UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

CARACTERIZACIÓN DE LA TÉCNICA JAMMING PARA EVALUAR EL NIVEL DE SEGURIDAD EN REDES INALÁMBRICAS IEEE 802.11

Previa la obtención del Título

INGENIERA EN TELECOMUNICACIONES

ELABORADA POR:
Melisa Estefania González Ortega

DIRECTOR
MsC. Edwin Palacios Meléndez.

Guayaquil, 20 de Febrero del 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por la Srta. **Melisa Estefania González Ortega** como requerimiento parcial para la obtención del título de INGENIERA EN TELECOMUNICACIONES.

Guayaquil, 20 de Febrero del 2014

DIRECTOR

_____

MsC. Edwin Palacios Meléndez.

REVISADO POR

_____

Ing. Juan López Cañarte.

Revisor Metodológico

_____

Ing. Marcos Montenegro Tamayo.

Revisor de Contenido

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

MELISA ESTEFANIA GONZÁLEZ ORTEGA

DECLARÓ QUE:

El proyecto de tesis denominado “Caracterización de la técnica JAMMING para evaluar el nivel de seguridad en redes inalámbricas IEEE 802.11” ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Guayaquil, 20 de Febrero del 2014

EL AUTOR

MELISA ESTEFANIA GONZÁLEZ ORTEGA

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, MELISA ESTEFANIA GONZÁLEZ ORTEGA

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del proyecto titulado: "Caracterización de la técnica JAMMING para evaluar el nivel de seguridad en redes inalámbricas IEEE 802.11", cuyo contenido, ideas y criterios es de mi exclusiva responsabilidad y autoría.

Guayaquil, 20 de Febrero del 2014

EL AUTOR

MELISA ESTEFANIA GONZÁLEZ ORTEGA

DEDICATORIA

Este trabajo de tesis lo dedico con mucho cariño a Dios, por permitirme llegar con esfuerzo y dedicación a esta meta tan anhelada y agradecerle por regalarme una gran familia que siempre estará apoyándome en cada paso importante de mi vida.

A mis padres, que han estado conmigo, cuidándome y dándome fortaleza para seguir adelante, a mis hermanas, mi cuñado y mis dos sobrinitos por su cariño y confianza,, a cada uno de ellos que son el motivo y la razón que me ha llevado a seguir superándome día a día.

EL AUTOR

MELISA ESTEFANIA GONZÁLEZ ORTEGA

AGRADECIMIENTO

Agradezco en primer lugar a Dios por haberme permitido terminar con éxito esta etapa de mi vida; de manera especial a cada uno de los miembros de mi familia, a mis PADRES Sergio y Martha, por su esfuerzo y su apoyo incondicional, a mis hermanas, a mi cuñado y a mis dos sobrinos por motivarme para seguir adelante.

A mi Director de tesis quién además de ser mi amigo me ayudó en todo momento MsC. Edwin Palacios, y a todos los docentes de esta prestigiosa Universidad que con su experiencia fueron parte importante de mi formación académica.

EL AUTOR

MELISA ESTEFANIA GONZÁLEZ ORTEGA

Índice General

Índice de Figuras

Capítulo 2

Capítulo 3

Capítulo 4

Índice de Tablas

Capítulo 2

Capítulo 4

Resumen

Para el presente trabajo de titulación se estudió el comportamiento de una red inalámbrica (WLAN) en la capa MAC, mediante la caracterización de la técnica *jamming* que se describe en el capítulo 4. Todos estos ataques se pudieron emular o simular a través de la plataforma OPNET Modeler. Las simulaciones realizadas se obtuvieron excelentes resultados, evidenciando las consecuencias de los ataques *jamming.*

En el capítulo 1 se expone la descripción general del trabajo de titulación, donde describimos la introducción, antecedente, definición del problema, objetivos del problema a investigar, hipótesis o idea a defender y la metodología de investigación a utilizar.

En el capítulo 2 y 3 se realiza la descripción y aprendizaje, tanto para redes inalámbricas como del simulador OPNET Modeler respectivamente.

En el capítulo 4 se realiza el diseño de redes WLAN y la simulación en OPNET Modeler, en el mismo se especifica cual caracterización de la técnica *jamming* es la más apropiada.

CAPÍTULO 1: GENERALIDADES DEL TRABAJO DE TITULACIÓN

1.1. Introducción.

Las empresas proveedoras de comunicaciones inalámbricas conocidas como WLAN, han crecido exponencialmente en la última década y está desplegando en todos los ámbitos de redes tradicionales. La mayoría de empresas tanto privadas como instituciones públicas y hogares que prefieren por este sistema en alternativa a las soluciones habituales que utilizan cableado.

Las WLAN's tienen ventajas importantes, entre las más relevantes son la movilidad y flexibilidad, debido a que los usuarios se conectan a redes disponibles y trasladarse libremente dentro del área de cobertura, como por ejemplo, la Red Inalámbrica de la Universidad Católica de Santiago de Guayaquil tiene cobertura en todo el campus, fuera del mismo no se podrán conectar a la WLAN. Es decir, que mientras sigan dentro del área de cobertura, seguirán con servicio de datos en sus dispositivos. Obviamente, esto significa se eliminan las acciones de instalación de cables y tomas de red utilizadas en las redes cableadas, lo que supone un ahorro de tiempo y dinero.

Aunque parezca ser una ventaja no requerir un medio físico para trabajar u operar, se vuelve un inconveniente. Las WLAN's deben certificar que la información recibida no tenga pérdidas, que muchas veces son provocadas por falta de fiabilidad del canal de comunicación. Además teniendo en cuenta que las transmisiones están a disposición de cualquiera dentro del alcance de la red, la seguridad se vuelve un asunto más que importante.

Para el desarrollo del trabajo de titulación se centrará en el estudio y caracterización del nivel de seguridad en redes WLAN's, para lo cual se iniciará en la vulnerabilidad de la capa MAC frente a ataques producidos sobre la misma capa. Estos ataques son realizados a través de tramas enviadas de

manera malintencionada, lo que provocaría interferencias durante la transmisión entre las estaciones.

1.2. Antecedentes.

Jamming (también llamada interferencia) es la radiación de energía electromagnética en un canal de comunicación que reduce el uso eficaz del espectro electromagnético para la comunicación legítima. Jamming resulta en una pérdida de fiabilidad de enlace, el aumento del consumo de energía, los retrasos de paquetes largos y la interrupción de las rutas de extremo a extremo.

Jamming puede ser a la vez malicioso con la intención de bloquear la comunicación de un adversario o no malicioso en forma de interferencia de canal no deseado.

En el contexto de las redes inalámbricas integradas para operación crítica en tiempo crítico y de seguridad como en los dispositivos médicos y las redes de control industrial, es esencial que los mecanismos de resistencia a las interferencias sean nativos del protocolo de comunicación. La resistencia a las interferencias y su evitación, denominados colectivamente como anti-jamming, es un problema práctico duro como el jammer tiene una ventaja injusta en la detección de la actividad de comunicación debido a la naturaleza de difusión del canal.

Los nodos de comunicación son incapaces de diferenciar señales de interferencia de las transmisiones legítimas o los cambios en la actividad de comunicación debido al movimiento de nodo o nodos de apagar sin algún tipo de procesamiento mínimo, a expensas de los recursos locales y de red.

Finalmente, con la intención de delimitar el ámbito del problema se va realizar una explicación teórica en el capítulo 2 de las tecnologías empleadas en el presente trabajo de titulación.

1.3. Definición del Problema.

Los ataques mediante técnicas de jamming generan intencionadamente una señal desde un dispositivo inalámbrico (Wireless) con la intención de que interfiera en las señales genuinas, en la que jamming resulta siempre desde una estación avara que transmite tramas de manera selectiva a otras estaciones, que producen recepciones erróneas y así las estaciones aumenten su ventana de contención. Por esto surge la necesidad de caracterizar la técnica jamming modelando mediante simulación el nivel de seguridad en WLAN's (IEEE 802.11).

1.4. Objetivos del Problema de Investigación.

Una vez que se describe el problema de investigación, en el presente acápite se especificarán tanto el objetivo general como específicos del trabajo de titulación.

1.4.1. Objetivo General.

Caracterizar la técnica jamming para su ejecución, mediante simulación en OPNET Modeler, de los ataques a la seguridad en una red inalámbrica IEEE 802.11.

1.4.2. Objetivos Específicos.

- Realizar un acercamiento de la fundamentación teórica o estado del arte de las redes inalámbricas a través del estándar 802.11.

- Explicar el funcionamiento de la interfaz de modelación OPNET que permita llevar a cabo la simulación de ataques malintencionados mediante la técnica jamming.
- Realizar el diseño y simulación del funcionamiento y efectividad de la técnica jamming mediante el programa OPNET Modeler.

1.5. Idea a Defender.

Mediante la descripción del estado del arte y aplicando OPNET para simular los ataques, permitirá que los estudiantes conozcan de la técnica jamming, su funcionalidad y a la vez tendrán una nueva herramienta de simulación para sistemas de redes de comunicación de datos.

1.6. Metodología de Investigación.

El presente trabajo de titulación es Exploratorio y Explicativo. Es exploratorio, porque pretendemos examinar la técnica de ataque o *jamming* en redes inalámbricas (WLAN) que causan el fenómeno en cuestión; y es explicativo porque se describirá la situación del por qué ocurre el fenómeno (usando una herramienta de simulación real). Adicionalmente, el trabajo de titulación es Empírico-Analítico con enfoque cuantitativo.

CAPÍTULO 2: Fundamentación Teórica de Redes Inalámbricas.

2.1. Introducción a Redes Inalámbricas.

Los clientes se enfrentan hoy en día con una amplia variedad de tecnologías inalámbricas, sistemas y proveedores para hacer frente a las necesidades de recopilación de datos inalámbrica. Sin embargo, la mayoría de los clientes se encuentran con que no hay una solución inalámbrica simple adecuada para todas las aplicaciones. Por ejemplo, la mensajería de bajo volumen puede ser servido por las muchas opciones disponibles para la paginación de dos vías y PCS de banda estrecha (Sistema de Comunicación Personal).

Para mayores volúmenes de datos, redes de área local inalámbricas (WLAN) ofrecen una solución excelente para un área local. Para las comunicaciones inalámbricas a través de una ciudad, estado o país, las opciones de red metropolitana o de área amplia inalámbricas son las posibles soluciones.

Proveedores tales como Celulares Analógicos, Bell South (antes RAM), Ardis, GSM, GPRS, TETRA, DECT, Celulares Digitales o PCS pueden ofrecer soluciones para voz/datos integrados a través de una amplia área. Por último, GEO (órbita geoestacionaria de la Tierra) y LEO (Low Earth Orbit) son soluciones satelitales cada vez más disponibles en una escala global.

Mientras que los clientes pueden elegir entre muchas soluciones inalámbricas de datos, la mayoría de ellos pueden seleccionar un sistema inalámbrico para satisfacer las necesidades de los datos. Las WLAN´s proporcionan alta velocidad, comunicaciones de datos fiables en un edificio o entorno de campus, así como la cobertura en las zonas rurales. Las LAN´s inalámbricas son fáciles de instalar y no incurren en pagos de los usuarios mensuales o cargos por transmisión de datos.

2.2. Topologías de LAN´s Inalámbricas

Las LAN´s inalámbricas pueden ser construidas con cualquiera de las dos topologías: basada punto a punto (peer-to-peer) o basada en punto de acceso. Para la topología de punto a punto, los dispositivos cliente dentro de la célula inalámbrica se comunican directamente entre sí, tal como se ilustra en la figura 2.1.

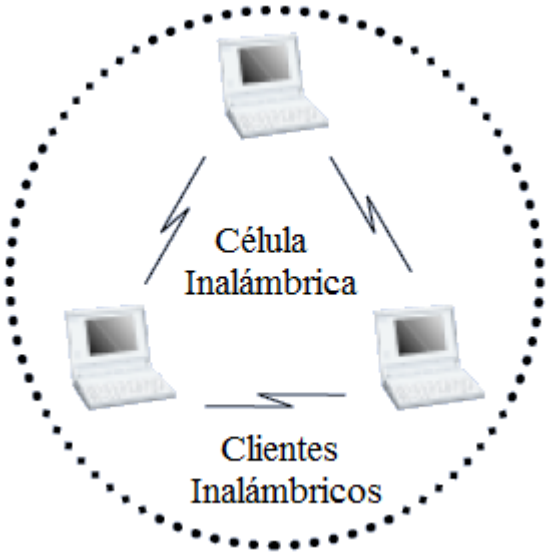


Figura 2. 1: Configuración punto a punto (peer-to-peer).
Fuente: López O., F. (2002).

Mientras que en la otra topología, es decir, el punto de acceso es un puente que conecta a un dispositivo cliente inalámbrico a una red cableada. La mencionada topología se basa en un punto de acceso, que utiliza puntos de acceso para tender un puente sobre el tráfico en un esqueleto por cable (Ethernet o Token Ring) o de forma inalámbrica, tal como se muestra en la figura 2.2.

El punto de acceso permite a un dispositivo cliente inalámbrico comunicarse con otros dispositivos con cable o inalámbrico de la red. La topología de punto de acceso es comúnmente la más utilizada, lo que demuestra que las WLAN´s no reemplazan las LAN´s cableadas, sino que simplemente extienden la conectividad a los dispositivos móviles.

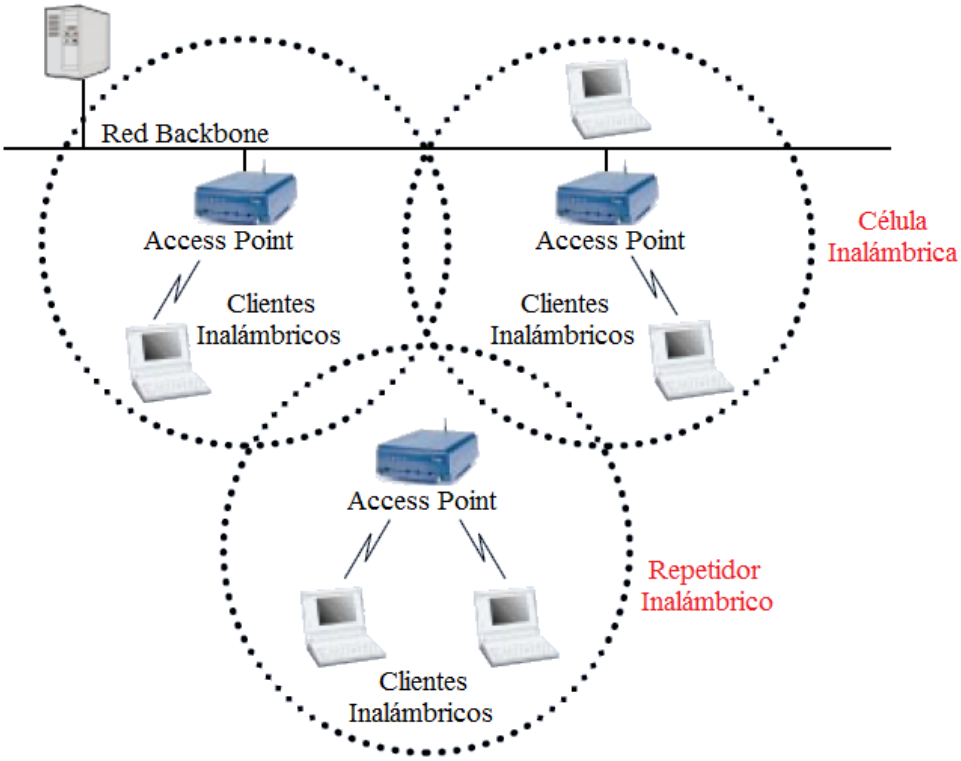


Figura 2. 2: Configuración punto de acceso.
Fuente: López O., F. (2002).

Otra popular topología de redes inalámbricas es el puente de punto a multipunto. Un puente se define como un nodo (o par de nodos) con un dispositivo de cliente transceptor que conecta dos redes que utilizan protocolos similares. Los puentes inalámbricos conectan una red LAN en un edificio a una LAN en otro, incluso si los edificios están a muchos kilómetros de distancia (véase las figuras 2.3 y 2.4).

Estas conexiones requieren una línea de visión clara (es decir, no hay obstáculos, como edificios, colinas o árboles) entre los edificios. La gama de la línea de visión varía en función del tipo de puente inalámbrico y la antena utilizada, así como las condiciones ambientales.

