UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TEMA: "Diseño y Validación de un Marco Experimental para la Detección de Ataques de Jamming en Redes 2.4 GHz Utilizando PortaHack H2".

AUTOR

Domínguez Vásquez Joseph Xavier

TRABAJO DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TELECOMUNICACIONES

TUTOR

Ing. Amaya Fariño Luis Miguel, MSc.

Santa Elena, Ecuador

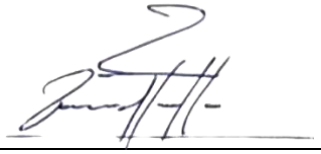
Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

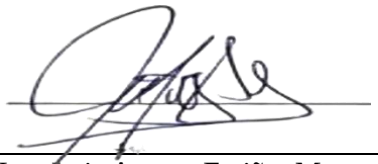
TRIBUNAL DE SUSTENTACIÓN

Ing. Ronald Rovira Jurado. Ph. D.
DIRECTOR DE LA CARRERA

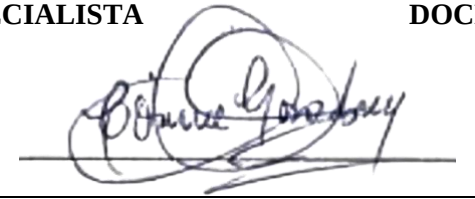
Ing. Luis Amaya Fariño. Mgtr.
TUTOR



Ing. Daniel Jaramillo Chamba. M.Sc.
DOCENTE ESPECIALISTA



Ing. Luis Amaya Fariño. Mgtr.
DOCENTE GUÍA UIC



Ing. Corina Gonzabay De La A. Mgtr
SECRETARIA

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por JOSEPH XAVIER DOMINGUEZ VASQUEZ, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 20 días del mes de DICIEMBRE del año 2024

TUTOR

Ing. Luis Miguel Amaya Fariño. Mgtr

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **JOSEPH XAVIER DOMINGUEZ VASQUEZ**

DECLARO QUE:

El trabajo de Titulación, Diseño y Validación de un Marco Experimental para la Detección de Ataques de Jamming en Redes 2.4 GHz Utilizando PortaHack H2 previo a la obtención del título en Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 20 días del mes de DICIEMBRE del año 2024

EL AUTOR

Joseph Domínguez Vásquez

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado (Titulo del ensayo), presentado por el estudiante, JOSEPH XAVIER DOMINGUEZ VASQUEZ fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al XX%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

Documento	TT_Gonzalez_John.docx (D96390558)
Presentado	2021-02-23 22:35 (-05:00)
Presentado por	T.W.D@hotmail.es
Recibido	luis.alban01.ucsg@analysis.urkund.com
Mensaje	TT_ González John Mostrar el mensaje completo
	2% de estas 42 páginas, se componen de texto presente en 6 fuentes.

TUTOR

Joseph Domínguez Vásquez

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **JOSEPH XAVIER DOMINGUEZ VASQUEZ**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.[1]

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 20 días del mes de diciembre del año 2024

EL AUTOR

Joseph Domínguez Vásquez

AGRADECIMIENTO

Agradezco en primer lugar a Dios por brindarme la fortaleza de seguir día a día y a mis padres por ser mi fortaleza y seguir siempre a mi lado, a mis amigos y las personas cercanas por estar siempre a mi lado. A mis docentes que día a día impartieron conocimientos y enseñanzas que nos ayudan tanto en el ámbito laboral y la vida. Un agradecimiento especial para mi tutor Ing. Luis Amaya quien me brindo su tiempo y sus conocimientos para poder culminar esta etapa.

Joseph Xavier Domínguez Vásquez

DEDICATORIA

Dedico este logro a todas las personas que me apoyaron en el camino, que nunca me dejaron desmayar en los momentos complicados, a mis padres, José y María, quienes han sido mi mayor inspiración, apoyo emocional y una guía para la vida y esta etapa. A mis hermanas por siempre confiar en mí. A mi Tía Celia, quien fue de gran apoyo durante esta etapa siendo como una segunda madre en mi vida. A mis hermanos de la vida Martha, Alex, Gino y Joao, quienes la vida ha puesto en mi camino y siempre han sido un apoyo fundamental en cada etapa de mi vida, su sostén y palabras siempre fueron fuente de inspiración. A mi amiguita Kerly Beltran por siempre estar presente brindándome su amistad y sus palabras. A todos Gracias de corazón.

Joseph Xavier Domínguez Vásquez

RESUMEN

El incremento en el uso de redes inalámbricas en la banda de 2.4 GHz ha traído consigo desafíos significativos en términos de seguridad, entre ellos los ataques de jamming, los cuales buscan interrumpir la comunicación entre dispositivos. En este contexto, la presente investigación tiene como objetivo principal diseñar y validar un marco experimental que permita la detección eficaz de estos ataques, utilizando el dispositivo PortaPack H2 como herramienta de análisis.

El marco experimental se basa en la captura y procesamiento de señales de radiofrecuencia en tiempo real, identificando patrones espectrales anómalos que indican la presencia de interferencias maliciosas. Para ello, se desarrollaron algoritmos de análisis estadístico y espectral que permiten diferenciar señales legítimas de aquellas que resultan de ataques de jamming. La validación del marco se llevó a cabo mediante simulaciones controladas en un entorno experimental, replicando escenarios de jamming continuo, pulsante y aleatorio.

Los resultados obtenidos demuestran que el marco experimental es capaz de detectar ataques de jamming con alta precisión, alcanzando una tasa de acierto promedio superior al 90%. Además, el uso del PortaPack H2 como herramienta central ofrece una solución accesible y portátil para el análisis y monitoreo de redes inalámbricas.

En conclusión, el marco propuesto representa un avance significativo en la detección temprana de ataques de jamming en redes de 2.4 GHz, con aplicaciones potenciales en la seguridad de sistemas IoT, redes domésticas y entornos industriales. Los resultados sugieren que este enfoque puede ser ampliado y adaptado a otras bandas de frecuencia y escenarios de comunicación inalámbrica.

PALABRAS CLAVE: Redes inalámbricas, Banda de 2.4 GHz, Ataques de jamming, Marco experimental, PortaPack H2, Detección de interferencias, Análisis espectral, Seguridad en redes, Algoritmos estadísticos, Sistemas IoT

ABSTRAC

The increase in the use of wireless networks in the 2.4 GHz band has brought with it significant challenges in terms of security, including jamming attacks, which seek to interrupt communication between devices. In this context, the main objective of this research is to design and validate an experimental framework that allows the effective detection of these attacks, using the PortaPack H2 device as an analysis tool.

The experimental framework is based on the capture and processing of radio frequency signals in real time, identifying anomalous spectral patterns that indicate the presence of malicious interference. To this end, statistical and spectral analysis algorithms were developed that allow us to differentiate legitimate signals from those that result from jamming attacks. Validation of the framework was carried out through controlled simulations in an experimental environment, replicating continuous, pulsed and random jamming scenarios.

The results obtained demonstrate that the experimental framework is capable of detecting jamming attacks with high precision, reaching an average success rate greater than 90%. Additionally, using the PortaPack H2 as a central tool offers an affordable and portable solution for wireless network analysis and monitoring.

In conclusion, the proposed framework represents a significant advance in the early detection of jamming attacks in 2.4 GHz networks, with potential applications in the security of IoT systems, home networks and industrial environments. The results suggest that this approach can be extended and adapted to other frequency bands and wireless communication scenarios.

KEYWORDS: Wireless networks, 2.4 GHz band, Jamming attacks, Experimental framework, PortaPack H2, Jamming detection, Spectral analysis, Network security, Statistical algorithms, IoT systems

ÍNDICE GENERAL

INDICE DE ILUSTRACIONES

LISTA DE ACRÓNIMOS

LAN	Local Area Network (Red de Área Local)
SDR	Software Defined Radio. (Radio Definido por Software)
IEEE	Institute of Electrical and Electronics Engineers.
TWT	Target Wake Time
BSS Color	Basic Service Set. (Conjunto de Servicios Básicos)

INTRODUCCIÓN

En telecomunicaciones, la demanda de servicios de transmisión inalámbrica de datos está aumentando, lo que impone mayores exigencias a la red. Al pasar de la comunicación cotidiana a la operación e interacción de infraestructura en el entorno empresarial, los sistemas Wi-Fi se han convertido en la columna vertebral de la conectividad actual. Pero esta dependencia también las hace vulnerables a diversas amenazas de red, razón por la cual el estudio de las redes inalámbricas se ha vuelto más importante para las personas.

Debido a esto, se enfocan estudios en la seguridad, contra posibles ataques y como identificarlos, lo que resulta necesario debido a la exposición de la privacidad e integridad de datos emitidos mediante dichas redes. A través de este estudio se busca el análisis de una red que proporcione privacidad a los datos transmitidos, ya sea estos en una empresa o una vivienda.

La banda de 2,4 GHz es una de las frecuencias más utilizadas ampliamente debido a su capacidad para atravesar obstáculos físicos y su alcance efectivo en ambientes, tanto interiores como exteriores. Pero su popularidad también lo hace vulnerable a la congestión y a ataques maliciosos como los jamming. Un ataque de interferencia es un intento deliberado de interrumpir señales inalámbricas legítimas, haciendo que una red Wi-Fi sea inaccesible o ineficaz para los usuarios autorizados. Estos ataques pueden llevarse a cabo utilizando dispositivos especializados que emiten señales de radiofrecuencia en la misma banda de frecuencia que la red Wi-Fi objetivo, sobrecargando el canal y afectando la calidad de la conexión.

Para mitigar y analizar ataques de interferencia Wi-Fi en la radiofrecuencia de 2,4 GHz, el dispositivo PortaHack H2 se convierte en una herramienta importante. Dicho artefacto es conocido por su versatilidad y capacidad para ejecutar diversas aplicaciones y scripts personalizados, lo que lo convierte en una opción estratégica para detectar y analizar patrones de interferencia de ataques Jamming.

PortaHack H2 se encuentra equipado con funciones de RF avanzadas para detectar y registrar señales en la banda de 2,4 GHz, esto incluye la capacidad de analizar el

espectro, detectar anomalías de frecuencia y evaluar la intensidad de la señal, parámetros que al ser analizados pueden indicar la presencia de un ataque de interferencia Jamming.

En un entorno controlado, el PortaHack H2 puede ser configurado para realizar pruebas exhaustivas de evaluación educativa sobre la resistencia de las redes Wi-Fi frente a ataques de jamming. Esto implica la ejecución de escenarios simulados de jamming para evaluar la efectividad de las medidas de seguridad implementadas y desarrollar estrategias de mitigación adecuadas.

1 CAPÍTULO I

1.1 ANTECEDENTES

A medida que avanzaba el desarrollo de estas tecnologías, la IEEE adoptó y estandarizó nuevos protocolos que revolucionaron la forma en que se transmiten y reciben datos, sentando las bases para lo que conocemos hoy como Wi-Fi. En 1997, se introdujo el primer estándar WLAN, el **IEEE 802.11**, que opera en la banda de frecuencia de 2.4 GHz. Este estándar permitió la creación de redes inalámbricas sin necesidad de una licencia especial, lo que promovió su adopción a nivel mundial.

