicación provee de amplia información a los conductores y viajeros, además permite aplicaciones de seguridad para incrementar la seguridad vial proporcionando un manejo confortable. Los principales componentes del sistema son la Unidad de Aplicación (AU), Unidad a bordo (OBU) y RSU. Típicamente el RSU es el que tiene la

aplicación nativamente y provee de servicios mientras que el *OBU* es un dispositivo que usa los servicios proveídos.

2.2 Redes MANET.

Las redes Ad-Hoc móviles nacieron de una necesidad militar al igual que ha sucedido en muchas otras ocasiones dentro del ámbito de las comunicaciones electrónicas, esta necesidad era la de interconectar dispositivos tácticos desplazados en zonas de conflicto sin requerir de una infraestructura. Esta tecnología inició con la investigación de lo que se conocía como Red de Radio Paquetes la cual usaba una combinación de protocolos ALOHA y CSMA como técnica de acceso al medio, unida a un tipo de enrutamiento Vector – Distancia. Con el incremento de la movilidad que ofrecen los dispositivos electrónicos y requieren los usuarios hoy en día, ha hecho presente un nuevo escenario de operación, en el mercado dentro de las redes MANET. Estas redes nacen bajo el concepto de autonomía e independencia, ya que no requieren de una infraestructura ni administración en esquemas centralizados como lo hacen las redes de infraestructura (Calderón & QUINTERO, 2004).

Si pensamos en el futuro, la tecnología de la información será mayormente enfocada en una tecnología inalámbrica, las redes celulares tradicionales, aún se encuentran en cierta manera limitadas por su necesidad de una infraestructura. Con las redes MANET esta limitación no existe (Giordano, 2002), ya que como su nombre lo indica, estas añaden la peculiaridad de movilidad de sus nodos, debido a esto los enlaces entre nodos se rompen y que además haya enlaces que se incorporen o abandonen la red continuamente, por lo que la topología de red es muy cambiante y aleatoria. En una red MANET todos los nodos pueden actuar tanto como receptores, emisores y enrutadores, esto es un requerimiento debido a que las rutas para llegar a un destino pueden requerir de varios saltos. Un nodo puede ser cualquier tipo de dispositivo que posea una tarjeta de red inalámbrica tal como: celulares, tables, ordenadores portátiles, entre otros (Ugas, 2009).

La Figura 7 muestra la manera en la que opera una red Ad-Hoc. El nodo 1 se puede comunicar directamente con el nodo 2 mediante un salto, de igual manera con el nodo 3 y 4. Pero si el nodo 1 se quiere comunicar con el nodo 5, el nodo 2, 3 o 4 deben actuar como intermediario entre el nodo 1 y 5 transmitiendo la información entre estos. Esta comunicación es una comunicación de múltiples saltos.

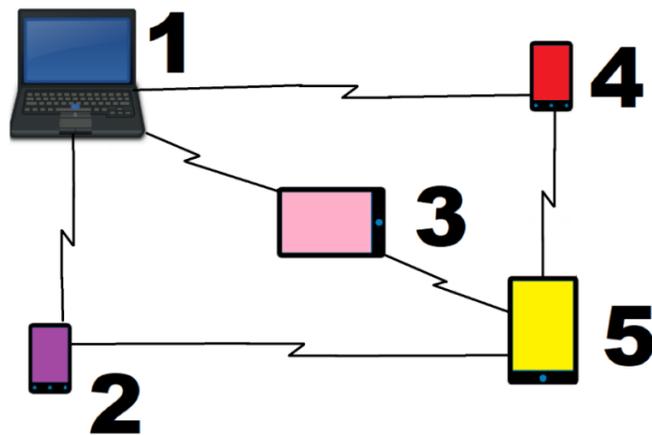


Figura 7 Comunicación en una red MANET.

Fuente: Autor

Elaborado por: Autor.

2.2.1. Características de las redes MANET.

Giordano (2002) menciona que las redes MANET heredan los problemas tradicionales de las demás redes inalámbricas como son la optimización de ancho de banda, control de energía y calidad de transmisión. Además, la naturaleza de salto múltiple y la falta de infraestructura fija generan nuevos problemas, como la configuración, el descubrimiento y el mantenimiento, así como el direccionamiento Ad-Hoc y el enrutamiento automático. En las redes móviles Ad-Hoc, la topología es altamente dinámica y aleatoria. Además, la distribución de nodos y, eventualmente, su capacidad de autoorganización juega un papel importante.

Las principales características según (Giordano, 2002; Loo, Mauri, & Ortiz, 2016; Ugas, 2009) son las siguientes:

- Cada terminal puede actuar como un nodo independiente funcionando como un transmisor, receptor o rúter, lo cual hace que las redes MANET tengan una topología muy dinámica.
- Las redes MANET están basadas en enlaces inalámbricos, los cuales continúan teniendo una capacidad significativamente menor a su contraparte cableada.
- Las redes MANET tienen un funcionamiento distribuido debido a que no existe ningún elemento principal que se encargue de gestionar y controlar la red. Salvo caso de las redes MANET jerárquicas donde los nodos son administrados por un jefe de grupo.
- La topología es altamente dinámica y cambios regulares en la topología podrían ser difíciles de predecir.

- La capacidad de los nodos puede variar debido a que no todos necesariamente tienen las mismas características.
- Las redes móviles Ad-Hoc se ven afectadas por mayores tasas de pérdida, y pueden experimentar mayores retardos y fluctuaciones que las redes fijas debido a la transmisión inalámbrica.
- La seguridad física es limitada debido a sus enlaces inalámbricos.
- Los nodos en las redes MANET dependen de baterías u otras fuentes de energía agotables. Como consecuencia de esto, el ahorro de energía es un factor de diseño importante. Además, los nodos deben ser conscientes de la potencia: el conjunto de funciones que ofrece un nodo depende de su potencia disponible (CPU, memoria, etc.).
- Una red MANET tiene varias ventajas sobre redes cableadas, incluyendo su capacidad de despliegue instantáneo debido a su naturaleza de no requerir de una infraestructura.

2.2.2. Aplicaciones de las redes MANET.

Las redes MANET presentan una solución ideal para situaciones donde se necesite de una red que se pueda montar al instante sin necesidad de una infraestructura, esto resulta muy útil en situaciones donde no se tiene el presupuesto para una infraestructura, las características propias del lugar no permiten desplegar una infraestructura o sencillamente se necesita una red temporal.

Las aplicaciones según (Goyal, Parmar, & Rishi, 2011; Loo et al., 2016) son las siguientes:

- **Militares campo de batallas:** el equipo militar ahora contiene habitualmente algún tipo de equipo informático. Las redes Ad-Hoc pueden ser muy útiles para establecer la comunicación de voz entre un grupo de soldados en operaciones tácticas y también para que los militares aprovechen la tecnología de red habitual para mantener una red de información entre los soldados, los vehículos y la sede de información militar. Las redes Ad-Hoc también cumplen con los requisitos del mecanismo de comunicación muy rápidamente porque la red Ad-Hoc se puede configurar sin planificación e infraestructura, lo que facilita la comunicación entre las tropas militares a través del enlace inalámbrico. El otro factor importante que hace que MANET sea muy útil y que le permita encajar en el entorno militar es el hecho de que los objetos militares, como aviones, tanques y buques de guerra, se mueven a altas velocidades, y esta aplicación requiere de la comunicación rápida y confiable de MANET. La Figura 8 muestra un ejemplo de red Ad-Hoc en un entorno militar

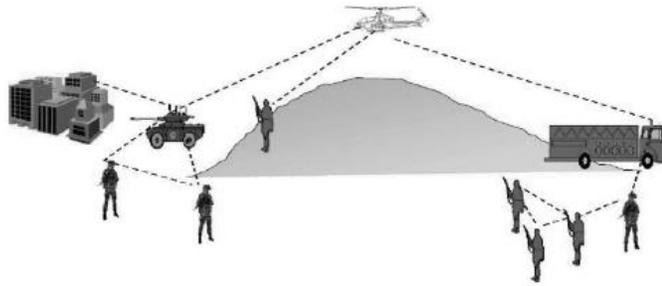


Figura 8 Aplicación militar de MANET.

Fuente: (Loo et al., 2016).

Elaborado por: (Loo et al., 2016).

- Sector comercial:** otro tipo de entorno que utiliza una red Ad-Hoc es la operación de rescate de emergencia. La forma de comunicación Ad-Hoc es especialmente útil en aplicaciones de seguridad pública, búsqueda y rescate. Los equipos médicos requieren comunicaciones rápidas y efectivas cuando se apresuran a un área de desastre para tratar a las víctimas. No pueden permitirse el tiempo para poner un cableado e instalar hardware de red. El equipo médico puede emplear redes Ad-Hoc como computadoras portátiles, teléfonos móviles, tabletas y pueden comunicarse a través del enlace inalámbrico con el hospital y el equipo médico en el sitio. Por ejemplo, un usuario en un lado del edificio puede enviar un paquete destinado a otro usuario en el otro extremo de la instalación, mucho más allá del rango de punto a punto de la WLAN, al hacer que los datos se enruten a través de dispositivos cliente hasta que llegue a su destino. Esto puede extender el alcance de la WLAN de cientos de metros a kilómetros, dependiendo de la concentración de usuarios inalámbricos. La comunicación en tiempo real también es importante ya que la comunicación de voz predomina en la comunicación de datos en tales escenarios. La Figura 9 muestra la aplicación de búsqueda y rescate en Ad-Hoc.



Figura 9 Aplicación de búsqueda y rescate de MANET.

Fuente: (Loo et al., 2016).

Elaborado por: (Loo et al., 2016).

- **Nivel local:** las redes Ad-Hoc pueden vincular de forma autónoma una red multimedia instantánea y temporal utilizando computadoras portátiles para difundir y compartir información entre los participantes en conferencias, reuniones o aulas. Otra aplicación de nivel local apropiada podría estar en redes domésticas, donde los dispositivos pueden comunicarse directamente para intercambiar información. De manera similar, en otros entornos civiles como taxis, estadios deportivos, barcos y aviones pequeños, las comunicaciones móviles Ad-Hoc tendrán muchas aplicaciones.
- **Redes de área personal (PAN):** es la interconexión de dispositivos de tecnología de la información dentro del rango de una persona, generalmente dentro de un rango de 10 m. Por ejemplo, una persona que viaja con una computadora portátil, un celular y una impresora portátil podría interconectarlos sin tener que enchufar nada utilizando alguna forma de tecnología inalámbrica. Por lo general, este tipo de PAN también podría interconectarse sin cables a Internet u otras redes. Una red de área personal inalámbrica (WPAN, por sus siglas en inglés) es prácticamente un sinónimo de PAN, ya que casi cualquier PAN necesitaría funcionar de forma inalámbrica. Conceptualmente, la diferencia entre un PAN y una WLAN es que el primero tiende a centrarse alrededor de una persona, mientras que el segundo es una red LAN que está conectada sin cables y sirve a múltiples usuarios. En la Figura 10 se muestra una red PAN.

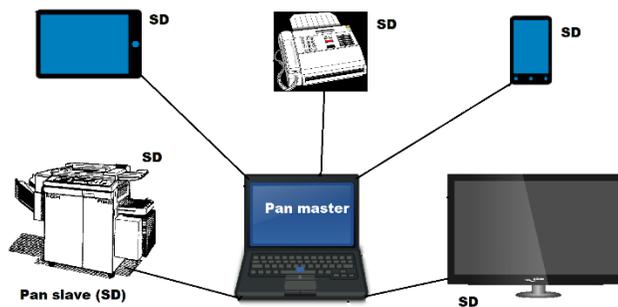


Figura 10 Red PAN.

Fuente: (Loo et al., 2016).

Elaborado por: Autor .

2.3. Protocolos de enrutamiento Ad-Hoc.

Se han diseñado varios protocolos Ad-Hoc para un enrutamiento preciso, rápido y confiable para un alto volumen de topología de red variable. Dichos protocolos deben lidiar con las limitaciones típicas de la topología de red cambiante, que incluyen alto consumo de energía, bajo ancho de banda y altas tasas de error. Estos protocolos de enrutamiento generalmente se

pueden clasificar en tres tipos principales: proactivo o basado en tablas, reactivo o según demanda, e híbrido. Esta clasificación diferencia los protocolos de enrutamiento según su técnica, su conteo de saltos, estado de enlace y enrutamiento de origen en un mecanismo de descubrimiento de ruta. En los protocolos basados en una técnica de conteo de saltos, cada nodo contiene información sobre el siguiente salto en su tabla de enrutamiento, vinculada al destino.

Tabla 1: Comparación de características de protocolos proactivos, reactivos e híbridos.

	Proactivo	Reactivo	Híbrido
Organización de red	Plano / jerárquico	Plano	Jerárquico
Difusión de la topología.	Periódico	Bajo demanda	Ambos
Latencia de ruta	Siempre disponible	Disponible cuando sea necesario	Ambos
Manejo de la movilidad	Actualizaciones periódicas	Mantenimiento de rutas	Ambos
Comunicación	Alto	Bajo	Medio

Fuente: (Loo et al., 2016).

Elaborado por: Autor

Los protocolos de enrutamiento de estado de enlace mantienen una tabla de enrutamiento para la topología completa, que se crea al encontrar la ruta más corta de los costos de enlace. En la técnica de enrutamiento de origen, todos los paquetes de datos llevan su información de enrutamiento como su encabezado. El nodo de origen puede obtener esta información de enrutamiento, por ejemplo: mediante un protocolo de enrutamiento de origen. La siguiente sección presentará los detalles de cada categoría de enrutamiento, incluidos algunos de los protocolos de enrutamiento existentes utilizados para esas categorías (Loo et al., 2016).

La tabla 1 proporciona una comparación de las características de los protocolos de enrutamiento híbridos, proactivos y reactivos (Loo et al., 2016).

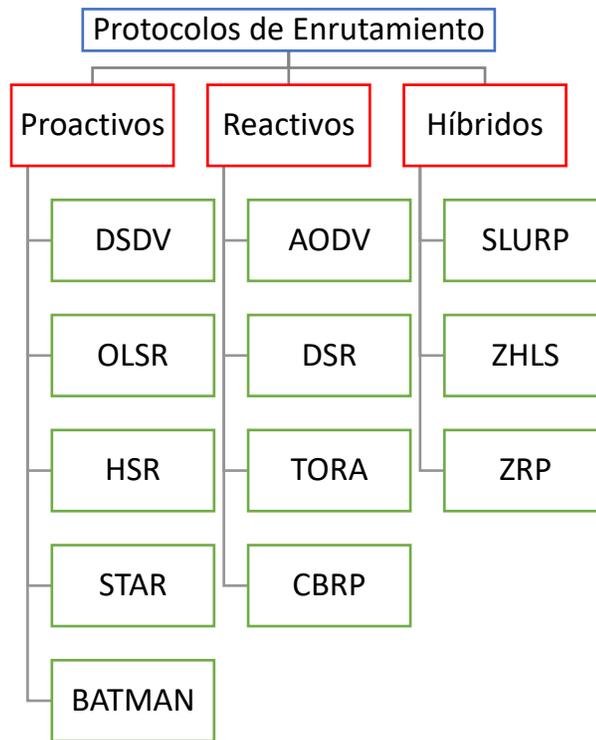


Figura 11 Protocolos de enrutamiento.

Fuente: Autor.

Elaborado por: Autor.

2.3.1. Protocolos de Enrutamiento Proactivo.

Los protocolos de enrutamiento controlados por tablas intentan mantener información de enrutamiento actualizada y consistente de cada nodo a cada otro nodo de la red. Estos protocolos requieren que cada nodo mantenga una o más tablas para almacenar información de enrutamiento, y responden a los cambios en la topología de la red mediante la propagación de actualizaciones en toda la red para mantener una vista de red consistente. Las áreas en las que difieren son el número de tablas necesarias relacionadas con el enrutamiento y los métodos por los cuales se transmiten los cambios en la estructura de la red. Las siguientes secciones discuten algunos de los protocolos de enrutamiento Ad-Hoc basados en tablas existentes (Royer, Toh, & others, 1999).

La Figura 12 ilustra el concepto de protocolos proactivos. Por ejemplo, si el nodo A decidió enviar algunos datos al nodo D, todo lo que tendría que hacer sería encontrar el nodo D en la tabla de topología reparada previamente, que se almacena en el nodo A. El análisis de la tabla es más rápido y equivale a menos potencia que la búsqueda de toda la red para un destino. Si los nodos de la red no tienen movilidad frecuente, la tabla de topología no consumirá

demasiada energía. En redes Ad-Hoc basadas en protocolos proactivos, el consumo de potencia y ancho de banda aumenta debido al intercambio de tablas de topología entre nodos después de cada cambio en la ubicación de los nodos. Esto ocurre incluso si la red está en modo de espera (por ejemplo, no hay transmisiones de datos en la red). El mejor contexto de red para los protocolos proactivos son las redes de movilidad baja (o ninguna) (Loo et al., 2016).

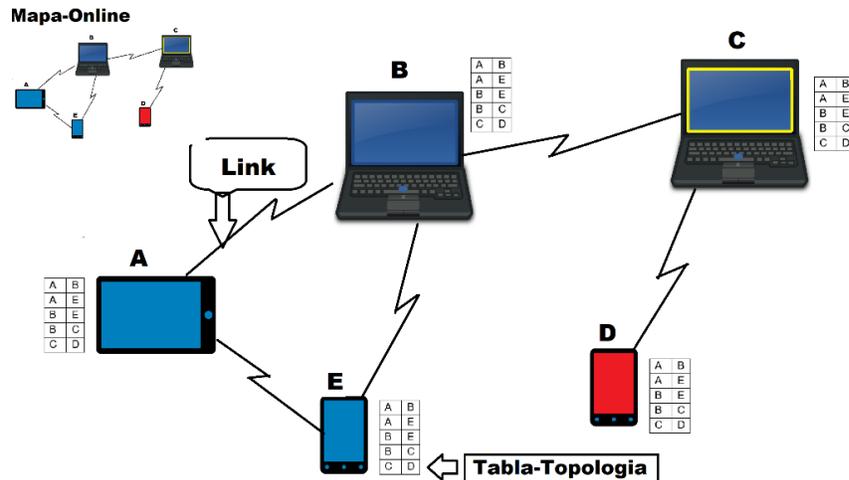


Figura 12: Protocolo de enrutamiento proactivo Ad-Hoc.

Fuente: (Loo et al., 2016).

Elaborado por: Autor

2.3.1.1. DSDV.

El protocolo DSDV es un protocolo proactivo (periódicamente, un nodo envía su tabla de rutas a sus vecinos) inspirado en el *Distance-Vector* junto con la implementación de números secuenciales. Estos permiten saber cuándo se ha cambiado una entrada en la tabla de enrutamiento (Dallora Moraes, Santos Xaud, & Santos Xaud, 2007; He, 2002).

Tabla de enrutamiento

Las entradas de la tabla de enrutamiento de este protocolo se tienen los siguientes campos:

- Los nodos de red que puede enviar datos: Destino.
- Siguiendo: Define para qué nodo adyacente el dato debe ser enviado para que llegue a su destino.

- Métrica: Es una medida de la distancia que muestra cómo muchos saltos es el destino.
- Número de secuencia: Número creado para la sincronización de la información recibida y la garantía de no - aparición de indeseables *bucles* sin fin.
- Tiempo de registro: Es una marcación temporal, a través de la cual se tomará la decisión de suprimir o no una nueva información topológica recibida.
- Estabilidad de los datos: Sirve como un puntero, indicando la tabla con la información sobre la estabilidad de la ruta (Dallora Moraes et al., 2007; He, 2002).

Actualización

Cuando un nodo recibe información de sus vecinos, éste comparará el número de secuencia de la información recibida y la de su propia tabla, si es más reciente, la actualización se realiza independientemente de otros parámetros, si es igual al de su tabla, sólo se realizará la actualización, si la métrica registrada es diferente de la recibida (Dallora Moraes et al., 2007; He, 2002).

Como solución para evitar la congestión en el medio se implementaron dos tipos de actualización:

La actualización incremental: En este tipo de actualización, el nodo envía a sus vecinos, en un solo paquete, solamente los cambios después de su presentación anterior, el nodo adyacente recibe el paquete y añade sus nuevas informaciones topológicas y lo repasa a sus adyacencias. Cuando no hay más espacio para los datos de este paquete, el tipo de actualización se cambia a actualización completa (Dallora Moraes et al., 2007; He, 2002).

Actualización completa: Es la situación en la que el nodo envía la información relativa a la totalidad de su mesa (Dallora Moraes et al., 2007; He, 2002).

2.3.1.2. OLSR.

Es un protocolo basado en estados de enlace, su función principal es limitar la cantidad de nodos de la red que reenvía los estados del enlace, a fin de que se puedan eliminar mensajes redundantes, para ello, utiliza una técnica llamada MPR (MultiPoint Relay). Para explicar mejor el funcionamiento de esta técnica, vamos a tomar de ejemplo una red Ad Hoc sin el uso del protocolo OLSR, en este caso, cuando un nodo recibe un paquete de control, normalmente retransmite estos datos a los nodos vecinos, por lo tanto, existe un fenómeno llamado

"inundación", por todos los que reciben los paquetes. Pero cada uno de ellos recibirá el mismo paquete varias veces desde diferentes vecinos, generando lo que se llama sobrecarga, es decir, la red operará sobrecargado de información redundante (Clausen et al., 2003; Dallora Moraes et al., 2007).