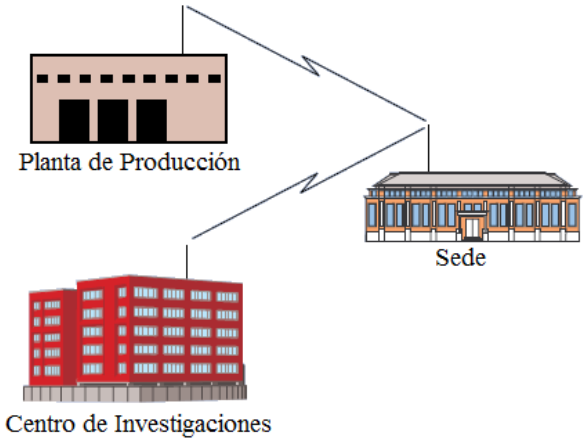


Figura 2. 3: Configuración del puente inalámbrico punto a multipunto.
Fuente: López O., F. (2002).

Los usuario de WLAN's están disponibles en una serie de formatos para su utilización en cualquiera de estas topologías de red. Las computadoras personales (PC's) pueden conectarse a una WLAN mediante ISA y tarjetas de adaptador de PC. Los módems inalámbricos pueden conectarse a los puertos paralelos RS232, 10BaseT, IRDA, u otras interfaces físicas populares en una PC u otro dispositivo.

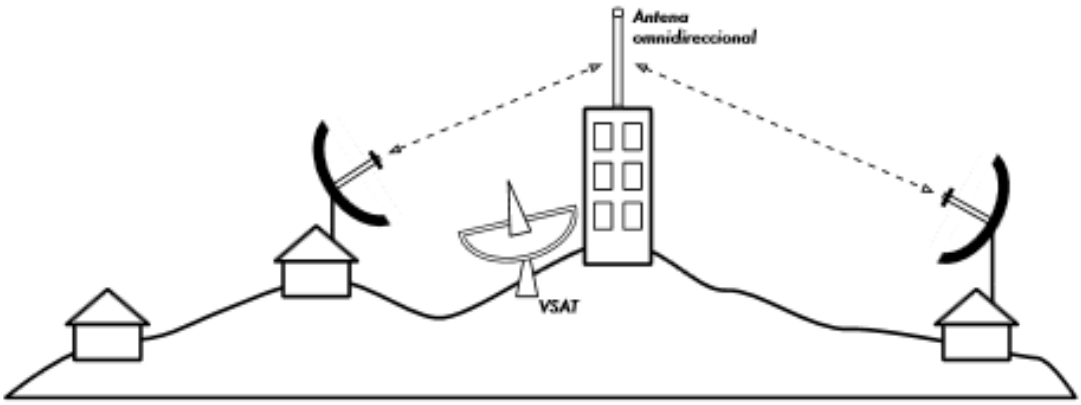


Figura 2. 4: Aplicación de un enlace punto a multipunto.
Fuente: Alchele, C., Flickenger, R., Fonda, C., Howard, I., Krag, T. & Zennaro, M. (2006).

En esta configuración, el dispositivo del usuario se comunica a través de la interfaz física (por ejemplo, ISA o adaptador de PC, RS232, etc.) del dispositivo de radio, que a su vez proporciona la interfaz física a la WLAN.

Para aplicaciones portátiles, las configuraciones más comunes son las tarjetas de adaptador PCMCIA para ordenadores portátiles y módulos LAN integrados para, terminales de mano de aplicaciones específicas.

2.3. Tecnologías Inalámbricas LAN.

Las tecnologías disponibles para su uso en redes WLAN incluyen infrarrojo, radio UHF (banda estrecha) y radios de espectro disperso. Más adelante se describirá infrarrojos y radio UHF. Dos técnicas de espectro ensanchado son actualmente prevalentes:

a) Salto de frecuencia (FHSS)

López O., F. (2002) en su trabajo de temas avanzados de Redes de Ordenadores del Curso de Doctorado de la Universidad Politécnica de Madrid, sostiene que FHSS transfiere parte de los datos en una única frecuencia en un tiempo de permanencia *(dwell time)* inferior a los $400\ ms$.

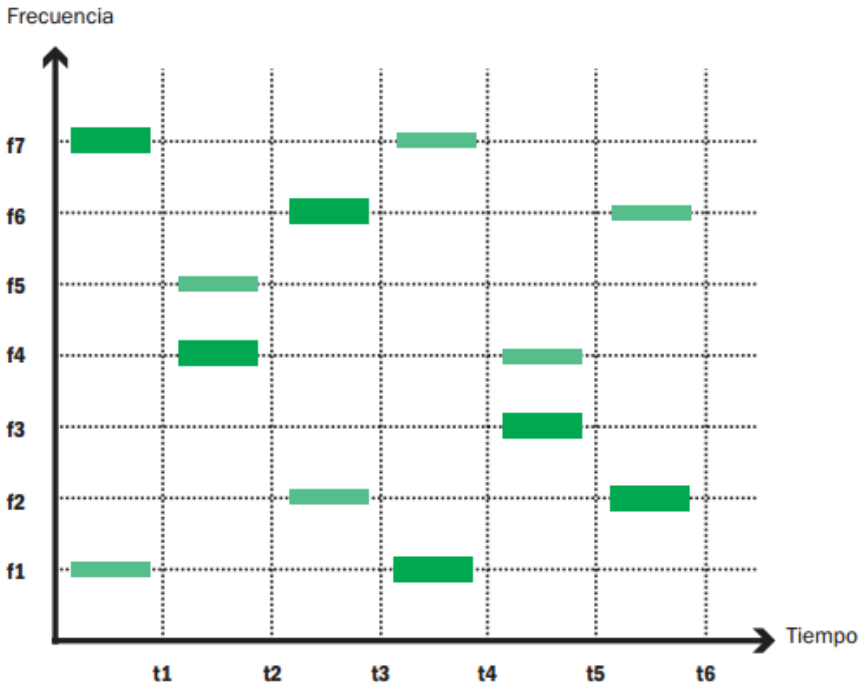


Figura 2. 5: Ejemplo de espectro ensanchando por salto de frecuencia.
Fuente: Andrade, R., Salas, P., & Santos P., Daniel (2008).

En otro trabajo similar al descrito anteriormente, los autores Andrade, R., Salas, P., & Santos P., Daniel (2008), indican que pasado el tiempo de permanencia la frecuencia de Tx cambia y después sigue su transmisión utilizando otra frecuencia (véase la figura 2.6), es decir, que una parte de los datos transmiten en una frecuencia diferente durante un tiempo muy bajo.

Tabla 2. 1: Parámetros capa física de espectro FHSS.

Parámetro	Valor	Notas
Slot time	50 µs	
SIFS time	28 µs	Del valor del SIFS se derivan los valores de los espacios intertrama (DIFS, PIFS y EIFS)
Tamaño de la ventana de contienda	15 - 1023 slots	
Duración del preámbulo	96 µs	Los símbolos del preámbulo son transmitidos a 1 MHz. Como un símbolo tarda 1 µs en ser transmitido, 96 bits requieren 96 µs
Duración del PLCP header	32 µs	32 bits del PLCP *header*
Máxima trama MAC	4095 bytes	802.11 recomienda un máximo de 400 símbolos (400 bytes en 1 Mbps, 800 bytes en 2 Mbps) para mantener una *performance* a lo largo de diferentes tipos de medios
Sensibilidad mínima	-80 dBm	

Fuente: Andrade, R., Salas, P., & Santos P., Daniel (2008).

b) Secuencia Directa (DSSS)

Lema O., R (2005) en su proyecto de grado, manifiesta que los sistemas de secuencia directa multiplican la portadora de radio frecuencia (RF) con el código pseudo ruido randómico.

Mientras que Charro S., F. & Erazo A., P. (2006) en su trabajo de grado, indica que la secuencia directa mezcla la información a transmitir con un patrón de bits pseudoaleatorios, en la que cada bit se modula a través de una secuencia de bits de código.

De manera similar al párrafo anterior, Andrade, R., et al (2008) sostiene que para transmitir una señal, esta se debe modular mediante secuencias de bits de alta velocidad conocidas como chips o ruido pseudoaleatorio, tal como se muestra en la figura

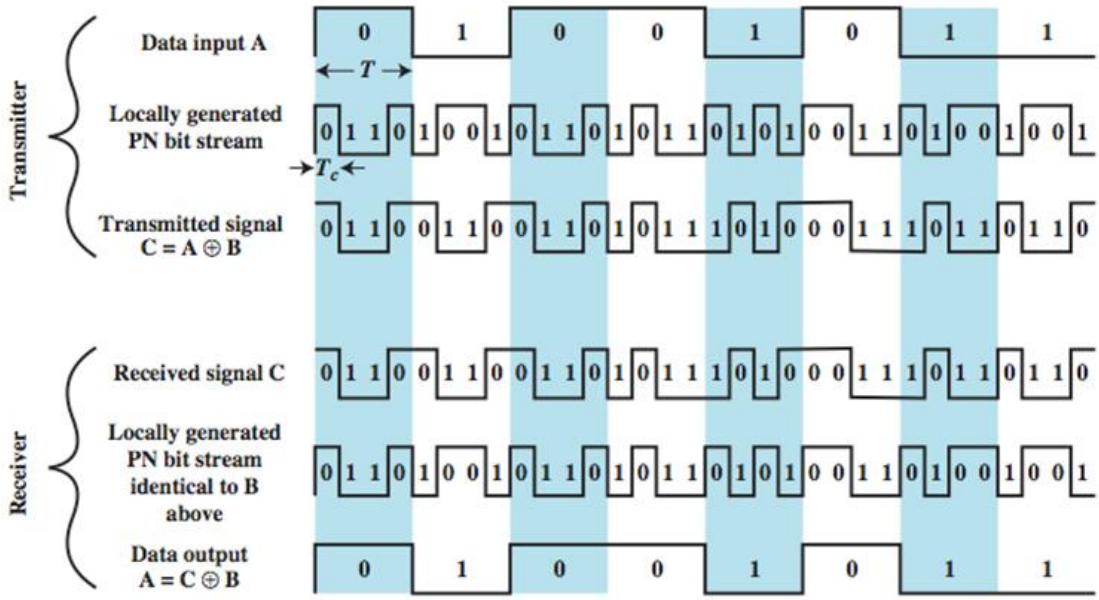


Figura 2. 6: Ejemplo de espectro ensanchando por secuencia directa.
Fuente: Andrade, R., et al (2008).

En los Estados Unidos, el ancho de banda de radio utilizado para las comunicaciones de espectro ensanchado cae en tres bandas (900 MHz, 2.4 GHz y 5.7 GHz), que la Comisión Federal de Comunicaciones (FCC) ha aprobado para las comunicaciones comerciales de área local en la década de 1980. En Europa, el Instituto de Normas Europeas de Telecomunicaciones (ETSI), introdujo regulaciones para 2.4 GHz en 1994, e Hiperlan es una familia de estándares en las bandas de frecuencia 5.15 a 5.7 GHz y 19.3 GHz.

2.3.1. Infrarrojos (IR).

Los Infrarrojos es una banda invisible de radiación que existe en el extremo inferior del espectro electromagnético visible. Este tipo de transmisión es más eficaz cuando existe una línea de visión clara entre el transmisor y el receptor.

Stallings, W. (2008) manifiesta que los IR’s se comporta como una celda individual en una red LAN interna, ya que no son capaces de atravesar paredes.

Hay dos tipos de soluciones WLAN de infrarrojos están disponibles: haz difuso y haz directo (o línea de visión). En la actualidad, las WLAN’s de haz directo ofrecen una tasa de datos más rápido que las redes de haz difuso, pero es más direccional ya que la tecnología de haz difuso utiliza rayos reflejados para transmitir/recibir una señal de datos, alcanza velocidades de datos más bajas en el rango de 1 a 2 Mbps.

Mientras que Tanenbaum, A. S. (2003), sostiene que al permitir una velocidad de 1 Mbps este empleará un esquema de codificación denominado Gray, es decir, que 4 bits codificados como una palabra de 16 bits (quince 0’s y un 1). Esto facilitaría a un pequeño error de sincronización de 1 bit en la salida.

Andrade, R., et al (2008) indica que existen señales ópticas infrarrojas utilizadas a menudo en aplicaciones de dispositivos de control remoto. Los usuarios que pueden beneficiarse de infrarrojos incluyen profesionales que continuamente establecen oficinas temporales, tales como auditores, vendedores, consultores y gestores que visitan a los clientes o sucursales. Estos usuarios se conectan a la red por cable local a través de un dispositivo de infrarrojos para la recuperación de información o el uso de las funciones de fax e impresión en un servidor.

Un grupo de usuarios también podrán crear una red por infrarrojos peer-to-peer, en vez de compartir impresoras, faxes, u otros servicios del servidor dentro de su propio entorno LAN. Las industrias de educación y medicina suelen utilizar esta configuración para moverse con facilidad dentro de las redes.

En la tabla 2.2 se muestran las ventajas y desventajas de utilizar tecnología de infrarrojos de corto alcance. Cuando se utiliza en interiores, puede ser limitado por los objetos sólidos, tales como puertas, paredes, mercancías o estanterías. Además, el entorno de iluminación puede afectar a la calidad de la señal.

Tabla 2. 2: Consideraciones para elegir la tecnología infrarroja.

Ventajas	No hay regulaciones del gobierno para controlar su uso.
	Inmunidad a ondas electromagnética (EMI) e interferencia de RF.
Desventajas	En general, una tecnología de corto alcance (30-50 radio de pies en condiciones ideales).
	Las señales no pueden penetrar objetos sólidos.
	Señal afectada por la luz, nieve, hielo, niebla.
	La suciedad puede interferir con infrarrojos.

Elaborado: Autor

Por ejemplo, la pérdida de las comunicaciones puede ocurrir debido a la gran cantidad de luz solar o la luz de fondo en un entorno. Las luces fluorescentes también pueden contener grandes cantidades de infrarrojos. Este problema puede ser resuelto mediante el uso de alta potencia de la señal y un filtro de ancho de banda óptica, que disminuye las señales infrarrojas provenientes de fuentes externas. En un ambiente al aire libre, la nieve, el hielo y la niebla pueden afectar el funcionamiento de un sistema basado en infrarrojos.

Debido a ciertas limitaciones, los infrarrojos no es una tecnología muy popular para las redes WLAN, debido a que infrarrojo tiene menos del 14% del mercado de la construcción de redes WLAN, y se espera que esta cuota de mercado caiga en el futuro.

2.3.2. UHF (Banda Estrecha)

Los sistemas de comunicación de datos inalámbricos UHF han estado disponibles desde principios de 1980. Estos sistemas normalmente transmiten en el rango de frecuencia 430 a 470 MHz, con raros sistemas utilizando segmentos de la gama de 800 MHz. La parte inferior de esta banda 430-450 MHz a menudo se hace referencia como sin protección (sin licencia) y 450-470 MHz se conoce como banda protegida (con licencia).

En la banda sin protección, no se conceden licencias de RF para las frecuencias específicas y nadie está autorizado a utilizar cualquier frecuencia de la banda. En la banda protegida, se conceden licencias de RF para las frecuencias específicas, dando a los clientes una garantía de que van a tener un uso completo de esa frecuencia.

Otros términos para UHF son de banda estrecha y RF de 400 MHz. Dado que los sistemas de banda estrecha de RF independientes no pueden coexistir en la misma frecuencia, las agencias gubernamentales asignan frecuencias de radio específicas para los usuarios a través de licencias de sitio RF. Una cantidad limitada de espectro sin licencia también está disponible en algunos países. Con el fin de tener muchas frecuencias que pueden asignarse a los usuarios, el ancho de banda dado a un usuario específico es muy pequeña.

El término "banda estrecha" se utiliza para describir esta tecnología debido a que la señal de RF se envía en un ancho de banda muy estrecha, típicamente 12,5 kHz o 25 kHz. Los niveles de energía van de 1 a 2 vatios para los sistemas de datos de RF de banda estrecha. Este ancho de banda estrecha combinada con resultados de alta potencia en distancias de transmisión más grandes, que están disponibles sistemas de espectro ensanchado de 900 MHz o 2,4 GHz, los cuales tienen niveles de potencia más bajos y anchos de banda más amplios.