Con el paso del tiempo, se desarrollaron versiones mejoradas de este estándar, como **IEEE 802.11b** en 1999, que aumentó la velocidad de transmisión de datos a 11 Mbps, y **IEEE 802.11g** en 2003, que alcanzó velocidades de 54 Mbps, utilizando técnicas de modulación avanzadas. Aunque el estándar **IEEE 802.11n**, lanzado en 2009, permitió mayores velocidades y mejoró la eficiencia al incorporar tecnología **MIMO** (Multiple Input Multiple Output), la banda de 2.4 GHz sigue siendo una opción clave para muchas redes Wi-Fi debido a su amplia cobertura y compatibilidad con dispositivos más antiguos. [1]

Paralelamente al desarrollo de las tecnologías Wi-Fi, surgieron nuevas amenazas, como los ataques de **jamming**, que representan una seria vulnerabilidad para las redes inalámbricas. Estos ataques consisten en la transmisión intencionada de señales interferentes en la misma banda de frecuencia, con el objetivo de interrumpir o degradar la comunicación. Entre las variantes más sofisticadas de este

ataque se encuentra el **Jump-Stay Jamming**, que alterna entre diferentes canales para evitar la detección. A lo largo de los años, diversas investigaciones han abordado las técnicas de mitigación de estos ataques, pero aún persisten desafíos significativos, especialmente en redes que operan en la banda de 2.4 GHz, donde la interferencia es más común debido al uso compartido del espectro con otros dispositivos.

El estándar más utilizado para redes inalámbricas en la banda de 2.4 GHz es el IEEE 802.11b, introducido en 1999, que ofrece velocidades de hasta 11 Mbps utilizando modulación DSSS (Direct Sequence Spread Spectrum). Posteriormente, en 2003, el estándar IEEE 802.11g mejoró las velocidades a hasta 54 Mbps mediante la modulación OFDM (Orthogonal Frequency-Division Multiplexing) y es compatible con 802.11b, facilitando la transición entre estándares. En 2009, el IEEE 802.11n introdujo capacidades avanzadas con velocidades de hasta 600 Mbps, utilizando la tecnología MIMO (Multiple Input Multiple Output) y operando en ambas bandas de 2.4 GHz y 5 GHz. Aunque el IEEE 802.11ac, lanzado en 2013, se enfoca principalmente en la banda de 5 GHz con velocidades de hasta 3.5 Gbps, también puede operar en 2.4 GHz en dispositivos de banda dual. Finalmente, el IEEE 802.11ax (Wi-Fi 6), publicado en 2019, ofrece velocidades teóricas de hasta 9.6 Gbps y mejoras en eficiencia y capacidad, operando en ambas bandas y utilizando técnicas avanzadas como OFDMA (Orthogonal Frequency Division Multiple Access). Cada evolución de los estándares ha proporcionado mejoras significativas en la velocidad y la eficiencia de las redes inalámbricas, adaptándose a las crecientes demandas de conectividad, aunque la banda de 2.4 GHz sigue siendo susceptible a interferencias de otros dispositivos, lo que puede afectar el rendimiento de la red. [2]

Los ataques de jamming representan una amenaza significativa para las redes Wi-Fi al interrumpir o degradar la comunicación inalámbrica mediante la transmisión intencionada de señales interferentes en la misma banda de frecuencia que la red. Este tipo de ataque puede llevar a una completa interrupción del servicio, impidiendo que los dispositivos se conecten o se comuniquen de manera efectiva. Incluso si el jamming no es total, puede reducir considerablemente la calidad de la señal, aumentando la tasa de errores y disminuyendo la velocidad de transferencia

de datos. Como resultado, los usuarios experimentan ralentizaciones y desconexiones intermitentes, afectando negativamente su experiencia y productividad.

Además de interrumpir el servicio, los ataques de jamming pueden impactar la seguridad de la red, facilitando otras formas de ataques, como la denegación de servicio (DoS). Los métodos tradicionales de mitigación, como el cambio de canal o la detección continua de interferencias, a menudo resultan ineficaces contra técnicas más sofisticadas como el Jamming, donde el jammer alterna entre diferentes canales para evadir la detección y la respuesta de la red. Para contrarrestar estos ataques, es crucial implementar estrategias avanzadas, como tecnologías de salto de frecuencia y técnicas robustas de modulación, así como métodos de detección y respuesta mejorados. La capacidad para analizar y mitigar estos ataques es esencial para mantener la integridad y el rendimiento óptimo de las redes Wi-Fi.

El análisis de ataques de jamming en redes Wi-Fi requiere el uso de herramientas y tecnologías especializadas que permitan detectar, estudiar y mitigar estos incidentes. Una de las herramientas clave en este campo es el Software Defined Radio (SDR), que ofrece flexibilidad para analizar y manipular señales de radio en tiempo real. Dispositivos como el PortaHack H2 permiten realizar capturas detalladas del espectro en frecuencias de 2.4 GHz, facilitando la identificación de patrones de interferencia provocados por ataques de jamming, como el Jamming. Esta herramienta es especialmente útil en entornos controlados, donde se pueden replicar ataques y medir el impacto en la red Wi-Fi.

Otra tecnología esencial para el análisis de jamming es el uso de análisis de espectro mediante software como GNU Radio, que permite visualizar y analizar las señales inalámbricas en el espectro afectado. Este tipo de software facilita la simulación y recreación de escenarios de ataque, permitiendo experimentar con diferentes técnicas de interferencia y evaluar su impacto en la red. Además, se pueden implementar sistemas de monitoreo en tiempo real para identificar la presencia de interferencias o anomalías en la red, permitiendo una respuesta rápida.

Finalmente, el uso de Wireshark es fundamental para capturar y analizar el tráfico de la red, permitiendo detectar cambios en los patrones de tráfico y posibles signos

de interferencia. A través de esta herramienta, los investigadores pueden correlacionar los cambios en la calidad del servicio (QoS) con la presencia de jamming, ayudando a validar los efectos del ataque y probar posibles soluciones. Estas tecnologías, combinadas, brindan un enfoque integral para el estudio y la mitigación de ataques de jamming en redes Wi-Fi.

Las investigaciones previas sobre ataques de jamming en redes Wi-Fi han sido cruciales para comprender la vulnerabilidad de las comunicaciones inalámbricas frente a interferencias maliciosas. Desde los primeros estudios sobre la denegación de servicio (DoS) en redes Wi-Fi, hasta los análisis más recientes de técnicas avanzadas como el Jamming, estas investigaciones han demostrado cómo los atacantes pueden interrumpir el funcionamiento de las redes inalámbricas utilizando estrategias sofisticadas que dificultan la detección y mitigación de estos ataques. En particular, estudios que examinan la eficacia de las tecnologías anti-jamming, como el cambio de canal y la detección de interferencias, han mostrado que estas medidas pueden ser insuficientes frente a ataques que cambian dinámicamente entre diferentes frecuencias, como el Jamming.

Investigaciones centradas en el uso de Software Defined Radio (SDR) han abierto nuevas posibilidades para el análisis y la simulación de estos ataques. Dispositivos como el HackRF One y herramientas de software como GNU Radio han sido fundamentales en el desarrollo de entornos experimentales controlados donde se pueden recrear y estudiar ataques de jamming. Estos estudios han permitido una mejor comprensión de cómo las redes Wi-Fi responden a interferencias activas y han ayudado a identificar patrones que pueden ser utilizados para detectar y mitigar jammers en tiempo real.

La relevancia de estas investigaciones para el tema de tesis "Análisis de bloques contra Ataques de Jamming en Sistemas de 2.4 GHz utilizando PortaHack H2" radica en la necesidad de continuar explorando la resistencia de las redes Wi-Fi frente a estos tipos de interferencias maliciosas. Este proyecto busca no solo aplicar técnicas de análisis avanzadas mediante SDR, sino también proporcionar un marco de referencia práctico para la detección y evaluación del impacto del jamming en entornos controlados. Además, este estudio contribuirá a la academia al generar

conocimiento que puede ser utilizado en futuras investigaciones, particularmente en el ámbito de la seguridad de redes inalámbricas y la implementación de redes más robustas frente a estos ataques.

El tema de tesis "Análisis de bloques contra Ataques de Jamming en Sistemas de 2.4 GHz utilizando PortaHack H2" se enmarca en un contexto educativo que busca capacitar a los estudiantes en el análisis y resolución de problemas relacionados con la seguridad de redes inalámbricas. En un entorno académico como la Universidad Estatal Península de Santa Elena, la investigación de ciberseguridad aplicada a redes Wi-Fi es fundamental para que los estudiantes de telecomunicaciones comprendan las vulnerabilidades de las tecnologías actuales, así como los métodos para evaluar y mitigar estos riesgos. Dado el creciente uso de dispositivos Wi-Fi en casi todos los ámbitos, es necesario que los futuros profesionales cuenten con habilidades especializadas en la detección y análisis de amenazas como el jamming.

La aplicación práctica de este proyecto se centrará en el uso de herramientas avanzadas como el PortaHack H2 y Software Defined Radio (SDR) para realizar pruebas en un entorno controlado dentro de los laboratorios de la universidad. Estas pruebas permitirán a los estudiantes y académicos entender cómo funcionan los ataques de jamming y su impacto en las redes de 2.4 GHz. El desarrollo de escenarios experimentales con redes Wi-Fi afectadas por este tipo de interferencias permitirá no solo el estudio de las vulnerabilidades presentes en las redes, sino también la simulación de situaciones reales de ataque, preparando a los estudiantes para desafíos en el mundo laboral.

Este proyecto de investigación busca analizar y evaluar los ataques de **Jamming** en redes Wi-Fi de 2.4 GHz utilizando herramientas como **PortaHack H2** y **Software Defined Radio (SDR)**. Los estudios previos sobre ciberseguridad y redes inalámbricas destacan la importancia de comprender y mitigar estas vulnerabilidades, y esta investigación proporcionará un enfoque práctico que permitirá a los estudiantes y académicos analizar estos problemas en un entorno controlado, contribuyendo al avance del conocimiento en seguridad de redes Wi-Fi.

Además, la tesis proporcionará a la universidad un marco teórico y práctico que podrá ser reutilizado en futuras investigaciones y proyectos académicos. Este conocimiento será valioso para otros estudiantes y profesionales interesados en la seguridad de redes inalámbricas, fomentando el desarrollo de nuevas soluciones y estrategias para la protección de infraestructuras críticas de comunicación. Asimismo, el proyecto contribuirá a fortalecer la infraestructura educativa de la universidad, dotando a los laboratorios de un entorno donde se puedan replicar y estudiar ataques cibernéticos de forma segura y controlada, lo que es clave para el aprendizaje práctico en ciberseguridad.

1.2 DEFINICIÓN DEL PROBLEMA

El avance de las nuevas tecnologías y las mejoras en las capacidades, impulsan a mantener el mundo a estar en constante innovación. En las comunicaciones sucede lo mismo, debido a una mayor demanda de conectividad y estabilidad en las conexiones a internet hacen que las redes innoven y mejoren características para brindar un mejor servicio.

Las redes inalámbricas que operan en la banda de frecuencia de 2,4 GHz comúnmente utilizada en los sistemas Wi-Fi se han convertido en una infraestructura importante para los usuarios domésticos y comerciales. Sin embargo, debido a la apertura de la transmisión inalámbrica y la popularidad de esta banda de frecuencia, estas redes enfrentan muchas amenazas a la seguridad, entre las que destacan los ataques de interferencia. Uno de los métodos de ataque más sofisticados y difíciles de mitigar es el "Jamming", donde los atacantes cambian inteligentemente entre diferentes canales para evitar una fácil detección y lograr una interrupción efectiva del servicio.

El principal inconveniente con las redes inalámbricas es que las técnicas de defensa tradicionales usadas contra ataques de interferencia, como la detección continua de interferencias o el cambio de canal, son insuficientes contra el Jamming. Estos ataques pueden desestabilizar periódicamente las redes inalámbricas, provocando una degradación significativa de la calidad de servicio (QoS), pérdida de paquetes y aumento de la latencia, lo que afecta negativamente la experiencia del usuario y la eficiencia empresarial.