Con el funcionamiento del OLSR, el número de nodos que retransmitirá los paquetes será limitado. Esto funciona de la siguiente manera: entre los nodos de la red, habrá aquellos denominados MPR. La elección de cada MPR se realiza mediante un consenso entre sus nodos vecinos situados a un hop (salto). Entonces, cuando una información debe ser actualizada en la red, los paquetes enviados por un nodo llegarán a todos sus vecinos, pero sólo aquellos denominados MPR podrán retransmitir la información a continuación. Este proceso se repite con los próximos nodos a recibir los paquetes. De esta manera, cada nodo recibirá una sola vez la información, es decir, no habrá recibido los paquetes más de una vez (Clausen et al., 2003; Dallora Moraes et al., 2007).

El protocolo OLSR constituye un modo más organizado y eficiente de administrar el tráfico de paquetes de control entre dos nodos, siempre buscando el camino más corto (Clausen et al., 2003; Dallora Moraes et al., 2007).

2.3.2. Protocolos de Enrutamiento Reactivo.

Este tipo de enrutamiento crea rutas solo cuando lo desea el nodo de origen, cuando un nodo requiere una ruta a un destino, inicia un proceso de descubrimiento de ruta dentro de la red, este proceso se completa una vez que se encuentra una ruta o se han examinado todas las posibles excepciones de ruta, una vez que se ha establecido una ruta, se mantiene mediante un procedimiento de mantenimiento de la ruta hasta que el destino se vuelve inaccesible a lo largo de cada ruta desde la fuente o hasta que la ruta ya no sea deseada (Royer et al., 1999).

La Figura 13 muestra el protocolo de enrutamiento reactivo Ad-Hoc, en el cual no hay una tabla de topología en cada nodo. Cuando hay una solicitud en el nodo A para transmitir datos al nodo D, el proceso de descubrimiento de ruta se inicia mediante la difusión a todos los nodos que buscan el nodo D, cuando el nodo D recibe este mensaje, responde a la solicitud para construir la ruta al nodo A, el proceso se completa una vez que se encuentra una ruta o se han examinado todas las permutaciones de ruta posibles, una vez que se ha establecido una ruta, se mantiene mediante un procedimiento de mantenimiento de la ruta hasta que el destino se vuelve inaccesible a lo largo de cada ruta desde la fuente o la ruta ya no se desea.

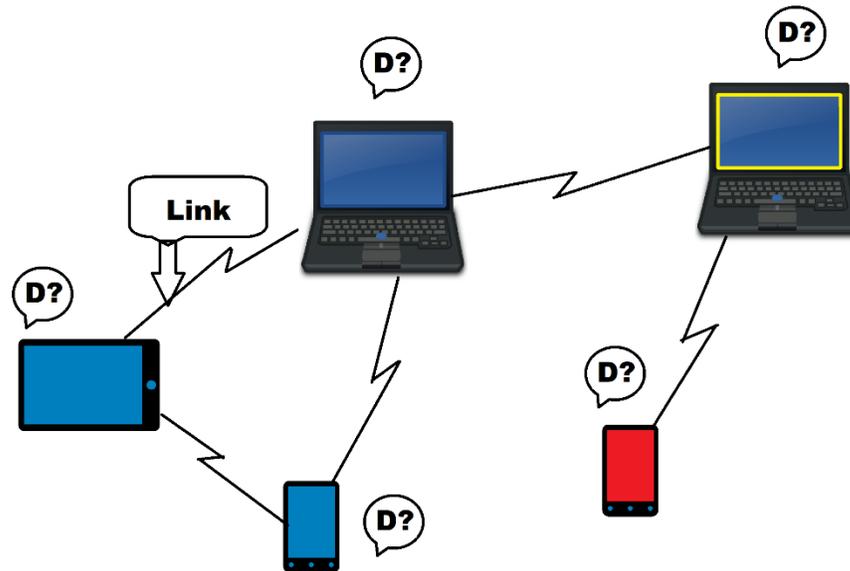


Figura 13: Protocolo de enrutamiento reactivo Ad-Hoc.

Fuente: (Loo et al., 2016).

Elaborado por: Autor

Una red que trabaja con un protocolo bajo demanda o reactivo, no almacenara la información de enrutamiento correcta para todos los nodos en todo momento, como alternativa, tal información de enrutamiento logra obtener bajo pedido, si un nodo necesita transmitir un mensaje y no dispone de la información necesaria de enrutamiento para enviar el mensaje al destino, se debe obtener la información necesaria, normalmente, el nodo quiere por lo menos determinar el siguiente salto (entre sus vecinos) para el paquete, no obstante el nodo podría sencillamente transmitir el paquete a todos los vecinos, esto produce una congestión grave en numerosos casos. No obstante, estas transmisiones se utilizan en un proceso de descubrimiento de ruta, ya que todavía no hay otra información disponible sobre el siguiente salto.

La ventaja de los protocolos de enrutamiento bajo demanda o reactivos radica en que el canal inalámbrico no requiere llevar una gran cantidad de datos de sobrecarga de enrutamiento para rutas que ya no se utilizan, esta ventaja puede reducirse en ciertos escenarios en los que hay mucho tráfico hacia una amplia gama de nodos, por lo tanto, estos escenarios tienen un fuerte impacto en el rendimiento, en un escenario que incluye grandes cantidades de tráfico a varios nodos, el tráfico de configuración de la ruta puede aumentar más que el tráfico constante de base para salvaguardar la información de enrutamiento precisa en cada nodo. No obstante, si

hay suficiente capacidad disponible, la eficiencia compacta (mayor sobrecarga) no puede influir en otros métodos de rendimiento como el rendimiento o la latencia (Loo et al., 2016).

2.3.2.1. AODV.

El protocolo AODV fue programado con el objetivo de ser un protocolo adaptativo a escenarios de alta movilidad, con el fin de evitar desperdicio de banda y minimizar el procesamiento en los nodos, que actúan como *cluters* en la red. Se utilizan tablas de enrutamiento tradicionales, es decir, se almacena sólo el siguiente salto para el nodo destino en cuestión (Dallora Moraes et al., 2007; Kumar Maurya, Sharma, Sahu, Roberts, & Srivastava, 2012).

Siendo un protocolo reactivo, cuando es necesario el envío de paquetes a un nodo destino que no consta en su tabla de enrutamiento, se inicia el Proceso de Descubrimiento de Rutas (Dallora Moraes et al., 2007; Kumar Maurya et al., 2012).

En el protocolo AODV, es importante resaltar la importancia del Mantenimiento de Rutas. Vista como un sub-protocolo de AODV, tiene el objetivo de validar las rutas contenidas en la caché. Como los nodos son móviles, su movimiento puede ocasionar la ruptura de un enlace antes existente y presente en las tablas de enrutamiento de los nodos. En este protocolo las rutas para el mantenimiento, se envían periódicamente paquetes llamados HOLA entre los nodos para verificar la existencia y ruptura de rutas. Cuando uno de estos paquetes es esperado por algún nodo, pero no se recibe, éste detecta el error de transmisión (por ejemplo, un salto de conexión y, a continuación, se envía inmediatamente un paquete de indicador de error (RERR) al nodo de origen y para todos los nodos que sean necesarios avisando sobre el error, un nodo, al recibir este paquete, tiene su caché actualizada, para eliminar de sus rutas almacenadas todas las sub rutas posteriores a las conexiones rotas (Dallora Moraes et al., 2007; Kumar Maurya et al., 2012).

2.3.3. Protocolos de Enrutamiento Híbrido.

Basados en la combinación de ambos protocolos de enrutamiento proactivos y reactivos, se han propuesto algunos protocolos de enrutamiento híbrido para combinar las ventajas de los protocolos proactivos y reactivos. El protocolo híbrido más típico es un protocolo de enrutamiento de zona. Con respecto a la división principal de los protocolos de enrutamiento, la

Los protocolos de enrutamiento híbridos se prefieren usar en las redes de gran tamaño con una gran cantidad de nodos. La gran mayoría de protocolos híbridos están basados en zonas, el enrutamiento dentro de la zona se realiza proactivamente mientras que fuera de la zona se realiza reactivamente (Rey, Quiñones, & García, 2014).

Algunos protocolos híbridos son:

ZRP (Zone Based Routing Protocol)

El protocolo de enrutamiento de zona, como su nombre lo indica, se basa sobre el concepto de zonas. Se define una zona de enrutamiento para cada nodo por separado, y las zonas de vecinos los nodos se superponen. La zona de enrutamiento tiene un radio p expresado en lúpulo La zona incluye los nodos, cuya distancia desde el nodo en cuestión es como máximo p saltos(Beijar, 2002).

CAPÍTULO III. VOZ SOBRE IP

3.1. VoIP.

VoIP es la transmisión de "paquetes de datos" de voz de una dirección IP a otra a través de Internet. Desarrollado alrededor de 1995, originalmente sirvió como una solución alternativa para las tarifas telefónicas internacionales y de larga distancia. Con menos de dos décadas, VoIP ha revolucionado la comunicación en todo el mundo ("The History of VoIP - From The Beginning Til Present Time," 2016).

Hoy en día, es muy común que las grandes empresas utilicen VoIP debido a que este permite disminuir gastos, gracias a que no se necesita pagar grandes cuentas telefónicas gracias a esta tecnología.

3.1.1. Funcionamiento de VoIP.

VoIP opera mediante la transferencia de señales de voz entre direcciones IP, lo que significa que estas señales deben transformarse en datos lo suficientemente pequeños como para transmitir, las muestras vocales del remitente se dividen en "paquetes" de voz, que reciben información de enrutamiento y se envían al extremo receptor. Los paquetes se transmiten uno por uno, luego se vuelven a formar tan cerca del estado original como sea posible, creando una voz completa, este proceso comprime la señal de voz y luego descomprime la señal del lado receptor ("The History of VoIP - From The Beginning Til Present Time," 2016).

En la Figura 14 se muestra un sistema VoIP.

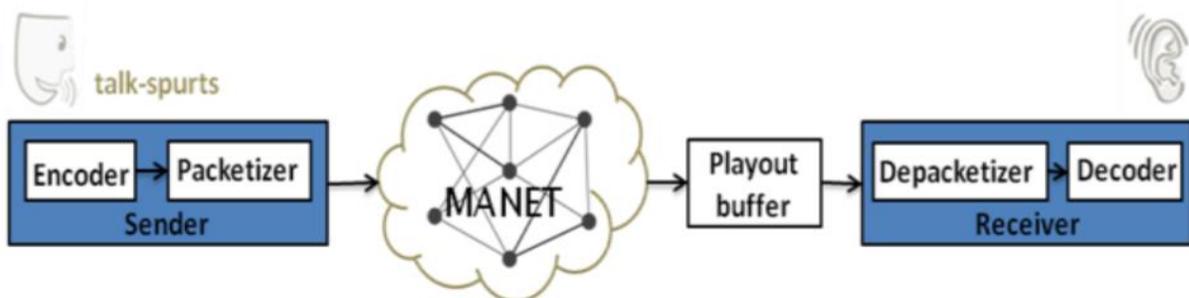


Figura 14: Sistema VoIP.

Fuente: (Bouhorma, Boudhir, & others, 2011).

Elaborado por: Bouhorma, Boudhir, & others.

3.1.2. Calidad de la voz.

Una de las principales preocupaciones sobre VoIP es la calidad de voz, los factores que afectan la calidad de la voz incluyen el retardo, el *jitter* y la pérdida de paquetes, el retardo, se define

como el tiempo promedio de "viaje" que tarda un paquete en pasar por la red, desde el origen hasta el destino. Hay básicamente dos tipos de retardo en la red actual: retardo de propagación y retardo de manejo. El retardo de propagación (aproximadamente 1 milisegundo por cada 161 kilómetros) ocurre cuando los paquetes viajan a través de cables basados en fibra óptica o basados en cobre, el retardo en el manejo se debe a que los dispositivos de hardware procesan la información de voz (Chong & Matthews, 2004).

Se necesita tiempo para digitalizar, comprimir, empaquetar una señal de voz para su transmisión en la red de datos, se transmite a través de conmutadores, enrutadores, y almacena en el extremo distante para asegurarse de que todos los paquetes lleguen antes de transmitirlos al usuario final. En el extremo opuesto, se necesita más tiempo para desempaquetar, descomprimir y convertirlo de nuevo en una señal de voz, este proceso es típico de todas las transmisiones de red.

Para las transmisiones de datos típicas, la latencia no es un problema importante, sin embargo, para las llamadas de voz, la latencia puede causar un retardo molesto entre cuando se pronuncia una palabra y cuando se escucha.

Por lo tanto, la característica de "mejor esfuerzo" de Internet no es lo suficientemente buena, dado que los paquetes de voz compiten con el tráfico de datos no en tiempo real, si hay ráfagas de tráfico en la red o un problema de congestión, esto puede resultar en tiempos de llegada variados para los paquetes de voz, cuando los paquetes de voz consecutivos llegan a intervalos irregulares, el resultado es una distorsión del sonido, que puede hacer que el hablante sea inentendible si la distorsión es grave.

El jitter máximo es de 75 milisegundos, pero para tener una comunicación clara se recomienda como máximo 50 milisegundos para que los paquetes de voz se entreguen correctamente, la pérdida de paquetes es el porcentaje de paquetes no entregados en la red de datos, cuando se pierden paquetes de datos, una computadora receptora simplemente puede solicitar una retransmisión, cuando los paquetes de voz se pierden o llegan demasiado tarde, se descartan en lugar de retransmitirse, el resultado es lagunas desconcertantes en la conversación, según los estándares de la industria, la pérdida de paquetes se divide en dos grupos pérdida en ráfaga y pérdida total en la conversación la pérdida máxima tolerada en ráfaga es de 3% mientras que la pérdida máxima total es de 20% (Chong & Matthews, 2004; Matango, 2016; Kelly, 2002).

3.1.3. Ventajas de VoIP.

Cuando se introdujo la tecnología de voz sobre IP, a finales de los años 90, su principal función era la de ahorrar dinero al hacer una llamada al otro lado del país o del planeta, ya que mediante la tecnología de VoIP la llamada tenía el costo de una llamada local. En estos inicios la calidad de voz era muy baja pero lo suficiente mente buena para una llamada de tipo personal, hoy en día esto ha cambiado gracias a las nuevas tecnologías, esto ha hecho que su popularidad aumente ya que consta de más ventajas que solo su costo reducido (Falcón, 2007).

Según Asián Arantxa (2014) algunas de las ventajas de usar un sistema de VoIP son:

- **Infraestructura simplificada.** La eliminación de las líneas de voz especializadas significa que ya no se necesitará separar la red de voz de la de datos. Debido a esto se reducirán los costos ya que ahora los dos funcionan sobre los mismos equipos y solo se necesita de un equipo para dar mantenimiento a los sistemas.
- **Administración más sencilla.** Dado que el paso a VoIP se basa en software más que en hardware, es más sencillo de modificar y de mantener.
- **Mayor productividad.** VoIP trata la voz como cualquier otro dato por lo cual los usuarios pueden adjuntar documentos a mensajes de voz o llevar parte en reuniones virtuales con datos compartidos y videoconferencias.
- **Escalabilidad.** Los sistemas telefónicos basados en la tradicional central telefónica privada vienen en diferentes tamaños y es probable que de vez en cuando sea necesario descartar los sistemas y reemplazar el hardware. Esto no sucede con los sistemas VoIP ya que como mencionamos anterior mente estos se basan en software por lo que son fácil mente escalables sin necesidad de reemplazar el hardware.
- **Conexiones flexibles.** Si su empresa tiene su propia red privada virtual (VPN) y la combina con VoIP, puedes establecer una oficina en cualquier lugar donde haya una conexión de banda ancha. Con un teléfono VoIP, puedes realizar o recibir llamadas como si estuviera en su oficina ya que los teléfonos IP al funcionar con una dirección IP se los puede llevar a cualquier parte y mantendrá el mismo número telefónico.

3.1.4. Características de VoIP.

Según Contreras Leidy (2009) las principales características son:

- Permite controlar el tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento.

- Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.
- Es independiente del hardware utilizado.
- Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.
- Permite la integración de Video y TPV

3.2. Voz sobre IP en Redes MANET.

El aumento que se ha producido en los últimos años de las aplicaciones multimedia por medios inalámbricos y especialmente sobre redes MANET, como son: VoIP, audio conferencias y video conferencias. Estas aplicaciones también necesitan que se ofrezca garantías de QoS, debido a que las aplicaciones multimedia son sensibles a la variabilidad de los recursos que provee la red (Murazzo, Rodriguez, Guevara, & Scheffer, 2014).

Gracias a la tecnología de VoIP la señal de voz puede viajar a través de la red usando el protocolo IP, mediante el envío de una señal de voz digitalizada, por medio de paquetes de datos, a diferencia de enviarla en forma análoga por medio de circuitos, como lo hace la telefonía convencional como PSTN (Public Switched Telephone Network). Combinando esto con el uso de las redes MANET abre la puerta a muchas posibilidades de conexión en lugares remotos o donde no sea posible desplegar una infraestructura de red.

VoIP es un servicio que se efectúa en tiempo real en el que el retardo y pérdidas influyen directamente en la calidad de la llamada, sumando esto a el uso de las redes MANET las cuales presentan más desafíos por la movilidad de los nodos y los recursos limitados de los mismos, se presenta el desafío de brindar a los usuarios los usuarios QoS igual o similar al que puede proporcionar las redes PSTN.

CAPÍTULO IV. PARÁMETROS DE CALIDAD Y ENTORNO DE SIMULACIÓN

4.1. Parámetros de QoS en Redes MANET.

Con el uso incremental que ha surgido de aplicaciones multimedia y aplicaciones de gestión con requisitos específicos en cuanto al ancho de banda o retardo en las redes, ha causado que la provisión de un nivel de calidad de servicio en la red sea un objetivo primordial.

Como se ha mencionado con anterioridad las redes MANET, son dinámicas y aleatorias; por esta razón, las situaciones de tráfico son muy variables, haciendo que proveer QoS a las aplicaciones sea complicado, asimismo, las variaciones y las limitaciones de energía que tienen los nodos pueden producir cambios frecuentes en la topología y conectividad. Por lo cual las MANET deben adaptarse dinámicamente para ser aptos de mantener las conexiones activas a pesar de estos cambios (Murazzo et al., 2014).

El término QoS hace referencia a la capacidad de una red para dar garantía de proveer un grado de fiabilidad en el servicio de transmisión de información, a través de una red (Murazzo et al., 2013). Los parámetros que utilizaremos para medir las mismas se han mencionado anteriormente y son: el retardo, el jitter y la pérdida de paquetes.

Según Hanzo & Tafazolli (2007) los problemas frente a la disposición de QoS en MANETS son:

- **Canal inalámbrico no confiable:** el canal inalámbrico es propenso a errores de bit debido a la interferencia de otras transmisiones, ruido térmico, sombreado y efectos de desvanecimiento por trayectos múltiples. Esto hace que sea imposible proporcionar una relación de entrega de paquetes duros o garantías de longevidad de enlace.
- **Movilidad del nodo:** Los nodos en un MANET pueden moverse de forma completamente independiente y aleatoria en lo que respecta a los protocolos de comunicación, esto significa que la información de la topología tiene una duración limitada y debe actualizarse con frecuencia para permitir que los paquetes de datos se enruten a sus destinos. Nuevamente, esto invalida cualquier relación de entrega de paquetes o garantías de estabilidad del enlace, además, un estado de QoS que depende de la posición del enlace o del nodo debe actualizarse con una frecuencia que ocurra por movilidad del nodo.

Una suposición general importante también debe indicarse aquí: para que cualquier protocolo de enrutamiento pueda funcionar correctamente, la tasa de cambio de topología no debe ser mayor que la tasa de propagación de información de estado, de lo contrario, la información de enrutamiento siempre será obsoleta y el enrutamiento será

ineficiente o incluso podría fallar por completo, esto se aplica igualmente al estado de QoS y la información de ruta de QoS. Una red que satisface esta condición se dice que es combinatoriamente estable.

- **Falta de control centralizado:** la principal ventaja de una red Ad-Hoc es que puede configurarse de forma espontánea, sin planificación, y sus miembros pueden cambiar dinámicamente. Esto hace que sea difícil proporcionar cualquier forma de control centralizado, como tales, se prefieren los protocolos de comunicaciones que utilizan solo el estado disponible localmente y operan de manera completamente distribuida, esto generalmente aumenta la complejidad de un algoritmo, ya que la información del estado de QoS debe diseminarse de manera eficiente.
- **Contención del canal:** Para descubrir la topología de red, los nodos de MANET deben comunicarse en un canal común. Sin embargo, esto introduce los problemas de interferencia y contención del canal, para las comunicaciones de datos de igual a igual, se pueden evitar de varias maneras, una forma es intentar la sincronización del reloj global y usar un sistema basado en TDMA (División de tiempo de acceso múltiple) donde cada nodo pueda transmitir en un momento predefinido. Esto es difícil de lograr debido a la falta de un controlador central, la movilidad de los nodos y la complejidad y los gastos generales involucrados.

Otras formas son usar una banda de frecuencia diferente o un código de expansión como CDMA para cada transmisor, esto requiere un mecanismo de selección de canal distribuido, así como la difusión de información del canal. Sin embargo, las comunicaciones de datos tienen lugar, sin un controlador central, parte de la configuración, el descubrimiento de nuevos vecinos y las operaciones de control deben tener lugar en un canal común, de hecho, evitando las complicaciones mencionadas anteriormente, gran parte de la investigación de MANET, así como la tecnología de redes inalámbricas Ad-Hoc (802.11x) actualmente más popular, se basa en el acceso total a un canal común, es decir, con acceso múltiple con detección de portadora y colisión, evitación (CSMA / CA).