2.3.3. Tecnología de Radio sintetizada.

Muchos sistemas de UHF modernos utilizan tecnología de radio sintetizado, que se refiere a la forma en frecuencias de canal se generan en la radio. Los productos de cristal controlado en productos UHF heredados requieren instalación en la fábrica de cristales únicos para cada posible canal de frecuencia.

La tecnología sintetizada utiliza una sola frecuencia del cristal estándar y deriva la frecuencia del canal requerido dividiendo la frecuencia del cristal hacia abajo a un valor pequeño, a continuación, multiplicándolo hasta la frecuencia de canal deseada. Los factores de división y multiplicación son únicos para cada frecuencia de canal deseado, y están programadas en la memoria digital en la radio en el momento de la fabricación.

Las soluciones basadas en UHF sintetizados ofrecen la posibilidad de instalar los equipos sin la complejidad de los cristales del hardware. El equipo común se puede comprar y la frecuencia de UHF es especificada para cada dispositivo, se puede ajustar en base a los requisitos de ubicación específicos. Además, las radios UHF sintetizados no presentan el problema derivada de la frecuencia con experiencia en radios UHF controlado por cristal, una función que elimina los problemas de ajuste después de que las instalaciones han estado funcionando durante un periodo de tiempo.

2.3.4. Operación de frecuencia múltiple.

Los Sistemas UHF modernos permiten puntos de acceso configurados de forma individual para la operación en una de varias frecuencias pre-programadas. Los terminales están programados con una lista de todas las frecuencias utilizadas en los puntos de acceso instalados, lo que les permite cambiar las frecuencias en itinerancia. Para aumentar el rendimiento, los puntos de acceso pueden ser instalados con la superposición de la cobertura, pero empleando diferentes frecuencias.

2.4. Estándares Inalámbricos LAN.

Varias normas actuales y emergentes son importantes para entender cuando se considera la tecnología LAN inalámbrica. En la tabla 2.3 se resume las principales normas y sus alcances. En la figura 2.7 se muestra el estado relativo de cada uno de los estándares.

Tabla 2. 3: Estándares de WLAN.

WLI Forum OpenAir	2,4 GHz de espectro ensanchado por salto de frecuencia.
IEEE 802.11	Define la interoperabilidad entre los productos de redes inalámbricas de múltiples proveedores, infrarrojos, la frecuencia de 2,4 GHz de salto y 2,4 GHz de espectro ensanchado de secuencia directa. Normas de 2.4GHz y 5GHz alta velocidad futuros.
Home RF	Protocolo de Acceso Inalámbrico Compartidos (SWAP) para las redes inalámbricas dentro de una casa.
Bluetooth	Enlaces de radio de corto alcance que utilizan la frecuencia de 2.4 GHz de espectro ensanchado por salto.

Elaborado: Autor

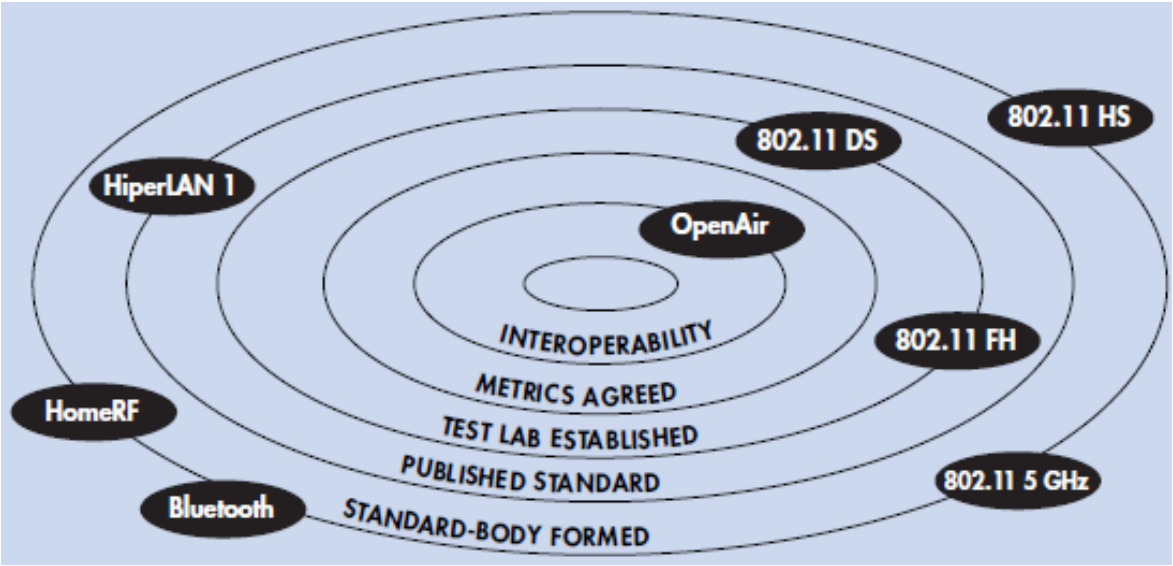


Figura 2. 7: Estándares Universales de WLAN's.
Fuente: Andrade, R., et al (2008).

2.5. Estándares Inalámbricos 802.11.

En 1997, el IEEE publicó el estándar original 802.11, para la industria se refiere a menudo a la 802.11 como privilegiada, ya que era el estándar inalámbrico inicial. Fue revisado en 1999 y se reafirmó en 2003 como 802.11. Por esta reafirmación final más de los siguientes subconjuntos de la norma tienen su propia sección dedicada a la idiosincrasia de cada uno.

El estándar original permitía velocidades de datos en 1 o 2 Mbps. Contenía tres cláusulas que definen capas físicas. En la cláusula 16 se define la capa física de infrarrojos (IR) que para 802.11 es obsoleto. La cláusula 14 se define un salto de frecuencia de espectro amplio (FHSS) de la capa física, esta tecnología tiene sus raíces que remontan a la Segunda Guerra Mundial con la primera patente conocida de su tipo. La cláusula 15 definen a los dispositivos de espectro de frecuencia DSSS y son la raíz de las sucesivas modificaciones de los dispositivos de radio 802.11a/b/g. La cláusula 16 o dispositivos de infrarrojos no se consideran una tecnología de radio frecuencia, y debido a su carácter obsoleto, no serán considerados en este documento.

Estos estándares IEEE 802.11 están especificados en 9 estándares, desde la IEEE 802.11a hasta IEEE 802.11i

2.5.1. IEEE 802.11a (también llamado WiFi5).

Es un estándar de la capa física (PHY), que funciona en la banda de radio sin licencia 5 GHz utilizando multiplexación por división de frecuencia ortogonal (OFDM). Es compatible con velocidades de datos de 6 Mbps hasta 54 Mbps. Se utilizará la misma capa MAC 802.11. El estándar 802.11a incluye características como prioridad para ciertos tipos de tráfico, también ofrece mucho menos potencial de la radio frecuencia (RF) que otros PHY (por ejemplo, 802.11b y 802.11g). Con altas velocidades de datos y relativamente poca interferencia, 802.11a hace un gran trabajo de apoyo a las aplicaciones multimedia y entornos de usuario densamente pobladas.

2.5.2. Estándar 802.11b (también llamada WiFi).

Es un estándar un poco mayor que soporta velocidades de 5.5 Mbps y 11 Mbps, además de las tasas de datos de 1Mbps y 2Mbps. Ha desplegado en la banda de radio de 2,4 GHz. IEEE 802.11b utiliza la modulación por código complementario (CCK) para proporcionar altas velocidades de datos. IEEE 802.11 finaliza este estándar (IEEE 802.11b) a finales de 1999. Varios proveedores ofrecen productos que se ajusten a esta norma.

2.5.3. Estándar 802.11c.

El estándar 802.11c proporciona información necesaria para garantizar el funcionamiento de puentes adecuados. Este proyecto está terminado y desarrolladores de productos utilizan esta hoja técnica en el desarrollo de los puntos de acceso (Access Point). Realmente no hay mucho más en esta norma relevante para los instaladores de redes LAN inalámbrica.

2.5.4. Estándar 802.11d.

Cuando estaba disponible por primera vez el estándar 802,11, sólo existía un puñado de dominios reguladores (por ejemplo, Estados Unidos, Europa y Japón), los cual tenían reglas para el funcionamiento de las redes WLAN 802.11. Con el fin de apoyar una amplia adopción, el grupo de tareas 802.11d tenía que definir las regulaciones legales de la capa física, que satisfagan a la armonización global. Esto es especialmente importante para la operación en las bandas de 5 GHz debido a que el uso de estas frecuencias difiere mucho de un país a otro.

2.5.5. Estándar 802.11e.

Esta norma funciona en cuestión de calidad de servicio en redes de área local para optimizar la transmisión de voz y video. Actualmente no hay un mecanismo efectivo para priorizar el tráfico en 802.11. Como resultado, el

grupo de trabajo 802.11e fue de refinar la 802.11MAC para mejorar la QoS para un mejor soporte de audio y video. El grupo 802.11e finalizó la norma a mediados del año 2003.

Debido a que 802.11e cae dentro de la capa MAC, será común que todas las 802.11 físicas ser compatible con WLAN 802.11 existentes.

2.5.6. Estándar 802.11f.

Hoy en día, un usuario roamming entre puntos de acceso puede perder algunos paquetes durante la transferencia entre los dispositivos de diferentes fabricantes. El grupo de trabajo 802.11 existente, propuso este elemento con el fin de proporcionar flexibilidad en el trabajo con diferentes sistemas de distribución. El problema, sin embargo, es que los puntos de acceso de diferentes proveedores pueden no interoperar cuando el apoyo de itinerancia. Estándar 802.11f asegura múltiples proveedores de punto de acceso a través de la interoperabilidad del Protocolo de iner-Access Point.

CAPÍTULO 3: SIMULADOR OPNET.

3.1. Introducción al Simulador OPNET.

La plataforma de simulación OPNET nos permite modelar o simular el funcionamiento y el rendimiento de cualquier tipo de red. La principal diferencia con otros simuladores radica en su potencia y versatilidad. Este simulador hace posible trabajar con modelo OSI, de la capa 7 a la modificación de los demás parámetros físicos esenciales. En la figura 3.1 se muestra el entorno del software OPNET Modeler.

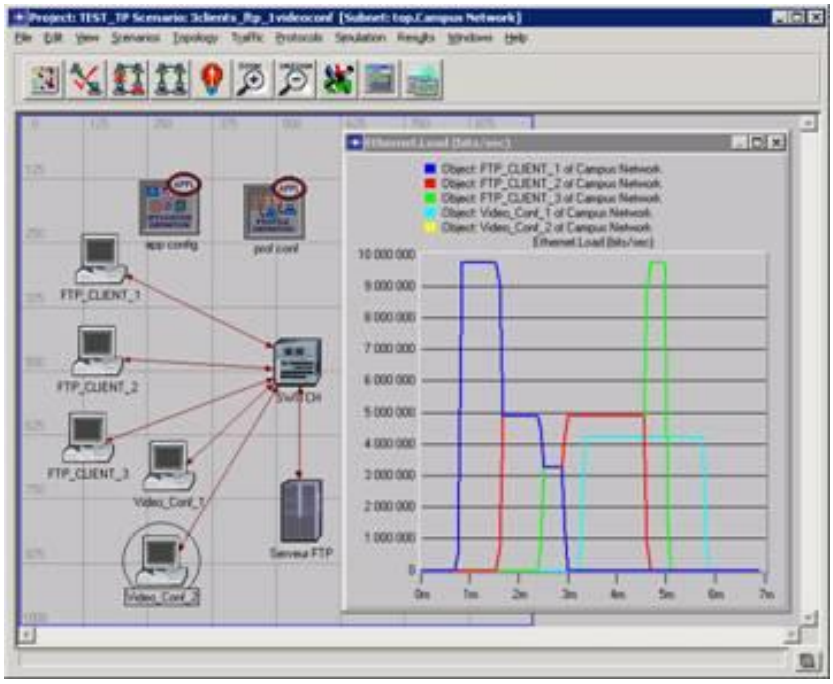


Figura 3. 1: Entorno gráfico de OPNET Modeler.
Fuente: Pan, J. (2008).

En este capítulo se pretenderá que los lectores o estudiantes de la Carrera de Ingeniería en Telecomunicaciones comprendan la utilidad de una herramienta de simulación en un ámbito de aplicación telemática y por qué el perfil de un Ingeniero comienza a ser solicitado en las grandes empresas internacionales.

Se ha resumido este capítulo en cuatro secciones importantes. El objetivo de la primera parte es dar una visión global de OPNET Modeler. La segunda parte ofrece conceptos básicos sobre la simulación de programación entornos. La tercera parte va a través de la implementación de las redes avanzadas. La última parte se ocupa de una de las utilidades más útiles del simulador para empresas de ISP: la predicción del comportamiento de las redes grandes con el fin de validar su diseño

3.2. Implementación de una Red.

El primer escenario consiste en lo siguiente: hay una empresa con una red con topología en estrella (véase el escenario actual de la red en la figura 3.2), que requiere poner en marcha la misma infraestructura en un segundo piso. Ambas redes son interconectadas con un router. El propósito de este ejemplo es comprobar si la red la soportará.

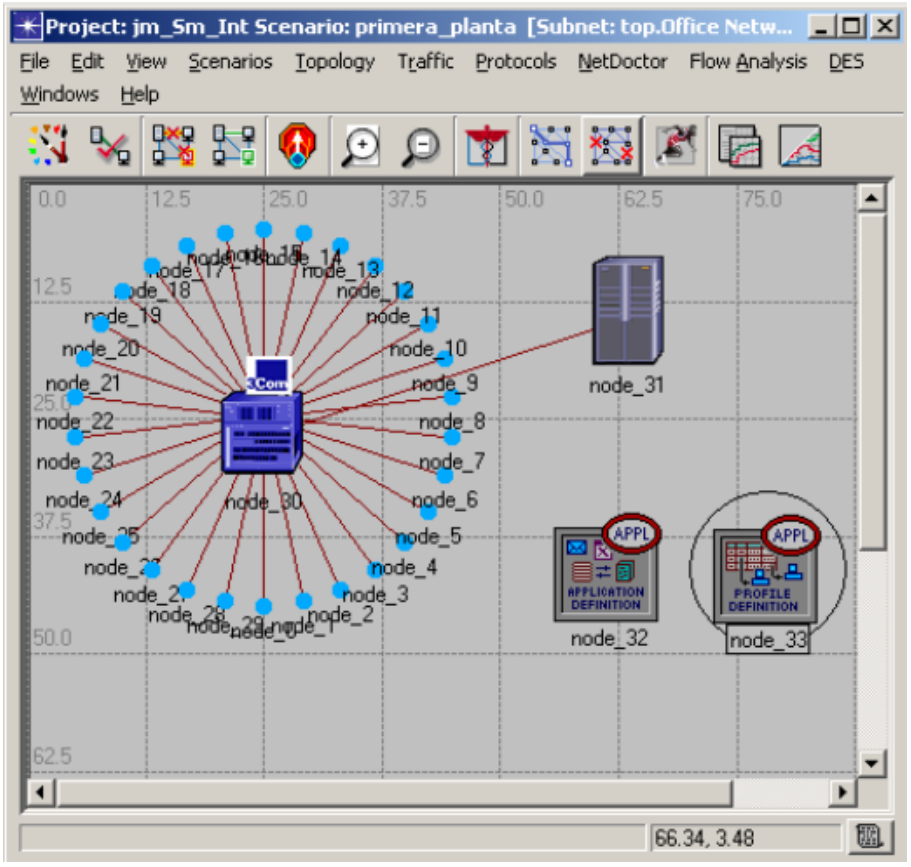


Figura 3. 2: Escenario inicial de una red con topología en estrella.
Fuente: OPNET Modeler.

En la figura 3.2 se muestra la implementación inicial de la topología y con esta se procederá a realizar las simulaciones correspondientes. Posteriormente, realizamos la ampliación de la red, tal como se muestra la figura 3.3 en la cual volvemos a realizar las simulaciones, comparando los diferentes resultados obtenidos y tomar algunas decisiones.