Este desafío se amplifica en entornos empresariales donde la disponibilidad y estabilidad de las redes Wi-Fi son fundamentales para la continuidad del negocio. Además, la falta de herramientas disponibles y efectivas para detectar y analizar este tipo de ataques pone a los administradores de red en desventaja cuando intentan proteger su infraestructura de amenazas avanzadas.

En este contexto, el dispositivo PortaHack H2, con sus capacidades avanzadas de análisis de espectro y detección de señales, se considera una herramienta prometedora para resolver este problema. Sin embargo, su potencial para detectar y prevenir ataques de interferencia en redes Wi-Fi de 2,4 GHz no se ha aprovechado al máximo, por lo que se requiere un análisis sistemático y en profundidad del uso de PortaHack H2. Mejora de la seguridad y robustez de las redes inalámbricas.

1.3 DESCRIPCIÓN

La presente investigación, analizará cada escenario utilizando el dispositivo de seguridad PortaHack H2 para investigar los diferentes tipos de ruido que tienden a afectar los sistemas de 2,4 GHz a partir de ataques Jamming, enfocándose en los últimos avances tecnológicos que coinciden con cada bloque, qué ataque es una forma de interferencias maliciosas que pueden interrumpir las conexiones inalámbricas al cambiar aleatoria y rápidamente de un canal a otro. Esto presenta un desafío importante para la detección y mitigación.

Estos tipos de ciberataques son conocidos por su capacidad de interrumpir periódicamente las señales inalámbricas cambiando aleatoriamente entre diferentes canales, lo que representa una amenaza importante para la estabilidad y seguridad de las redes inalámbricas. Los métodos antiinterferencias tradicionales, como el cambio de canal o la detección continua de interferencias, han demostrado ser insuficientes para proteger contra este tipo de ataques, que pueden eludir las contramedidas tradicionales y afectar de forma silenciosa y gradual a la calidad del servicio (QoS).(Pirayesh & Zeng, 2023)

En este contexto, el dispositivo PortaHack H2, conocido por sus capacidades avanzadas de análisis del espectro de RF, ofrece un enfoque innovador para identificar y analizar patrones de ataque Jammer. La versatilidad del PortaHack H2

permite realizar pruebas exhaustivas en un entorno controlado para evaluar la resistencia de las redes Wi-Fi a este tipo de interferencias maliciosas. Al capturar y analizar datos del espectro, nos esforzamos en desarrollar nuevas estrategias y protocolos de defensa para mejorar la detección temprana de ataques, reducir su impacto y garantizar la continuidad del servicio. (Osanaiye O, Alfa A, Hancke G, 2018)

El objetivo principal de este artículo es proporcionar un análisis en profundidad de cómo PortaHack H2 puede identificar y mitigar eficazmente los ataques Jamming. Se realizarán pruebas experimentales en un entorno controlado para medir el impacto de estos ataques en la red y evaluar la eficacia de las técnicas de defensa propuestas. Los resultados de esta investigación ayudarán a desarrollar soluciones más sólidas para proteger las redes Wi-Fi, especialmente en entornos empresariales donde la seguridad y la estabilidad de la red son fundamentales para las operaciones comerciales.

La investigación también utilizará PortaHack H2 para desarrollar e implementar métodos basados en el análisis del espectro de RF para mejorar la resiliencia de la red contra ataques de interferencia de alto nivel. De esta forma, pretende contribuir a la seguridad informática ofreciendo nuevas soluciones que permitan combatir una de las amenazas más complejas en las redes inalámbricas de 2,4 GHz.

Las nuevas generaciones de tecnologías inalámbricas, como la radio definida por software (SDR), ofrecen oportunidades significativas para mejorar la seguridad y eficiencia de las redes. En el contexto de la presente tesis, que aborda el análisis de ataques de Jamming en redes Wi-Fi de 2.4 GHz utilizando el PortaHack H2, estas tecnologías permiten un enfoque profundo y práctico hacia la protección de las comunicaciones inalámbricas. La implementación de un manual que explore el uso de SDR, complementado con el análisis de ataques de jamming, no solo es relevante para el fortalecimiento del conocimiento académico en telecomunicaciones, sino que también proporciona una base sólida para futuros proyectos de investigación en la Universidad Estatal Península de Santa Elena. Este estudio serviría como antecedente valioso para el desarrollo de programas de cuarto nivel, como las maestrías, y ofrecería una guía técnica que beneficiaría a los estudiantes y

profesionales interesados en la seguridad de redes y la implementación de tecnologías avanzadas en entornos académicos y laborales.

1.4 JUSTIFICACIÓN

El presente trabajo de investigación está motivado por la creciente dependencia de las redes inalámbricas, especialmente aquellas que operan en la banda de frecuencia de 2,4 GHz, ampliamente utilizada en hogares y entornos comerciales. Estas redes son esenciales para las comunicaciones diarias y el funcionamiento de infraestructuras críticas, lo que las convierte en blanco de ciberataques como interrupciones, un tipo de interrupción que altera la disponibilidad y calidad de los servicios de red.

Este tipo de ataque se caracteriza por la capacidad de cambiar aleatoriamente entre diferentes canales y evitar las tradicionales defensas de interferencia. Los métodos tradicionales, como la simple conmutación de canales o la detección continua de interferencias, han demostrado ser ineficaces frente a estas tecnologías más avanzadas, dejando la red expuesta y vulnerable a ataques. Las interrupciones silenciosas y graduales de la calidad del servicio (QoS) pueden causar pérdidas financieras significativas a las empresas que dependen de conexiones constantes, al tiempo que afectan la experiencia del usuario.

La razón para utilizar PortaHack H2 en este estudio son sus capacidades avanzadas de análisis de espectro y detección de señales, que pueden identificar patrones de ataque y desarrollar contramedidas efectivas. La investigación propuesta no sólo contribuye a la seguridad de las redes inalámbricas, sino que también hace una contribución significativa a la comunidad académica y profesional al proporcionar soluciones prácticas y asequibles para mitigar dichas amenazas. Además, este estudio sienta una base sólida para futuras investigaciones en el campo de la ciberseguridad y las comunicaciones inalámbricas, posicionando a la Universidad Estatal Península de Santa Elena como un referente en análisis de redes y técnicas de defensa contra ciberataques avanzados.

Finalmente, este estudio tiene implicaciones educativas ya que puede conducir al desarrollo de materiales y manuales que pueden usarse para proyectos de

capacitación en telecomunicaciones y seguridad de la información que ayuden a preparar a futuros profesionales en estos campos críticos.

1.5 ALCANCE

El presente proyecto está destinado a aportar conocimientos en la parte académica de estudiantes de nuestra facultad dentro del alma Máter, esto se realizará a través de la simulación de ataques Jammer mediante diagramas de bloques enfocados en diferentes modulaciones, mientras se analizan diferentes escenarios de ataques mediante tecnología SDR. A continuación, se detallan los aspectos y límites específicos del proyecto:

1. **Análisis del Espectro en la Banda de 2.4 GHz**: El proyecto incluirá la utilización del PortaHack H2 para capturar y analizar el espectro de radiofrecuencia en la banda de 2.4 GHz. Esto permitirá identificar y caracterizar los patrones de interferencia asociados con ataques Jamming.

2. **Desarrollo y Evaluación de Diagramas de Bloques**: Se desarrollarán diagramas de bloques que representen los patrones de interferencia y técnicas de jamming utilizadas en ataques. Estos diagramas servirán para visualizar y entender cómo estos ataques afectan la red y para diseñar estrategias de mitigación efectivas.

3. **Simulación de Ataques y Pruebas en un Entorno Controlado**: Se llevará a cabo la simulación de ataques Jamming en un entorno controlado utilizando el PortaHack H2. La simulación permitirá observar el impacto de estos ataques en la red Wi-Fi y evaluar la efectividad de las contramedidas propuestas.

4. **Desarrollo de Estrategias de Mitigación**: Basado en el análisis y simulación de ataques, se desarrollarán y evaluarán estrategias y protocolos de mitigación para proteger las redes Wi-Fi contra los ataques Jamming. Esto incluirá recomendaciones para mejorar la detección temprana y la resiliencia de la red.

5. **Documentación de Procedimientos y Resultados**: Se documentarán detalladamente los procedimientos utilizados para el análisis y simulación de ataques, así como los resultados obtenidos. Esta documentación servirá como referencia para futuras investigaciones y para la implementación de soluciones de seguridad en redes inalámbricas.

6. **Limitaciones del Proyecto**: El proyecto se enfocará exclusivamente en el análisis de ataques Jamming en la banda de 2.4 GHz. La investigación se llevará a cabo en un entorno de laboratorio controlado y no incluirá pruebas en redes en producción o en entornos exteriores. El uso del PortaHack H2 estará limitado a su capacidad para análisis del espectro y detección de interferencias.

7. **Aplicación y Extensibilidad**: Los resultados y metodologías desarrollados en este proyecto podrán ser aplicados para mejorar la seguridad en redes Wi-Fi en entornos empresariales y académicos. Los diagramas de bloques y estrategias de mitigación propuestas estarán diseñados para ser adaptables y útiles en investigaciones futuras sobre ciberseguridad y redes inalámbricas.

Este alcance está diseñado para proporcionar una comprensión exhaustiva de cómo los ataques Jamming afectan a las redes Wi-Fi y para desarrollar soluciones prácticas que fortalezcan la seguridad en esta área crítica.

1.6 OBJETIVOS

1.6.1 OBJETIVO GENERAL

Diseñar, implementar y validar un marco experimental para la detección de ataques de jamming en redes inalámbricas de 2.4 GHz, utilizando PortaHack H2 como herramienta principal, con el propósito de identificar patrones característicos de ataques y proponer criterios efectivos para su detección.

1.6.2 OBJETIVOS ESPECÍFICOS

- Configurar un entorno experimental para la simulación de ataques de jamming en redes 2.4 GHz.
- Analizar el comportamiento de la red y los patrones de tráfico bajo diferentes tipos de ataques.
- Proponer y validar un sistema de detección basado en los patrones identificados.

1.7 RESULTADOS ESPERADOS

El presente trabajo de investigación tiene como objetivo principal desarrollar métodos eficaces para detectar y mitigar ataques de Jamming en redes Wi-Fi que operan en la banda de 2.4 GHz, utilizando el dispositivo PortaHack H2. Los resultados esperados para validar este objetivo son los siguientes:

1. Desarrollo de un protocolo de análisis del espectro de RF: Se espera diseñar y ejecutar un protocolo que utilice el PortaHack H2 para monitorear y analizar el espectro de radiofrecuencia en la banda de 2.4 GHz, enfocándose en la identificación de patrones asociados con ataques de Jamming.
2. Identificación y caracterización de patrones de interferencia: A través del análisis de datos espectrales capturados, se logrará identificar los patrones específicos de interferencia utilizados en los ataques Jamming, proporcionando una comprensión detallada de cómo estos ataques afectan la red.

3. Evaluación de la efectividad de las contramedidas propuestas: Se implementarán y evaluarán estrategias y protocolos de defensa para mitigar los efectos de los ataques Jamming. Se medirán mejoras en la estabilidad y calidad del servicio (QoS) en la red Wi-Fi bajo ataque.
4. Diseño de un modelo de simulación para ataques de jamming: Se desarrollará un modelo de simulación en un entorno controlado para reproducir ataques Jamming y evaluar la respuesta de la red, utilizando las capacidades del PortaHack H2 para capturar y analizar el impacto de estos ataques.
5. Propuesta de un diagrama de bloques de mitigación: Se creará un diagrama de bloques que describa las técnicas y herramientas recomendadas para detectar y mitigar ataques Jamming, basándose en los datos y análisis obtenidos durante la investigación.
6. Generación de recomendaciones para la implementación práctica: A partir de los resultados obtenidos, se proporcionarán recomendaciones prácticas para la implementación de soluciones de seguridad en redes Wi-Fi, con el objetivo de mejorar la resiliencia contra ataques de jamming avanzados.
7. Documentación y capacitación en técnicas de análisis y defensa: Se desarrollará un manual detallado sobre el uso del PortaHack H2 para la detección y análisis de ataques Jamming, que servirá como recurso educativo y práctico para futuras investigaciones y aplicaciones en el campo de las telecomunicaciones.
8. Evaluación de la aplicabilidad de los resultados en entornos empresariales y académicos: Se analizará cómo los métodos y soluciones propuestas pueden ser aplicadas y adaptadas para mejorar la seguridad de redes Wi-Fi en diferentes contextos, incluyendo entornos empresariales y educativos.