Sin embargo, CSMA / CA complica enormemente el cálculo del rendimiento potencial y el retardo del paquete, en comparación con los enfoques basados en TDMA, esto se debe a que los nodos también deben tener en cuenta el tráfico en todos los nodos dentro de su rango de detección de portadora. Además, también surge la posibilidad de colisiones. Las colisiones desperdician la capacidad del canal, así como la energía de la

batería del nodo, aumentan el retardo y pueden degradar la proporción de entrega de paquetes.

- **Recursos limitados del dispositivo:** hasta cierto punto, esta es una limitación histórica, ya que los dispositivos móviles son cada vez más potentes y capaces, sin embargo, sigue siendo cierto que, en general, tales dispositivos tienen menos potencia de cómputo, menos memoria y una fuente de alimentación limitada, en comparación con los dispositivos como las computadoras de escritorio que se suelen emplear en las redes cableadas, este factor tiene un gran impacto en la provisión de garantías de QoS, ya que la baja capacidad de memoria limita la cantidad de estado de QoS que se puede almacenar, lo que requiere actualizaciones más frecuentes, lo que conlleva una mayor sobrecarga.

El enrutamiento de QoS generalmente conlleva una mayor sobrecarga que el enrutamiento de mejor esfuerzo en primer lugar, debido a la información adicional que se está difundiendo, estos factores llevan a un mayor consumo de energía limitada de la batería de los nodos móviles, finalmente, dentro del conjunto de problemas de enrutamiento de QoS, muchos son NP-completos (tiempo polinomial no determinista) y, por lo tanto, se requieren complicadas heurísticas para resolverlos, lo que puede poner una tensión indebida en los procesadores menos potentes de los nodos móviles.

4.2. Parámetros fundamentales que influyen en el desempeño de las aplicaciones de voz.

El primer paso para elegir métricas importantes que evalúen el comportamiento real de las redes Ad-Hoc en un contexto de VoIP es definir las diferentes situaciones que experimentará el usuario, él puede sentir una comunicación normal, su comunicación puede ser perturbado por clics o pérdida de su interlocutor o simplemente puede tener la sensación de que está teniendo una comunicación distante.

Todas estas situaciones se pueden traducir en dos escenarios diferentes para los protocolos de enrutamiento Ad-Hoc: existe una ruta entre los dos usuarios, o actualmente no existe una ruta válida entre los usuarios. En este último caso, se está buscando o reparando una ruta (Thibodeau, Youssef, & Houle, 2006).

En el primero de los dos casos, la red retransmite paquetes de datos normalmente puede haber una pequeña tasa de pérdida de paquetes, si se vuelve demasiado grande, el protocolo de enrutamiento invalidará la ruta y dejará este modo, por lo tanto, la relación de pérdida de paquetes puede ser una métrica estudiada.

La principal preocupación cuando la red tiene una ruta válida entre dos usuarios es el retardo, este es un tema crítico en VoIP, el retardo unidireccional tolerable de ninguna manera debe exceder los 400 ms y el retardo promedio debe ser inferior a 150 ms para que el usuario permanezca casi inadvertido, según lo define la UIT G.114, esta métrica ya está bien descrita y se utiliza en la evaluación de redes Ad-Hoc.

Vinculado al retardo está la métrica del jitter, VoIP utiliza buffers para minimizar el efecto de la fluctuación de fase, pero agregan cierto retardo, lo que deja menos margen para el retardo de transmisión en la red. Esta métrica de red debe minimizarse absolutamente para optimizar el retardo detectado por el usuario (Thibodeau et al., 2006).

4.2.1. Pérdida de paquetes.

El evento de pérdida siempre está relacionado con la red. Una red IP presenta algunas características de correlación a corto plazo, es decir, si se pierde el paquete n , también se podría perder el paquete $(n + 1)$. Este fenómeno provoca la pérdida de reventón, aparte del porcentaje global de paquetes perdidos, la ráfaga es importante, en particular, para una estimación correcta de la calidad de la voz, de hecho, aproximar las pérdidas por estallido como serían aleatorias implica una sobreestimación de la degradación de la calidad del habla, la pérdida generalmente se modela mediante un modelo de Gilbert de dos estados (Modelo de Gilbert ver el anexo 1). Por lo general, el umbral de la tasa global de pérdida de paquetes para una buena calidad se fija en el 20%, esto significa que para valores mayores de pérdida general, la calidad de voz se verá afectada (Fabrizio, 2010; Matango, 2016).

Para calcular la pérdida de paquetes se utiliza la ecuación 1:

$$Pp = Pt - Pr$$

Ecuación 1: Pérdida de paquetes.

Donde:

Pp = Paquetes perdidos

Pt = Paquetes transmitidos (todos los paquetes)

Pr = Paquetes recibidos

4.2.2. Retardo.

Las aplicaciones de VoIP son muy sensibles al retardo, aunque pueden tolerar la pérdida de paquetes hasta cierto punto, el retardo de extremo a extremo o extremo a intermedio es uno de los principales factores que afectan la QoS y según ITU-T G.114 tenemos algunas recomendaciones sobre el retraso, donde los retrasos menores a 200ms se consideran

aceptables, mientras que, 200 a 400 ms merecen atención y más de 400 ms se consideran inaceptables ya que la señal de voz se degrada demasiado. En UIT-T G.114 tenemos el gráfico que se muestra en la Figura 16. El retardo puede ocurrir en el extremo del remitente, el extremo del receptor y en la red. El retardo en el remitente se debe al CODEC (Codificador/Descodificador), la paquetización y el procesamiento. Puede ocurrir en todo el proceso antes de transmitir los paquetes de voz. El retardo en el receptor se debe a la decodificación, al descomprimir los paquetes de voz. Los retardos de cola, transmisión y propagación se incluyen en la categoría de retardo de red (Chandel & Sharma, 2016; ITU-T, 2003).

G.114 es una recomendación de la UIT que aborda los retrasos aceptables para las aplicaciones de voz, está orientada a las telecomunicaciones nacionales y es más estricta que lo que normalmente se aplica en las redes de voz privadas.

Una de las cosas que aborda es el retraso de la voz. Dice que <150 milisegundos es aceptable,> 400 milisegundos es inaceptable y entre personas se debe informar sobre problemas de calidad. Los retrasos prolongados pueden hacer que las personas se "hablen" involuntariamente durante una conversación.

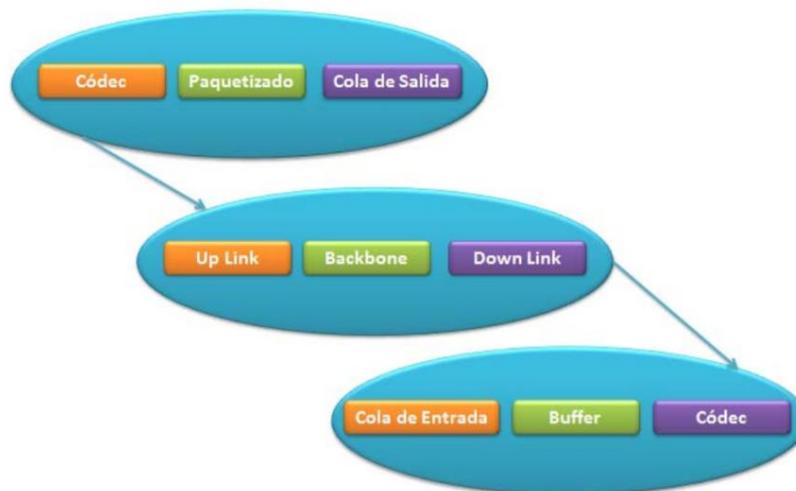


Figura 15: Distintos componentes del retardo.

Fuente: (Sing-Borrajo & Rodríguez-López, 2012).

Elaborado por: Autor.

Los componentes fundamentales en el retardo de extremo a extremo son los siguientes:

- Retardo de la Red.
- Retardo del CODEC.
- Retardo del Buffer receptor.

El retardo también incluye el tiempo que sea necesario para calcular una nueva ruta y cualquier otro retardo de ruteo, por ejemplo, otro nodo Ad Hoc.

Para calcular el retardo se utiliza la ecuación 2:

$$Retardo = \frac{delaySum}{rxPackets} E$$

Ecuación 2: Retardo.

Donde:

delaySum = Suma de todos los retrasos de extremo a extremo para todos los paquetes recibidos del flujo.

rxPackets = Número total de paquetes recibidos para el flujo.

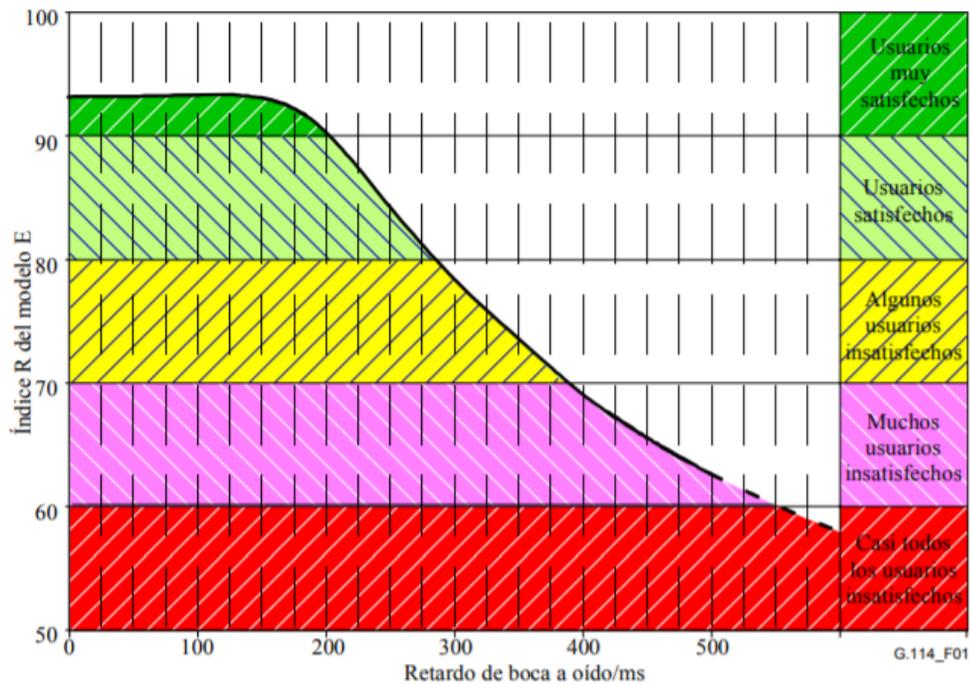


Figura 16: Distintos componentes del retardo.

Fuente:(ITU-T, 2003).

Elaborado por: ITU-T.

4.2.3. Jitter.

Uno de los factores más perjudiciales es el jitter de transmisión de paquetes durante la transmisión, denominada fluctuación de fase, causada por la variabilidad temporal de las condiciones de la red (Atzori, Boi, & Nonnis, 2008).

Tiene más efectos negativos en la calidad de voz, el buffer de jitter se utiliza para almacenar los paquetes que no se reciben al mismo tiempo, el número de paquetes almacenados en el buffer de fluctuaciones crea una cola que hace que la conversación sea fluida, a veces, la cantidad de paquetes recibidos es mayor que el tamaño del buffer por lo cual puede ocurrir una condición de desbordamiento de buffer, la condición de desbordamiento de buffer también puede ocurrir cuando se necesitan paquetes para consumir, pero no hay paquetes en el buffer, por lo tanto, se introducen varios algoritmos de buffer adaptativo, para ajustar el tamaño del buffer para mejorar la calidad de VoIP, el jitter como norma general no debe superar los 50ms (Chandel & Sharma, 2016; Kelly, 2002).

Para calcular el jitter se utiliza la ecuación 3:

$$jitter = \frac{jitterSum}{rxPackets - 1}$$

Ecuación 3: Jitter.

Donde:

jitterSum = Suma de todos los valores de jitter para todos los paquetes recibidos del flujo.

rxPackets = Número total de paquetes recibidos para el flujo.

4.2.4. Codec.

De uno de los parámetros que depende QoS, en una red VoIP, es del tipo de CODEC usado para transmitir la conversión de paquetes de voz analógica a digital, en el extremo del remitente y de digital a analógico en el extremo del receptor se requiere del CODEC. El CODEC es la base de la aplicación VoIP. Hay una variedad de CODECS con diferente ancho de banda y características. Existen muchas técnicas de codificación desarrolladas y estandarizadas por la ITU (Internacional Telecommunications Union) (Chandel & Sharma, 2016).

La Figura 16 muestra como antes de transmitir un paquete sobre la red, la señal de voz tiene que ser digitalizada en el transmisor y el proceso inverso se realizado en el receptor.

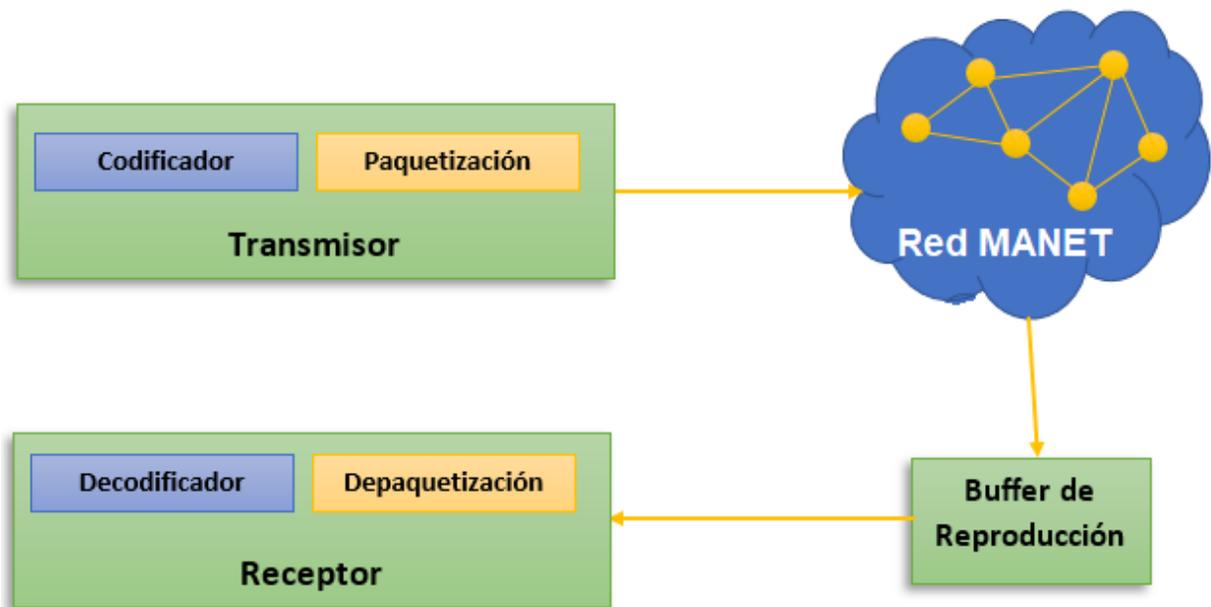


Figura 17: Sistema VoIP.

Fuente: (Chandel & Sharma, 2016).

Elaborado por: Autor.

Los codecs utilizados para VoIP son G.711, G.722, G.723, G.726, G.728 y G.729A. Estos codecs tienen una calidad de sonido diferente, el ancho de banda requerido, el tamaño del paquete IP, el retardo de codificación y el algoritmo de codificación. La tabla 2 muestra las características de los codecs más populares G.711, G.723.1, G.729A y GSM (Chandel & Sharma, 2016; Perdana, Munadi, & Perdana, 2016).

Tabla 2: Atributos de los diferentes codecs de VoIP.

CODEC	Razón de Bits (kbps)	Tamaño de la muestra (bytes)	Paquetes por segundo	Tamaño del payload (bytes)
G.711	64	80	50	160
G.723.1	6.3	24	34	20
G.729A	32	20	34	80
GSM	13	20	50	33

Fuente: (Chandel & Sharma, 2016; Perdana et al., 2016).

Elaborado por: Autor.

El codec que se usará en este proyecto es el G.711 el cual es un codec de banda completa. El mismo que presenta una nueva experiencia en la transmisión de audio, que no solo busca proporcionar calidad en la voz humana, sino que pretende captar el sonido ambiental.

4.3. Requerimientos del simulador.

El software a ocupar debe cumplir la mayor parte de los siguientes requisitos. Si no cumple alguno de los requisitos se deberá ver cuáles son las implicaciones de este y si es factible que se implemente:

- El simulador debe ser capaz de representar la pérdida de paquetes, el retardo y el jitter.
- Soportar protocolos Wi-Fi más comunes, protocolos de enrutamiento para redes MANET y la pila de protocolos TCP/IP.
- Tener un módulo para aplicaciones de VoIP o posibilidad de su implementación.
- Ser un simulador aceptado dentro de la comunidad científica.
- Que sea posible de configurar modelos de movilidad, modelos de propagación, extensión del área de movilidad, posicionamiento de nodos, potencia de los nodos.

4.4. Network Simulator (NS3).

NS3 es un simulador de red de eventos discretos, enfocado principalmente para la investigación y el uso educativo. NS3 es software libre bajo la licencia de GNU GPLv2, que está disponible públicamente para su uso. NS3 fomenta el desarrollo de modelos de simulación que sean lo suficientemente realistas como para permitir que NS3 se use como un emulador de red en tiempo real que pueda interconectarse con el mundo real y que permita que muchas implementaciones de protocolos del mundo real sean reutilizadas dentro de NS3, el núcleo de simulación de NS3 admite la investigación en redes IP y no IP, la mayoría de sus usuarios se centran principalmente en simulaciones inalámbricas / IP que incluyen modelos para las capas 1 y 2 y una variedad de protocolos de enrutamiento estático o dinámico, como OLSR y AODV para aplicaciones basadas en IP (Patel & Kamboj, 2015).

NS3 también admite un programador en tiempo real que facilita una serie de casos de uso de "simulación en el bucle" para interactuar con sistemas reales. Por ejemplo, los usuarios pueden enviar y recibir paquetes generados por NS3 en dispositivos de red reales, y NS3 puede funcionar como un marco de interconexión entre máquinas virtuales (Patel & Kamboj, 2015).

Cada simulador tiene sus ventajas y desventajas, por ende, cada uno es más adecuado para un propósito específico, para este trabajo se ha escogido NS3, debido a que cumple con los requerimientos especificados, además de la gran cantidad de documentos en forma de tutoriales, artículos, con los que cuenta lo hacen un simulador ideal para este trabajo. Su instalación se explica en el anexo 2.

Algunos puntos importantes de NS3 son:

- NS3 no es compatible con versiones anteriores de NS2; Está construido desde cero para reemplazar a NS2.
- NS3 está escrito en C ++, el lenguaje de programación Python puede usarse opcionalmente como interfaz.
- NS3 está tratando de resolver los problemas presentes en NS2.
- Hay un número muy limitado de códigos contribuidos realizados con NS3 en comparación con NS2.
- En NS2, el sistema bilingüe hace que la depuración sea compleja (C ++ / Tcl), pero para NS3 el conocimiento único de C ++ es suficiente (la arquitectura en un solo idioma es más robusta a largo plazo).
- NS3 tiene un modo de emulación, que permite la integración con redes reales.

4.4.2. Clases fundamentales.

Aquí veremos unos términos que son comúnmente usados en redes, pero tienen un significado específico en NS3.

Para poder trabajar con NS3 es fundamental familiarizarse con las clases y módulos de C++ que se encuentran implementados y son fundamentales para simular cualquier tipo de red. Todas las funcionalidades de NS3 están implementadas en clases de C++ que se encuentran en el código del programa.

4.4.2.1. *Application (aplicación).*

En NS3, la abstracción básica para un programa de usuario que genera cierta actividad a simular es la aplicación. Esta abstracción está representada en C ++ por la clase *Application*. La clase *Application* proporciona métodos para administrar las representaciones de nuestra versión de aplicaciones de nivel de usuario en simulaciones (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

4.4.2.2. Channel (canal).

En el mundo simulado de NS3, uno conecta un *Node* a un objeto que representa un canal de comunicación. En este caso, la abstracción de subred de comunicación básica se denomina canal y está representada en C ++ por la clase *Channel* (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

La clase *Channel* proporciona métodos para administrar objetos de subred de comunicación y conectar nodos a ellos, los canales también pueden ser especializados por los desarrolladores en el sentido de la programación orientada a objetos. Una especialización de canal puede modelar algo tan simple como un cable, el canal especializado también puede modelar cosas tan complicadas como un gran conmutador Ethernet o un espacio tridimensional lleno de obstáculos en el caso de las redes inalámbricas (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

4.4.2.3. Node (nodo).

En el idioma de Internet, un dispositivo informático que se conecta a una red se denomina host. Porque NS3 es un simulador de red, no específicamente un simulador de Internet, intencionalmente no usamos el término host ya que está estrechamente asociado con Internet y sus protocolos. En su lugar, usamos un término más genérico también usado por otros simuladores que se originan en la Teoría de Grafos – *Node* (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

En NS3, la abstracción del dispositivo informático básico se denomina Node. Esta abstracción está representada en C ++ por la clase Node. La clase Node proporciona métodos para gestionar las representaciones de dispositivos informáticos en simulaciones (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

Debe pensar en un nodo como una computadora a la que agregará funcionalidad. Uno agrega cosas como aplicaciones, las pilas de protocolos y las tarjetas periféricas con sus controladores asociados permiten que la computadora haga un trabajo útil. Usamos el mismo modelo básico en NS3 (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

4.4.2.4. *NetDevice (dispositivo de red).*

En NS3, la abstracción del dispositivo de red cubre tanto el controlador de software como el hardware simulado. Un dispositivo de red está "instalado" en un nodo para permitir que el nodo se comunique con otros nodos en la simulación a través de los canales. Al igual que en un computador real, un nodo puede estar conectado a más de un canal a través de múltiples *NetDevices* (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

La abstracción del dispositivo de red está representada en C ++ por la clase *NetDevice*. La clase *NetDevice* proporciona métodos para administrar conexiones a objetos de *Node* y *Channel*; y puede ser especializado por los desarrolladores en el sentido de la programación orientada a objetos. Al igual que una NIC (Tarjetas de Interfaz de Red del inglés Network Interface Cards) Ethernet está diseñada para funcionar con una red Ethernet, *CsmaNetDevice* está diseñada para funcionar con un *CsmaChannel*; El dispositivo *PointToPointNetDevice* está diseñado para funcionar con un canal *PointToPoint* y un dispositivo *WifiNet*. El dispositivo está diseñado para funcionar con un canal Wifi (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

4.4.3. Topologías de ayuda.

En una red real, encontrará computadoras host con NIC agregadas (o integradas). En NS3 encontrará Nodos con *NetDevices* adjuntos. En una gran red simulada, tendrá que organizar muchas conexiones entre *Node*, *NetDevices* y *Channel* (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

Dado que conectar *NetDevices* a nodos, *NetDevices* a canales, asignar direcciones IP, etc., son tareas comunes en NS3, este proporciona topologías de ayuda para que esto sea lo más fácil posible (ns-3 Tutorial Release ns-3.23 ns-3 project, 2015).