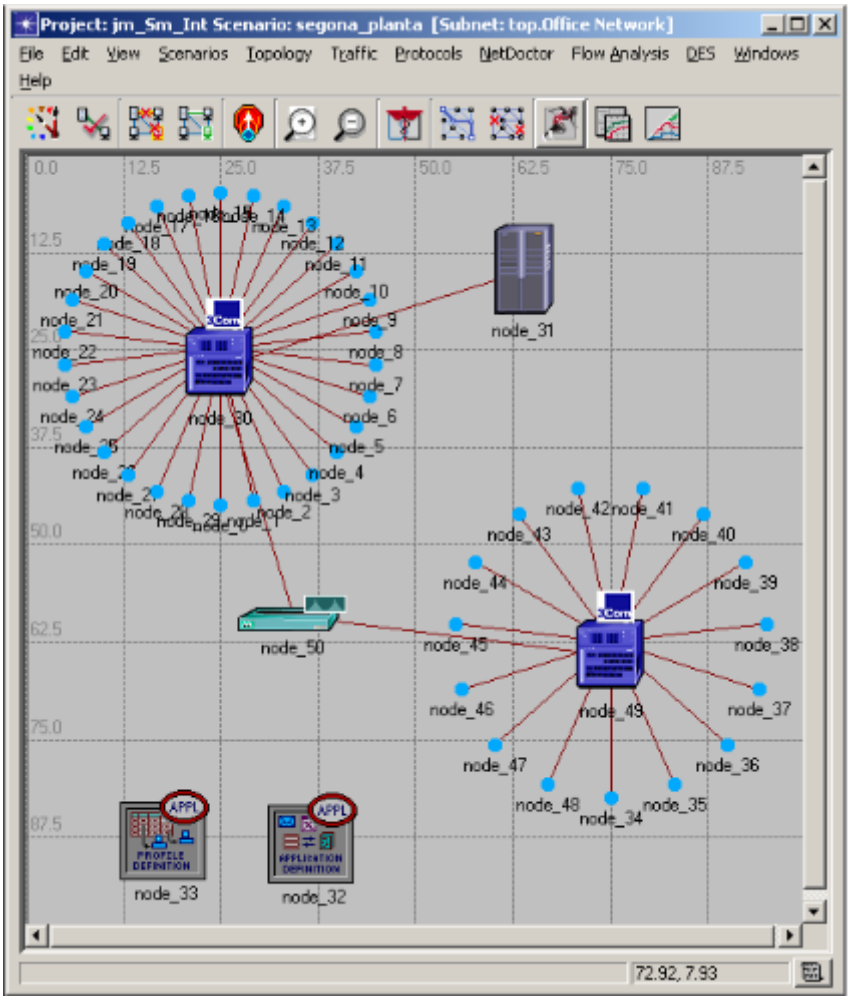


Figura 3. 3: Escenario actual (ampliación) de una red con topología en estrella.
Fuente: OPNET Modeler.

Los lectores o estudiantes podrán obtener gráficos de carga del servidor y de retardo de red. Además, están invitados a realizar prácticas con el editor de nodos y el editor de procesos, el análisis de la estructura de puestos de trabajo y la forma en que siguen el modelo OSI.

Cuando se implementa el diseño de la red del primer piso, se debe proceder a la ampliación. Posterior a la ampliación, es necesario pedir al lector o estudiantes obtener las mismas estadísticas con el fin de compararlas, tal como se muestra en la figura 3.4.

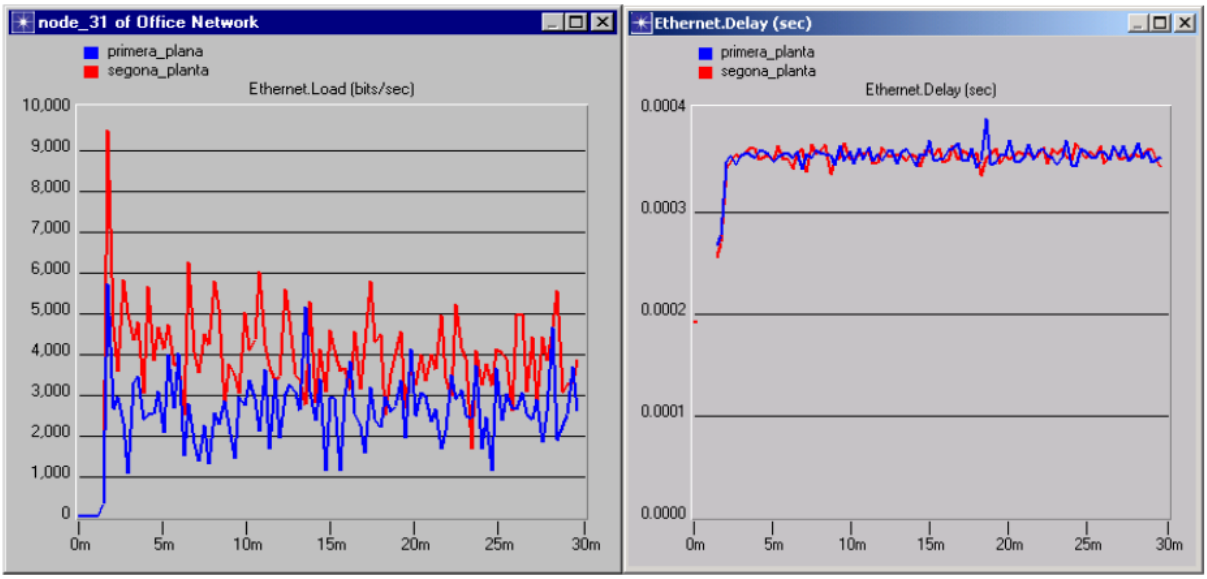


Figura 3. 4: Comparativas de la carga del servidor y del retardo de la red.
Fuente: OPNET Modeler.

3.3. Diseño de Bajo Nivel.

En este acápite se pretende dar un amplio conocimiento sobre el nodo Editor. Los lectores o estudiantes van a crear un nodo que funciona como un tampón, específicamente como una cola infinita, donde el primero viene es el primero servido (FIFO), también conocido como cola de M/M/1.

En la figura 3.5 se muestra el diseño teórico del nodo, donde los paquetes que llegan a la memoria intermedia siguen una distribución de Poisson. La función de servidor es suministrar los paquetes en la memoria intermedia a una velocidad constante.

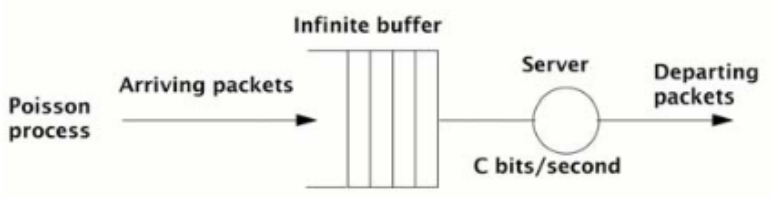


Figura 3. 5: Modelo teórico de un nodo.
Fuente: http://www.riverbed.com/products-solutions/products/opnet.html?redirect=opnet

En la figura 3.6 se muestra la implementación final, donde los procesos están vinculadas por los datos de flujo líneas (línea azul), uno de la fuente a la cola, y el otro de la cola a la pileta.

Figura 3. 6: Diseño del nodo en OPNET.
Fuente: OPNET Modeler.

Cuando la implementación del modelo de nodo está terminada, se deberá crear un modelo de red. Después de todo, se pide la simulación. Esta simulación se realiza con la *Editor Probe* en lugar de utilizar el simulador DES. Las estadísticas recogidas son el retardo introducido por la memoria intermedia y el tamaño de la cola (paquetes), se muestran en la figura 3.7.

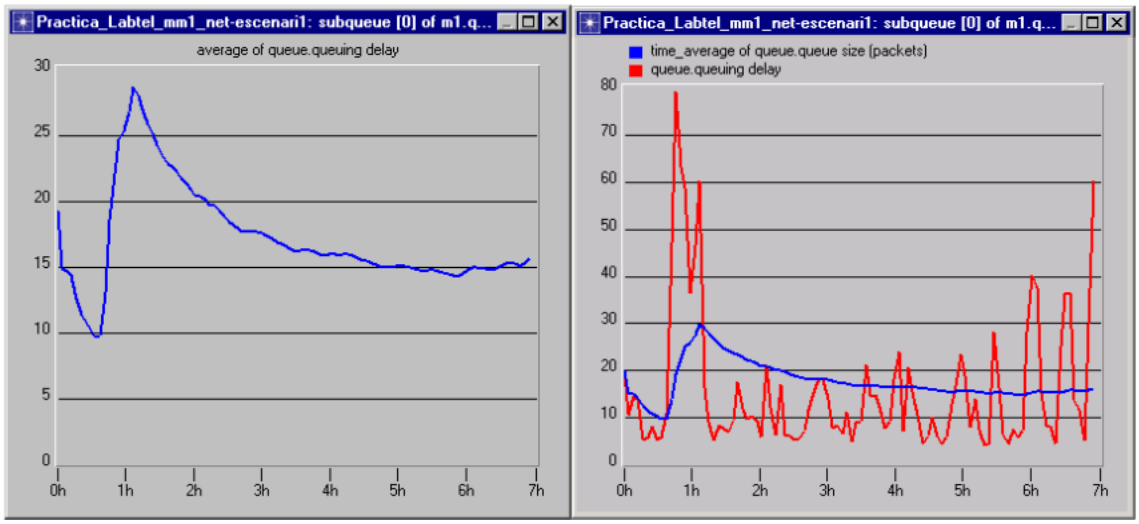


Figura 3. 7: Retardos de la memoria intermedia y de los paquetes.
Fuente: OPNET Modeler.

De la primera gráfica (ver figura 3.7), el pico es debido a la sensibilidad promedio cuando se toma un pequeño número de muestras. A medida que pasa el tiempo, el retraso o retardo se estabiliza. En relación con el tamaño de la cola (ver figura 3.7), el lector deberá darse cuenta de cómo la cola envía 1 paquete por segundo, si el retardo medio es de 15 segundos, parece lógico que la ocupación promedio fue de 15 paquetes.

3.4. Tecnología MPSL.

Es importante que los lectores conozcan la introducción teórica de la tecnología MPLS. En este ejemplo se da a los estudiantes la oportunidad de probar el comportamiento de una nueva tecnología, como es MPLS. En primer lugar, un escenario de referencia se creó con el fin de observar algunos problemas que puede llegar a los protocolos de enrutamiento.

Entonces, se puede configurar el mismo escenario, pero la introducción de la tecnología MPLS con la Ingeniería de Tráfico, en la que se utilizan dos LSP’s para compartir el tráfico entre los caminos. El último escenario introducirá la configuración necesaria para aplicar la QoS entre los diferentes tipos de tráfico.

El primer escenario implementado se muestra en la figura 3.8, la topología de red y el protocolo de enrutamiento (OSPF) ya están configurados, se deberá pasar por la configuración de tráfico entre los nodos. En primer lugar, tienen que configurar las aplicaciones utilizadas por los usuarios, y, a continuación, el perfile para estas aplicaciones.

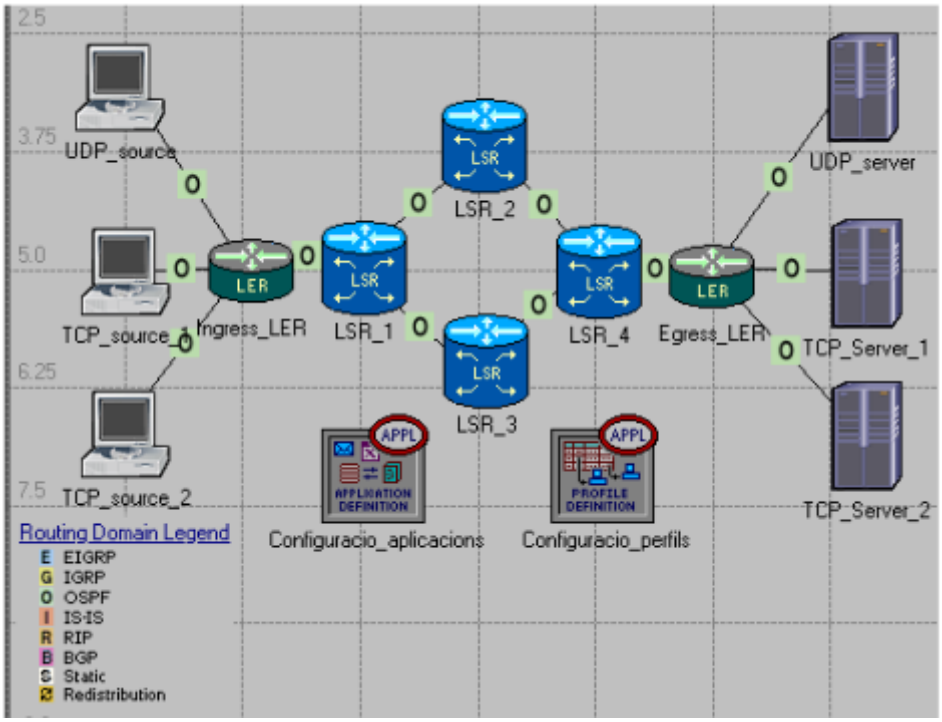


Figura 3. 8: Configuración de la topología de red y protocolo OSPF.
Fuente: OPNET Modeler.

A través de la simulación se generan tres flujos de datos (véase la figura 3.9), el primero va desde UDP_source a udp_server, y que utiliza UDP en la capa de transporte; mientras que los otros flujos van de TCP_source1 y TCP_source2 a TCP_server1 y TCP_server2 respectivamente, con un tráfico TCP constante de 1,5 Mbps. El siguiente enlace punto a punto se recogen datos estadísticos, tales como el rendimiento (bits/segundo) y direcciones.

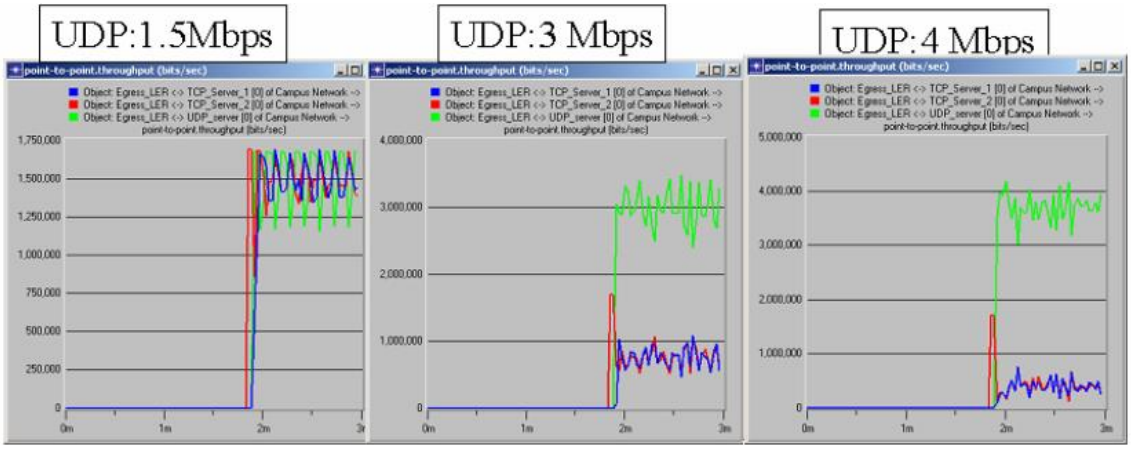


Figura 3. 9: Flujos de datos de la red de la figura 3.8.
Fuente: OPNET Modeler.

Para el segundo escenario, los pasos que se deben seguir para incluir la tecnología MPLS son: definir las diferentes clases FEC, definir los troncos de tráfico perfiles, crear los LSP, asignar la interface/paquetes con las diferentes clases FEC, un mapa de la FEC en los troncos de tráfico y asignar las troncales del tráfico en los LSP. En la figura 3.10 se muestra los flujos de datos para la misma red incluyendo la tecnología MPLS.