Estos resultados proporcionarán una base sólida para mejorar la seguridad en redes Wi-Fi y contribuirán al avance del conocimiento en el área de la ciberseguridad inalámbrica.

Proponer un diagrama de bloques en GNU Radio para la tecnología SDR que transmita datos mediante las frecuencias definidas en el proyecto y que a su vez sea modificable para futuras practicas dentro del campus educativo.

1.8 METODOLOGÍA

El estudio se centrará en evaluar cómo estos ataques afectan la estabilidad y la calidad del servicio en redes inalámbricas, con el objetivo de desarrollar estrategias efectivas para su detección y funcionalidad en un modelo educativo, cumpliendo los objetivos específicos mencionados. La investigación abordará las siguientes áreas clave:

1.8.1 MÉTODO DE INVESTIGACIÓN

El método de investigación para este proyecto se basa en un enfoque sistemático y estructurado para analizar el impacto de los ataques Jamming en redes Wi-Fi de 2.4 GHz utilizando el PortaHack H2. Este enfoque permitirá evaluar tanto la naturaleza de los ataques como la efectividad de las estrategias de mitigación.

Este método de investigación proporcionará una comprensión exhaustiva de los ataques Jamming en redes Wi-Fi y desarrollará soluciones prácticas basadas en datos empíricos, mejorando así la seguridad de las redes inalámbricas.

1.8.1.1 INVESTIGACIÓN CUANTITATIVA

La investigación cuantitativa nos permite analizar nuestras hipótesis mediante pruebas, establecer relaciones causales mediante análisis y prueba o confirmar inductivamente nuestros objetivos generales. El objetivo de este proyecto de investigación cuantitativa es evaluar el impacto de los ataques Jamming en redes Wi-Fi de 2,4 GHz y desarrollar estrategias de mitigación efectivas. Utilizando un enfoque sistemático y estructurado, cuyo principal enfoque es obtener resultados imparciales que confirmen las hipótesis y cumplan con los objetivos generales de la investigación. Los métodos cuantitativos utilizados se describen a continuación:

- **1. Observación Estandarizada:** La investigación comenzará con una revisión exhaustiva de la literatura relevante sobre ataques de jamming, particularmente Jamming, y sobre el uso del PortaHack H2 para análisis del espectro de RF. Esta revisión permitirá establecer una base teórica sólida y comprender los mecanismos de ataque y las técnicas de mitigación existentes.

- **2. Experimentos y Pruebas:** Se diseñarán y ejecutarán experimentos en los que se simularán ataques de jamming con diferentes configuraciones (frecuencia de cambio de canal, intensidad de interferencia, etc.). Estos experimentos se llevarán a cabo en un ambiente controlado para asegurar la validez y la reproducibilidad de los resultados. Durante los experimentos, se recopilarán datos cuantitativos sobre el rendimiento de la red, incluyendo métricas como tasa de pérdida de paquetes, latencia y ancho de banda. Estos datos se analizarán para identificar el impacto de los ataques y la efectividad de las estrategias de mitigación.
- **3. Análisis de Datos:** Los datos recolectados serán analizados utilizando técnicas estadísticas para identificar patrones y correlaciones. Se utilizarán métodos de análisis de varianza (ANOVA), pruebas de hipótesis y otras técnicas estadísticas para interpretar los resultados de los experimentos. Se compararán los datos obtenidos durante y después de los ataques, así como la eficacia de las estrategias de mitigación. Esto permitirá determinar cómo afectan los ataques a la red y qué medidas son más efectivas para reducir su impacto.

1.8.1.2 INSTRUMENTOS PARA LA OBTENCIÓN DE DATOS Y SIMULACIÓN

Para el análisis de bloques contra ataques de Jamming en sistemas de 2.4 GHz utilizando PortaHack H2, se emplearán una serie de instrumentos y herramientas especializados. El PortaHack H2 será fundamental para la captura y análisis del espectro de RF, permitiendo visualizar y registrar interferencias en tiempo real, lo cual es crucial para identificar la intensidad y el impacto de los ataques de jamming. Además, se utilizarán equipos de red Wi-Fi que operan en la banda de 2.4 GHz, configurados para simular una red Wi-Fi típica, lo que permitirá evaluar cómo las interferencias afectan la comunicación entre dispositivos y el rendimiento general de la red.

Para el desarrollo y prueba de algoritmos relacionados con la detección de interferencias y la mitigación de ataques, se utilizará GNU Radio, un software de procesamiento de señales de código abierto. Este software permitirá la

implementación de diagramas de bloques y la simulación de diferentes escenarios de ataque. Wireshark, por otro lado, será utilizado para capturar y analizar el tráfico de red durante los experimentos, proporcionando datos detallados sobre métricas como la pérdida de paquetes, la latencia y el ancho de banda.

Además, se emplearán medidores de ancho de banda y herramientas de monitoreo de red para evaluar el rendimiento de la red y detectar problemas de conectividad. Estos instrumentos ayudarán a medir el impacto de los ataques de jamming en la capacidad de la red y a garantizar una supervisión continua de la infraestructura. Finalmente, se utilizarán herramientas de documentación y reportes para elaborar informes detallados, gráficos y tablas que presenten de manera clara y profesional los resultados de los experimentos y el análisis de datos. Esta combinación de herramientas y técnicas garantizará una comprensión exhaustiva del impacto de los ataques y la efectividad de las estrategias de mitigación propuestas.

1.8.1.3 ESCENARIO DE PRUEBAS

El tema seleccionado para esta investigación se centra en la implementación y análisis de ataques de jamming en redes Wi-Fi de 2.4 GHz, utilizando el dispositivo PortaHack H2. Para el análisis de bloques contra ataques de jamming en sistemas de 2.4 GHz utilizando PortaHack H2, se diseñarán varios escenarios de prueba que permitan evaluar de manera exhaustiva el impacto de estos ataques en la red. Primero, se configurará una red Wi-Fi en un entorno controlado, utilizando equipos que operan en la banda de 2.4 GHz, para simular un entorno realista donde se puedan replicar las condiciones de ataque. En este escenario, se implementará un ataque de jamming utilizando PortaHack H2 para observar cómo el dispositivo interfiere con la señal Wi-Fi y cómo afecta la calidad de la conexión y la integridad de los datos transmitidos.

Posteriormente, se realizarán pruebas adicionales variando los parámetros del ataque, como la frecuencia de cambio de canal y la duración de las interferencias, para evaluar cómo estos factores influyen en la efectividad del ataque y en la respuesta de la red. Además, se utilizarán herramientas de análisis como Wireshark para capturar y analizar el tráfico de red durante los ataques, permitiendo la evaluación de métricas como la pérdida de paquetes, la latencia y el ancho de banda.

Los datos obtenidos de estas pruebas se utilizarán para desarrollar y ajustar estrategias de mitigación, así como para validar la efectividad de las contramedidas implementadas. Estos escenarios de prueba proporcionarán una visión detallada del impacto de los ataques de jamming y contribuirán al desarrollo de soluciones más robustas para la protección de redes Wi-Fi contra interferencias maliciosas.

Esta metodología constará de tres fases en función del cumplimento de cada una se podrá empezar en una nueva fase, caso contrario se ajustará hasta la obtención de resultados favorables para el proyecto.

- **PRIMERA FASE: CONFIGURACIÓN Y SIMULACIÓN PRELIMINAR**

En esta fase inicial, se llevará a cabo la configuración de la red Wi-Fi en un entorno controlado utilizando equipos de red que operan en la banda de 2.4 GHz. Se implementará una red de prueba que replicará un entorno realista, asegurando que todos los dispositivos estén correctamente configurados y conectados.

- **Configuración de la Red:** Instalación y configuración de routers y puntos de acceso para establecer una red Wi-Fi operativa.
- **Preparación para Ataques:** Configuración del PortaHack H2 para realizar pruebas de jamming en condiciones controladas. Se definirán los parámetros básicos del ataque, como la frecuencia y la duración de las interferencias.

- **SEGUNDA FASE: EJECUCIÓN DE ATAQUES Y CAPTURA DE DATOS**

Esta fase se centra en la ejecución de ataques de jamming utilizando PortaHack H2 en la red configurada. El objetivo es capturar datos sobre cómo las interferencias afectan la calidad de la señal y el rendimiento de la red.

- **Ejecución de Ataques:** Implementación de ataques de jamming con PortaHack H2, variando los parámetros del ataque como la frecuencia de cambio de canal y la intensidad de la interferencia.

- **Monitoreo y Captura de Datos:** Utilización de herramientas como Wireshark para capturar el tráfico de red durante los ataques. Se recogerán datos sobre la pérdida de paquetes, latencia, ancho de banda y otros indicadores de rendimiento.
- **Análisis de Interferencias:** Evaluación del impacto de los ataques sobre la red, incluyendo la calidad de la conexión y la integridad de los datos transmitidos.

➢ **TERCERA FASE: ANÁLISIS DE DATOS Y PRESENTACIÓN DE RESULTADOS**

La fase final se centra en el análisis de los datos recopilados y en la presentación de los resultados del estudio.

- **Análisis de Resultados:** Revisión detallada de los datos obtenidos durante las pruebas de ataque para identificar patrones y evaluar el impacto de los ataques de jamming en la red.
- **Elaboración de Informes:** Desarrollo de informes detallados que incluyan gráficos, tablas y descripciones de los resultados obtenidos. Estos informes ofrecerán una visión clara del impacto de los ataques y permitirán entender mejor el comportamiento de la red bajo condiciones de interferencia.
- **Presentación de Resultados:** Preparación y presentación de los hallazgos a través de presentaciones y documentos, destacando los efectos observados y las implicaciones para la red Wi-Fi en el contexto del análisis de ataques de jamming.

2 CAPÍTULO II

2.1 MARCO TEÓRICO

2.1.1 REDES INALÁMBRICAS EN LA BANDA DE 2.4 GHZ

Hoy en día es de mucho conocimiento el gran aporte que tiene la banda de 2.4GHz, debido a que en la actualidad surgen tendencias muy grandes dentro del entorno de las comunicaciones inalámbricas, por ende, todos hemos escuchado sobre el alcance de las bandas de frecuencia tanto de, 2.4GHz y 5GHz, anteriormente estas tenían el nombre de WiFi N y WiFi AC, sin embargo, en el 2018 WIFI Alliance cambio estos nombres por nomenclaturas sencillas como: Wi-Fi 4, Wi-Fi 5 y Wi-Fi 6.

Esta banda es considerada una de las más antiguas, e incluso la mayoría de los routers que se encuentran en el mercado la han incorporado, debido a que va desde 2.412 MHz hasta los 2.472 MHz dividendos en 13 canales y cada uno va de 20MHz, tal y como se muestra en la figura 1 a su vez se añadió un canal más (canal 14), este queda alejado del espectro de frecuencia Wi-Fi de 2.4 GHz, por ende no todos los dispositivos son compatibles con dicho canal, este opera desde los 2.484 MHz hasta los 2.495 MH.