Ejemplos de topologías de ayuda:

- *NodeContainer*: proporciona una forma conveniente para crear, administrar y acceder a cualquier objeto, nodo que haya sido creado para usar una simulación.
- *InternetStackHelper*: instala un *stack* de protocolos en los nodos.
- *Ipv4AddressHelper*: administra la asignación de direcciones IP.
- *Ipv4InterfaceContainer*: en NS3 se hace una asociación entre una dirección IP y un dispositivo usando un objeto *Ipv4Interface*. En muchas ocasiones es preciso una lista de *NetDevice* creados. El *Ipv4InterfaceContainer* proporciona esta facilidad.

4.5. Modelos de pérdidas de propagación y retardo.

El modelo de canal de NS3 admite diferentes modelos de pérdida de propagación, incluidos Friis, Nakagami, Log-distance, TwoRayGround, modelos de *Jakes* entre otros. Además, el NS3 admite diferentes modelos de retardo de propagación, incluidos: velocidad constante y modelo de retardo aleatorio de propagación (Murazzo et al., 2013).

Las que se usarán en este proyecto son las siguientes:

- Clase ConstantSpeedPropagationDelayModel
La llamada a esta clase implica que exista un retardo de propagación constante en el canal.
- Clase FriisPropagationLossModel
El FriisPropagationLossModel, es una versión simplificada del modelo de pérdida de propagación de distancia de registro. En lugar de utilizar coeficientes de pérdida que deben ser adquiridos y validados empíricamente, simplifica el cálculo de la pérdida de propagación al indicado en la ecuación 4. No es preciso para distancias muy pequeñas (la distancia mínima predeterminada en NS-3.10 es de .5 metros) (Ikeda, Kulla, Barolli, Takizawa, & Miho, 2011; Kumar, Paulus, Agrawal, & Agrawal, 2018).

$$P_r(d) = P_t \frac{G_t G_r \lambda^2}{(4\pi d)^2 L}$$

Ecuación 4: Pérdida de propagación.

Donde:

$P_r(d)$ - es igual a la potencia de la señal recibida en vatios expresado en función de la separación $-d$ metros entre el transmisor y el receptor.

P_t - es igual a la potencia a la que se transmitió la señal en vatios.

G_t y G_r - son iguales a las Ganancias de las antenas transmisoras y receptoras en comparación con una antena isotrópica radiante con ganancia unitaria de λ

λ - es la longitud de onda.

En las simulaciones es común seleccionar $G_t=G_r=1$ y $L=1$. El modelo de espacio libre básicamente representa un rango de comunicación como un círculo alrededor del transmisor. Si el receptor está dentro del círculo, se reciben los paquetes, si está fuera se pierden (Ikeda et al., 2011; Kumar et al., 2018).

4.5.1. Modelo de movilidad.

Un modelo de movilidad es un conjunto de características de movimiento que se describe por un nodo móvil dentro del entorno de estudio. Cada modelo de movilidad hace lo posible por representar y ajustarse a algún contexto real que se pueda dar en una aplicación o un entorno de estudio determinado. Cada terminal móvil de la red se moverá dentro del entorno de estudio siguiendo el modelo de movilidad escogido.

- RandomWaypoint
- El modelo de movilidad RandomWaypoint incluye tiempos de pausa entre cambios de dirección y/o velocidad. Un nodo móvil comienza permaneciendo en una ubicación durante un cierto período de tiempo, es decir, un tiempo de pausa, una vez que este tiempo expira, el nodo móvil elige un destino aleatorio en el área de simulación y una velocidad que se distribuye uniformemente entre (minspeed, maxspeed). El nodo móvil luego viaja hacia el destino recién elegido a la velocidad seleccionada, a su llegada, el nodo móvil se detiene durante un período de tiempo específico antes de volver a iniciar el proceso.

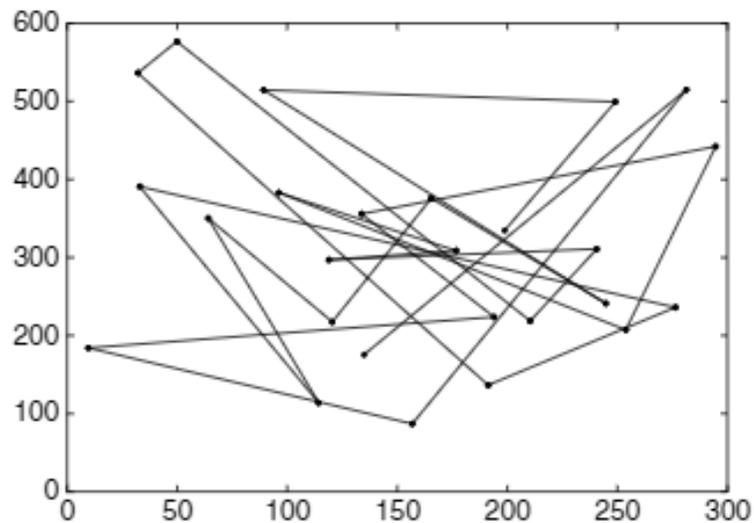


Figura 18: Patrón de desplazamiento de un nodo móvil utilizando el modelo de movilidad RandomWaypoint.

Fuente: (Camp et al., 2002).

Elaborado por: (Camp et al., 2002).

- La Figura 17 muestra un ejemplo de patrón de desplazamiento de un nodo móvil utilizando el modelo de movilidad RandomWaypoint que comienza en un punto o

posición elegidos al azar (133,180); la velocidad del nodo móvil en la figura se elige uniformemente entre 0 y 10 m/s, notamos que el patrón de movimiento de un nodo móvil que usa el modelo de movilidad de punto de ruta aleatorio es similar al modelo de movilidad de caminata aleatoria si el tiempo de pausa es cero y [minspeed, maxspeed] = [speedmin, speedmax] (Camp, Boleng, & Davies, 2002).

CAPÍTULO V. SIMULACIÓN POR TIPOS DE ESCENARIOS

5.1. Escenarios.

En la tabla 3, se muestran los valores o parámetros establecidos para la simulación. Dichos experimentos se realizan con el fin de identificar como se ven afectados los servicios de calidad de VoIP en las redes MANET, que en el caso específico serían 54 escenarios. En la tabla 4, se visualizan los 18 escenarios aplicados para 1 conexión, los cuales son los mismos para los 18 escenarios con 5 conexiones simultáneas y 18 escenarios con 10 conexiones simultáneas, solo se tiene que agregar a la simulación el parámetro de las 5 y 10 conexiones simultáneas.

Tabla 3. Parámetros para escenarios con un tiempo de 150 y 300 segundos.

Parámetro	Valor
Protocolo de enrutamiento	OLSR/DSDV/AODV
Área	1000 x 1000
Número de nodos	30/50/100
Número de conexiones	1/5/10
Mac/Phy	802.11b
Tipo de tráfico	VoIP
CODEC	G.711
Tiempo de simulación	150 s/300 s
Modelo de movilidad	RandomWaypoint

Fuente: Autor.

Elaborado por: Autor

Tabla 4. Escenarios con 1 conexión.

Número escenario	Protocolo	Tiempo simulación en segundos (s)	Número nodos
1	AODV	150	30
2	DSDV	150	30
3	OLSR	150	30
4	AODV	300	30
5	DSDV	300	30
6	OLSR	300	30
7	AODV	150	50
8	DSDV	150	50
9	OLSR	150	50
10	AODV	300	50
11	DSDV	300	50
12	OLSR	300	50
13	AODV	150	100
14	DSDV	150	100
15	OLSR	150	100
16	AODV	300	100
17	DSDV	300	100
18	OLSR	300	100

Fuente: Autor.

Elaborado por: Autor.

5.2. Creación de escenarios en NS3.

La creación de escenarios en NS3 fue posible utilizando el código fuente de red MANET disponible en: https://www.nsnam.org/doxygen/manet-routing-compare_8cc_source.html el cual se modificó para que cumpla con los requerimientos necesarios para este trabajo, las modificaciones realizadas fueron:

1. Incorporación de nuevos módulos para la creación de tráfico VoIP.

Para la creación de tráfico VoIP se utilizó el código abierto de (Mata, 2018) el cual incluye todos los archivos y código necesario para la creación de tráfico VoIP.

Una vez se integra los paquetes que proporciona Saulo de Mata y se debe integrar en el script, este será un script el cual crea tráfico VoIP.

Los pasos que se siguió para integrar el código y los archivos necesarios se pueden observar el anexo 3.

2. Ingreso de número de nodos, tiempo de simulación y protocolo a simular por teclado.

Para facilitar las simulaciones y asegurar consistencia en las simulaciones se opta por ingresar los valores de número de nodos, tiempo de simulación y el protocolo a simular por teclado, la selección del protocolo es posible ya que en el código de red MANET sobre el que se trabaja, se encuentran todos los protocolos integrados en un "Switch case" por lo cual se puede seleccionar el protocolo al momento de correr la simulación ingresando un valor por teclado.

Los pasos que se siguió para realizar la selección de los parámetros mencionados por teclado se pueden observar el anexo 4.

3. Creando archivos de rastreo.

Para crear estos archivos se integra *PCAP Tracing* el cual permite tener archivos de rastreo los cuales podremos visualizar usando WireShark.

Además de esto se implementa la impresión de las rutas de la red, la creación de los archivos de traza ASCII, lo cual facilita el análisis de los datos y la creación de graficas.

5.3. Simulaciones por escenarios.

Una vez se ha implementado todo en el script se debe simular el mismo en todos los escenarios escogidos, los cuales suman 18. Para realizar las simulaciones el primer paso es entrar dentro

del directorio de NS3 en este caso *Documentos/ns-allinone-3.28.1/ns-3.28.1*, una vez dentro del directorio se debe correr la simulación usando `./waf --run scratch/nombre del script`, si se desea ver visualmente como está funcionando la red se agrega después del nombre del script `-vis`, esta visualización se puede observar en la Figura 18 . Luego de esto se deberá escoger los parámetros del escenario de acuerdo con lo establecido en nuestros escenarios como se observa en la Figura 19.

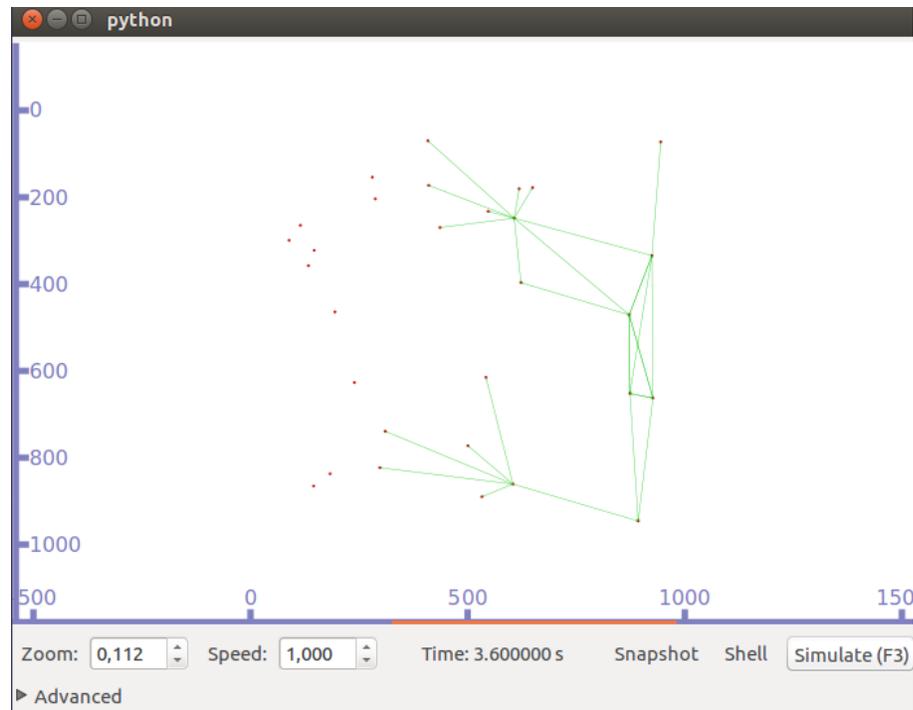


Figura 19: Visualización de la simulación de 30 nodos con un tiempo de 150 s utilizando el protocolo AODV y modelo de movilidad RandomWaypoint.

Fuente: Autor.

Elaborado por: Autor.

```

david@DavidPC: ~/Documentos/ns-allinone-3.28.1/ns-3.28.1
Ingrese número de nodos:
30
Ingrese tiempo total:
150
Ingrese el protocolo (1 OLSR, 2 AODV, 3 DSDV):
2
PING 10.1.1.30 56(84) bytes of data.
64 bytes from 10.1.1.30: icmp_seq=0 ttl=61 time=312 ms

```

Figura 20: Ingreso de número de nodos, tiempo de simulación y protocolo a simular por teclado.

Fuente: Autor.

Elaborado por: Autor.

CAPÍTULO VI. RESULTADOS

6.1. Resultados de pérdida de paquetes.

Los resultados de pérdida de paquetes se presentan de todo el tráfico generado, ya que si se realiza solo de la aplicación no se podría evidenciar las diferencias entre los protocolos proactivos y reactivos, debido a que el tráfico de aplicación se toma desde el momento que se realiza la conexión y no toma en cuenta el tiempo que tarda en realizar la conexión.

6.1.1. Experimento 1: Pérdida de paquetes (1 conexión).

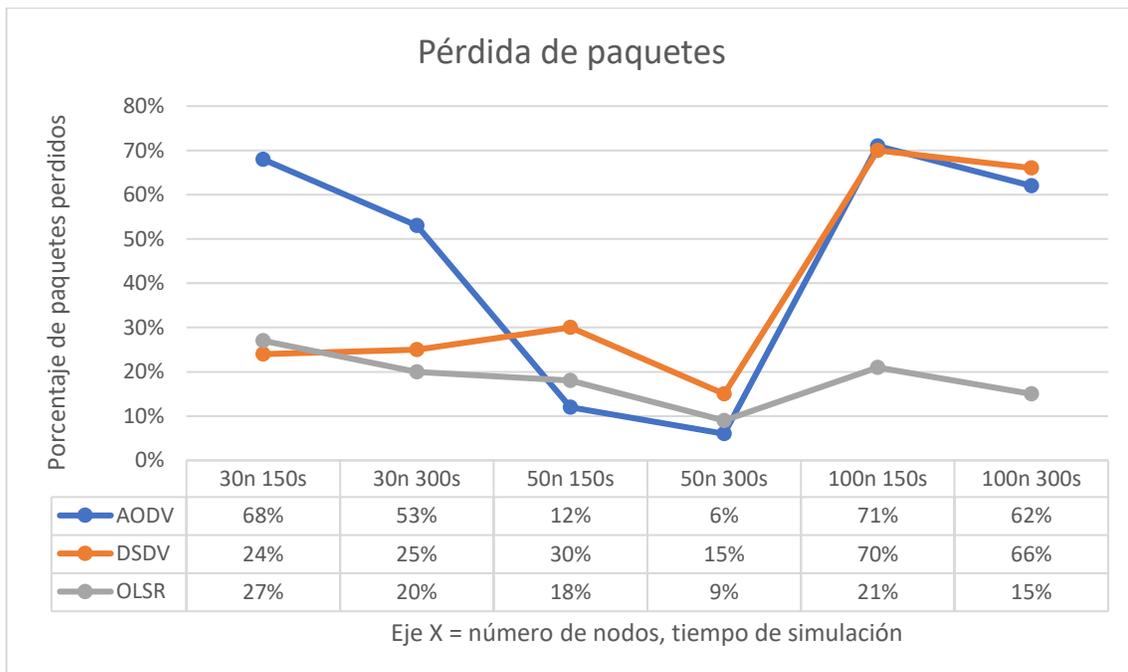


Figura 21: Resultados de pérdida de paquetes 1 conexión.

Fuente: Autor.

Elaborado por: Autor

Como se menciona en el capítulo 4 sección 4.2.1, la pérdida aceptable es de un 20%, ya que luego de esto la calidad de voz se ve degradada.

Como se observa en la Figura 21, los mejores resultados a nivel general considerando todos los escenarios los tiene el protocolo OLSR, mientras que el mejor resultado absoluto lo da el protocolo AODV, en el escenario 10 (50 nodos, 300 s y el protocolo AODV) dando tan solo 6% de pérdida. Además, se puede observar que OLSR es el protocolo más estable, ya que no presenta picos severos como lo hacen los protocolos AODV y DSDV. Solamente dos escenarios con el protocolo OLSR se encuentran fuera de los niveles aceptables de pérdida de paquetes.

En la tabla 5 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y una conexión con 30, 50 y 100 nodos, en el cual el mejor escenario es el escenario 7 (50 nodos y protocolo AODV) y el peor escenario es el escenario 13 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo OLSR, aun siendo este el mejor escenario no se encuentra dentro de los niveles aceptables de pérdida de paquetes (20% ver sección 4.2.1), mientras que el peor escenario es el escenario 1, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 7, que utiliza el protocolo AODV, mientras que el peor escenario es el escenario 8, que utiliza el protocolo DSDV. El mejor escenario con 100 nodos es el escenario 15, que utiliza el protocolo OLSR, aun siendo este el mejor escenario este no se encuentra dentro de los niveles aceptables de pérdida de paquetes, mientras que el peor escenario es el escenario 13, que utiliza el protocolo AODV.

Tabla 5. Pérdida de paquetes con tiempo de simulación 150 s y 1 conexión.

Tiempo simulación (s)	Número de nodos	Protocolo	Porcentaje de pérdida
150	30	AODV	68
		DSDV	24
		OLSR	27
	50	AODV	12
		DSDV	30
		OLSR	18
	100	AODV	71
		DSDV	70
		OLSR	21

Fuente: Autor.

Elaborado por: Autor.

En la tabla 6 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y una conexión, en el cual el mejor escenario es el escenario 10 (50 nodos y protocolo AODV) y el peor escenario es el escenario 17 (100 nodos y protocolo DSDV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 6, que utiliza el protocolo OLSR, el peor escenario es el escenario 4, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 7, que utiliza el protocolo AODV, el peor escenario es el escenario 11, que utiliza el protocolo DSDV. El mejor

escenario con 100 nodos es el escenario 15, que utiliza el protocolo OLSR, el peor escenario es el escenario 17, que utiliza el protocolo DSDV.

Tabla 6. Pérdida de paquetes con tiempo de simulación 300 s y 1 conexión.

Tiempo simulación (s)	Número de nodos	Protocolo	Porcentaje de pérdida
300	30	AODV	53
		DSDV	25
		OLSR	20
	50	AODV	6
		DSDV	15
		OLSR	9
	100	AODV	62
		DSDV	66
		OLSR	15

Fuente: Autor.

Elaborado por: Autor.

Los resultados que se encuentran dentro de los niveles aceptables de pérdida de paquetes se ilustran en la tabla 7.

Tabla 7. Escenarios con valores aceptables de pérdida de paquetes con 1 conexión.

Número de nodos	Tiempo de simulación (s)	Protocolo del escenario	Escenario	Porcentaje de pérdida
30	300	OLSR	6	20
50	150	AODV	7	12
		OLSR	9	18
50	300	AODV	10	6
		DSDV	11	15
		OLSR	12	9
100	300	OLSR	18	15

Fuente: Autor.

Elaborado por: Autor.