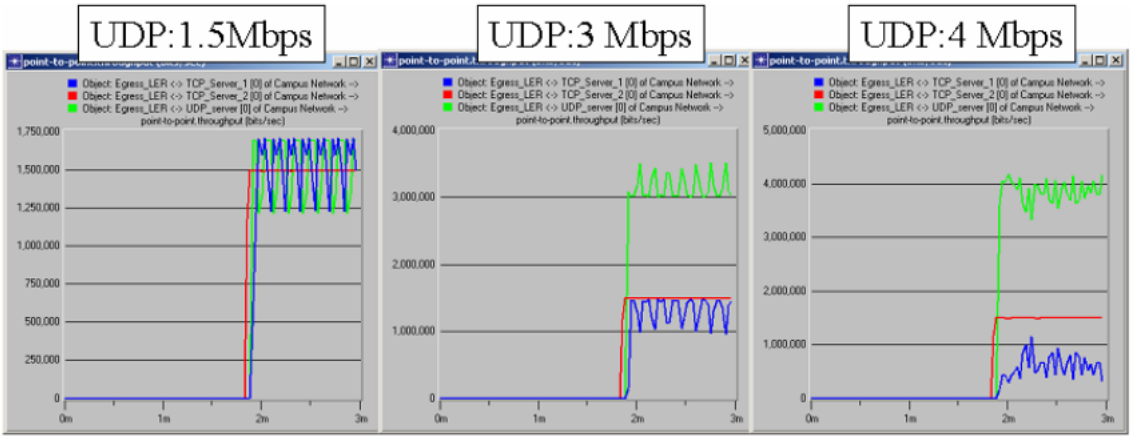


Figura 3. 10: Flujos de datos de la red incluyendo tecnología MPLS.
Fuente: OPNET Modeler.

Finalmente, tenemos el último escenario, donde se añade QoS (Calidad o Servicio) tal como se ilustra en la figura 3.11.

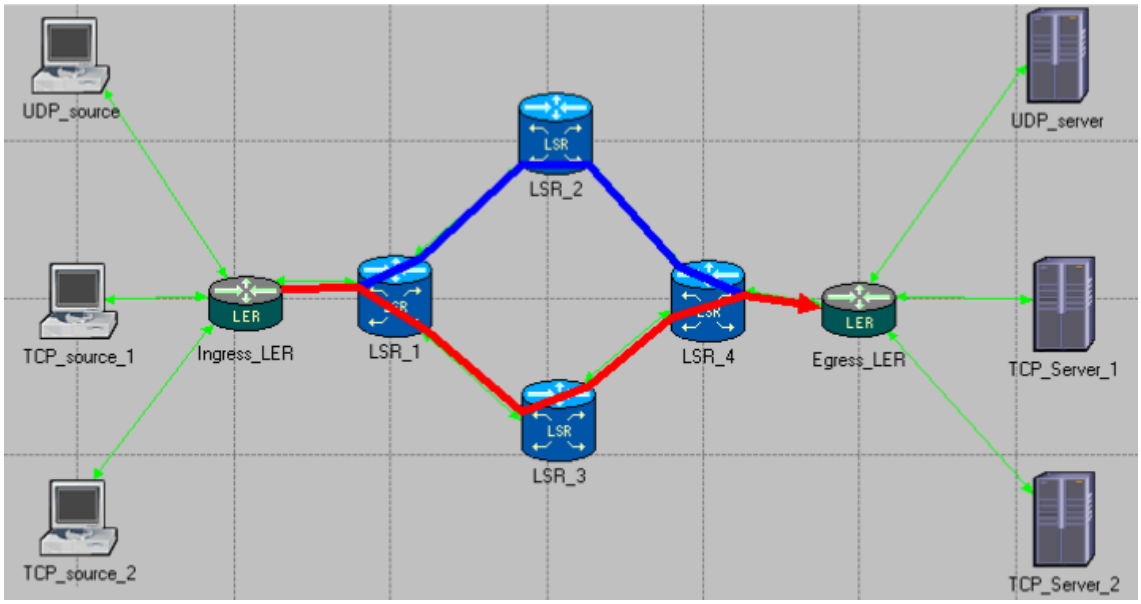


Figura 3. 11: Configuración de una red de datos añadiendo QoS.
Fuente: OPNET Modeler.

Cuando el esquema de QoS que se mostró en la figura 3.11 se ha definido, es necesario especificar a qué tipo de servicio cada tráfico pertenece. El último paso consiste en simular el escenario y tomar conclusiones sobre los gráficos obtenidos

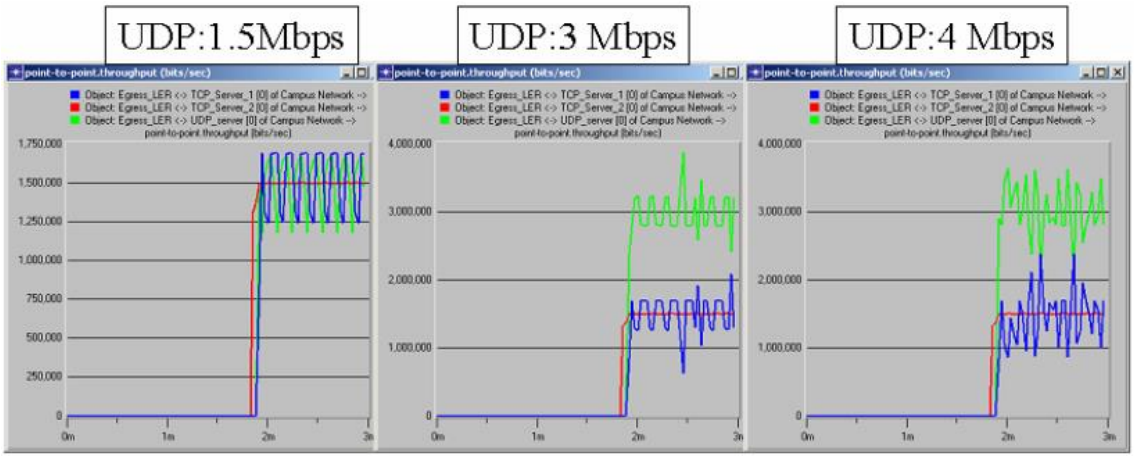


Figura 3. 12: Flujos de datos de la red incluyendo QoS.
Fuente: OPNET Modeler.

3.5. Predicción y validación de Redes.

OPNET simulador es muy útil cuando se trabaja con redes complejas con un gran número de dispositivos y de los flujos de tráfico, o en redes en las que un pequeño cambio puede ser crítico.

Antes de implementar cualquier cambio, es posible predecir el comportamiento y verificar las configuraciones de los dispositivos. OPNET cuenta con diferentes herramientas, que permiten a los administradores a analizar sus redes y las futuras implementaciones que requieran hacerlo.

Dentro de este conjunto de herramientas, tenemos a *NetDoctor*, *ACE* y *MVI*. En esta parte de la práctica, los alumnos tienen que evaluar estas herramientas utilizando escenarios complejos proporcionados por OPNET.

CAPÍTULO 4: DISEÑO Y SIMULACIÓN EN OPNET DEL TRABAJO DE TITULACIÓN

En el presente capítulo se desarrollará la implementación y simulación de ataques a través de la técnica jamming, para lo cual el código fuente se ha programado para modelar una red WLAN tipo MAC mediante la plataforma de simulación OPNET Modeler.

4.1. Caracterización de la Técnica Jamming.

En esta sección se desarrollará el código que permita implementar las técnicas jamming, para lo cual se va a describir las variables necesarias para la implementación, mediante los segmentos de código del programa fuente que evaluará la técnica ya descrita.

La estructura de datos *Wlan_Flags* contiene todos los *flags* (banderas) para determinar las condiciones de activación o desactivación de cada tipo de jamming. En código fuente se muestra en la figura 4.1, para lo cual utilizaré tres tipos de banderas de jamming:

a. **On:** activa al jamming.
b. **Ready:** es la trama previa que será programada como ataque jamming y recibida por el nodo jammer.
c. **Finished:** es aquella trama que será enviada siempre que se le haya realizado el jamming.

```
Boolean cts_jamming_on;          /* Activado jamming a CTS*/
Boolean cts_jamming_ready;       /* Trama de jamming lista para ser enviada*/
Boolean cts_jamming_finished;    /* Enviada trama de jamming a CTS*/
Boolean data_jamming_on;         /* Activado jamming a datos*/
Boolean data_jamming_ready;      /* Trama de jamming lista para ser enviada*/
Boolean data_jamming_finished;   /* Enviada trama de jamming a datos*/
Boolean ack_jamming_on;          /* Activado jamming a ACK*/
Boolean ack_jamming_ready;       /* Trama de jamming lista para ser enviada*/
Boolean ack_jamming_finished;    /* Enviada trama de jamming a ACK*/
```

Figura 4. 1: Código para activación tipos de banderas *jamming*.
Elaborado: La Autora.

La estructura mi *Wlan_jm_state* contiene las variables de estado del modelo, en la cual se le añaden variables, estas son fijadas por el programador o usuario desde la interfaz de atributos tal como se muestra en la figura 4.2.

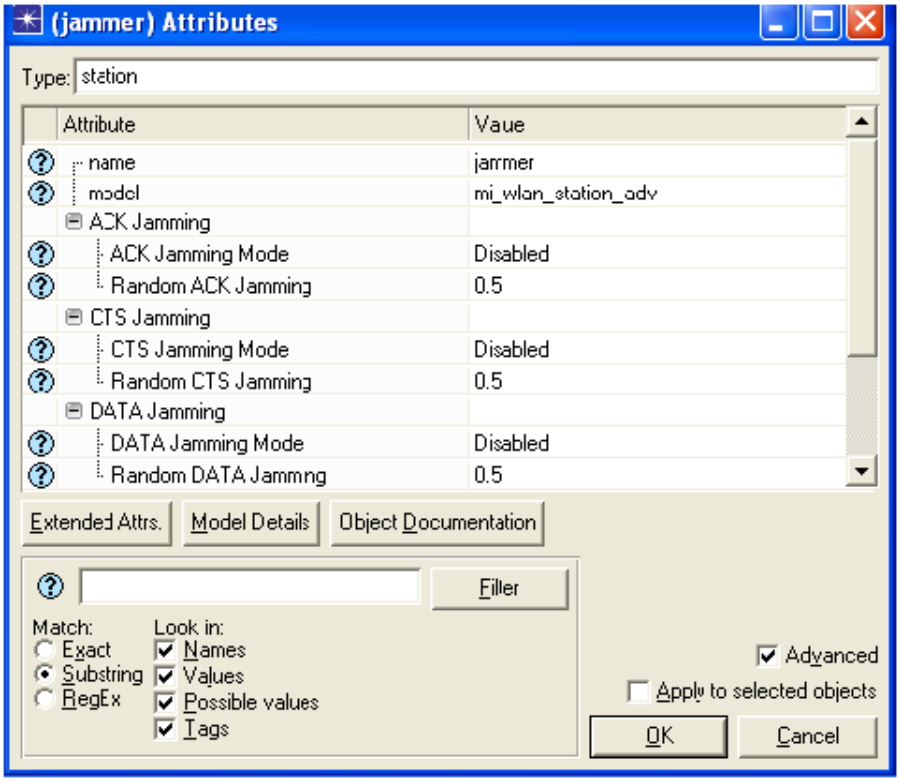


Figura 4. 2: Ventana de atributos del *jamming*.
Elaborado: La Autora.

Mientras que la figura 4.3 nos muestra el código de la declaración de las variables mencionadas en el anterior párrafo. Estas variables son de dos tipos:

a. **Jamming mode:** permite guardar un número que depende del tipo de modo jamming, configurado desde la interfaz. Estos números son: “0” que inhabilita *(disabled)* el jamming, “1” jamming normal, “2” jamming continuo y “3” jamming aleatorio *(Random)*.

b. **Jamming parameter:** es configurado de acuerdo a la variable anterior, es decir, si es del tipo aleatorio inmediatamente guarda valores entre 0 y 1, lo que significaría la probabilidad de que ocurra el ataque o jamming. Conocido también como Random TIPO Jamming.

```
int cts_jamming_mode;           /* Modo de jamming a CTS */
int data_jamming_mode;          /* Modo de jamming a DATOS */
int ack_jamming_mode;           /* Modo de jamming a ACK */
double cts_jamming_parameter;   /* Umbral para jamming a CTS aleatorio */
double data_jamming_parameter;  /* Umbral para jamming a DATOS aleatorio */
double ack_jamming_parameter;   /* Umbral para jamming a ACK aleatorio */
```

Figura 4. 3: Código para los estados *mode* y *parameter*.
Elaborado: La Autora.

En la rutina *wlan_sv_inicio*, que es de inicialización, se obtendrán de la interfaz valores que han sido introducidos la asignación de variables previamente por el usuario, tal como se ilustra en la figura 4.4.

```
/* Captura de parámetros para jamming desde la interfaz */
op_ima_obj_attr_get(my_objid,"CTS Jamming Mode",&cts_jamming_mode);
op_ima_obj_attr_get(my_objid,"CTS Random Parameter",&cts_jamming_parameter);
op_ima_obj_attr_get(my_objid,"DATA Jamming Mode",&data_jamming_mode);
op_ima_obj_attr_get(my_objid,"DATA Random Parameter",&data_jamming_parameter);
op_ima_obj_attr_get(my_objid,"ACK Jamming Mode",&ack_jamming_mode);
op_ima_obj_attr_get(my_objid,"ACK Random Parameter",&ack_jamming_parameter);
```

Figura 4. 4: Código para obtención de parámetros jamming a través de la interfaz.
Elaborado: La Autora.

Mientras que la figura 4.5 muestra la asignación de valores iniciales a los *flags* restantes.

```
if(cts_jamming_mode ==0)
    wlan_flags->cts_jamming_on   = OPC_FALSE;
  else
    wlan_flags->cts_jamming_on   = OPC_TRUE;
  wlan_flags->cts_jamming_ready      = OPC_FALSE;
  wlan_flags->cts_jamming_finished   = OPC_FALSE;

  if(data_jamming_mode ==0)
    wlan_flags->data_jamming_on = OPC_FALSE;
  else
    wlan_flags->data_jamming_on = OPC_TRUE;
  wlan_flags->data_jamming_ready     = OPC_FALSE;
  wlan_flags->data_jamming_finished    = OPC_FALSE;

  if(ack_jamming_mode ==0)
    wlan_flags->ack_jamming_on   = OPC_FALSE;
  else
    wlan_flags->ack_jamming_on   = OPC_TRUE;
  wlan_flags->ack_jamming_ready      = OPC_FALSE;
  wlan_flags->ack_jamming_finished   = OPC_FALSE;
```

Figura 4. 5: Código de inicio flags restantes.
Elaborado: La Autora.

En la rutina wlan_physical_layer_data son activados los procesos de jamming. De acuerdo al tipo de jamming, la activación se realizará de la siguiente manera:

a. Para la conversión de jamming a CTS, se activa siempre que recibamos al RTS destinado para otra estación (véase la figura 4.6).

```
/* Jamming a CTS */
if(cts_jamming_mode==2||(cts_jamming_mode==1 && total_hlpk_num >0)||
  (cts_jamming_mode==3 && wlan_random_jamming(cts_jamming_parameter)))
    {

    fresp_to_send = WlanC_Cts;
    wlan_flags->cts_jamming_ready=OPC_TRUE;

    if(log_jamming)
      wlan_log_print_jamming_info(1);
    }
```

Figura 4. 6: Código para conversión y activación de jamming a CTS.
Elaborado: La Autora.

b. Para la conversión de jamming a datos, se activa siempre que recibamos al CTS destinada hacia otra estación (véase la figura 4.7).

```
/* Jamming a datos */
if(data_jamming_mode==2||(data_jamming_mode==1 && total_hlpk_num >0)||
  (data_jamming_mode==3 && wlan_random_jamming(data_jamming_parameter)))
    {
    fresp_to_send = WlanC_Cts;
    wlan_flags->data_jamming_ready=OPC_TRUE;
    if(log_jamming)
      wlan_log_print_jamming_info(2);
    }
```

Figura 4. 7: Código para conversión y activación de jamming a Datos.
Elaborado: La Autora.

c. Para va conversión de jamming a ACK, se activa si se recibe la trama de datos cuyo destino es otra estación (véase la figura 4.8).

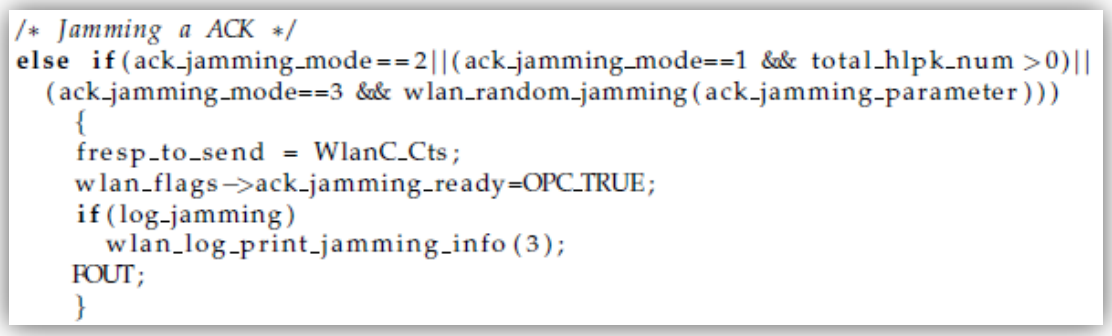


Figura 4. 8: Código para conversión y activación de jamming a ACK.
Elaborado: La Autora.