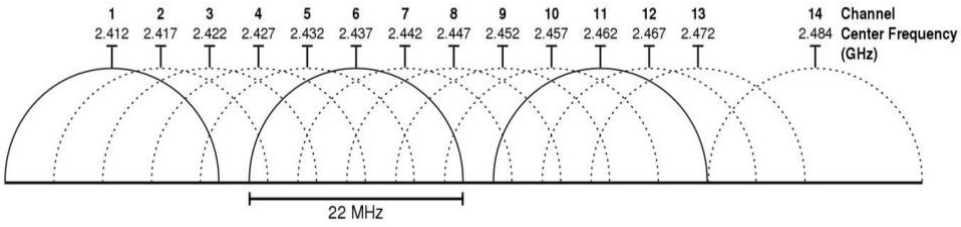


Ilustración 1.- Canales de bandas inalámbricas

Esta banda es la más usada en la actualidad, debido a que es compatible con otros dispositivos, esto se debe a que, a todos los dispositivos de WIFI tienen acceso a esta banda, mientras que otros aun no son compatibles , como lo es el caso de la banda de 5GHz, de tal modo que la banda de 2.4GHz es más saturada, puesto que la mayoría de dispositivos ya sea mandos o teléfonos inalámbricos funcionan en esta misma banda, cabe recalcar que no significa que compartan tecnología, debido

a que cada dispositivo se desarrolla de acuerdo a sus beneficios, pero con respecto a el estudio de sus radiofrecuencias todos se encuentran bajo la misma proyección.

2.1.1.1 CARACTERÍSTICAS DE LA BANDA DE 2.4 GHZ

ISM o como sus siglas lo indican “Banda de Frecuencia” ya sea para el área científica, medica e industrial, es considera una banda basada en el estudio de frecuencias de microondas o radios, el cual son destinadas para equipos científicos y médicos entre otros que basen su estudio en radiofrecuencias, en equipos industriales ya sean maquinas MRI basan su estudio mediante un radiotelescopio en frecuencias ISM.

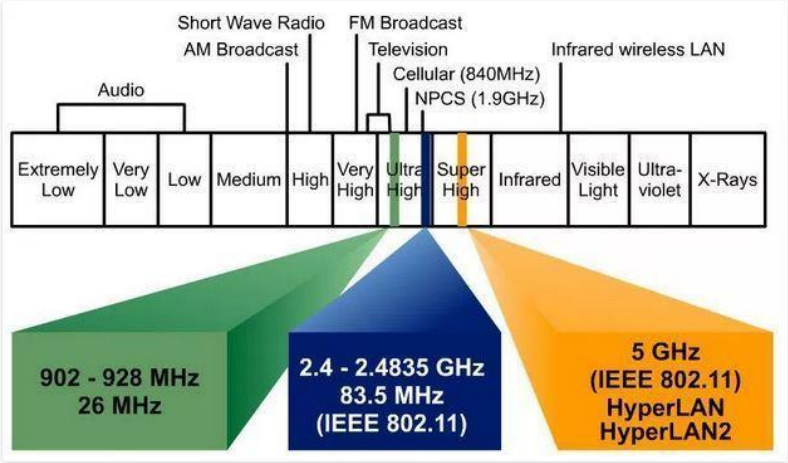


Ilustración 2.- Características de la banda 2.4 GHz

La gran mayoría de dispositivos usados en las telecomunicaciones han funcionado a frecuencias más bajas que 2.4GHz, teniendo otros dispositivos que solo tienden a funcionar en un rango de determinado, por ello IMS, tiene como uno de los objetivos el reducir las interferencias, significa que mientras se use un enrutador inalámbrico o un celular durante el mismo tiempo no se obtendrá ninguna interferencia entre los dos. Es importante conocer que 2.4Ghz no es la única frecuencia ISM, sin embargo, es considera la más común debido a que en los dispositivos no hace falta su autorización, existiendo otras frecuencias ISM que son igual de altas como la 24.125 GHz o hasta incluso más bajas como 13.56MHz, esto dependerá de su ubicación y de la distribución de radio con gran flexibilidad

La distribución de dichas frecuencias de radio IMS se encuentra estipuladas por la ITU (Unión Internacional de Telecomunicaciones). La ITU ha documentado a

través de una tabla de distribución mundial de ISM que esta puede varia ligeramente dependiendo de su ubicación y por lo tanto, los usuarios deben aceptar las regulaciones y términos para poder garantizar la seguridad.

Estas bandas son usadas en varias tecnologías entre ellas:

- Redes inalámbricas: Se utiliza en redes como WIFI y Bluetooth, de esta manera permite la transmisión de información entre dispositivos que se encuentren a distancias largas, brindándole a el usuario una gran flexibilidad y alcance para los dispositivos de conexiones inalámbricas
- Control Remoto: Es utilizado para el control de dispositivos electrónicos, ya sean, DVD, televisores, entre otros dispositivos de uso doméstico, ofreciendo a el usuario la capacidad de poder tener el control de cada artefacto desde cualquier lugar sin la necesidad de contar con cables e instalaciones adicionales.
- Automatización industrial: Se utiliza en industrias como minerías y agricultura entre otras con el objetivo de transmitir informaciones entre varios equipamientos industriales sin necesidad de cables, reduciendo el costo de proyectos e instalaciones complejas

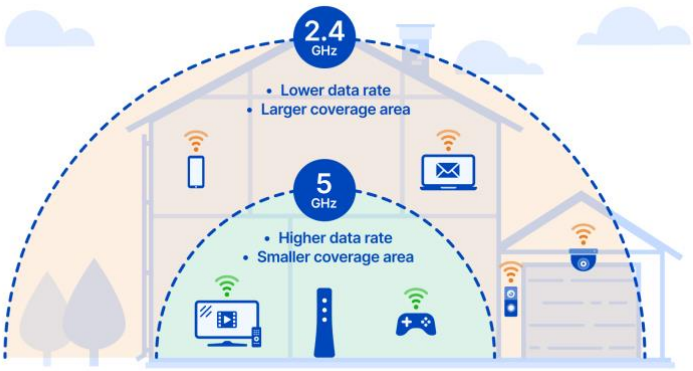


Ilustración 3.- Características de la banda 2.4 y 5 GHz

2.1.1.1.1 VENTAJAS

- **Alta confiabilidad:** Las bandas ISM son consideradas confiables, manteniendo un diseño robusto frente a interferencias externas

- **Bajo costo:** La tecnología ISM es mucho más barata que otras al momento de comunicarse, permitiendo reducir gastos generales que son utilizados para la implementación del sistema

- **Fácil instalación:** el diseño estándar y simple que abarca el sistema hace que este sea fácil de instalarlo y a su vez configurarlo, de esta manera no hace falta contratar personal especializado y tampoco realizar cambios brucos entorno a la estructura de la empresa

2.1.1.1.2 DESVENTAJAS

- **Interferencia externa:** las señales emitidas por bandas ISM pueden llegar hacer interferidas por otros equipos electromagnéticos ya sean; luces fluorescentes u horno microondas, entre equipos que se encuentren situados en torno a las antenas, dificultando el funcionamiento del sistema.
- **Distancia limitada**. La conexión que existe entre las bandas ISM tiene un alcance limite debido a la interferencia ambiental el cual prevale en muchos entornos por lo tanto no siempre cubre con grandes distancias.

Ilustración 4.- Comparación entre la banda de 2.4 y 5 GHz

2.1.2 PROTOCOLOS Y ESTÁNDARES

2.1.2.1 ESTÁNDARES

2.1.2.1.1 IEEE 802.11 (Wi-Fi)

Este estándar 802.11 establece los niveles inferiores del modelo OSI para el desarrollo de conexiones inalámbricas, el cual utilizan ondas electromagnéticas, como, por ejemplo, en el caso de la capa física (a veces abreviada capa PHY) esta ofrece 3 tipos de codificación. La capa de enlace de datos cuenta con dos subcapas: control de acceso al medio (MAC) y control de enlace lógico (LLC).

La capa física es definida como el ejemplo de modulaciones de ondas de radio y de señalización para poder transmitir datos, a diferencia de la capa de enlace de datos en donde, se define la interfaz entre la capa física y el bus de equipos, este es considerado como el método de acceso utilizado en el estándar Ethernet, y entre las estaciones de la red. En realidad, el estándar 802.11 consta con 3 capas físicas, están tienden a establecer los modos de transmisión alternativos tal y como se muestra en la figura 5:

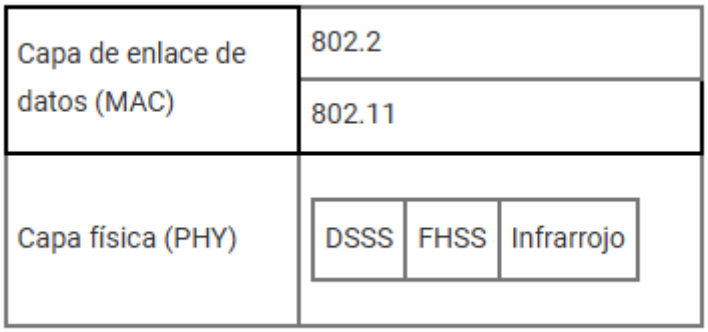


Ilustración 5.- Modos de transmisión alternativos de las Capas Física y Enlace de Datos

Por lo tanto cualquier protocolo que forme parte del nivel superior se puede utilizar en redes inalámbricas wifi y de la misma manera pueden utilizarse en una red Ethernet.

- **Descripción**: Es considerado es estándar para redes inalámbricas de área local (WLAN).
- **Frecuencia**: Utiliza una banda de 2.4 GHz y bandas (como 5 GHz).
- **Modulación**: Usa modulaciones OFDM (Orthogonal Frequency-Division Multiplexing) y DSSS (Direct Sequence Spread Spectrum).
- **Versiones**: 802.11b/g/n operan en la banda de 2.4 GHz.
    - **802.11b**: limite 11 Mbps.
    - **802.11g**: limite 54 Mbps.
    - **802.11n**: limite 600 Mbps (con MIMO).

2.1.2.1.2 BLUETOOTH

- **Descripción**: Estándar para comunicación inalámbrica, pero a corta distancia.
- **Frecuencia**: Opera en bandas de 2.4 GHz.
- **Modulación**: Usa modulaciones FHSS (Frequency-Hopping Spread Spectrum).
- **Versiones**: Bluetooth de 1.0 hasta 5.0
    - **Bluetooth 4.0**: Incluye Bluetooth Low Energy (BLE), en bajo consumo de energía.

2.1.2.1.3 ZIGBEE

- **Descripción**: Es un estándar utilizado para sensores y aplicaciones de automatización de un hogar.
- **Frecuencia**: Opera en la banda de 2.4 GHz
- **Modulación**: Utiliza DSSS.
- **Velocidad**: tiene una velocidad de hasta 250 kbps.

2.1.2.1.4 Z-WAVE

- **Descripción**: se utiliza en tecnologías basadas en automatización del hogar.
- **Frecuencia**: Utiliza bandas diferentes, es decir, depende de la región (como 908.42 MHz en EE.UU.)

2.1.2.1.5 THREAD

- **Descripción**: Protocolo de la red basado en IPv6
- **Frecuencia**: Opera en bandas de 2.4 GHz.
- **Modulación**: Utiliza DSSS.
- **Velocidad**: límite de 250 kbps.