6.1.2. Experimento 2: Pérdida de paquetes (5 conexiones simultáneas).

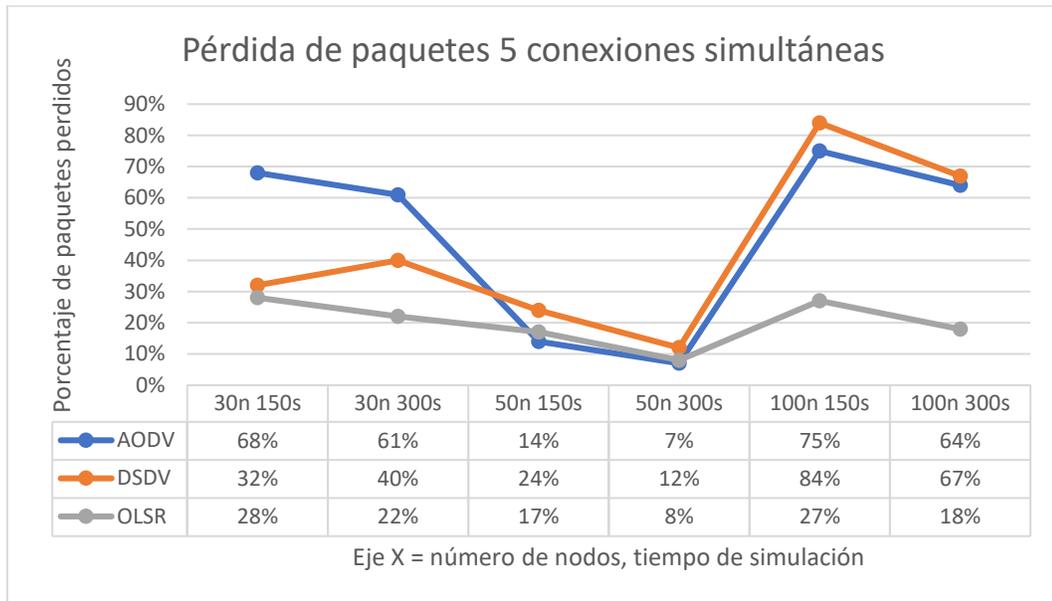


Figura 22: Resultados de pérdida paquetes 5 conexiones simultáneas.

Fuente: Autor.

Elaborado por: Autor.

Como se observa en la Figura 22, al igual que en el experimento 1 los mejores resultados a nivel general considerando todos los escenarios los tiene el protocolo OLSR. El mejor resultado absoluto está dado por el escenario 10 (50 nodos, 300 s y el protocolo AODV). Se puede observar también que, tanto los protocolos AODV como DSDV presentan picos severos, al pasar de los escenarios 10 y 11 a los escenarios 13 y 14 respectivamente, esto hace que no sean los óptimos ya que estos picos pueden afectar la red en caso de un nivel de usuarios alto. En AODV se presentan picos altos en los escenarios 1 y 4.

En la tabla 8 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y 5 conexiones simultáneas, en el cual el mejor escenario es el escenario 7 (50 nodos y protocolo AODV) y el peor escenario es el escenario 14 (100 nodos y protocolo DSDV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo OLSR, aun siendo este el mejor escenario este no se encuentra dentro de los niveles aceptables de pérdida de paquetes, mientras que el peor es el escenario 1, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 7, que utiliza el protocolo AODV, mientras que el peor es el escenario 8, que utiliza el protocolo DSDV. El mejor escenario con 100 nodos es el escenario 15, que utiliza el protocolo OLSR, aunque este sea el mejor escenario, no se encuentra dentro de los niveles

aceptables de pérdida de paquetes, mientras que el peor escenario es el escenario 14, que utiliza el protocolo DSDV.

Tabla 8. Pérdida de paquetes con tiempo de simulación 150 s y 5 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Porcentaje de pérdida
150	30	AODV	68
		DSDV	32
		OLSR	28
	50	AODV	14
		DSDV	24
		OLSR	17
	100	AODV	75
		DSDV	84
		OLSR	27

Fuente: Autor.

Elaborado por: Autor.

Tabla 9. Pérdida de paquetes con tiempo de simulación 300 s y 5 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Porcentaje de pérdida
300	30	AODV	61
		DSDV	40
		OLSR	22
	50	AODV	7
		DSDV	12
		OLSR	8
	100	AODV	64
		DSDV	67
		OLSR	18

Fuente: Autor.

Elaborado por: Autor.

En la tabla 9 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y 5 conexiones simultáneas, en el cual el mejor escenario es el escenario

10 (50 nodos y protocolo AODV) y el peor escenario es el escenario 17 (100 nodos y el protocolo DSDV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 6, que utiliza el protocolo OLSR, aunque este sea el mejor escenario, no se encuentra dentro de los niveles aceptables de pérdida de paquetes, el peor escenario es el escenario 4, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 10, que utiliza el protocolo AODV, el peor escenario es el escenario 11, que utiliza el protocolo DSDV, siendo este el peor escenario, no se encuentra fuera de los niveles aceptables de pérdida de paquetes. El mejor escenario con 100 nodos es el escenario 18, que utiliza el protocolo OLSR, el peor escenario es el escenario 17, que utiliza el protocolo DSDV.

Los resultados que se encuentran dentro de los niveles aceptables de pérdida de paquetes se ilustran en la tabla 10.

Tabla 10. Escenarios con valores aceptables de pérdida de paquetes con 5 conexiones simultáneas.

Número de nodos	Tiempo de simulación (s)	Protocolo del escenario	Escenario	Porcentaje de pérdida
50	150	AODV	7	14
		OLSR	9	17
50	300	AODV	10	7
		DSDV	11	12
		OLSR	12	8
100	300	OLSR	18	18

Fuente: Autor.

Elaborado por: Autor.

6.1.3. Experimento 3: Pérdida de paquetes (10 conexiones simultáneas).

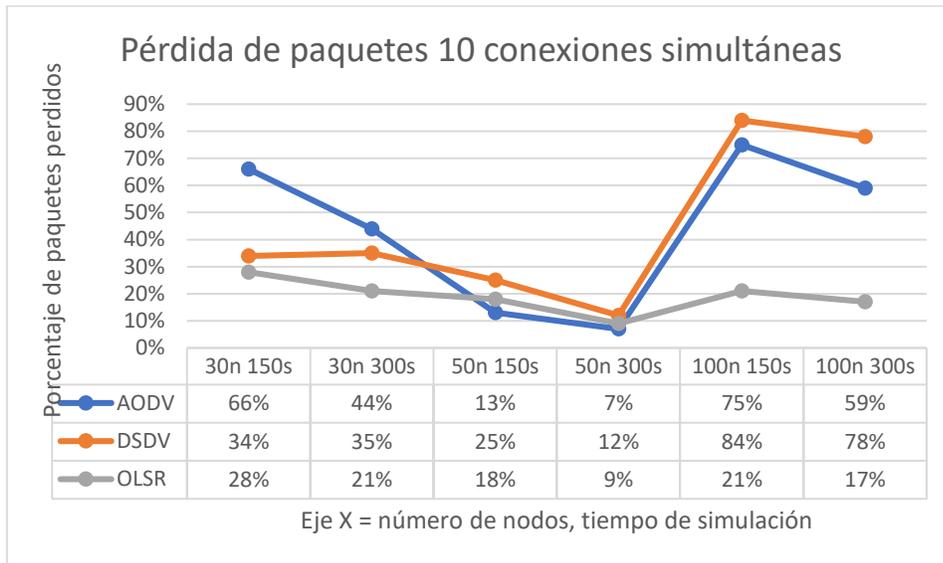


Figura 23: Resultados de pérdida paquetes 10 conexiones simultáneas.

Fuente: Autor.

Elaborado por: Autor.

Como se observa en la Figura 23, los mejores resultados a nivel general considerando todos los escenarios los tiene el protocolo OLSR, siguiendo la misma tendencia del experimento 1 y 2, el mejor resultado esta dado por el escenario 10 (50 nodos, 300 s y el protocolo AODV). Al igual que en el experimento 1 y 2, se puede observar que, tanto los protocolos AODV como DSDV presentan picos severos al pasar de los escenarios 10 y 11 a los escenarios 13 y 14 respectivamente, de igual manera esto hace que no sean los más ideales ya que estos picos pueden afectar la red en caso de un nivel de usuarios alto. AODV también presentan picos altos en los escenarios 1 y 4.

En la tabla 11 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y 10 conexiones simultáneas, en el cual el mejor escenario es el escenario 7 (50 nodos y protocolo AODV), el peor escenario es el escenario 14(100 nodos y protocolo DSDV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo OLSR, aun siendo este el mejor escenario no está dentro de los niveles aceptables de pérdida de paquetes, mientras que el peor escenario es el escenario 1, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 7, que utiliza el protocolo AODV, mientras que el peor escenario es el escenario 8, que utiliza el protocolo DSDV. El mejor escenario con 100 nodo es el escenario 15, que utiliza el protocolo OLSR, aun siendo este el mejor escenario, no se encuentra dentro de

los niveles aceptables de pérdida de paquetes, mientras que el peor escenario es el escenario 14, que utiliza el protocolo DSDV.

Tabla 11. Pérdida de paquetes con tiempo de simulación 150 s y 10 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Porcentaje de pérdida
150	30	AODV	66
		DSDV	34
		OLSR	28
	50	AODV	13
		DSDV	25
		OLSR	18
	100	AODV	75
		DSDV	84
		OLSR	21

Fuente: Autor.

Elaborado por: Autor.

Tabla 12. Pérdida de paquetes con tiempo de simulación 300 s y 10 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Porcentaje de pérdida
300	30	AODV	44
		DSDV	35
		OLSR	21
	50	AODV	7
		DSDV	12
		OLSR	9
	100	AODV	59
		DSDV	78
		OLSR	17

Fuente: Autor.

Elaborado por: Autor.

En la tabla 12 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y 10 conexiones simultáneas, en el cual el mejor escenario es el escenario

10 (50 nodos y protocolo AODV), el peor escenario es el escenario 17 (100 nodos y protocolo DSDV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 6, que utiliza el protocolo OLSR y el peor escenario es el escenario 1, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 10, que utiliza el protocolo AODV, el peor escenario es el escenario 11, que utiliza el protocolo DSDV, aunque de igual manera este se encuentra dentro de los márgenes aceptables de pérdida de paquetes. El mejor escenario con 100 nodos es el escenario 18, que utiliza el protocolo OLSR y el peor escenario es el escenario 17, que utiliza el protocolo DSDV.

Tabla 13. Escenarios con valores aceptables de pérdida de paquetes con 10 conexiones simultáneas.

Número de nodos	Tiempo de simulación (s)	Protocolo del escenario	Escenario	Porcentaje de pérdida
50	150	AODV	7	13
		OLSR	9	18
50	300	AODV	10	7
		DSDV	11	12
		OLSR	12	9
100	300	OLSR	18	17

Fuente: Autor.

Elaborado por: Autor.

Los resultados que se encuentran dentro de los niveles aceptables de pérdida de paquetes aceptables se ilustran en la tabla 13.

6.1.4. Estadísticas de pérdida de paquetes.

La Media y la Varianza representan valores estadísticos importantes al momento de contrastar los resultados de los experimentos:

Con el cálculo de la *Media* podemos conocer cuál es el valor promedio de pérdida de paquetes, retardo o jitter. Lo cual nos permitirá ver datos estadísticos de cada escenario a través de los múltiples experimentos, para poder realizar recomendaciones en base a los parámetros de calidad establecidos para el uso de VoIP en las redes MANET dando una perspectiva clara de cuales escenarios son mejores o con cuántas conexiones se tiene los mejores resultados.

Por otro lado, el valor de la *Varianza* nos indica cuan dispersos están los valores dentro de los experimentos que se compara; mientras más pequeño es el número, mejores son los resultados, ya que esto indica que los resultados se encuentran poco dispersos. Esto se utilizará para poder realizar recomendaciones sobre los mejores escenarios a usar para las

conexiones VoIP en las redes MANET, ya que si el valor de varianza es menor se puede decir que los valores son similares entre los experimentos realizados, por lo cual ese escenario es más estable en lo que refiere a número de conexiones.

Las ecuaciones para el cálculo de la media y varianza, así como sus conceptos y un ejemplo de cómo se obtienen, se pueden ver en el anexo 5.

Tabla 14. Estadísticas de pérdida de paquetes 150 s.

Escenario	Media (%)	Varianza (%)	Tiempo simulación (s)	Protocolo	Número de nodos
1	67.33	0.89	150	AODV	30
2	30.00	18.67	150	DSDV	30
3	27.67	0.22	150	OLSR	30
7	13.00	0.67	150	AODV	50
8	26.33	17.67	150	DSDV	50
9	17.67	0.22	150	OLSR	50
13	73.67	3.56	150	AODV	100
14	79.33	43.56	150	DSDV	100
15	23.00	8.00	150	OLSR	100

Fuente: Autor.

Elaborado por: Autor.

En la tabla 14, se observan las estadísticas de media y varianza por cada escenario con 150 s, utilizando los resultados de los tres experimentos anteriores y en la tabla 15, se visualizan las mismas estadísticas con un tiempo de 300 s.

Tabla 15. Estadísticas de pérdidas de paquetes 300 s.

Escenario	Media (%)	Varianza (%)	Tiempo simulación (s)	Protocolo	Número de nodos
4	52.67	48.22	300 s	AODV	30
5	33.33	38.89	300 s	DSDV	30
6	21.00	0.67	300 s	OLSR	30
10	6.67	0.22	300 s	AODV	50
11	13.00	2.00	300 s	DSDV	50
12	8.67	0.22	300 s	OLSR	50
16	61.67	4.22	300 s	AODV	100
17	70.33	29.56	300 s	DSDV	100
18	16.67	1.56	300 s	OLSR	100

Fuente: Autor.

Elaborado por: Autor.

Tabla 16. Estadísticas de pérdida de paquetes por número de conexiones.

Número de conexiones	Media (%)	Varianza (%)
1	35.89	19.82
5	37.11	615.77
10	34.00	526.22

Fuente: Autor.

Elaborado por: Autor.

En la tabla 16, se muestran las estadísticas de la media y varianza de acuerdo con la cantidad de conexiones simultáneas. En la tabla 17, se visualizan las mismas estadísticas, pero tomando solamente los valores de los escenarios que se encuentren dentro de los márgenes aceptables de pérdida de paquetes.

Tabla 17. Estadísticas de pérdida de paquetes por número de conexiones simultáneas con valores aceptables

Número de conexiones	Media (%)	Varianza (%)
1	13.57	20.82
5	12.67	17.22
10	12.67	15.56

Fuente: Autor.

Elaborado por: Autor.

6.1.5. Resultados generales de pérdida de paquetes.

Se puede ver que, a nivel general dentro de los tres experimentos, los mejores escenarios en relación con el número de nodos y tiempo de simulación son los que utilizan el protocolo OLSR, ya que presenta los mejores valores en casi todos los escenarios, a excepción de cuando se usa 50 nodos con un tiempo de 150 s y 300 s, donde los mejores escenarios son los escenarios 7 y 10 que se encuentran dados por el protocolo AODV.

El mejor escenario en los tres experimentos es el escenario 10, dando el menor porcentaje de pérdida de paquetes, aunque se puede ocupar cualquiera de los resultados presentados en las tablas 8, 11 y 14, debido a que estos representan los escenarios aceptables dependiendo de la cantidad de conexiones simultáneas.

Para 150 s el mejor escenario es el escenario 7 (50 nodos y protocolo AODV), ya que este presenta el mejor promedio referente a pérdida de paquetes, por lo cual si no se sabe el número exacto de conexiones simultáneas a usar este sería la mejor opción.

Para 300 s el mejor escenario es el escenario 10 (50 nodos y protocolo AODV), ya que este presenta el mejor promedio referente a pérdida de paquetes, por lo cual si no se sabe el número exacto de conexiones simultáneas a usar este sería la mejor opción.

6.2. Resultados de retardo.

Los resultados de retardo se presentan de todo el tráfico generado, ya que si se realiza solo de la aplicación no se podría evidenciar las diferencias entre los protocolos proactivos y reactivos, debido a que el tráfico de aplicación se toma desde el momento que se realiza la conexión y no toma en cuenta el tiempo que tarda en realizar la conexión.

6.2.1. Experimento 4: Retardo (1 conexión).

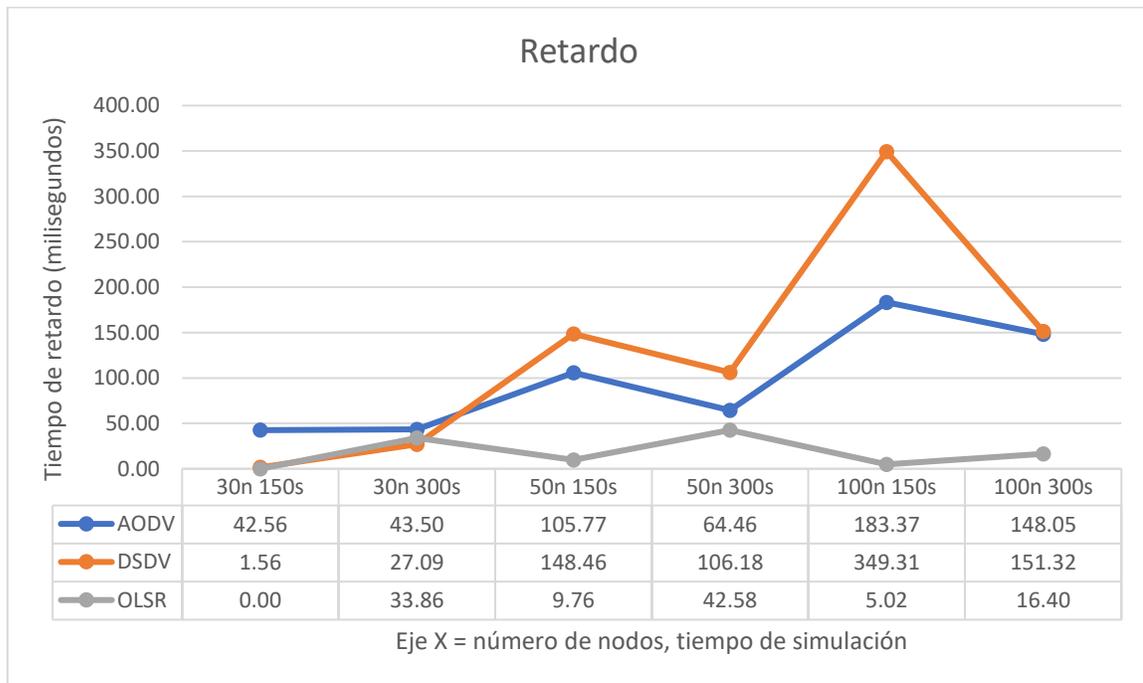


Figura 24: Resultados de retardo 1 conexión.

Fuente: Autor.

Elaborado por: Autor.

Para analizar los resultados referentes a retardo se debe tener en cuenta lo mencionado en el capítulo 4 sección 4.2.2. Retrasos menores a 200 ms se consideran aceptables, mientras que, los de 200 a 400 ms merecen atención y más de 400 ms se consideran inaceptables. Tomando en cuenta esto se observa en la Figura 24, que los mejores resultados en todos menos un escenario, los da el protocolo OLSR, además de esto se puede evidenciar que todos menos uno de los resultados, son aceptables, siendo el resultado no aceptable el escenario 14 (100 nodos, 150s y el protocolo DSDV), que en la gráfica se presenta como un pico, este requiere de atención debido a que supera los 200ms de retraso.

En la tabla 18 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y una conexión, en el cual el mejor escenario es el escenario 3 (30 nodos y

protocolo OLSR) y el peor escenario es el escenario 14(100 nodos y protocolo DSDV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 1, que utiliza el protocolo AODV, aunque siendo este el peor escenario, se encuentra dentro de los niveles aceptables de retardo (valores menores a 200ms, ver sección 4.2.2).

El mejor escenario con 50 nodos es el escenario 9, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 8, que utiliza el protocolo DSDV, aunque siendo este el peor escenario se encuentra dentro de los niveles aceptables de retardo. El mejor escenario con 100 nodos es el escenario 15, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 14, que utiliza el protocolo DSDV.

Tabla 18. Retardo con tiempo de simulación 150 s y 1 conexión.

Tiempo simulación (s)	Número de nodos	Protocolo	Retardo (ms)
150	30	AODV	42.56
		DSDV	1.56
		OLSR	0.00
	50	AODV	105.77
		DSDV	148.46
		OLSR	9.76
	100	AODV	183.37
		DSDV	349.31
		OLSR	5.02

Fuente: Autor.

Elaborado por: Autor.

En la tabla 19 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y una conexión, en el cual el mejor escenario es el escenario 18 (100 nodos y protocolo OLSR), y el peor es el escenario 17 (100 nodos y protocolo DSDV), aunque siendo este el peor escenario se encuentra dentro de los niveles aceptables de retardo. A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 5, que utiliza el protocolo DSDV, el peor escenario es el escenario 4, que utiliza el protocolo AODV, aunque siendo este el peor escenario, se encuentra dentro de los niveles aceptables de retardo. El mejor escenario con 50 nodos es el escenario 12, que utiliza el protocolo OLSR, el peor escenario es el escenario 11, que utiliza el protocolo DSDV, aunque siendo este el peor escenario, se encuentra dentro de los niveles aceptables de retardo.

Tabla 19. Retardo con tiempo de simulación 300 s y 1 conexión.

Tiempo simulación (s)	Número de nodos	Protocolo	Retardo (ms)
300	30	AODV	43.50
		DSDV	27.09
		OLSR	33.86
	50	AODV	64.46
		DSDV	106.18
		OLSR	42.58
	100	AODV	148.05
		DSDV	151.32
		OLSR	16.40

Fuente: Autor.

Elaborado por: Autor.