Para todos los tipos se ejecutará el jamming, si está habilitado, hay que tener en cuenta el modo: si el modo es continuo, se ejecutará siempre; si es modo es normal cuando está vacía la cola de transmisión; y si el modo es aleatorio entonces la función wlan_random_jamming devolverá CIERTO.

En la figura 4.8 se ilustra el código de la función jamming aleatorio, que permite el procesamiento del jamming de forma aleatoria. Como ya se explicó anteriormente los números aleatorios se distribuyen uniformemente entre 0 y 1, pero para el caso de ser menor al valor ingresado del parámetro de jamming aleatorio (tipo jamming parameter), esto inmediatamente ejecuta el jamming.

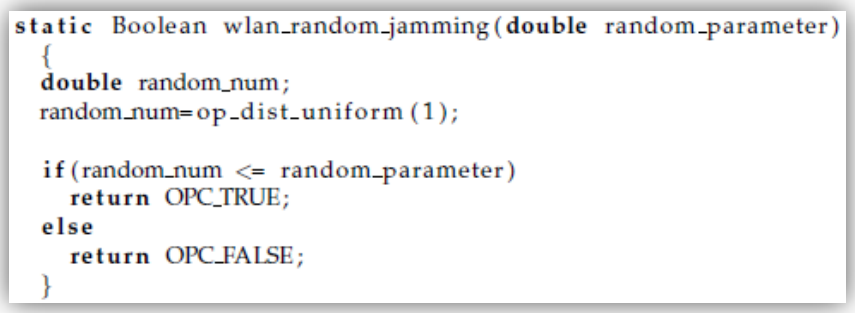


Figura 4. 9: Código de la función jamming aleatorio.
Elaborado: La Autora.

Mientras que la figura 4.10 se aprecia el código wlan_tramas_tx, la que se encarga de transmitir las tramas. Mediante este código se actualizarán los flags desactivando el *jamming ready* y a la vez activa el *jamming finished*, todo esto ocurre si previamente se ha enviado las tramas CTS.

```
if(wlan_flags->cts_jamming_on && wlan_flags->cts_jamming_ready)
    {
    wlan_flags->cts_jamming_ready=OPC_FALSE;
    wlan_flags->cts_jamming_finished=OPC_TRUE;
    if(log_jamming)
      wlan_log_print_jamming_info(1);
    }
if(wlan_flags->data_jamming_on && wlan_flags->data_jamming_ready)
    {
    wlan_flags->data_jamming_ready=OPC_FALSE;
    wlan_flags->data_jamming_finished=OPC_TRUE;
    if(log_jamming)
      wlan_log_print_jamming_info(2);
    }
if(wlan_flags->ack_jamming_ready)
    {
    wlan_flags->ack_jamming_ready=OPC_FALSE;
    wlan_flags->ack_jamming_finished=OPC_TRUE;
    if(log_jamming)
      wlan_log_print_jamming_info(3);
    }
```

Figura 4. 10: Código para procesar *jamming finished*.
Elaborado: La Autora.

Para finalizar el proceso de jamming se deben restaurar los flags utilizados para que puedan ser utilizados nuevamente para el siguiente jamming, en la figura 4.11 se muestra el código que realiza lo explicado.

```
if(wlan_flags->cts_jamming_on && wlan_flags->cts_jamming_finished)
  {
  wlan_flags->cts_jamming_finished=OPC_FALSE;
  if(log_jamming)
    wlan_log_print_jamming_info(1);
  }
else if(wlan_flags->data_jamming_on && wlan_flags->data_jamming_finished)
  {
  wlan_flags->data_jamming_finished=OPC_FALSE;
  if(log_jamming)
    wlan_log_print_jamming_info(2);
  }
else if(wlan_flags->ack_jamming_on && wlan_flags->ack_jamming_finished)
  {
  wlan_flags->ack_jamming_finished=OPC_FALSE;

  if(log_jamming)
    wlan_log_print_jamming_info(3);
  }
```

Figura 4. 11: Código para reiniciar los *flags*.
Elaborado: La Autora.

4.2. Valoración de los ataques.

Para poder realizar la valoración de los ataques, describiremos la información relativa de los ataques a través de la técnica jamming que serán implementados. En la sección 4.2.1 se describirá la configuración de escenarios, la que se ha diseñado para ejecutar las simulaciones, definiendo los roles, atributos y perfiles de tráfico de los nodos de la red; y finalmente analizaremos los resultados obtenidos.

4.2.1. Configuración de los escenarios.

En este apartado describiremos la configuración de escenarios que han sido diseñados, para así ejecutar las simulaciones. En los siguientes acápites se expondrán escenarios específicos, roles y atributos de los nodos presentes en ellos y los perfiles de tráfico usados en las simulaciones.

a. Escenarios y roles de los nodos.

Para poder realizar la evaluación del *jamming* emplearemos dos escenarios: jamming y normal. En el primer escenario <<jamming>> realizamos ataques a través de la simulación de la técnica jamming implementada para el presente trabajo de titulación. En la figura 4.12 se muestra el escenario explicado, que cuenta con tres nodos: jammer: transmite datos y ejecuta el *jamming*; nodo_tr: continua transmitiendo datos y es atacado por la técnica *jamming*; y el nodo_rc: reciben los datos que fueron transmitidos por los nodos *jammer* y tr.

Para el segundo escenario <<normal>> sirve para comprobar y/o comparar los resultados obtenidos en la simulación de ambos escenarios. Es decir, que este escenario será equivalente al *jammer*, excepto que no realiza jamming. Siempre consideremos que se comportan de acuerdo al estándar 802.11.

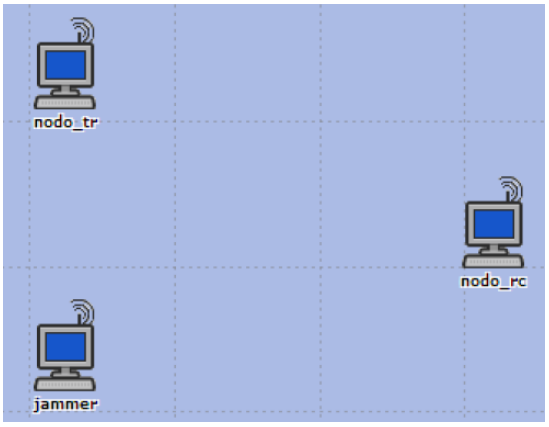


Figura 4. 12: Modelo escenario *jammer*.
Elaborado: La Autora.

El escenario normal se muestra en la figura 4.13 similar al de la figura 4.12, pero sin necesidad de introducir ataques mediante técnica jamming.

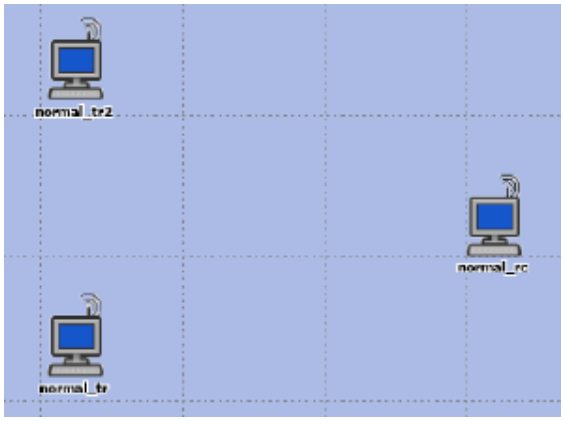


Figura 4. 13: Modelo escenario normal.
Elaborado: La Autora.

Posteriormente, se ejecuta la simulación para analizar el resultado obtenido en ambos escenarios, para poder compararlas se emplearon los datos estadísticos del escenario normal (normal_tr), y de jamming (nodo_tr y jammer), lo que permite diferenciar los dos últimos comportamiento del estándar.

Es necesario que se entienda que el diseño de los tres nodos fue necesario para cubrir el número de roles necesarios para demostrar los ataques. Ahora, esto no cambia si configuramos más nodos porque al final se obtendrán los mismos resultados, sin aportar con nada nuevo.

b. Atributos de los nodos

Cada uno de los nodos tienen una serie de atributos, estos son exportados a nivel del nodo y que sean configurados desde el escenario. Los parámetros de los atributos se muestran en la figura 4.14.

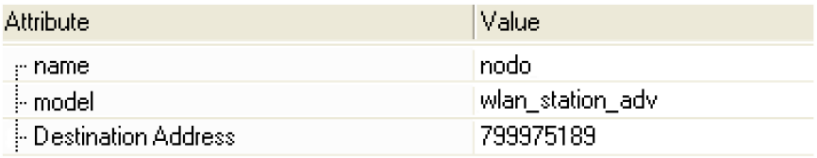


Figura 4. 14: Parámetros generales de los nodos.
Elaborado: La Autora.

Posteriormente de la figura 4.14 se especifica la función de los atributos asignados para ejecutar las simulaciones (véase la tabla 4.1). Para la configuración de la dirección MAC considerar que estas deben ser las mismas para los escenarios jammer y normal.

Tabla 4. 1: Descripción de los parámetros generales.

Name:	representan el nombre del nodo.
Model:	modelo de nodo que implementa.
Destination Address:	es la dirección MAC de la estación a la que se enviarán las tramas desde este nodo.

Mientras que los parámetros *jamming* <<CTS, Data y ACK>>, son los encargados de generar el jamming. En la tabla 4.2 se muestra detallada cada uno de los parámetros, que imposibilita el *jamming* o elegir entre los tipos de *jamming* desarrollados.

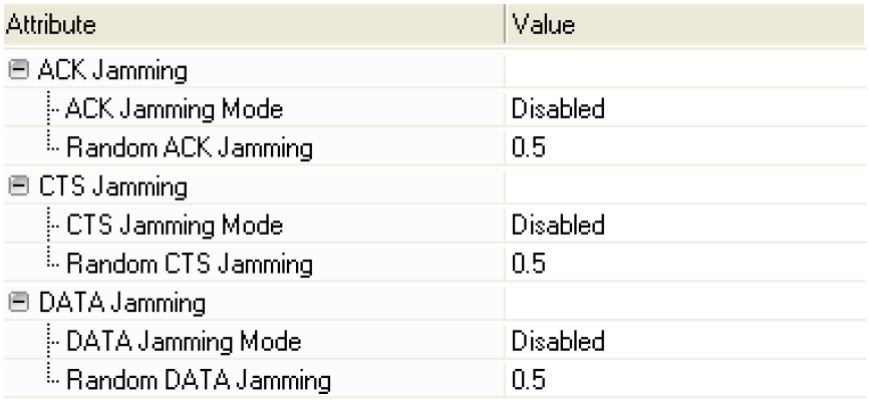


Figura 4. 15: Parámetros del jamming.
Elaborado: La Autora.

Tabla 4. 2: Descripción de los parámetros del *jamming*.

Disabled	dehabilitar modo jamming y se comporta de acuerdo al estándar IEEE 802.11.
Normal	ejecuta el jamming siempre que espere datos para ser enviados.
Continuous	ejecuta el jamming siempre, independientemente si existen datos para enviar.
Random	ejecuta el jamming en modo normal pero de forma aleatoria, que depende de un número aleatorio comprendido entre 0 y 1.

Para el caso de *Log Parameters*, la utilidad de generación de *logs* también ha sido desarrollada para este proyecto. Los parámetros se muestran en la figura 4.16, donde se habilitan todos los atributos.

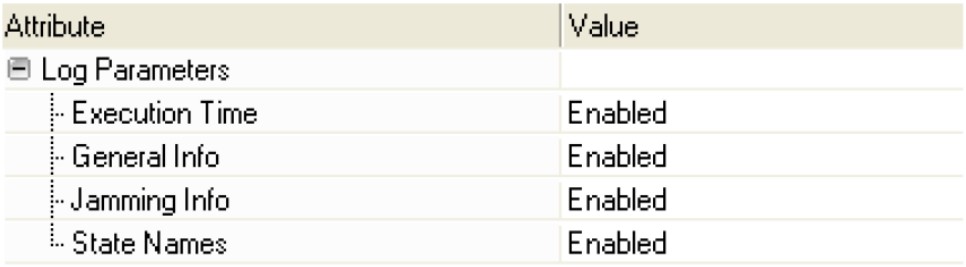


Figura 4. 16: Parámetros del *Log*.
Elaborado: La Autora.

En la tabla 4.3 se muestra detallada cada uno de los parámetros de *Log*.

Tabla 4. 3: Descripción de los parámetros *log*.

Execution Time	tiempo de ejecución en que se produce antes de todos los mensajes de Log.
General Info	registra en el log mensajes de información general (envío de tramas, incremento de contadores de retransmisiones, descarte de tramas, etc.)
State Names	nombre de estados del log durante la simulación.
Jamming Info	nos muestra la información del jamming, que pueden ser: inicio, envío de trama y fin.

En la figura 4.17 se muestra la ventana que permite configurar los atributos de *Traffic Generation Parameters,* logrando así generar paquetes en las capas superiores.

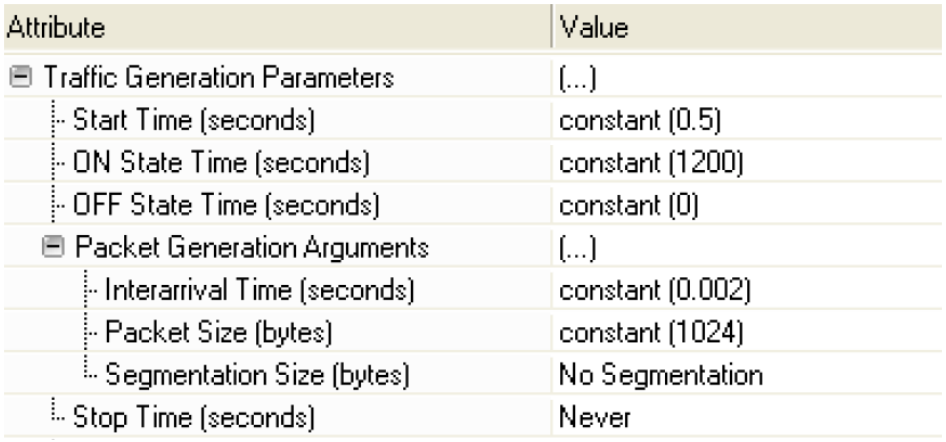


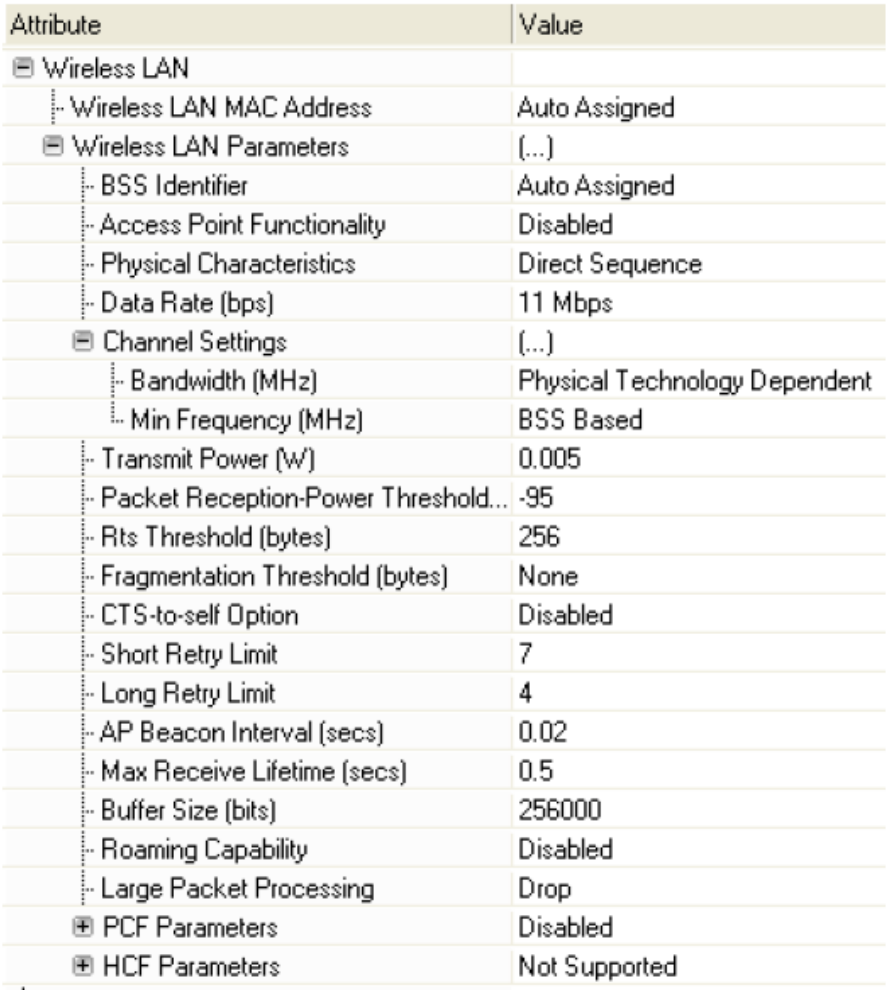
Figura 4. 17: Parámetros de la generación de tráfico.
Elaborado: La Autora.