2.1.2.2 ESTÁNDARES WIFI

El estándar 802.11 es considerado el primer estándar, permitiendo un ancho de banda de 1 a 2 Mbps, este estándar original ha sido modificado para poder optimizar el ancho de banda (incluyendo estándares 802.11a, 802.11b y 802.11g, denominados estándares físicos 802.11) o también para especificar los componentes de mejor forma con el objetivo de garantizar una mayor seguridad y compatibilidad a continuación se muestran las diferentes modificaciones del estándar 802.11 y sus significados:

Estándar	***Nombre***	***Descripción***
802.11ª	*Wi-Fi 2*	*El estándar 802.11 (denominado wifi 5) permite un ancho de banda superior, por lo tanto, el rendimiento máximo es de 54 Mbps aunque en sus diferentes prácticas es de 30 Mpbs. Este estándar 802.11a contiene ocho canales de radio en la banda de frecuencia de 5 GHz.*
802.11b	*Wi-Fi 1*	*El estándar 802.11 en la actualidad es el más utilizado debido a que ofrece un rendimiento máximo de 11 Mpbs (6 Mpbs en la práctica) por lo tanto llega a tener un alcance de hasta 300 metros en espacios abiertos y utiliza un rango de frecuencia de 2,4 GHz con 3 canales de radio disponibles.*
802.11c	*Combinación del 802.11 y el 802.1d*	*El estándar combinado 802.11c, este no ofrece tanto interés para el usuario, debido a que es considerada una versión que ha sido modificada del estándar 802.1d permitiendo combinar el 802.1d con dispositivos compatibles 802.11 (en la capa de enlace de datos).*
802.11d	*Internacionalización*	*El estándar 802.11d es considero el complemento del estándar 802.11 que se ha considerado la idea de poder permitir el uso internacional de las redes 802.11 locales. Este estándar permite el intercambio de*

		información en rangos de frecuencia según se les permite en su país.
802.11e	*Mejora de la calidad del servicio*	*El estándar 802.11e se encuentra destinado a el mejoramiento de la calidad de servicio en los niveles de la capa de enlace de datos. Tiene como objetivo del estándar la definición de los requisitos de varios paquetes en cuanto al ancho de banda y su retardo de transmisión para mejoras de transmisiones en audio y vídeo.*
802.11f	*Itinerancia*	*El 802.11f es recomendada para proveedores que mantengan puntos de acceso permitiendo que los productos sean compatibles, utilizando el protocolo IAPP el cual, permite a un usuario itinerante modificarse de un punto de acceso a otro mientras se mueve sin importar las marcas de puntos de acceso se utilizan dentro infraestructura de la red.*
802.11g	*Wi-Fi 3*	*El estándar 802.11g maneja un ancho de banda elevado, es decir, mantiene un rendimiento total máximo de 54 Mbps, sin embargo en sus prácticas es hasta de 30 Mbps, en el rango de 2,4 GHz. El estándar 802.11g es considerado compatible con el estándar anterior, el 802.11b, esto significa que los dispositivos admiten el estándar 802.11g también llegan a funcionar con el 802.11b*
802.11n	*Wi-Fi 4*	*Utiliza de manera simultánea las bandas de 2,4 GHz y 5GHz. alcanzando velocidades de hasta 600 Mbps en conexiones de tres antenas. Fue dado a conocer en 2009 y fue el primero en emplear la tecnología MIMO permitiendo el uso de varios canales al mismo. ("IEEE 802.11: qué es, WiFi, características, para qué sirve - CCM")*
802.11ac	*Wi-Fi 5*	*Se estandarizó en 2014 y su función es únicamente en la banda de 5 GHz proporcionando una velocidad de 433*

		Mbps en conexión de 1 antena y de hasta 1.300 Mbps. en conexiones 3x3, es decir ,3 antenas.
802.11ax	*Wi-Fi 6*	*Se lanzó en 2019, operando en las frecuencias de 2,4 GHz y 5 GHz, soportando conexiones de 4 y 8 antenas y ofreciendo un avance con velocidades de hasta 10 Gbps.*
802.11i		*El estándar **802.11i** se encuentra destinado para la mejora de seguridad en la transferencia de datos, administrando estos con claves. Este estándar es basado en el **AES** (estándar de cifrado avanzado) y permite transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g. ("Estándar IEEE 802.11 - Sutori")*
802.11Ir		*El estándar 802.11r fue elaborado para que se puedan utilizar las señales infrarrojas, por lo tanto, este estándar se ha vuelto tecnológicamente obsoleto.*
802.11j		*El estándar 802.11j es utilizado para la regulación japonesa lo que el 802.11h es para la regulación europea. ("Introducción a Wi-Fi (802.11) - RedTauros")*

Tabla 1.- Estándares de WiFi

2.1.2.3 REGULACIONES Y RESTRICCIONES EN LA BANDA ISM

Las bandas ISM se encuentran sujetas a regulaciones y restricciones, puesto que se utilizan para la transmisión de datos durante una amplia variedad de dispositivos electrónicos, desde un horno microondas hasta los teléfonos inalámbricos. A continuaciones se mencionarán sobre las reglas y restricciones más importantes asociadas con su uso

- Los equipos que operan dentro de esta banda deben cumplir con varios requisitos por el regulador local, incluyendo límites máximos de la potencia que se va a transmitir, los cambios entre emisiones y el tiempo de transmisión
- Algunas regiones tienen límites para el uso de esta banda, entre estas restricciones está el tipo y numero de dispositivos que se les permite, por lo tanto, algunas regiones no permiten transmisiones fuera de su territorio nacional y por lo tanto deben cumplir estas normas locales
- Las emisiones de estas bandas no deben interferir con otras de forma legal dentro de su rango asignado, debido a que, si se detecta una interferencia inusual se suspende temporalmente hasta encontrar la causa del problema.
- El usuario final es responsable del mantenimiento y actualización periódica de todos los equipos que operan en la banda ISM garantizando su conformidad con las regulaciones vigentes, esto debe incluir prácticas periódicas para comprobar los límites máximos permitidos por la ley. ("Banda ISM - Qué es, definición y concepto - Muy Tecnológicos")

2.1.2.4 ¿EN QUÉ CONSISTE EL RANGO Y FLUJO DE DATOS?

Los estándares 802.11a, 802.11b y 802.11g, son considerados como "estándares físicos", y son modificaciones del estándar 802.11, el cual, operan de modos distintos, lo que permite alcanzar diferentes velocidades en la transferencia de datos dependiendo sus rangos, tal y como se muestra en la siguiente tabla 2

Estándar	***Frecuencia***	***Velocidad***	***Rango***
wifi A (802.11a)	*5 GHz*	*54 Mbit/s*	*10 m*
wifi B (802.11b)	*2.4 GHz*	*11 Mbit/s*	*100 m*
wifi G (802.11b)	*2.4 GHz*	*54 Mbit/s*	*100 m*

Tabla 2.- Modos de operación del estándar 802.11

2.1.2.4.1 802.11a

El estándar 802.11 en teoría mantiene un flujo de datos de 54 Mbps, este a su vez, es cinco veces el del 802.11b y solo tiene un rango de 30 metros aproximadamente.

El estándar 802.11a es basado en la tecnología llamada OFDM (*multiplexación por división de frecuencias ortogonales*). (“multiplexacion por division de division de frecuencias”)

Velocidad hipotética	***Rango***
54 Mbit/s	*10 m*
48 Mbit/s	*17 m*
36 Mbit/s	*25 m*
24 Mbit/s	*30 m*
12 Mbit/s	*50 m*
6 Mbit/s	*70 m*

Tabla 3.- Velocidad y rango del estándar 802.11a

2.1.2.4.2 802.11b

El estándar 802.11b nos permite un máximo de transferencia de envió de datos de 11 Mbps entre un rango de 100 metros aproximadamente en ambientes que se encuentran cerrados y de más de 200 ms al aire libre (puede ser más que ese espacio mediante el uso de antenas direccionales).

Velocidad hipotética	***Rango (en ambientes cerrados)***	***Rango (al aire libre)***
11 Mbit/s	*50 m*	*200 m*
5,5Mbit/s	*75 m*	*300 m*
2Mbit/s	*100 m*	*400 m*
1Mbit/s	*150 m*	*500 m*

Tabla 4.- Velocidad y rango del estándar 802.11b

2.1.2.4.3 802.11g

El estándar 802.11g también es capaz de transferir datos de 54 Mbps en rangos comparables a los del estándar 802.11b y debido a que el estándar 802.11g utiliza una frecuencia de 2.4 GHz con codificación OFDM, igual es compatible con los dispositivos 802.11b excepto dispositivos más antiguos

Velocidad hipotética	*Rango (en ambientes cerrados)*	*Rango (al aire libre)*
54 Mbit/s	*27 m*	*75 m*
48 Mbit/s	*29 m*	*100 m*
36 Mbit/s	*30 m*	*120 m*
24 Mbit/s	*42 m*	*140 m*

Tabla 5.- Velocidad y rango del estándar 802.11g

2.1.3 PORTAPACK H2

El Portapack H2 es un dispositivo el cual permite la conexión a una plataforma de software-defined radio (SDR) como el HackRF One. A continuación, se dará a conocer algunas funcionalidad y características del Portapack H2:

1. **Compatibilidad**: Se conecta al HackRF One para proporcionar una interfaz gráfica y capacidades autónomas, sin necesidad de una computadora.
2. **Pantalla y Controles**: Incluye una pantalla táctil LCD y controles físicos, permitiendo un uso más intuitivo y portátil.
3. **Software y Firmware**: Funciona con el firmware "Havoc" que ofrece una amplia gama de aplicaciones, como análisis de espectro, decodificación de señales, y modos de transmisión específicos.

2.1.3.1 MODOS DE OPERACIÓN

4. **Transmisión**: Permite transmitir señales en una amplia gama de frecuencias (1 MHz a 6 GHz).
5. **Recepción**: Puede recibir y demodular señales en el mismo rango de frecuencias.
6. **Playback y Grabación**: Permite grabar señales de radio para su posterior reproducción.

2.1.3.2 APLICACIONES

- **Radioaficionados**: Usado para experimentar con diferentes modos de radioaficionado.

- **Seguridad y Análisis**: Utilizado para probar y analizar señales de radiofrecuencia en aplicaciones de seguridad y telecomunicaciones.
- **Educación y Experimentación**: Ideal para proyectos educativos y de investigación en el campo de la radiofrecuencia y las comunicaciones.

El Portapack H2, en conjunto con el HackRF One, es una herramienta poderosa y flexible para entusiastas de la radiofrecuencia, ingenieros y educadores.

2.1.4 *TÉCNICAS DE DETECCIÓN DE JAMMING*

Para detectar y protegerse del jamming, lo más opcional es detectar la señal de interferencia mediante los dispositivos GPS y transmitir una alerta inmediata al servidor, para seguir un protocolo de acción. ("¿Qué es el jamming GPS y cómo evitarlo? - Delta Tracking")

Si bien las aplicaciones de rastreo satelital pueden detectar la presencia de un jammer, estas dependerán de la información que se transmita a los dispositivos GPS. Adicionalmente es recomienda do instalar los GPS en un lugar oculto, para dificultar la detección física, sin duda el uso del **jamming** tiene como objetivo un reto importante para las empresas de transporte, debido a que no existe ninguna tecnología que sea 100% inmune a los jammers.

2.1.4.1 MÉTODOS DE DETECCIÓN DE ANOMALÍAS

En el caso de los entornos IoT, ha dado como resultado avances en nuestra vida cotidiana debido a las facilidades que nos llegan a ofrecer los dispositivos, sin embargo, su utilización también expone desafíos para la seguridad de la información con la que se trabaja, algunas de las herramientas que se han utilizado para mantener seguros este entorno, son los sistemas de detección de anomalías, estos analizan e identifican patrones inusuales en los datos enviados por los dispositivos IoT, por ende, el desarrollo de algoritmos para la detección de anomalías han encajado con las tecnologías, debido a que muchos procesos utilizan técnicas de Machine Learning durante sus procesos de predicción, etc. Es un método de trabajo que está normalizado, con el fin de seguir ampliando este campo para el perfeccionamiento en el uso de técnicas con redes neuronales. Detectar

anomalías en señales de jamming se considera crucial al momento de mantener la integridad de las comunicaciones.