6.2.2. Experimento 5: Retardo (5 conexiones simultáneas).

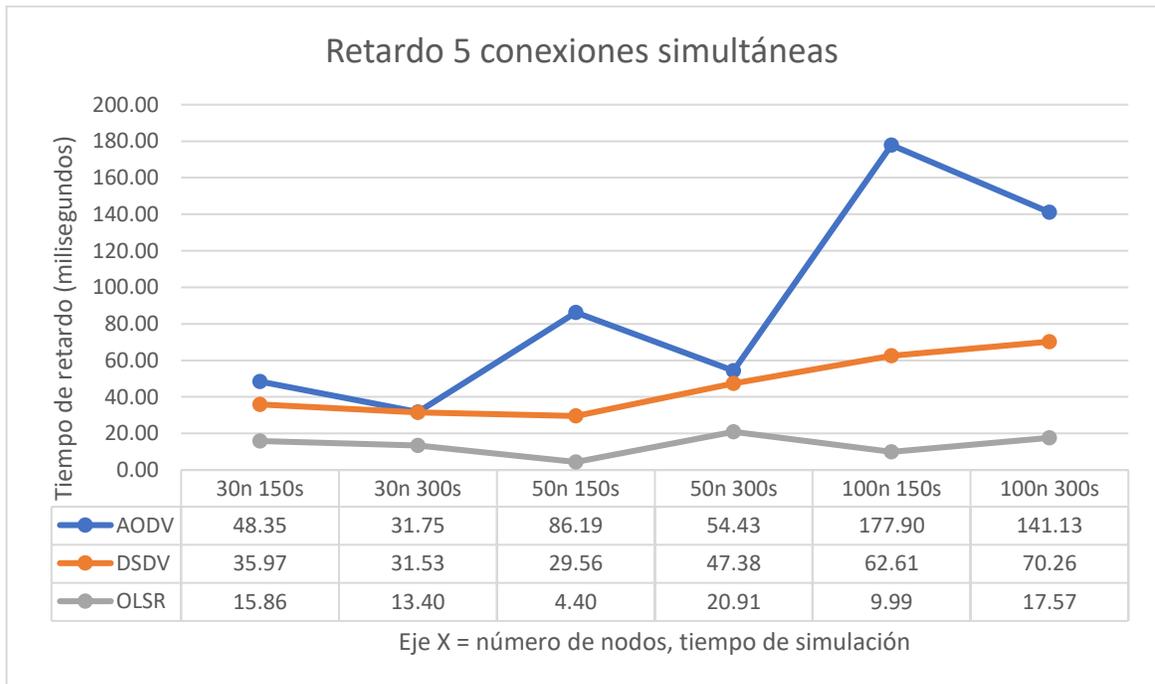


Figura 25: Resultados de retardo 5 conexiones simultáneas.

Fuente: Autor.

Elaborado por: Autor.

Como se observa en la Figura 25, siguiendo la tendencia del experimento 4, los mejores resultados los da el protocolo OLSR. Además, se ve que todos los resultados están en el rango

aceptable de retardo, por lo cual, todos los resultados serían aceptables ya que ninguno de estos supera los 200ms de retardo.

En la tabla 20, se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y 5 conexiones simultáneas, en el cual el mejor escenario es el escenario 9 (50 nodos y protocolo OLSR) y el peor escenario es el escenario 13 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo AODV, mientras que el peor escenario es el escenario 1, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 9, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 7, que utiliza el protocolo AODV. El mejor escenario con 100 nodos es el escenario 15, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 13, que utiliza el protocolo AODV.

Tabla 20. Retardo con tiempo de simulación 150 s y 5 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Retardo (ms)
150	30	AODV	48.35
		DSDV	35.97
		OLSR	15.86
	50	AODV	86.16
		DSDV	29.56
		OLSR	4.40
	100	AODV	177.90
		DSDV	62.61
		OLSR	9.99

Fuente: Autor.

Elaborado por: Autor.

En la tabla 21 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y 5 conexiones simultáneas, en el cual el mejor escenario es el escenario 6 (30 nodos y protocolo OLSR), y el peor escenario es el escenario 16 (100 nodos y protocolo AODV), aunque siendo este el peor escenario, se encuentra dentro de los niveles aceptables de retardo. A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 6, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 4, que utiliza el protocolo AODV, aunque siendo este el peor escenario, se

encuentra dentro de los niveles aceptables de retardo. El mejor escenario con 50 nodos es el escenario 12, que utiliza el protocolo OLSR, el peor escenario es el escenario 10, que utiliza el protocolo AODV, aunque siendo este el peor escenario, se encuentra dentro de los niveles aceptables de retardo. El mejor escenario con 100 nodos es el escenario 18, que utiliza el protocolo OLSR, el peor escenario es el escenario 16, que utiliza el protocolo AODV, aunque siendo este el peor escenario, se encuentra dentro de los niveles aceptables de retardo.

Tabla 21. Retardo con tiempo de simulación 300 s y 5 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Retardo (ms)
300	30	AODV	31.75
		DSDV	31.53
		OLSR	13.40
	50	AODV	54.43
		DSDV	47.38
		OLSR	20.91
	100	AODV	141.13
		DSDV	70.26
		OLSR	17.57

Fuente: Autor.

Elaborado por: Autor.

6.2.3. Experimento 6: Retardo (10 conexiones simultáneas).

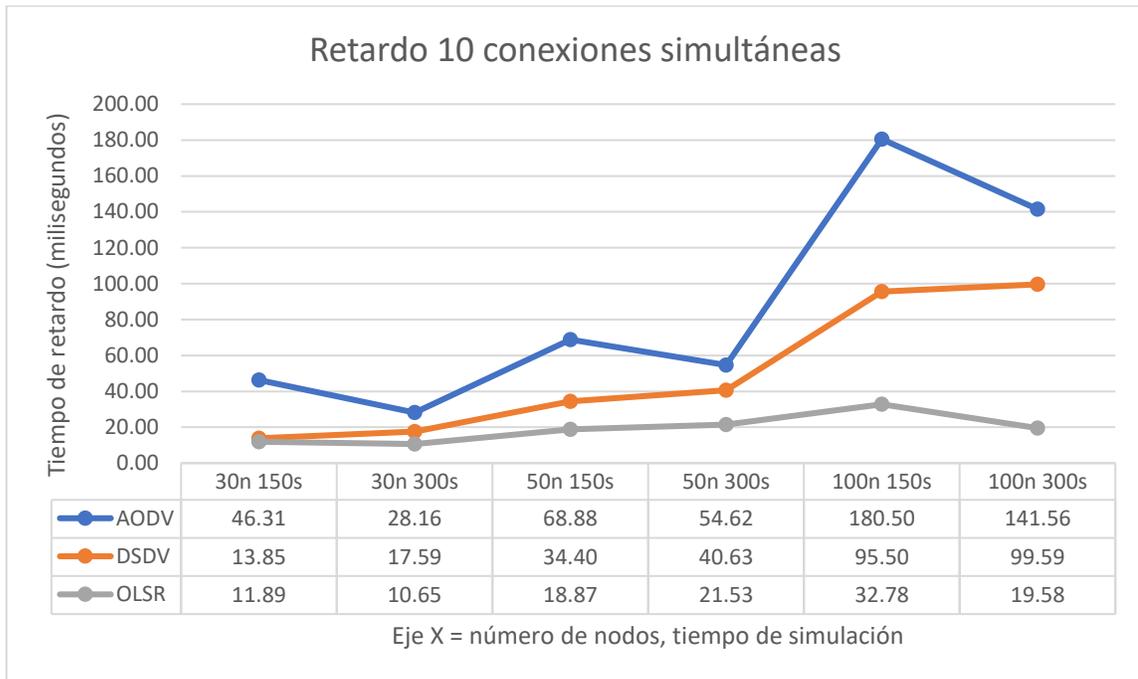


Figura 26: Resultados de retardo 10 conexiones simultáneas.

Fuente: Autor.

Elaborado por: Autor.

Como se observa en la Figura 26, siguiendo la tendencia de los experimentos 4 y 5, los mejores resultados están dados por el protocolo OLSR. Además, se observa que todos los resultados están en el rango aceptable de retardo por lo cual, todos los resultados serían aceptables ya que ninguno de estos supera los 200ms de retardo.

En la tabla 22 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y 10 conexiones simultáneas, en el cual el mejor escenario es el escenario 3 (30 nodos y protocolo OLSR) y el peor escenario es el escenario 13 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 1, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 9, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 7, que utiliza el protocolo AODV. El mejor escenario con 100 nodos es el escenario 15, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 13, que utiliza el protocolo AODV.

Tabla 22. Retardo con tiempo de simulación 150 s y 10 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Retardo (ms)
150	30	AODV	46.31
		DSDV	13.85
		OLSR	11.89
	50	AODV	68.88
		DSDV	34.40
		OLSR	18.87
	100	AODV	180.50
		DSDV	95.50
		OLSR	32.78

Fuente: Autor.

Elaborado por: Autor.

Tabla 23. Retardo con tiempo de simulación 300 s y 10 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Retardo (ms)
300	30	AODV	28.16
		DSDV	17.59
		OLSR	10.65
	50	AODV	54.62
		DSDV	40.63
		OLSR	21.53
	100	AODV	141.56
		DSDV	99.59
		OLSR	19.58

Fuente: Autor.

Elaborado por: Autor.

En la tabla 23 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y 10 conexiones simultáneas, en el cual el mejor escenario es el escenario 6 (30 nodos y protocolo OLSR), el peor escenario es el escenario 16 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 6, que utiliza el protocolo AODV, el peor escenario es el escenario 4, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 12, que utiliza el protocolo OLSR, el peor escenario es el escenario 10, que utiliza el protocolo AODV. El mejor

escenario con 100 nodos es el escenario 18, que utiliza el protocolo OLSR, el peor escenario es el escenario 16, que utiliza el protocolo AODV.

6.2.4. Estadísticas de retardo.

En la tabla 24 se puede observar las estadísticas de media y varianza por cada escenario con 150 s, utilizando los resultados de los experimentos 4, 5 y 6 y en la tabla 25 se visualizan las mismas estadísticas con un tiempo de 300 s.

Tabla 24. Estadísticas retardo 150 s.

Escenario	Media (ms)	Varianza (ms)	Tiempo simulación (s)	Protocolo	Número de nodos
1	45.74	5.76	150	AODV	30
2	17.13	202.78	150	DSDV	30
3	9.25	45.39	150	OLSR	30
7	86.95	227.14	150	AODV	50
8	70.81	3019.07	150	DSDV	50
9	11.01	35.69	150	OLSR	50
13	180.59	12.73	150	AODV	100
14	169.14	16411.38	150	DSDV	100
15	15.93	146.05	150	OLSR	100

Fuente: Autor.

Elaborado por: Autor.

En la tabla 26 se observan las estadísticas de la media y varianza de acuerdo con la cantidad de conexiones simultáneas. En la tabla 27 se muestran las mismas estadísticas, tomando solamente los valores de los escenarios que se encuentren dentro de los márgenes aceptables de retardo.

Tabla 25. Estadísticas retardo 300 s.

Escenario	Media (ms)	Varianza (ms)	Tiempo simulación (s)	Protocolo	Número de nodos
4	34.47	42.93	300 s	AODV	30
5	25.40	33.83	300 s	DSDV	30
6	19.30	107.23	300 s	OLSR	30
10	57.84	21.96	300 s	AODV	50
11	64.73	866.66	300 s	DSDV	50
12	28.34	101.50	300 s	OLSR	50
16	143.58	10.01	300 s	AODV	100
17	107.06	1122.89	300 s	DSDV	100
18	17.85	1.72	300 s	OLSR	100

Fuente: Autor.

Elaborado por: Autor.

Tabla 26. Estadísticas retardo por número de conexiones simultáneas.

Número de conexiones	Media (ms)	Varianza (ms)
1	82.18	7518.77
5	49.96	1996.75
10	52.05	2190.49

Fuente: Autor.

Elaborado por: Autor.

Tabla 27. Estadísticas retardo por número de conexiones simultáneas con valores aceptables

Número de conexiones	Media (ms)	Varianza (ms)
1	66.47	66528.82
5	49.96	1996.75
10	52.05	2190.49

Fuente: Autor.

Elaborado por: Autor.

6.2.5. Resultados generales de retardo.

Se puede ver que a nivel general dentro de los tres experimentos los mejores escenarios en relación con el número de nodos y tiempo de simulación son los que utilizan el protocolo OLSR ya que presenta los mejores valores en casi todos a excepción del experimento 4 con 30 nodos y 300 segundos, donde el mejor resultado está dado por el escenario 5, que utiliza el protocolo DSDV. En el experimento 4 el mejor escenario es el escenario 3, en el experimento 5 el escenario 9 y en el experimento 6 el escenario 6.

Para 150 s el mejor escenario es el escenario 3(30 nodos y protocolo OLSR), ya que este presenta el mejor promedio referente a retardo, por lo cual si no se sabe el número exacto de conexiones simultáneas a usar este sería la mejor opción.

Para 300 s el mejor escenario es el escenario 18 (100 nodos y protocolo OLSR), ya que este presenta el mejor promedio referente a retardo, por lo cual si no se sabe el número exacto de conexiones simultáneas a usar este sería la mejor opción.

6.3. Resultados de jitter.

Los resultados de jitter se presentan de todo el tráfico generado ya que si se realiza solo de la aplicación no se podría evidenciar las diferencias entre los protocolos proactivos y reactivos, debido a que el tráfico de aplicación se toma desde el momento que se realiza la conexión y no toma en cuenta el tiempo que tarda en realizar la conexión.

6.3.1. Experimento 7: Jitter (1 conexión).

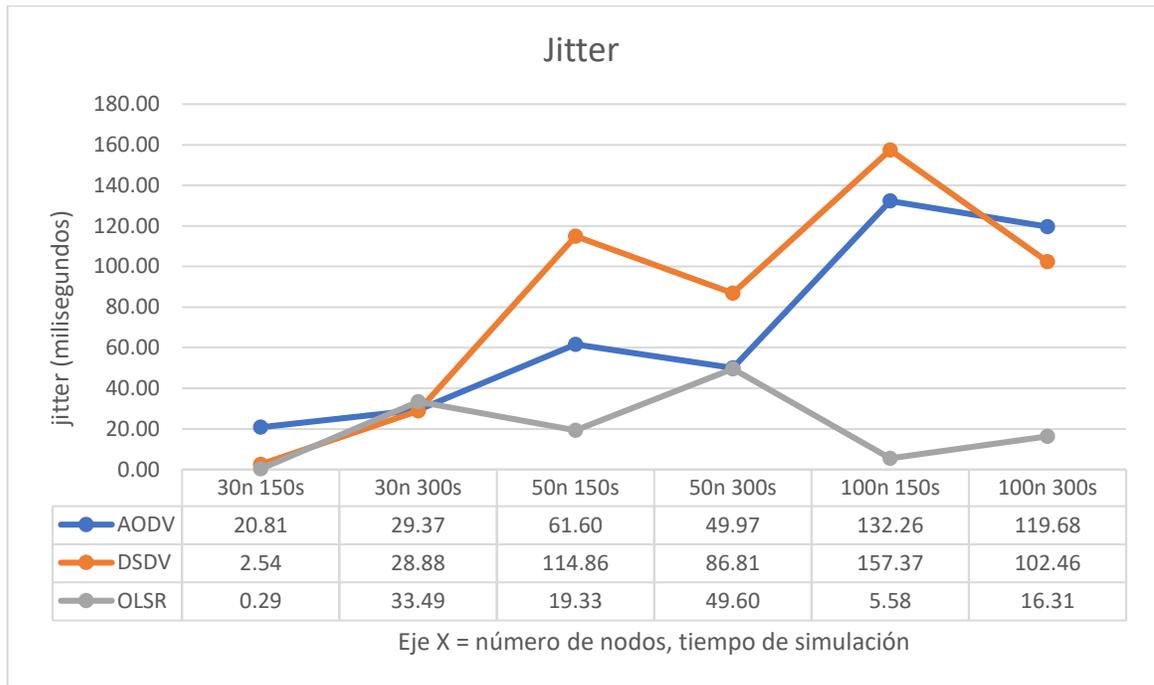


Figura 27: Resultados de jitter 1 conexión.

Fuente: Autor.

Elaborado por: Autor.

Para analizar los resultados referentes a retardo se debe tener en cuenta lo mencionado en el capítulo 4 sección 4.2.3. El jitter como norma general no debe superar los 50ms. Tomando en cuenta esto, podemos observar en la Figura 27, que los mejores resultados a nivel general considerando todos los escenarios los tiene el protocolo OLSR. También se observa que los escenarios con los protocolos AODV Y DSDV, tienen picos lo cual hace que estos superen en muchos de los escenarios los niveles aceptables de jitter. Los escenarios aceptables referentes jitter se ilustran en la tabla 15.

En este experimento, siete de los escenarios se encuentran fuera de los niveles aceptables de jitter.

En la tabla 28 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y una conexión, en el cual el mejor escenario es el escenario 3 (30 nodos y protocolo OLSR), el peor escenario es el escenario 14 (100 nodos y el protocolo DSDV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 1, que utiliza el protocolo AODV, a pesar de ser este el peor escenario se encuentra dentro de los niveles aceptables de jitter (no debe superar los 50ms ver sección 4.2.3). El mejor

escenario con 50 nodos es el escenario 9, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 8, que utiliza el protocolo DSDV. El mejor escenario con 100 nodos es el escenario 15, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 14, que utiliza el protocolo DSDV.

Tabla 28. Jitter con tiempo de simulación 150 s y 1 conexión.

Tiempo simulación (s)	Número de nodos	Protocolo	Jitter (ms)
150	30	AODV	28.81
		DSDV	2.54
		OLSR	0.29
	50	AODV	61.60
		DSDV	114.86
		OLSR	19.33
	100	AODV	132.26
		DSDV	157.37
		OLSR	5.58

Fuente: Autor.

Elaborado por: Autor.

Tabla 29. Jitter con tiempo de simulación 300 s y 1 conexión.

Tiempo simulación (s)	Número de nodos	Protocolo	Jitter (ms)
300	30	AODV	29.37
		DSDV	28.88
		OLSR	33.49
	50	AODV	49.97
		DSDV	86.81
		OLSR	49.60
	100	AODV	119.68
		DSDV	102.46
		OLSR	16.31

Fuente: Autor.

Elaborado por: Autor.

En la tabla 29 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y una conexión, en el cual el mejor escenario es el escenario 18 (100

nodos y protocolo OLSR), el peor escenario es el escenario 16 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 5, que utiliza el protocolo DSDV, el peor escenario es el escenario 6, que utiliza el protocolo OLSR, a pesar de ser este el peor escenario se encuentra dentro de los niveles aceptables de jitter. El mejor escenario con 50 nodos es el escenario 12, que utiliza el protocolo OLSR, el peor escenario es el escenario 11, que utiliza el protocolo DSDV. El mejor escenario con 100 nodos es el escenario 18, que utiliza el protocolo OLSR, el peor escenario es el escenario 16, que utiliza el protocolo AODV.

Los resultados que se encuentran dentro de los niveles aceptables de jitter se ilustran en la tabla 30.

Tabla 30. Escenarios con valores aceptables de jitter con 1 conexión.

Número de nodos	Tiempo de simulación (s)	Protocolo del escenario	Escenario	Jitter (ms)
30	150	AODV	1	20.81
		DSDV	2	2.54
		OLSR	3	0.29
30	300	AODV	4	29.37
		DSDV	5	28.88
		OLSR	6	33.49
50	150	OLSR	9	19.33
50	300	AODV	10	49.97
		OLSR	12	49.60
100	150	OLSR	15	5.58
100	300	OLSR	18	16.31

Fuente: Autor.

Elaborado por: Autor.

6.3.2. Experimento 8: Jitter (5 conexiones simultáneas).

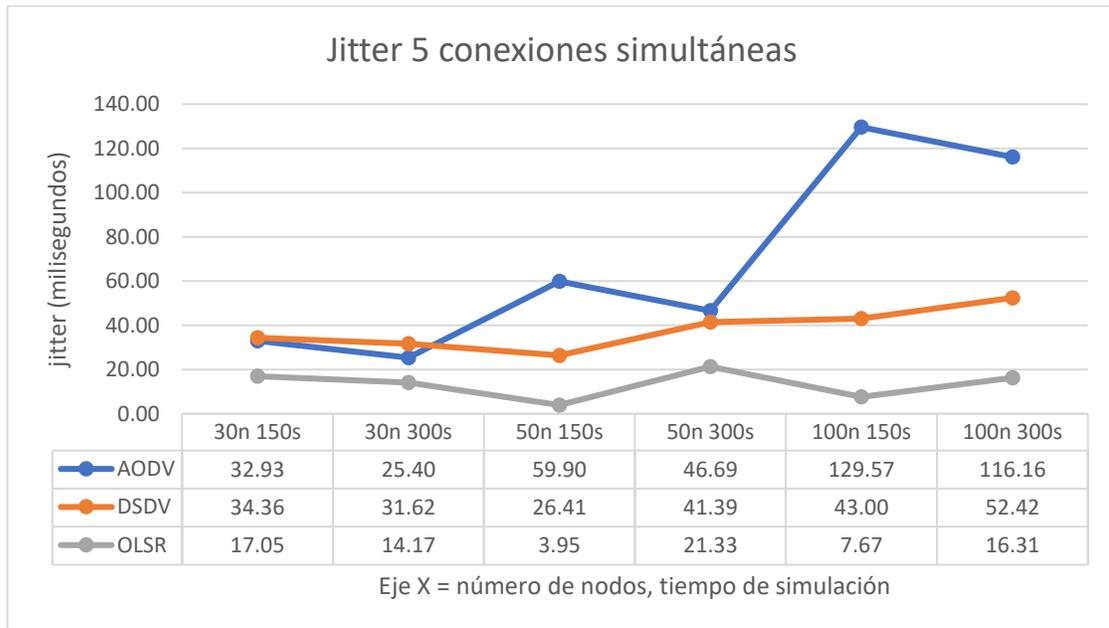


Figura 28: Resultados de jitter 5 conexiones simultáneas.