En la tabla 4.4 se muestra detallada cada uno de los parámetros de generación de tráfico.

Tabla 4. 4: Descripción de los parámetros de generación de tráfico.

Start time	Tiempo de inicio para ejecución de paquetes. Mantener fijo en todas las simulaciones de los nodos en 0.5s, a menos que se desee un tráfico de no transmisión.
ON State Time	Activa el tiempo de inicio para generación de tráfico. Se activará si el valor asignado es mayor al Start time.
OFF State Time	Desactiva el tiempo de generación de tráfico. En este caso debe ser ingresado el valor 0.
Interarrival Time	Tiempo entre llegada de paquetes sucesivos previamente generados, que dependerá del valor de tráfico generado.
Packet Size	Tamaño en Bytes de cada paquete generado, que por lo general será siempre 1024 Bytes.
Segmentation Size	Segmentación de paquetes si es mayor a 1024 Bytes. Se fijará un valor igual o menor a 1024 Bytes para no ejecutar la segmentación.
Stop Time	Tiempo que se detiene la generación de paquetes. Fijamos en NEVER para evitar que se detenga.

Ahora describiremos brevemente los parámetros WLAN, lo que permite configurar todas las características físicas del medio de transmisión de una red inalámbrica. En la figura 4.18 se muestra la ventana que permite configurar los atributos de la WLAN.



Attribute	Value
⊟ Wireless LAN	
⊢ Wireless LAN MAC Address	Auto Assigned
⊟ Wireless LAN Parameters	(...)
⊢ BSS Identifier	Auto Assigned
⊢ Access Point Functionality	Disabled
⊢ Physical Characteristics	Direct Sequence
⊢ Data Rate (bps)	11 Mbps
⊟ Channel Settings	(...)
⊢ Bandwidth (MHz)	Physical Technology Dependent
⊢ Min Frequency (MHz)	BSS Based
⊢ Transmit Power (W)	0.005
⊢ Packet Reception-Power Threshold...	-95
⊢ Rts Threshold (bytes)	256
⊢ Fragmentation Threshold (bytes)	None
⊢ CTS-to-self Option	Disabled
⊢ Short Retry Limit	7
⊢ Long Retry Limit	4
⊢ AP Beacon Interval (secs)	0.02
⊢ Max Receive Lifetime (secs)	0.5
⊢ Buffer Size (bits)	256000
⊢ Roaming Capability	Disabled
⊢ Large Packet Processing	Drop
⊞ PCF Parameters	Disabled
⊞ HCF Parameters	Not Supported

Figura 4. 18: Parámetros de WLAN.
Elaborado: La Autora.

Mientras que en la tabla 4.5 se describen cada uno de los atributos que deben ser configurados previamente para redes inalámbricas con sus respectivas capas físicas.

Tabla 4. 5: Descripción de los parámetros WLAN.

Wireless LAN MAC Addres	Es la dirección MAC del nodo. En los escenarios que ya se describieron asignaremos el valor Auto Assigned generado automáticamente, mientras que los nodos receptores la MAC asignada será 799975189.
BSS Identifier	Reconoce a la BSS que pertenece a la MAC de la WLAN. Mantener por defecto Auto Assigned y así las estaciones pertenecen al mismo BSS.
RTS Threshold	Es el umbral en Bytes para el intercambio RTS/CTS previo a las transmisiones de datos. Fijamos en 256 Bytes para mantener el intercambio ya que los paquetes de datos se establecio en 1024 Bytes.
Fragmentation Threshold	Tamaño de los fragmentos de paquetes que fueron enviados. Fijaremos None para que no se realice la fragmentación.
Short Retry Limit	Es el número de límite máximo de intentos para retransmitir tramas cuyo tamaño sea menor o igual que el determinado por el atributo RTS Threshold. Para la simulación mantenemos en 7 transmisiones.
Long Retry Limit	Es el número de límite máximo de intentos de retransmisión para las tramas cuyo tamaño sea mayor que el determinado por el atributo RTS Threshold. Para la simulación mantenemos en 4 transmisiones.
Buffer Size	Tamaño máximo en bits de la cola de transmisión de la capa superior. Si supera el límite los paquetes serán descartados hasta liberar espacio en la cola. Mantener por defecto de 256000 bits.
Physical Characteristics	Determina la tecnología de la capa física usada y será será empleada por la MAC para configurar algunos parámetros del protocolo 802.11.
Channel Settings	Ajusta las bandas de frecuencias que usará el Tx y Rx de radio conectados a la capa MAC.
Transmit Power	especifica la potencia de transmisión en vatios. Se conserva al valor por defecto de 0,005 vatios.
Packet Reception-Power Threshold	define la sensibilidad del receptor de radio en dBm para detectar la llegada de paquetes. Se deja al valor por defecto de -95 dBm.

c. Perfiles de tráfico

Ahora definiremos los perfiles de tráfico antes de realizar las simulaciones, para lo cual se representan tres situaciones de tráfico para nodos individuales que permitirá definir las etapas de la experimentación y a sacar conclusiones de las evaluaciones. Para configurarlos se usarán algunos de los atributos relacionados con los parámetros de generación de tráfico previamente descritos. Los perfiles diseñados son los siguientes:

- ✓ **Perfil de saturación:**
  Mediante el perfil de saturación, los nodos tienen paquetes en cola de transmisión, es decir, un tráfico continuo durante toda la simulación. Para que ocurra el tiempo entre llegadas fijaremos en los escenarios de la simulación en 0.002s.
- ✓ **Perfil de tasa media:**
  Mediante el perfil de tasa media, los nodos tienen tráfico no continuo. Es decir, que en cualquier instante de la simulación, no hay paquetes que enviar. Se fijará el *Interarrival Time* en 0,003s.
- ✓ **Perfil de no transmisión:**
  Con este perfil no habrá que transmitir, es decir que no enviarán paquetes durante toda la simulación. Para lograr eso fijamos el *Start Time* en *Never*.

A través de los perfiles descritos los nodos que transmiten paquetes generarán tráfico de acuerdo a lo explicado en cada etapa.

4.3. Resultados obtenidos.

En este apartado se mostrarán los resultados obtenidos durante la simulación para evaluar con datos/gráficas estadísticas que serán generadas por el simulador OPNET Modeler.

4.3.1. Caracterización de la técnica *jamming* en modo continúo.

De acuerdo al escenario *jammer* que se diseñó y explico anteriormente, se procedió a ejecutar la simulación mediante la técnica *jamming* en modo continuo, pero considerando un perfil de tráfico de no transmisión desde el nodo_tr. Adicionalmente, debemos consideran la configuración de los parámetros *jamming* <<CTS, Data y ACK>>, que se mostró en la figura 4.15 de la sección 4.2.1., para finalmente ser simulados en OPNET Modeler.

En la figura 4.19 se muestra la gráfica obtenida para el nodo_tr en relación tiempo y a la tasa de envío de datos (paquetes/s).

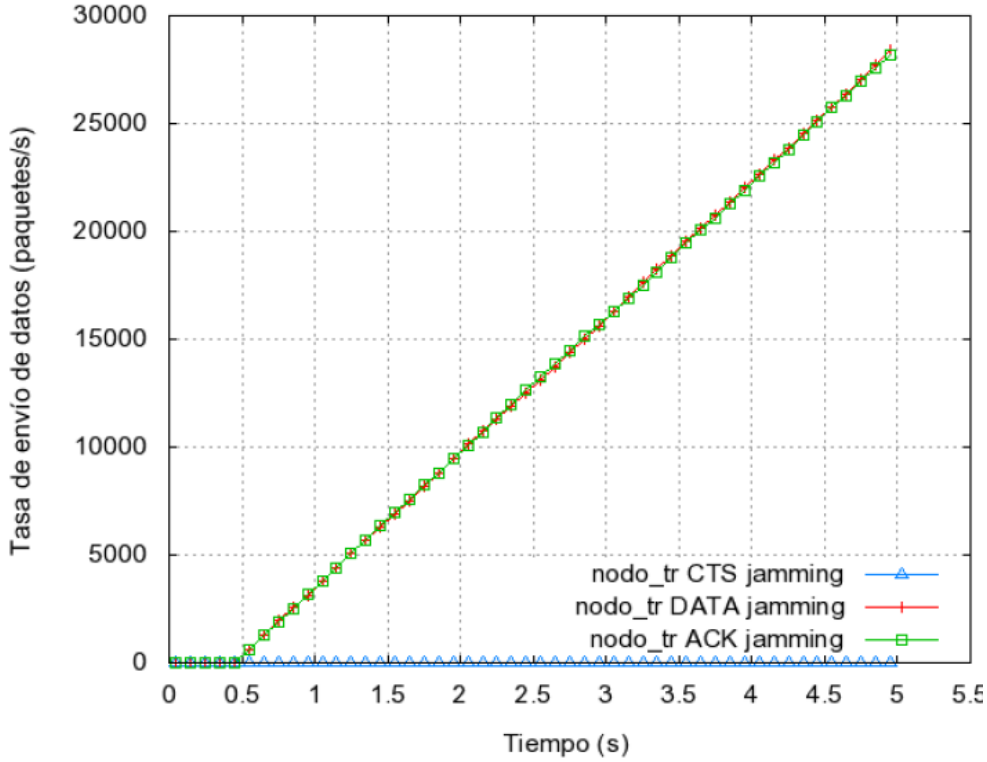


Figura 4. 19: Gráfico del nodo_tr en modo continúo.
Elaborado: La Autora.

En la figura 4.19 se puede observar que el nodo_tr CTS *jamming* no recibe datos o que la tasa de envío de datos es cero en toda la simulación; mientras que para el nodo_tr DATA *jamming* y nodo_tr ACK *jamming*, envían casi el mismo número de paquetes de datos, aunque DATA *jamming* las tramas no son receptadas por el nodo_rc, en tanto que ACK *jamming* las tramas enviadas por el nodo_rc tampoco son receptadas por el nodo_tr.

Finalmente, DATA y ACK envían datos pero nunca son receptados por el nodo_tr. En la tabla 4.6 se muestran las cantidades de paquetes que el nodo_tr ha generado durante la simulación en OPNET Modeler.

Tabla 4. 6: Cantidad de paquetes de datos formados por la técnica *jamming*.

nodo_tr	***Módulo***	***Formato Control (paquetes/s)***	***Formato MAC (paquetes/s)***	***Sin Formato (paquetes/s)***	***Total***
Jamming a CTS	wireless_mac	907			907
Jamming a DATA	wireless_mac	1420	355		1775
Jamming a ACK	wireless_mac	1408	352		1760

En la figura 4.20 se comprueba que el nodo_tr no transmite de forma correcta datos, esto ha ocurrido porque el nodo_rc no recibe paquetes, ósea que la información enviada por el nodo_tr no llega a destino.

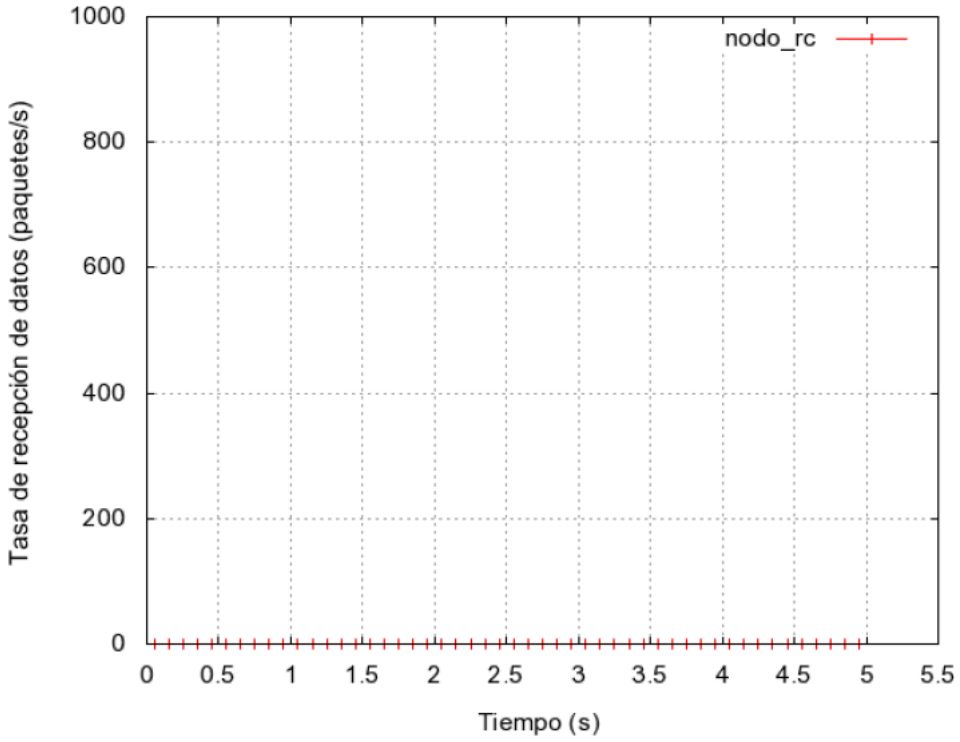


Figura 4. 20: Gráfico del nodo_rc en modo continúo.
Elaborado: La Autora.

Mientras que la figura 4.21 nos muestra el comportamiento de la tasa de envío de datos tanto para el nodo_tr datos descartados y nodo_tr datos enviados, es decir, que alcanzan el límite máximo para retransmisiones del nodo_tr. Si comparamos las gráficas de la figura 4.21, se observa que los datos enviados es igual a cuatro veces más que los datos descartados, que en la realidad sería el número de veces que ha intentado enviar una trama de datos antes de ser descartada.

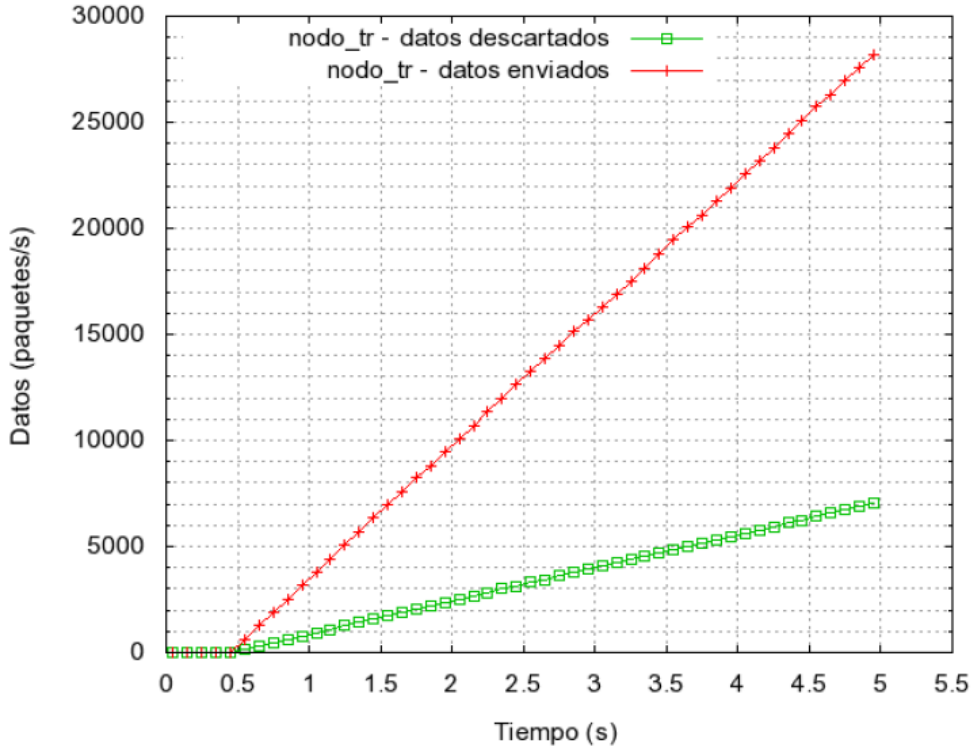


Figura 4. 21: Gráfico del nodo_rc en modo continúo.
Elaborado: La Autora.