A continuación, se presentan métodos comunes utilizados para la detección de anomalías en jamming:

2.1.4.1.1 ANÁLISIS ESPECTRAL

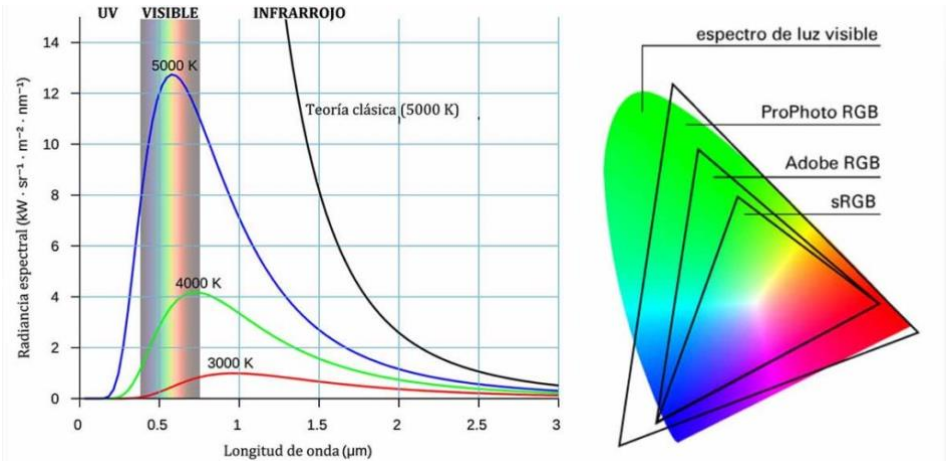


Ilustración 6.- Análisis Espectral

- **Espectrogramas:** Permiten la simulación de cómo la potencia espectral tiende a variar con el tiempo, revelando consigo patrones anómalos de interferencia.
- **Saltos de frecuencia:** Identifica cambios inusuales o rápidos dependiendo de la frecuencia portadora.

2.1.4.1.2 ANÁLISIS ESTADÍSTICO

- **Distribución de potencia:** Comparación de datos correspondientes a la distribución de potencia medida bajo condiciones normales que llegan a mostrarse mediante desviaciones causadas por el jamming.
- **Pruebas de hipótesis:** Realizar pruebas estadísticas con el fin de verificar si los parámetros de la señal ya sea la media y la varianza se encuentran alterados significativamente.

2.1.4.1.3 TÉCNICAS DE MACHINE LEARNING

- **Aprendizaje no supervisado:** implementar algoritmos como k-means o clustering espectral, de esta manera se identifican agrupaciones inusuales de señales que podrían indicar jamming.
- **Aprendizaje supervisado:** presentación de modelos con datos etiquetados de jamming y señales normales.

2.1.4.1.4 MÉTODOS DE REDES NEURONALES

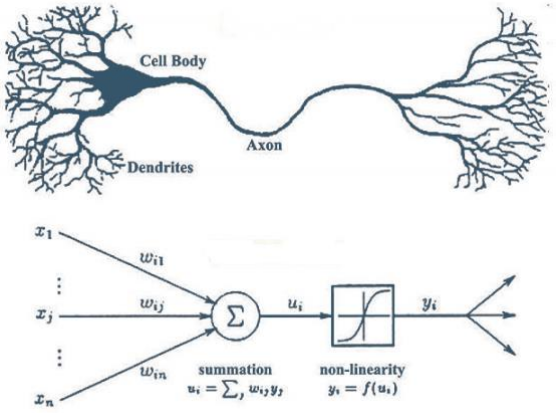


Ilustración 7.- Método de Redes Neuronales

- **Redes Neuronales Recurrentes:** Este método permite la detección de patrones temporales que puedan ser indicativos de jamming.
- **Redes Neuronales Convolucionales:** Este método permite la detección de caracteres espaciales en las señales que podrían indicar jamming.

2.1.4.1.5 TÉCNICAS DE PROCESAMIENTO ADAPTATIVO:

- **Filtrado adaptativo:** Ajuste dinámico mediante los coeficientes del filtro para adaptarse a condiciones cambiantes entorno a la señal, ayudando a mitigar el efecto del jamming y facilitando la detección de anomalías.

2.1.4.1.6 ANÁLISIS DE PATRONES TEMPORALES Y ESPACIALES

- **Correlación temporal y espacial:** Comparar la señal receptada con la esperada en diferentes momentos mediante ubicaciones

identificando algunas discrepancias que podría ser causada por jamming.

2.1.4.2 DETECCIÓN BASADA EN PROTOCOLO

La detección basada en protocolos se basa en el análisis y monitoreo del comportamiento ante los protocolos de comunicación con el objetivo de identificar posibles pruebas de jamming o interferencia maliciosa, a continuación, se muestran las técnicas utilizadas mediante la creación de modelos o técnicas de mitigación para contrarrestar estos ataques.

2.1.4.2.1 MONITOREO DE INTEGRIDAD DEL PROTOCOLO:

- **Verificación de Secuencias:** Existen sistemas de detección, y con ellos se puede llegar a verificar si las secuencias de los mensajes y respuestas entre los nodos de la red se encuentran con patrones o alteraciones inesperadas indicando los intentos de jamming.
- **Comprobación de Temporización:** Análisis de tiempos de respuesta y la sincronización de datos para detectar anomalías el cual son causadas por interferencia.

2.1.4.2.2 ANÁLISIS DE PATRONES DE TRÁFICO:

- **Flujos de Datos:** Examinar los patrones de tráfico de red con el objetivo de identificar cambios inusuales entorno a la cantidad o datos transmitidos, indicando intrusiones, a continuación en la figura 8 se muestra el traslado de información y congestión de la red correspondiente a el flujo de datos.

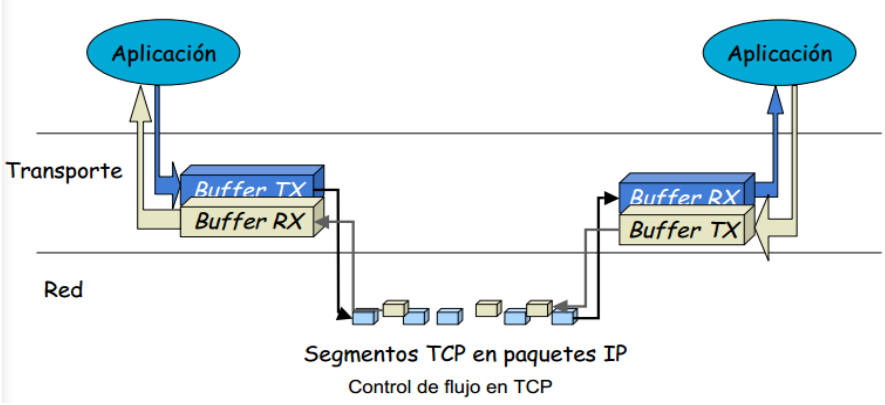


Ilustración 8.- Análisis de patrones de Tráfico

2.1.4.2.3 PRUEBAS DE CONSISTENCIA Y AUTENTICACIÓN:

- **Integridad de los Mensajes:** Verificar la autenticidad de los mensajes que son transmitidos utilizando firmas digitales o métodos criptográficos.
- **Control de Acceso:** Garantizar que los dispositivos estén autorizados ya su vez solo estos cuenten con acceso a la red para participar en la comunicación, reduciendo agentes maliciosos.

2.1.4.2.4 RESPUESTA Y MITIGACIÓN AUTOMÁTICAS:

- **Sistemas de Alerta:** Configurar los sistemas que generen alertas de manera automática ante la detección de anomalías, con el fin de permitir respuestas rápidas y mitigación proactiva, ante posibles ataques.
- **Reconfiguración Dinámica:** permite la Implementación de protocolos y sistemas que se ajustan a la configuración de la red.

2.1.4.2.5 ANÁLISIS DE TRÁFICO BASADO EN COMPORTAMIENTO:

- **Modelos de Comportamiento:** Utilizar técnicas de aprendizaje para la creación de modelos de comportamiento normal desplazados en la red detectando desviaciones significativas.

2.1.4.2.6 INTEGRACIÓN DE CAPAS DE SEGURIDAD:

- **Firewalls y Filtros:** Permite la implementación de firewalls o filtros que puedan bloquear el tráfico malicioso antes de que afecte las operaciones normales de la red.

Estas técnicas y modelos de detección son basados en protocolos para proteger las redes contra pruebas de jamming garantizando la integridad y autenticidad en función a los protocolos de comunicación utilizados.

2.1.4.3 ESTRATEGIAS DE MITIGACIÓN

2.1.4.3.1 FRECUENCIA HOPPING SPREAD SPECTRUM (FHSS)

FHSS es una técnica de modulación en espectro ensanchado en donde la señal es emitida sobre una serie de radio frecuencias y aparentemente tienden a ser aleatorias, estas modulaciones van saltando de frecuencia en frecuencia sincrónicamente mediante un transmisor, a su vez los receptores que no se encuentran autorizados escucharán la señal ininteligible, esta es una característica que convierte a esta modulación una técnica ideal para aplicaciones PLC. Esta tecnología de transmisión es utilizada en redes inalámbricas basada en la técnica de espectro ensanchado realizando saltos hacia la portadora en frecuencia, en este método dicha señal es modulada como una señal portadora, pero en una banda estrecha, la cual tiende a saltar en secuencias pseudoaleatoria. El uso de esta tecnología de salto en frecuencia es considerado como una solución altamente válida con el objetivo de poder evitar interferencias o distorsiones, por lo tanto, aumenta la capacidad de la señal, es capaz de mejorar la relación señal a ruido (SNR) y su gran eficiencia del ancho de banda de la comunicación por ende la comunicación salta en frecuencia es un tanto difícil llegar a interceptar la señal, aumentando así la privacidad entorno a su transmisión, en la figura 9 nos da a conocer las combinación entorno a las señales demostrada por diferentes fuentes para que estén dentro de un ancho de banda mayor, de esta manera evitaremos escuchar interferencias.

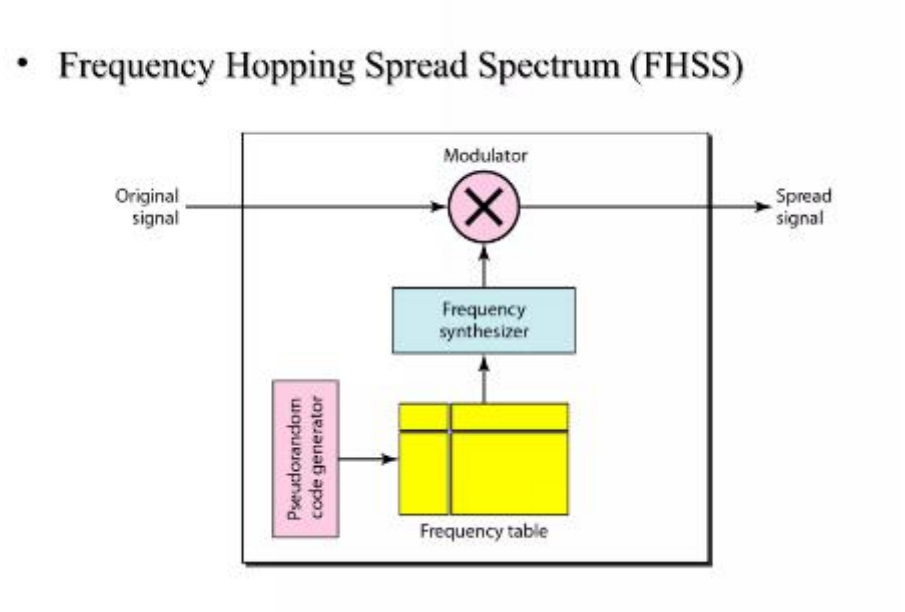


Ilustración 9.- FHSS

Esto también sucede debido a que ciertos números de canales se encuentran completamente reservados para las señales FH y dicha señal pasa de frecuencias a frecuencias pero en intervalos fijos, de esta manera, el transmisor es operado bajo un canal en un determinado tiempo y su números de bits son transmitidos usando el esquema de codificación, cabe recalcar que cada intervalo maneja una frecuencia seleccionada mientras el receptor es capaz de capturar varios mensajes el cual viajan en sincronismo, y en caso de existir un receptor no deseado, existe la posibilidad de que sea un impulso de ruido pero en corta duración.