Fuente: Autor

Elaborado por: Autor.

Como se puede observar en la Figura 28, al igual que en el experimento 7 los mejores resultados están dados por el protocolo OLSR. Cuatro escenarios no son aceptables debido a que se encuentran fuera de los niveles aceptables del jitter. También se puede observar, que en comparación con el experimento 7 los resultados de DSDV y OLSR son mucho más estables, experimentando menor cantidad de picos.

En la tabla 31 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y 5 conexiones simultáneas, en el cual el mejor escenario es el escenario 9 (50 nodos y protocolo OLSR), el peor escenario es el escenario 13 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 2, que utiliza el protocolo DSDV, a pesar de ser este el peor escenario se encuentra dentro de los niveles aceptables de jitter. El mejor escenario con 50 nodos es el escenario 9, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 7, que utiliza el protocolo AODV. El mejor escenario con 100 nodos es el escenario 15, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 13, que utiliza el protocolo AODV.

Tabla 31. Jitter con tiempo de simulación 150 s y 5 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Jitter (ms)
150	30	AODV	32.93
		DSDV	34.36
		OLSR	17.05
	50	AODV	59.90
		DSDV	26.41
		OLSR	3.95
	100	AODV	129.57
		DSDV	43.00
		OLSR	7.67

Fuente: Autor.

Elaborado por: Autor.

Tabla 32. Jitter con tiempo de simulación 300 s y 5 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Jitter (ms)
300	30	AODV	25.40
		DSDV	31.62
		OLSR	14.17
	50	AODV	46.69
		DSDV	41.39
		OLSR	21.33
	100	AODV	116.16
		DSDV	52.42
		OLSR	16.31

Fuente: Autor.

Elaborado por: Autor.

En la tabla 32 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y 5 conexiones simultáneas, en el cual el mejor escenario es el escenario 6 (30 nodos y protocolo OLSR), el peor escenario es el escenario 16 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 6, que utiliza el protocolo OLSR, el peor escenario es el escenario 5, que utiliza el protocolo DSDV, a pesar de ser este el peor escenario se encuentra dentro de los niveles aceptables de jitter. El mejor escenario con 50 nodos es el escenario 12, que utiliza

el protocolo OLSR, el peor escenario es el escenario 10, que utiliza el protocolo AODV, a pesar de ser este el peor escenario se encuentra dentro de los niveles aceptables de jitter. El mejor escenario con 100 nodos es el escenario 18, que utiliza el protocolo OLSR, el peor escenario es el escenario 16, que utiliza el protocolo OLSR.

Los resultados que se encuentran dentro de los niveles aceptables de jitter se ilustran en la tabla 33.

Tabla 33. Escenarios con valores aceptables de jitter con 5 conexiones simultáneas.

Número de nodos	Tiempo de simulación (s)	Protocolo del escenario	Escenario	Jitter (ms)
30	150	AODV	1	32.93
		DSDV	2	34.36
		OLSR	3	17.05
30	300	AODV	4	25.40
		DSDV	5	31.62
		OLSR	6	14.17
50	150	DSDV	8	26.41
		OLSR	9	3.95
50	300	AODV	10	46.69
		DSDV	11	41.39
		OLSR	12	21.33
100	150	DSDV	14	43.00
		OLSR	15	7.67
100	300	OLSR	18	16.31

Fuente: Autor.

Elaborado por: Autor.

6.3.3. Experimento 9: Jitter (10 conexiones simultáneas).

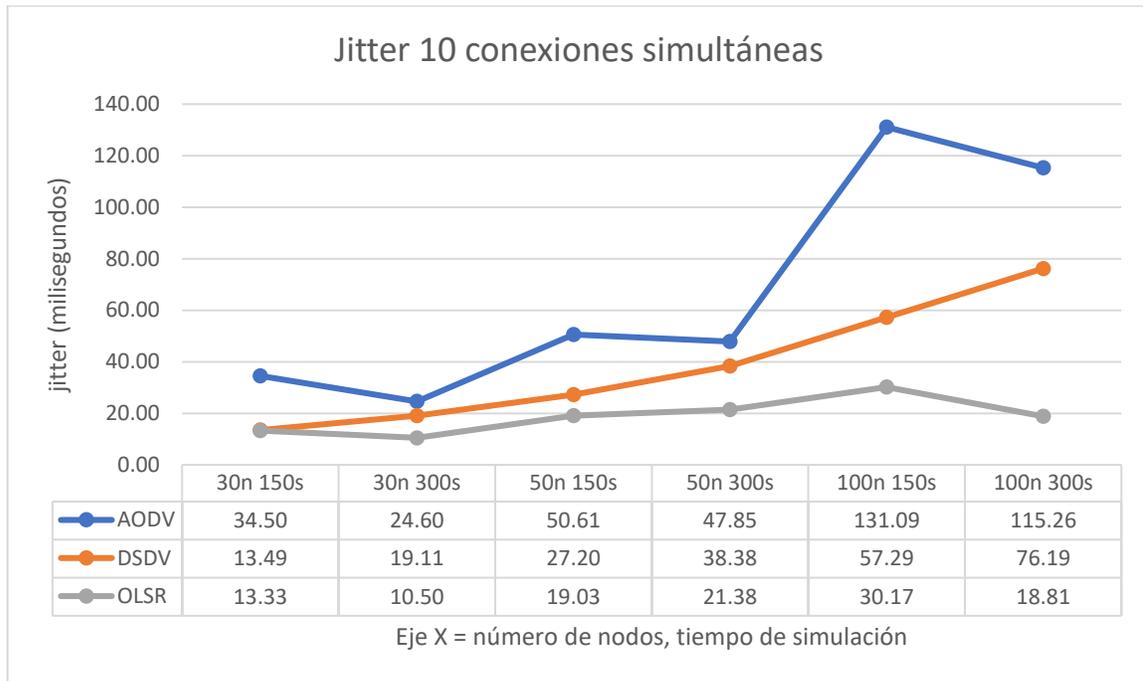


Figura 29: Resultados de jitter 10 conexiones simultáneas.

Fuente: Autor

Elaborado por: Autor.

Como se puede observar en la Figura 29, al igual que en los experimentos 7 y 8 los mejores resultados están dados por el protocolo OLSR. En este experimento hay 4 escenarios que no son aceptables, debido a que se encuentran fuera de los niveles aceptables del jitter. Además, se puede observar que en este experimento los picos en AODV se mantienen al igual que la estabilidad de OLSR, pero a diferencia de estos DSDV tiene un incremento sucesivo, mientras aumenta el número de nodos y tiempo de simulación, aumenta el nivel de jitter.

En la tabla 34 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 150 s y 10 conexiones simultáneas, en el cual el mejor escenario es el escenario 3 (30 nodos y protocolo OLSR), el peor escenario es el escenario 13 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 3, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 1, que utiliza el protocolo AODV, a pesar de ser este el peor escenario se encuentra dentro de los niveles aceptables de jitter. El mejor escenario con 50 nodos es el escenario 9, que utiliza el protocolo OLSR, mientras que el peor escenario es el escenario 7, que utiliza el protocolo AODV. El mejor escenario con 100 nodos es el escenario 15, que utiliza

el protocolo OLSR, mientras que el peor escenario es el escenario 13, que utiliza el protocolo AODV.

Tabla 34. Jitter con tiempo de simulación 150 s y 10 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Jitter (ms)
150	30	AODV	34.50
		DSDV	13.49
		OLSR	13.33
	50	AODV	50.61
		DSDV	27.20
		OLSR	19.03
	100	AODV	131.09
		DSDV	57.29
		OLSR	30.17

Fuente: Autor.

Elaborado por: Autor.

Tabla 35. Jitter con tiempo de simulación 300 s y 10 conexiones simultáneas.

Tiempo simulación (s)	Número de nodos	Protocolo	Jitter (ms)
300	30	AODV	24.60
		DSDV	19.11
		OLSR	10.50
	50	AODV	47.85
		DSDV	38.38
		OLSR	21.38
	100	AODV	115.26
		DSDV	76.19
		OLSR	18.81

Fuente: Autor.

Elaborado por: Autor.

En la tabla 35 se visualiza los resultados de las simulaciones de retardo con tiempo de simulación de 300 s y 10 conexiones simultáneas, en el cual el mejor escenario es el escenario 6 (30 nodos y protocolo OLSR), el peor escenario es el escenario 16 (100 nodos y protocolo AODV). A continuación, explicando a nivel de nodos podemos destacar que el mejor escenario con 30 nodos es el escenario 6, que utiliza el protocolo OLSR, el peor escenario es el escenario 4, que utiliza el protocolo AODV. El mejor escenario con 50 nodos es el escenario 12, que utiliza

el protocolo OLSR, el peor escenario es el escenario 10, que utiliza el protocolo AODV. El mejor escenario con 100 nodos es el escenario 18, que utiliza el protocolo OLSR, el peor escenario es el escenario 16, que utiliza el protocolo AODV.

Los resultados que se encuentran dentro de los niveles aceptables de jitter se ilustran en la tabla 36.

Tabla 36. Escenarios con valores aceptables de jitter con 10 conexiones simultáneas.

Número de nodos	Tiempo de simulación (s)	Protocolo del escenario	Escenario	Jitter (ms)
30	150	AODV	1	34.50
		DSDV	2	13.49
		OLSR	3	13.33
30	300	AODV	4	24.60
		DSDV	5	19.11
		OLSR	6	10.50
50	150	DSDV	8	27.20
		OLSR	9	19.03
50	300	AODV	10	47.85
		DSDV	11	38.38
		OLSR	12	21.38
100	150	OLSR	15	30.17
100	300	OLSR	18	18.81

Fuente: Autor.

Elaborado por: Autor.

6.3.4. Estadísticas de jitter.

Tabla 37. Estadísticas de jitter 150 s.

Escenario	Media (ms)	Varianza (ms)	Tiempo simulación (s)	Protocolo	Número de nodos
1	29.41	37.40	150	AODV	30
2	16.80	174.20	150	DSDV	30
3	10.22	51.64	150	OLSR	30
7	57.37	23.35	150	AODV	50
8	56.16	1723.29	150	DSDV	50
9	14.11	51.54	150	OLSR	50
13	130.97	1.21	150	AODV	100
14	85.89	2589.03	150	DSDV	100
15	14.47	123.98	150	OLSR	100

Fuente: Autor.

Elaborado por: Autor.

En la tabla 37 se pueden observar las estadísticas de media y varianza por cada escenario con 150 s, utilizando los resultados de los tres experimentos anteriores y en la tabla 38 se visualizan las mismas estadísticas con un tiempo de 300 s.

Tabla 38. Estadísticas de jitter 300 s.

Escenario	Media (ms)	Varianza (ms)	Tiempo simulación (s)	Protocolo	Número de nodos
4	26.46	4.35	300 s	AODV	30
5	26.54	28.81	300 s	DSDV	30
6	19.39	101.64	300 s	OLSR	30
10	48.17	1.85	300 s	AODV	50
11	55.53	490.89	300 s	DSDV	50
12	30.77	177.25	300 s	OLSR	50
16	117.04	3.64	300 s	AODV	100
17	77.02	417.68	300 s	DSDV	100
18	17.14	1.38	300 s	OLSR	100

Fuente: Autor.

Elaborado por: Autor.

En la tabla 39 se muestran las estadísticas de la media y varianza de acuerdo con la cantidad de conexiones simultáneas. En la tabla 40 se observan las mismas estadísticas, pero tomando solamente los valores de los escenarios que se encuentren dentro de los márgenes aceptables de jitter.

Tabla 39. Estadísticas de jitter por número de conexiones simultáneas.

Número de conexiones	Media (ms)	Varianza (ms)
1	57.29	5582.90
5	40.02	1079.31
10	41.60	1121.38

Fuente: Autor.

Elaborado por: Autor.

Tabla 40. Estadísticas de jitter por número de conexiones simultáneas con niveles aceptables

Número de conexiones	Media (ms)	Varianza (ms)
1	23.29	23.29
5	25.88	161.55
10	24.49	109.26

Fuente: Autor.

Elaborado por: Autor.

6.3.5. Resultados generales de jitter.

Se puede ver que, a nivel general, dentro de los tres experimentos los mejores escenarios en relación con el número de nodos y tiempo de simulación son los que utilizan el protocolo OLSR, ya que presenta los mejores valores en casi todos a excepción del experimento 7, cuando se utiliza 30 nodos con un tiempo de 300 s donde el mejor escenario es el escenario 5 dado por el protocolo DSDV.

En el experimento 7 el mejor escenario es el escenario 3, en el experimento 8 el escenario 9 y en el experimento 9 el escenario 6.

Para 150 s el mejor escenario es el escenario 3 (30 nodos y protocolo OLSR), ya que este presenta el mejor promedio referente a jitter, por lo cual si no se sabe el número exacto de conexiones simultáneas a usar este sería la mejor opción.

Para 300 s el mejor escenario es el escenario 18 (100 nodos y protocolo OLSR), ya que este presenta el mejor promedio referente a jitter, por lo cual si no se sabe el número exacto de conexiones simultáneas a usar este sería la mejor opción.

CONCLUSIONES

En este trabajo se evaluaron parámetros de QoS de VoIP mediante la simulación del soporte de aplicaciones de voz en las redes MANET.

Se presentaron fundamentos teóricos de las redes Ad-Hoc móviles, se analizaron sus principales características, funcionamiento y aplicaciones, lo que estableció la sustentación teórica para llevar a cabo este trabajo.

Se identificaron los parámetros que determinan la calidad de servicio percibida por el usuario, los cuales fueron: la pérdida de paquetes, retardo y el jitter, también se identificó el uso de tres protocolos los cuales fueron: AODV, DSDV y OLSR ya que de esta manera se integró el uso de protocolos proactivos y reactivos. Por último, se escogió el modelo de movilidad RandomWalk2 para simular la movilidad que pueden tener los nodos dentro de un entorno MANET.

Las redes MANET presentan una plataforma apropiada para el desarrollo de las redes móviles con VoIP. Por lo cual es importante dotar las mismas de QoS ya que estas permiten lograr comunicaciones de voz, en lugares donde no sería posible desplegar una red de infraestructura, además se puede desplegar estas redes en cuestión de poco tiempo en caso de emergencias o desastres naturales.

El modelo Random Walk2 puede imitar el movimiento errático de las entidades de la naturaleza, como son los movimientos impredecibles de una persona mientras utiliza un dispositivo móvil desplazándose dentro del área de la red.

Los parámetros de pérdida de paquetes, retardo y jitter fueron medidos dentro del simulador NS3, con los diferentes escenarios y experimentos establecidos, posteriormente se analizaron en la sección de resultados, con lo cual se llegó a las siguientes conclusiones:

1. A nivel general los mejores resultados para cualquier escenario, dentro de los parámetros escogidos de QOS se obtienen utilizando el protocolo OLSR, por lo cual se recomienda usar este protocolo si se desconoce el escenario exacto en el que se aplicará la red MANET con VoIP.
2. El protocolo AODV es el protocolo que presenta los peores resultados a nivel general en

lo que refiere a QoS, por lo cual no se recomienda su uso si se desea implementar una red MANET con VoIP.

3. El mejor escenario para tener una conexión es el escenario 18 el cual usa el protocolo OLSR con 100 nodos y un tiempo de simulación de 300 s.
4. El mejor escenario para tener cinco y diez conexiones simultáneas es el escenario 12 el cual usa el protocolo OLSR con 50 nodos y un tiempo de simulación de 300 s.
5. El mejor escenario para usar si es que no se conoce el número de conexiones que se tendrá es el escenario 12 ya que este presenta los mejores valores dentro de los parámetros establecidos de QoS.

Con este trabajo se ha logrado evidenciar que dotar de QoS a las redes MANET representa un gran desafío, sobre todo cuando se utiliza la comunicación de VoIP, debido a que este es muy susceptible a la variabilidad de los recursos de la red como es la pérdida de paquetes, el retardo y el jitter. No obstante, existe una gran posibilidad de usar las tecnologías de MANET y VoIP para brindar telefonía móvil de bajo costo gracias a las grandes ventajas de las redes MANET como son su facilidad de despliegue y carencia de infraestructura.

RECOMENDACIONES

A pesar de haberse cumplido los objetivos se recomienda:

- En trabajos futuros incluir otros codecs en las simulaciones de los escenarios y experimentos. Para de esta manera comprobar cómo afecta a la calidad de servicio la compresión, con el ancho de banda disponible en una red MANET y poder recomendar el codec más apropiado dentro de los escenarios.
- Integrar en trabajos futuros nuevos protocolos como BATMAN en las simulaciones de los escenarios y experimentos. Debido a que el protocolo BATMAN fue desarrollado para reemplazar al protocolo OLSR, y como hemos visto la mayoría de los mejores resultados los brinda OLSR, por lo cual se podría comprobar si BATMAN es un sustituto viable para OLSR y mejorar aún más la calidad de servicio en las redes MANET con VoIP.

BIBLIOGRAFÍA

- Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. *Journal of Network and Computer Applications*, 37, 380–392.
- Anguis, J. J. H. (2008). *Redes de Área Local Inalámbricas: Diseño de la WLAN de Wheelers Lane Technology College*. Tesis para obtener el Título de Ingeniero de las Telecomunicaciones. Universidad de Sevilla. España.
- Armendáriz, L. M. (2009). *Redes de Comunicaciones*. (Autoedición, Ed.).
- Asián Arantxa. (2014). Las mejores aplicaciones VoIP para empresas. Retrieved November 30, 2018, from <https://www.muypymes.com/2014/09/09/aplicaciones-voip>
- Atzori, L., Boi, F., & Nonnis, G. (2008). IP telephony over mobile ad hoc networks: Joint routing and playout buffering. In *Communications, 2008. ICC'08. IEEE International Conference on* (pp. 1861–1865).
- Batiste Troyano, A. (2011). Protocolos de encaminamiento en redes inalámbricas mesh: un estudio teórico y experimental.
- Beijar, N. (2002). Zone routing protocol (ZRP). *Networking Laboratory, Helsinki University of Technology, Finland*, 9, 1–12.
- Bouhorma, M., Boudhir, A. A., & others. (2011). VoIP over MANET (VoMAN): QoS & Performance Analysis of Routing Protocols for Different Audio Codecs. *IJCA Journal*, 36.
- Calderón, O. J., & QUINTERO, V. M. (2004). Un nuevo aspecto de la movilidad: Redes Ad Hoc-Conceptos. *Revista Colombiana de Tecnologías de Avanzada*, 1(3), 59–64.
- Camp, T., Boleng, J., & Davies, V. (2002). A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5), 483–502.
- Chandel, S. T., & Sharma, S. (2016). Experimental analysis of various protocols on VoIP traffic with different CODECs in Wireless LAN. In *Eco-friendly Computing and Communication Systems (ICECCS), 2016 Fifth International Conference on* (pp. 109–113).
- Chong, H. M., & Matthews, H. S. (2004). Comparative analysis of traditional telephone and voice-over-Internet protocol (VoIP) systems. In *IEEE International Symposium on Electronics and the Environment, 2004. Conference Record. 2004* (pp. 106–111). <https://doi.org/10.1109/ISEE.2004.1299697>
- Contreras Leidy. (2009). VoIP: Características y Funcionalidad del VoIP. Retrieved November 28, 2018, from <http://infovoiplc.blogspot.com/2009/02/caracteristicas-y-funcionalidad-del.html>
- Dallora Moraes, A. L., Santos Xaud, A. F., & Santos Xaud, M. F. (2007). Redes Ad Hoc - Protocolos. Retrieved May 15, 2019, from https://www.gta.ufrj.br/grad/09_1/versao-final/adhoc/aadv.html
- Fabrizio, B. O. I. (2010). QoS-based Playout Control in IP Telephony over NGNs.
- Falcón, J. A. C. (2007). *VoIP: la telefonía a de Internet*. Editorial Paraninfo.
- Giordano, S. (2002). Mobile ad hoc networks. *Handbook of Wireless Networks and Mobile Computing*, 325–346.
- Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management*, 11(2011), 32–37.
- Hanzo, L., & Tafazolli, R. (2007). A survey of QoS routing solutions for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials*, 9(2), 50–70.
- He, G. (2002). Destination-sequenced distance vector (DSDV) protocol. *Networking Laboratory, Helsinki University of Technology*, 1–9.
- Herrera-Ramírez, E., Díaz-Ramírez, A., & Calafate, C. T. (2007). Desarrollando el estándar IEEE 802.11 n, un paso adelante en WLAN. In *Segundo Congreso Internacional en Ciencias Computacionales, Baja California, México*.