En la tabla 4.7 se muestra la cantidad de paquetes destrozados por la técnica *jamming*.

Tabla 4. 7: Cantidad de paquetes destrozados por la técnica *jamming*.

nodo_tr	***Módulo***	***Formato Control (paquetes/s)***	***Formato MAC (paquetes/s)***	***Sin Formato (paquetes/s)***	***Total***
Jamming a ACK	wireless_mac	2816	352	1117	4285

4.3.2. Caracterización de la técnica *jamming* en modo normal.

Para esta sección mostraremos los resultados obtenidos a través de las simulaciones mediante la caracterización de la técnicas *jamming* en modo normal para el perfil de tráfico de saturación. Previamente se ha configurado el perfil de tráfico saturado al nodo *jammer*, y con tasa media al nodo_tr. Mediante la configuración descrita obtendremos el máximo aprovechamiento del canal del nodo jammer, ya que con el perfil de tráfico de saturación en todo momento tendrá datos para enviar.

En la Figura 4.22 mostramos el resultado obtenido por el nodo_jammer, en la cual presentamos la gráfica del tráfico de datos transmitido por el jammer hacia los diferentes tipos de *jamming*, en el cual los tres tipos aprovechan el canal enviando sus propias transmisiones.

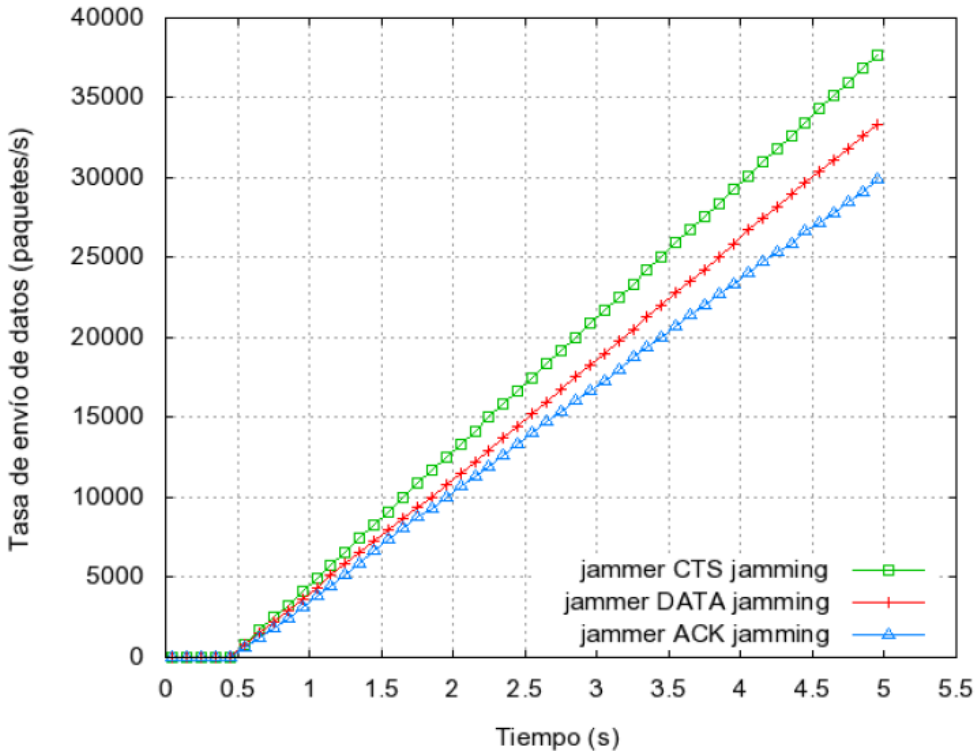


Figura 4. 22: Gráfico del nodo_jammer en modo normal.
Elaborado: La Autora.

De la figura 4.22 observemos que *jammer CTS j*amming logra enviar más datos que los otros dos tipos, es decir, que envía 217 más que *jammer DATA jamming* y *jammer ACK jamming*, tal como se indica en la tabla 4.8.

Tabla 4. 8: Cantidades de paquetes formados por *nodo_jammer* saturado.

nodo_tr	***Módulo***	***Formato Control (paquetes/s)***	***Formato MAC (paquetes/s)***	***Sin Formato (paquetes/s)***	***Total***
Jamming a CTS	wireless_mac	2028	1883		3911
Jamming a DATA	wireless_mac	2005	1666		3671
Jamming a ACK	wireless_mac	1963	1493		3456

También, se pudo obtener la gráfica (véase figura 4.23) de la cola de transmisión del *nodo_jammer* que permanece en su capacidad máxima en toda la simulación de todos los tipos de jamming.

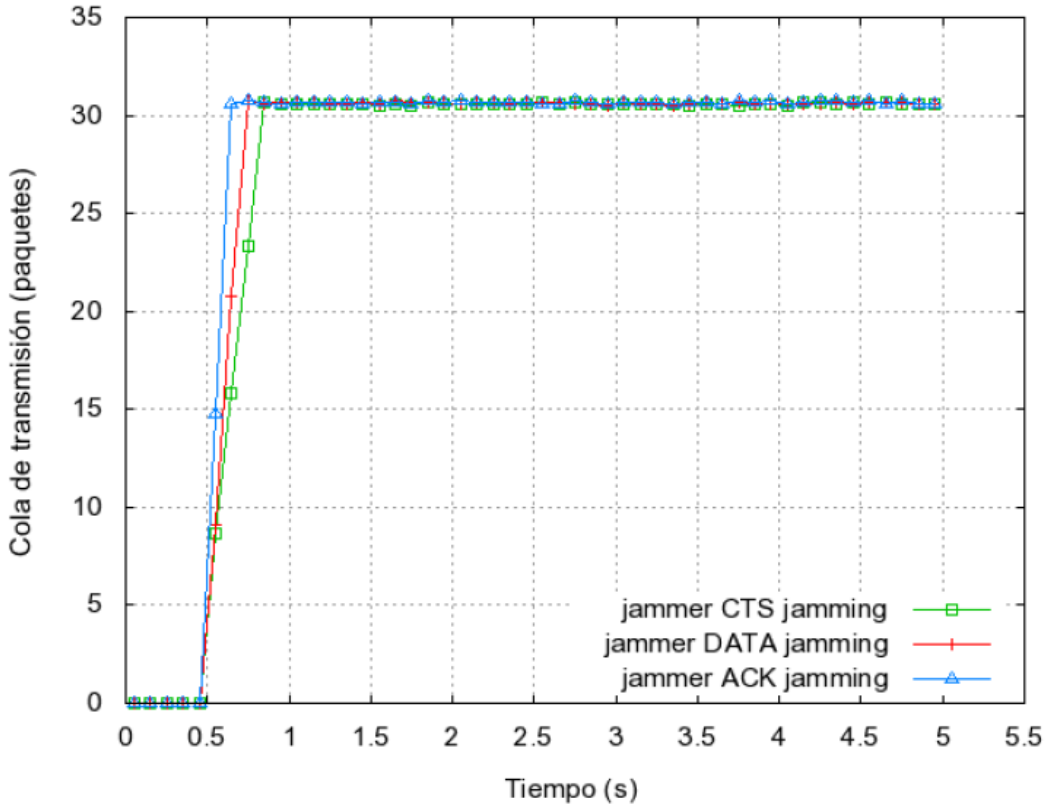


Figura 4. 23: Cola de transmisión del nodo_jammer en modo normal.
Elaborado: La Autora.

De la figura 4.23 podemos deducir que para *jammer CTS jamming*, la cola de transmisión se tarda con pocas décimas de segundos, esto ocurre porque este tipo de jamming logra transmitir más datos, por tanto la cola tardará más en alcanzar su límite. Y de manera similar, justificamos que para *jammer DATA jamming* la cola de transmisión se completa más tarde que el *jammer ACK jamming.*

De acuerdo a lo descrito en el párrafo anterior, el *jammer CTS jamming* requiere menos tiempo de acceso para transmisión de los datos, esto se muestra en la figura 4.24.

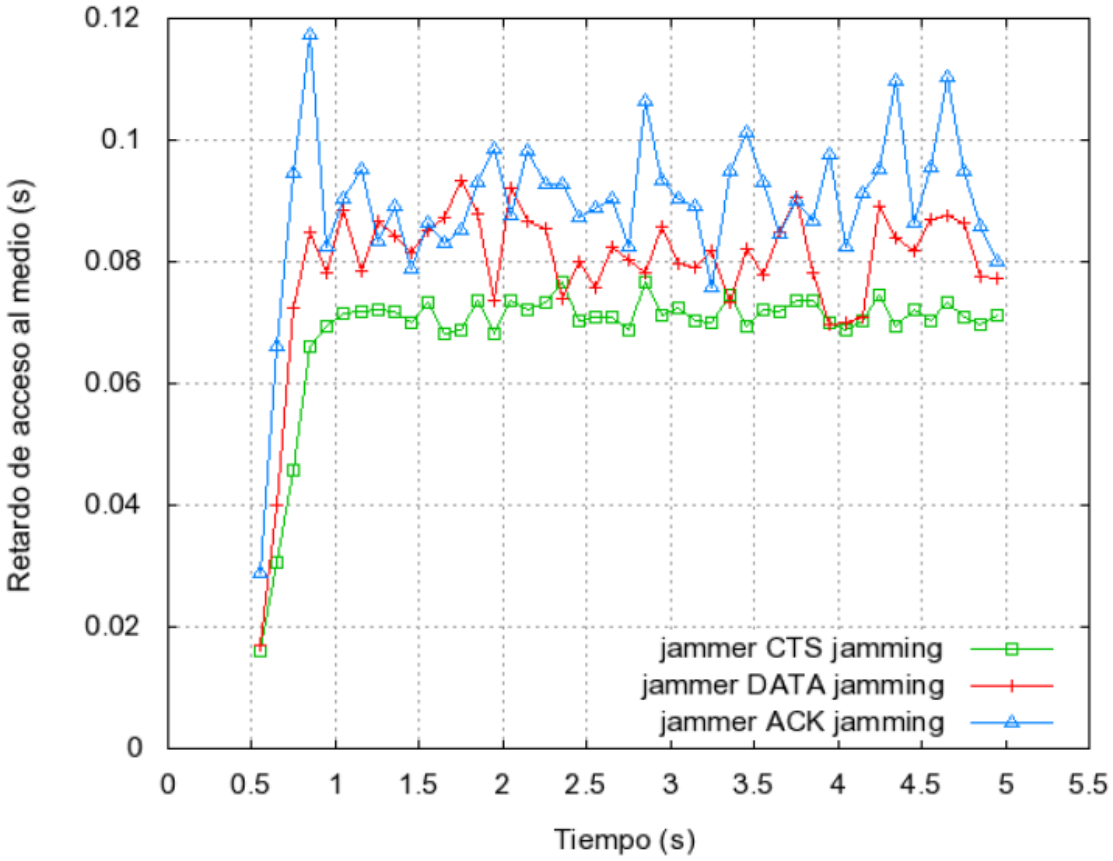


Figura 4. 24: Gráfica del retardo de acceso para transmisión de datos.
Elaborado: La Autora.

En todo caso, las tres gráficas si sufren retardos en la transmisión de datos, debido a que permanecen en cola antes de ser enviados, es decir, que deben esperar al nodo para que se pueda realizar el envío de datos.

Los resultados obtenidos por el nodo_tr en esta sección 4.3.2 son similares a la sección 4.3.1., es decir, que mediante los ataques *jamming* no permitirá la transmisión correcta de datos. Concluyendo esta sección, el nodo_tr que lo denominaré nodo egoísta, logra aprovechar el canal para transmisión de datos si bien se lleva a cabo el ataque jamming. Finalmente, el *jammer CTS jamming* resulta ser mucho más eficiente que los otros que se han simulado, debido al aprovechamiento máximo del canal para sus propios envíos.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES.

5.1. Conclusiones.

- En la descripción de la fundamentación teórica o también conocido como estado del arte de redes inalámbricas, se pudo entender y comprender porque este medio de transmisión es muy utilizado a nivel mundial para redes de área local, que inclusive se puede acceder de manera gratuita en lugares públicos, pero sin la mínima seguridad.

- A través de la descripción de la plataforma de simulación OPNET Modeler, nos permitió comprender que está herramienta es muy útil a la hora de realizar diseños de redes con cualquier medio de transmisión conocido o estudiado en la Carrera de Ingeniería en Telecomunicaciones, y con nuestra investigación se lleva a cabo la simulación de ataques malintencionados mediante la técnica jamming.

- Durante el diseño de las simulaciones en OPNET Modeler, se pudieron realizar las configuraciones necesarias para así emular una red real a través de la caracterización de la técnica *jamming* conocida como ataques *jamming*, los cuales dieron excelentes resultados, es decir, que para cada caso resultaron muy útiles los ataques *jamming*, pero el *jammer CTS jamming* se comprobó que fue la mejor solución.

5.2. Recomendaciones.

- Profundizar en el estudio de los estándares de redes inalámbricas, ya que no solo es una WLAN lo que nos permite comunicarnos de manera inalámbrica, sino como otro ejemplo sería la telefonía celular y que también no se han realizado estudios acerca de los posibles ataques a las que están expuestos.

- En asignaturas como Telemática, Sistemas de Comunicaciones y Gestión de la Red utilizar herramientas de simulación como en este trabajo de titulación se ha empleado a OPNET Modeler, que no es única herramienta para emulación de redes en modo real.

- Adquirir la licencia profesional del simulador OPNET Modeler que deberían ser utilizados para la formación de pregrado, posgrado y trabajos de investigación financiados por el SINDE.

REFERENCIAS BIBLIOGRÁFICAS

Alchele, C., Flickenger, R., Fonda, C., Howard, I., Krag, T. & Zennaro, M. (2006).*Redes Inalámbricas en los Países en Desarrollo.* Limehouse Book Sprint Team.

Andrade, R., Salas, P., & Santos P., Daniel (2008). *Tecnología Wi-Fi*. Revista Nuevas Tecnologías N° 5. ISBN 978-987-24110-6-0. Buenos Aires, Argentina.

Charro S., F. & Erazo A., P. (2006). *Estudio y diseño de una red LAN híbrida, utilizando las tecnologías WIMAX y WI-FI, para brindar servicios de video sobre IP e internet de banda ancha incluyendo transmisión de voz y datos, en la Universidad Central del Ecuador*. Trabajo de Grado publicada en la Escuela de Ingeniería, Escuela Politécnica Nacional (EPN), Quito, Ecuador.

Guerrero, F., Cardona, M., & Fuertes, J. (2007). *Análisis de interferencia entre las tecnologías inalámbricas Bluetooth e IEEE 802.11g*. Trabajo de Grado publicada por la Universidad del Cauca, Colombia.

Hernández O., J. M. (2007). *Protocolo de control de acceso al medio basado (MAC) en CSMA/CA que toma en cuenta requerimientos de calidad y servicio y que es eficiente en el consumo de energía.* Trabajo de Grado publicada en la Universidad de Baja California, México.

Lema O., R (2005). *Diseño de Procedimientos Técnicos para la Homologación de Equipos Terminales de Espectro Ensanchado*. Proyecto de Grado publicada en la Facultad de Ingeniería Electrónica, Escuela Politécnica del Ejército (ESPE), Quito, Ecuador.

Perrig, A., Canetti, R., Tygar, D., & Song, D. (2002). *SPINS: Security Protocols for Sensor Networks.* Wireless Networks 521-534.

Stallings, W. (2008). *Comunicaciones y Redes de Computadores.* Pearson Educación, Madrid.

Tanenbaum, A. S. (2003). *Redes de Computadoras*. Pearson Educación, México.

Wood, A., Stankovic, J. & Son, H. (2007). *DEEJAM: Defeating Energy-Efficient Jamming.* IEEE SECON.