- Ikeda, M., Kulla, E., Barolli, L., Takizawa, M., & Miho, R. (2011). Performance evaluation of wireless mobile ad-hoc network via NS-3 simulator. In *Network-Based Information Systems (NBIS), 2011 14th International Conference on* (pp. 135–141).
- ITU-T, R. G. 11. (2003). One-way transmission time.
- jblesa. (2017). Redes de vehículos con WSN: Introducción | B105 lab. Retrieved November 8, 2018, from <http://elb105.com/redes-de-vehiculos-con-wsn-introduccion/>
- Jose Antonio Del Peral Rosado. (2007). *MODELO DE PÉRDIDA DE PAQUETES PARA REDES HÍBRIDAS*. Retrieved from https://ddd.uab.cat/pub/trerecpro/2007/hdl_2072_5337/PFC_Peral.pdf
- Kelly, E. B. (2002). Quality of Service In Internet Protocol (IP) Networks. *International Communications Industries Association*.
- Kumar Maurya, P., Sharma, G., Sahu, V., Roberts, A., & Srivastava, M. (2012). An Overview of AODV Routing Protocol. *International Journal of Modern Engineering Research (IJMER) Www.Ijmer.Com*, 2(3). Retrieved from www.ijmer.com
- Kumar, V., Paulus, R., Agrawal, A., & Agrawal, N. (2018). Simulation based Analysis of AODV Routing Protocol in Ad Hoc Network under different Mobility and Propagation Loss Models using NS-3. *International Journal of Computer Applications*, 181, 22–26. <https://doi.org/10.5120/ijca2018917506>
- Liang, W., Li, Z., Zhang, H., Wang, S., & Bie, R. (2015). Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. *International Journal of Distributed Sensor Networks*, 11(8), 745303.
- Loo, J., Mauri, J. L., & Ortiz, J. H. (2016). *Mobile ad hoc networks: current status and future trends*. CRC Press.
- Mata, S. (2018). Saulo da Mata - VoIP Traffic Generator for ns-3. Retrieved June 10, 2019, from <https://www.saulodamata.com/dev/42-english/86-voip-traffic-generator-for-ns-3.html>
- Matango, F. (2016). Calidad de servicio de transmisión de voz con el protocolo Internet (VoIP). Retrieved from <http://www.servervoip.com/blog/tag/perdida-de-un-paquetes/>
- Murazzo, Maria Antonia, Rodriguez, N. R., Guevara, M. J., & Scheffer, M. (2014). Soporte de QoS con 802.11 e para tráfico heterogéneo en ambientes MANET. In *XX Congreso Argentino de Ciencias de la Computación (Buenos Aires, 2014)*.
- Murazzo, María Antonia, Rodríguez, N. R., Vergara, R., Carrizo, F., González, F., & Grosso, E. (2013). Administración de QoS en ambientes de redes de servicios convergentes. In *XV Workshop de Investigadores en Ciencias de la Computación*.
- ns-3 Tutorial Release ns-3.23 ns-3 project*. (2015). Retrieved from <https://www.nsnam.org/docs/release/3.23/tutorial/ns-3-tutorial.pdf>
- Patel, R., & Kamboj, P. (2015). Investigation of Network Simulation Tools and Comparison Study: NS3 vs NS2. *Transactions*, 14, 15.
- Pathak, P. H., & Dutta, R. (2011). A survey of network design problems and joint design approaches in wireless mesh networks. *IEEE Communications Surveys & Tutorials*, 13(3), 396–428.
- Pellejero, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica*. Marcombo.
- Perdana, H. T., Munadi, R., & Perdana, D. (2016). Analisis Performansi Voip Pada Vanet Dengan Menggunakan Codec Suara G. 711, G. 729, Dan Gsm. *EProceedings of Engineering*, 3(3).
- Red inalámbrica Mesh - EcuRed. (2011). Retrieved November 7, 2018, from http://www.ecured.cu/index.php/Red_inalámbrica_Mesh
- Rey, L. C., Quiñones, T. O. L., & García, W. B. (2014). Protocolos de enrutamiento aplicables a redes MANET. *Revista Telem@Tica*, 13(3), 59–74.
- Royer, E. M., Toh, C.-K., & others. (1999). A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Commun.*, 6(2), 46–55.

- Sing-Borrajo, P., & Rodríguez-López, C. (2012). Evaluación de desempeño de servicio de voz en redes MANET. *Universidad Central Marta Abreu de Las Villas*.
- The History of VoIP - From The Beginning Til Present Time. (2016). Retrieved November 27, 2018, from <https://bebusinessed.com/history/voip-history/>
- Thibodeau, E., Youssef, M., & Houle, A. C. (2006). Investigating MANET performance in a VoIP context. In *Electrical and Computer Engineering, 2006. CCECE'06. Canadian Conference on* (pp. 920–923).
- Ugas, J. C. (2009). Estudio y analisis de prestaciones de redes mviles ad hoc mediante simulaciones ns-2 para validar modelos analiticos. *Recercat. Net*.

ANEXOS

Anexo 1. Modelo de Gilbert-Elliot

“El modelo de Gilbert-Elliot ya que destaca por su sencillez. En 1960, Gilbert propuso un modelo de dos estados donde el estado “bueno” no tenía errores, y el estado “malo” representaba un estado con ráfagas de errores. Tres años después, Elliot propuso que el estado “bueno” también pudiera tener una probabilidad de error diferente a cero, pero menor a la del estado “malo”” (Jose Antonio Del Peral Rosado, 2007).

“Como se muestra en la Figura 6.1, el modelo de Gilbert-Elliot está formado por dos estados a los que llamamos G (estado bueno) y B (estado malo). Las probabilidades de las transiciones entre estados cumplen con $\Pr(B|G) = b$ (probabilidad de pasar al estado malo estando en el bueno), y con $\Pr(G|B) = g$ (probabilidad de pasar al estado bueno estando en el “malo”). Si nos fijamos, cada estado del modelo actúa exactamente como un canal binario simétrico (BSC, de sus siglas en inglés). Las probabilidades de cambio, es decir, las probabilidades de error en el estado bueno y en el estado malo son nombradas como P_G y P_B , respectivamente. Por consiguiente, el modelo de Gilbert-Elliot es un modelo de cuatro parámetros, que son: g , b , p_G y p_B .” (Jose Antonio Del Peral Rosado, 2007).

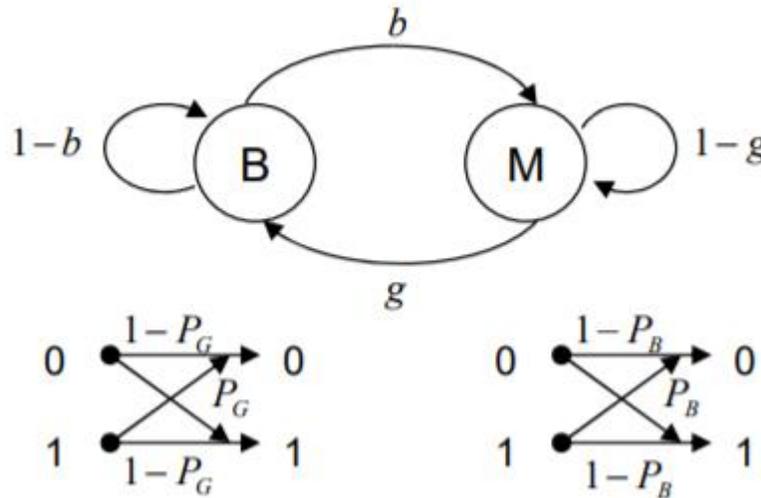


Figura 30: Diagrama del modelo de Gilbert-Elliot con las transiciones de los estados.

Fuente: (Del Peral Rosado, 2007).

Elaborado por: Del Peral Rosado.

Anexo 2. Instalación de NS3

Antes de la instalación de NS3 se necesita realizar algunos pasos que son los siguientes:

1. *\$ sudo apt-get update.*

Descarga las listas de paquetes de los repositorios y las "actualiza" para obtener información sobre las versiones más recientes de los paquetes y sus dependencias. Hará esto para todos los repositorios y PPAs.

2. *\$ sudo apt-get upgrade.*

buscará nuevas versiones de paquetes existentes en la máquina APT conoce estas nuevas versiones a través de *apt-get update*.

3. instalar todas las librerías que necesitara NS3 para su funcionamiento esto se hace mediante el siguiente comando:

```
$ sudo apt install build-essential autoconf automake libxmu-dev python-pygoocanvas python-pygraphviz cvs mercurial bzip2 git cmake p7zip-full python-matplotlib python-tk python-dev python-kiwi python-gnome2 python-gnome2-desktop-dev python-rsvg qt4-dev-tools qt4-qmake qt4-default gnuplot-x11 wireshark
```

Una vez realizados los pasos anteriores se podrá proceder a la instalación de NS3.¹

La instalación de NS3 es bastante sencilla ya que todo el código necesario se encuentra disponible en su sitio oficial www.nsnam.org, al ser software libre su descarga es muy sencilla también.

Para su instalación se requiere de una máquina que tenga instalado un sistema Linux en este caso se usó Ubuntu 16.4, además debe contar con los compiladores C++ (g++).

También se puede utilizar una máquina virtual en Windows como Virtual Box e instalarle un sistema operativo Linux, pero se puede experimentar problemas ya que al usar una máquina virtual no se reconocen todos los periféricos de red de un computador.

Como primer paso nos dirigimos a la página oficial de NS3, de aquí vamos a descargas, para este proyecto se usó la versión "ns-3.28" luego de encontrar la versión que se desea instalar se procede a la descarga del archivo con extensión ".tar.bz2". Una vez se tiene descargado el archivo se debe descomprimir el mismo, esto se hace mediante el siguiente comando en el terminal de Linux:

```
$ cd "dirección del archivo"
```

```
$ tar jxvf "nombre del archivo descargado".bz2
```

Ya extraído el archivo debemos acceder a esta carpeta:

¹ www.nsnam.org

```
$ cd "nombre carpeta"
```

Una vez dentro de la carpeta ejecutar el siguiente comando:

```
$ ./build.py --enable-examples --enable-tests
```

Con esto se finaliza la instalación de NS3 y se puede probar que el mismo esté funcionando mediante los ejemplos.

Anexo 3. Creación de tráfico VoIP en la red MANET

Se debe descargar los archivos disponibles en:

<https://www.dropbox.com/s/wz8zykmmdb7p7r7/voip-traffic-generator.zip?dl=1>, una vez descargado tendremos un archivo zip el cual deberemos descomprimir y copiar los archivos voip-client-server-helper.(h/cc) al directorio “/src/applications/helper”, como se observa en la Figura 31 y los archivos voip-client.(h,cc) , voip-server.(h,cc) al directorio “/src/applications/model”, como se observa en la Figura 32.

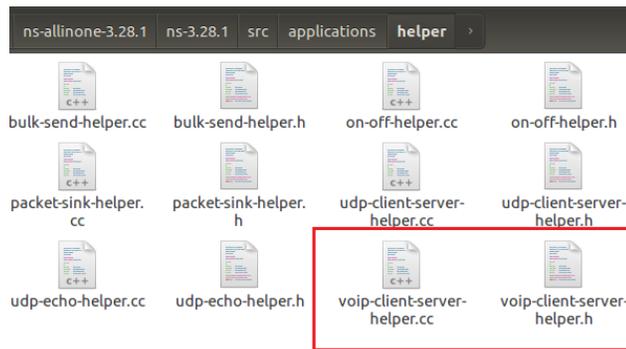


Figura 31: Archivos para generar tráfico VoIP agregados a la carpeta helper.

Fuente: Autor

Elaborado por: Autor.

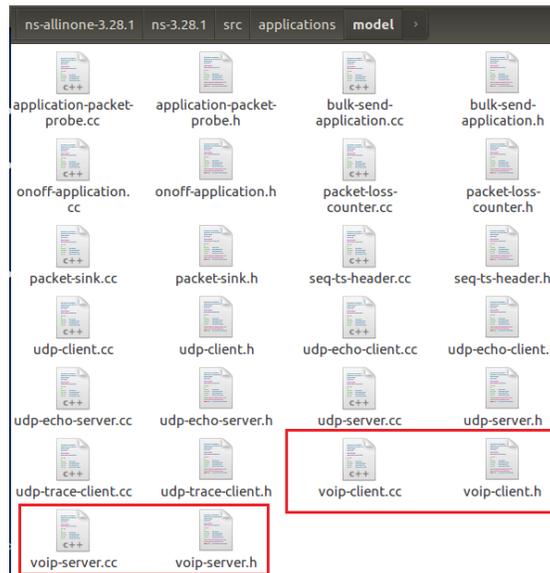


Figura 32: Archivos para generar tráfico VoIP agregados a la carpeta model.

Fuente: Autor

Elaborado por: Autor.

Agregar las entradas de estos archivos al script waf (wscript).

```
'model/voip-client.cc',  
'model/voip-server.cc',  
'helper/voip-client-server-helper.cc',  
'model/voip-client.h',  
'model/voip-server.h',  
'helper/voip-client-server-helper.h',
```



```
wscript (~/Documentos/ns-allinone-3.28.1/ns-3.28.1/src/applications) - gedit  
Abrir ▾   
  
def build(bld):  
    module = bld.create_ns3_module('applications', ['internet', 'config-store', 'stats'])  
    module.source = [  
        'model/bulk-send-application.cc',  
        'model/onoff-application.cc',  
        'model/packet-sink.cc',  
        'model/udp-client.cc',  
        'model/udp-server.cc',  
        'model/seq-ts-header.cc',  
        'model/udp-trace-client.cc',  
        'model/packet-loss-counter.cc',  
        'model/udp-echo-client.cc',  
        'model/udp-echo-server.cc',  
        'model/application-packet-probe.cc',  
        'model/voip-client.cc',  
        'model/voip-server.cc',  
        'helper/bulk-send-helper.cc',  
        'helper/on-off-helper.cc',  
        'helper/packet-sink-helper.cc',  
        'helper/udp-client-server-helper.cc',  
        'helper/udp-echo-helper.cc',  
        'helper/voip-client-server-helper.cc',  
    ]  
  
    applications_test = bld.create_ns3_module_test_library('applications')  
    applications_test.source = [  
        'test/udp-client-server-test.cc',  
    ]  
  
    headers = bld(features='ns3header')  
    headers.module = 'applications'  
    headers.source = [  
        'model/bulk-send-application.h',  
        'model/onoff-application.h',  
        'model/packet-sink.h',  
        'model/udp-client.h',  
        'model/udp-server.h',  
        'model/seq-ts-header.h',  
        'model/udp-trace-client.h',  
        'model/packet-loss-counter.h',  
        'model/udp-echo-client.h',  
        'model/udp-echo-server.h',  
        'model/application-packet-probe.h',  
        'model/voip-client.h',  
        'model/voip-server.h',  
        'helper/bulk-send-helper.h',  
        'helper/on-off-helper.h',  
        'helper/packet-sink-helper.h',  
        'helper/udp-client-server-helper.h',  
        'helper/udp-echo-helper.h',  
        'helper/voip-client-server-helper.h',  
    ]  
}
```

Figura 33: Entradas para archivos agregados al script waf (wscript).

Fuente: Autor

Elaborado por: Autor.

Insertar los include de los paquetes necesarios

```
#include "ns3/v4ping-helper.h"  
#include "ns3/voip-client.h"
```

```
#include "ns3/voip-server.h"  
#include "ns3/voip-client-server-helper.h"
```

Incorporar el código para la creación de tráfico VoIP en el script MANET.

Para poder integrar el código dentro de nuestro script solo se necesita integrar las variables que especifica en el código original con el nombre de las variables de nuestro script. Algunas variables se deben incorporar como el puerto a usar.

```
V4PingHelper ping (ad hocInterfaces.GetAddress (nWifis - 1));  
ping.SetAttribute ("Verbose", BooleanValue (true));  
  
VoipServerHelper voipServer (m_port);  
voipServer.SetAttribute ("Interval", TimeValue (Seconds (1.0)));  
voipServer.SetAttribute ("PacketSize", UIntegerValue (60));  
  
VoipClientHelper voipClient (ad hocInterfaces.GetAddress (nWifis-1), m_port);  
  
ApplicationContainer p = ping.Install (ad hocNodes.Get (0));  
p.Start (Seconds (0));  
p.Stop (Seconds (TotalTime) - Seconds (0.001));
```

Figura 34: Agregación del tráfico VoIP al script.

Fuente: Autor

Elaborado por: Autor.

Anexo 4. Inserción nodos, tiempo de simulación y protocolo al simular por teclado

Como primer paso se debe agregar tres variables de tipo enteros (int), los cuales se usarán para asignar los valores ingresados por teclado.

```
int nodo;  
  
int timeN;  
  
int proto;
```

Figura 35: Variables creadas para ingreso de datos.

Fuente: Autor

Elaborado por: Autor.

Por cada uno de los valores que se dese ingresar por teclado se debe presentar en consola un mensaje especificando el valor a ingresar y guardar en la variable correspondiente el valor ingresado.

```
int main (int argc, char *argv[])  
{  
    std::cout << "Ingrese número de nodos: \n";  
    std::cin >> nodo;  
  
    std::cout << "Ingrese tiempo total: \n";  
    std::cin >> timeN;  
  
    std::cout << "Ingrese el protocolo (1 OLSR, 2 AODV, 3 DSDV): \n";  
    std::cin >> proto;
```

Figura 36: Presentación de los valores a ingresar por teclado y almacenamiento del valor ingresado en las variables

Fuente: Autor

Elaborado por: Autor.

Por último, se debe asignar los valores ingresados por teclado a cada una de las variables correspondientes dentro del código de la red MANET, para que estos puedan interactuar en la simulación.

```
int nWifis = nodo;  
  
double TotalTime = timeN;  
  
m_protocol (proto)
```

Figura 37: Asignación de los valores ingresados por teclado a variables correspondientes del script.

Fuente: Autor

Elaborado por: Autor.

Anexo 5. Estadísticas media y varianza.

Media:

La media es el valor promedio de las muestras y es independiente de las amplitudes de los intervalos. Se simboliza como μ . Se encuentra sumando todos los valores y dividiendo por el número total de datos.

Para calcular la media se utiliza la ecuación 5.

$$\mu = \frac{\sum x}{n}$$

Ecuación 5: Media.

Donde:

μ = media de la población.

\sum = sumatoria.

x = término del conjunto de datos.

n = tamaño de la población.

Ejemplo:

Para calcular la media de un conjunto de datos se comienza con el conjunto de datos de la población. El término "población" refiere al total de datos de las observaciones relevantes. En este ejemplo se utiliza el total de datos del experimento 1.

Tabla 41. Conjunto de datos de la población.

	x
x1	42.56
x2	1.56
x3	0.00
x4	43.50
x5	27.09
x6	33.86
x7	105.77
x8	148.46
x9	9.76
x10	64.46
x11	106.18
x12	42.58
x13	183.37
x14	349.31
x15	5.02
x16	148.05
x17	151.32
x18	16.40

Fuente: Autor

Elaborado por: Autor

1. se realiza la sumatoria de todos los datos.

$$\mu = \sum x = 899.20$$

2. Se divide la sumatoria de todos los datos para el número de datos.

$$\mu = \frac{899.20}{18} = 49.96$$

La media de este conjunto de datos es 49.96.

Varianza:

La varianza es una medida de qué tan disperso es un conjunto de datos. Si la varianza es pequeña, significa que los valores del conjunto están bastante agrupados. Si la varianza es grande, significa que los números están más dispersos.

Para calcular la varianza se utiliza la ecuación 6.

$$\sigma^2 = \frac{\sum(x_i - \mu)^2}{n}$$

Ecuación 6: Varianza.

Donde:

σ = varianza de la población.

\sum = sumatoria.

x = término del conjunto de datos.

μ = media de la población.

n = tamaño de la población.

Ejemplo:

Se comienza con el conjunto de datos de la población. En este ejemplo se utiliza el total de datos del experimento 1.

El conjunto de datos del experimento 1 se pueden observar en la tabla 41.

1. Restamos la media obtenida anterior mente a cada punto de datos. Los puntos de datos cercanos a la media tendrán una diferencia más cercana a cero. Se repite la resta para cada punto de datos y se comienza a tener una noción aproximada de qué tan dispersos están los datos. Los resultados se pueden ver en la tabla 42.

Tabla 42. Resultados de $x - \mu$.

	x	x- μ
x1	42.56	-39.62
x2	1.56	-80.62
x3	0.00	-82.18
x4	43.50	-38.68
x5	27.09	-55.09
x6	33.86	-48.32
x7	105.77	23.59
x8	148.46	66.28
x9	9.76	-72.42
x10	64.46	-17.72
x11	106.18	24.00
x12	42.58	-39.60
x13	183.37	101.19
x14	349.31	267.13
x15	5.02	-77.16
x16	148.05	65.87
x17	151.32	69.14
x18	16.40	-65.78

Fuente: Autor

Elaborado por: Autor

2. Se al cuadrado todas las respuestas. Ahora, algunos de los números del paso anterior serán negativos mientras que otros serán positivos. Si dibujas tus datos en una línea numérica, estas dos categorías representarán los números que están a la izquierda de la media y los que están a la derecha de la media. Estos valores no son de mucha ayuda para calcular la varianza, ya que los dos grupos se cancelarían entre sí. Se eleva al cuadrado cada uno de los números para transformarlos en valores positivos.

Tabla 43. Resultados de $(x-\mu)^2$.

	x	x- μ	(x-μ)²
x1	42.56	-39.62	1569.94
x2	1.56	-80.62	6499.82
x3	0.00	-82.18	6753.55
x4	43.50	-38.68	1496.02
x5	27.09	-55.09	3034.75
x6	33.86	-48.32	2334.59
x7	105.77	23.59	556.64
x8	148.46	66.28	4393.58
x9	9.76	-72.42	5243.96
x10	64.46	-17.72	313.86
x11	106.18	24.00	575.90
x12	42.58	-39.60	1567.94
x13	183.37	101.19	10239.06
x14	349.31	267.13	71359.02
x15	5.02	-77.16	5953.61
x16	148.05	65.87	4338.67
x17	151.32	69.14	4779.79
x18	16.40	-65.78	4327.22

Fuente: Autor

Elaborado por: Autor

3. Se encuentra la media de los resultados. Se obtiene el valor para cada punto de datos, relacionado (indirectamente) con la dispersión que ese punto de datos tiene respecto de la media. Calculamos la media de estos valores sumándolos y luego dividiendo la suma por la cantidad de valores.

La suma de los valores de cada punto de datos da como resultado 135337.91.

$$\sigma^2 = \frac{135337.91}{18} = 7518.77$$

La varianza de este conjunto de datos es 7518.77.