Esta técnica fue presentada en la versión inicial de IEEE 802.11 especificando que las velocidades de transmisión deben ir de 1 y 2 Mbps, por lo tanto, debe operarse en un rango de frecuencias de 2.4 GHz, y para el funcionamiento de esta, la banda de frecuencias de 2.4 GHz es dividida en 79 canales de 1 MHz de ancho cada uno, dividiendo el flujo de tiempo en segmentos pequeños llamados *Hop Times*, tal y como se muestra en la figura 10.

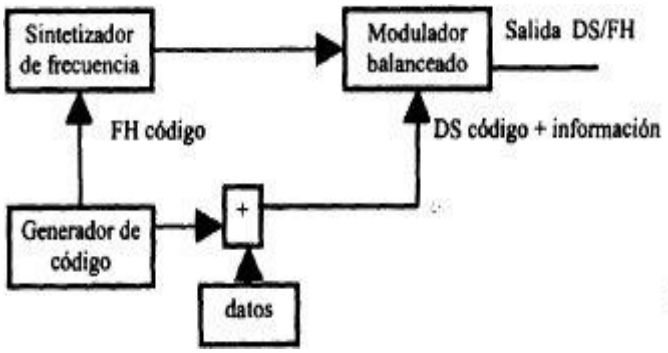


Ilustración 10.- Versión inicial de IEEE 802.11

Una manera muy común de explicar el espectro expandido es mediante una serie de trenes saliendo de una estación en un mismo tiempo, la carga que tiende a llevar cada tren es distribuida relativamente para todos los trenes , al llegar a su punto de destino, dicha carga es restada en cada tres, por lo tanto las duplicaciones de los datos llegan hacer comunes en el espectro, de modo que cuando estos datos falla en su envió la redundancia inherente proporciona la capacidad de interpretar el mensaje, con una arquitectura FHSS estos trenes salen de una manera diferente, no secuencialmente de tren 2 al tren N y los trenes que encuentran interferencias no se envían hasta que la interferencia cesa, a continuación en la figura 11 se muestran los intervalos de frecuencias manejados por FHSS.

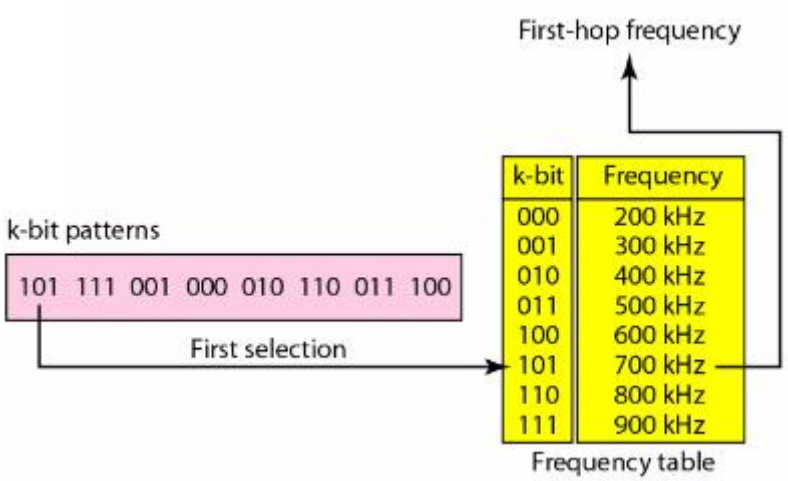


Ilustración 11.- Intervalos de frecuencias manejados por FHSS

El receptor FHSS está compuesto por:

- Amplificador de banda ancha
- Mezclador convencional

- Oscilador local sintetizado
- Amplificado de FI, este permite la reconstrucción de la señal FKS

2.1.4.3.2 SPREAD SPECTRUM

El Spread Spectrum fue desarrollado durante la época de los 50s, inicialmente limitado a aplicaciones militares, en 1985 y tras cuatro años de estudios, el FCC (Federal Communication Commission) encargada de regular y poder administrar el entorno de las telecomunicaciones, fue capaz de autorizar su uso para varias aplicaciones (CIVILES) asignando bandas IMS (Industria, Medica y Científica) basadas en el Spread Spectrum, las bandas IMS es "unlicensed" consiste en la asignación sin licencia en que FCC simplemente asigna y establece directrices, pero cabe recalcar que no decide a quien transmitir.

El Spread Spectrum se puede traducir como una técnica que se ha generado y utilizado en los sectores de la defensa por propiedades en cuanto a la inmunidad de interferencias y a las posibilidades que nos brinda por ser encriptada. En la figura 12 se muestra un esquema referente a el extracto analizado basado en una técnica de espectro ensanchado en la comunicación con el objetivo de garantizar una transmisión segura, dicho método utiliza el aire como medio y extiende el ancho de banda para poder crear una capa protectora para las señales, de esta manera, reduce el riesgo de interferencia. El "código extendido" es considerada una serie de números el cual van modelados y amplían el ancho de banda de una señal original, esta técnica se utiliza en situaciones en las que la transmisión segura es crucial.

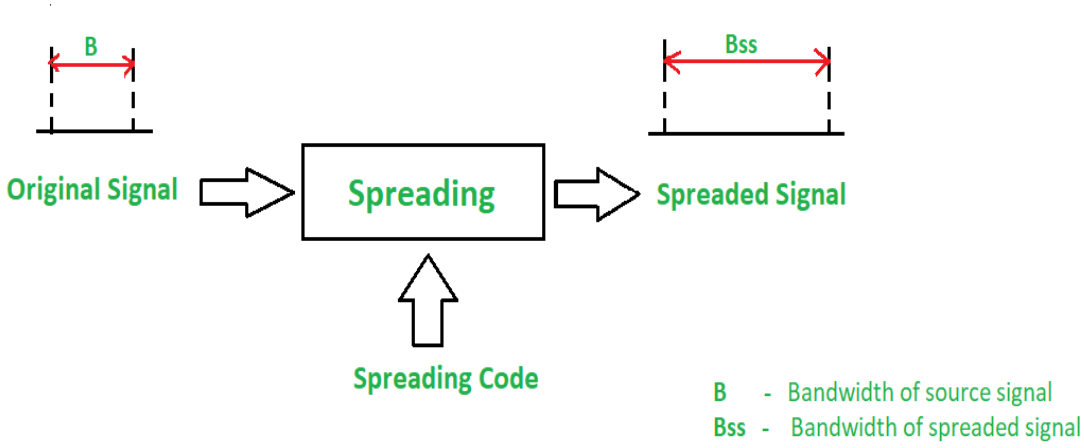


Ilustración 12.- Spread Spectrum

El sistema Spread Spectrum se basa en una señal transmitida, el cual esta es propagada en una banda por frecuencias amplias, aunque estas señales pueden coexistir mediante señales en bandas estrechas, pero añadiendo un ligero incremento, como un ruido de fondo, esta técnica es la transformación reversible de la señal, pero de forma en que la energía de esta se dispersa entre una banda mayor que la que se ocupaba originalmente.

Entre las características del Spread Spectrum se encuentran las siguientes:

- La transmisión de señal tiende hacer muy resistente a las interferencias de bandas estrecha basados en otros tipos de transmisión
- Es difícil detectar la señal, debido a que su nivel de potencia llega a quedar reducido por la dispersión espectral y en el caso de ser detectada, la transmisión es ininteligible para quien no conozca la señal
- La transmisión simultanea es posible mediante varias señales por el mismo medio, debido a que siempre que se cumplas las condiciones, entre ellas, que la señal pseudoaleatoria generada sean encerradas unas a otras, dicha transmisión será resistente a las interferencias de un canal sobre otro.

2.1.4.3.2.1 APLICACIÓN

El Spread Spectrum mediante la técnica de transmisión de señales tiene como propósito la expansión de la señal original con un ancho de banda, este ancho debe

ser mucho mayor al que se necesita para que sea transmitida, dicha técnica ha sido participe de propuestas de proyectos que han sido de suma importancia en la industria de la electrónica y las telecomunicaciones.

Una de las aplicaciones comunes del Spread Spectrum es en las comunicaciones inalámbricas, debido a que buscan la expansión de la señal original, de esta manera, se reduce la probabilidad de las interferencias y, por ende, mejora la calidad de las señales. Esto es importante para los entornos que manejan varias señales de radio diferentes, de las redes WiFi.

Otra de las aplicaciones importantes del Spread Spectrum es basado en sistemas de posicionamiento global, o también conocido como GPS. En este caso, las señales se extienden mediante el ancho de banda este debe ser mucho mayor para mejorar la precisión de la ubicación, esta aplicación también trae consigo el uso para los sistemas de radar con el objetivo de detectar señales en ambientes ruidosos. En la industria militar, el Spread Spectrum se utiliza para poder evitar todo tipo de interferencia y la interceptación de señales en comunicaciones, estas muchas veces son encriptadas, a su vez ayuda a la ubicación de misiles entre otras.

2.1.4.3.2.2 VENTAJAS

Las propiedades ventajosas del espectro ensanchado más importante conociendo el concepto de CDMA (Acceso múltiple por división de código) es la gran capacidad de acceso múltiple, por ende, el rechazo de la interferencia multitrayectoria, el rechazo hacia la banda angosta, y su entorno en la seguridad / privacidad de la comunicación, la baja probabilidad de intersección, no brinda como tal, múltiples usuarios usando un canal al mismo tiempo con múltiples señales DS traslapándose en frecuencia y el tiempo.

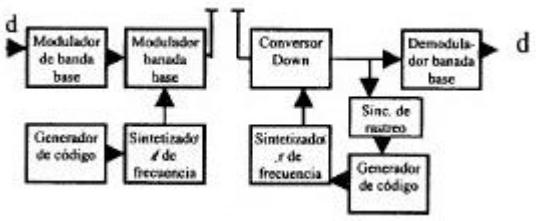


Ilustración 13.- Ventajas del Espectro Ensanchado

En el receptor las demodulaciones coherentes son utilizar para restar la modulación de código, esta modulación permite la concentración en la potencia del usuario deseado y el ancho de banda de la información, si las correlaciones cruzadas entre el código deseado y los códigos interferentes son pequeñas, la detección coherente solo tendrá una parte pequeña de la potencia de las señales interferentes dentro del ancho de banda. Si el patrón de código tiene una función de autocorrelación ideal, entonces dicha función de correlación es nula fuera de los intervalos (-To,To) donde To es la duración de un chip. Esto significa que, si las señales deseadas y una versión que es retrasada a partir de más de 2To son recibidas y la demodulación coherente tratará a la versión retrasada como señal interferente, colocando una parte pequeña de la potencia en el ancho de banda de dicha información.

2.1.4.4 PROTOCOLOS Y ALGORITMOS DE MITIGACIÓN

Las capacidades de mitigación hacen referencia a la disposición de un equipo de seguridad con la finalidad de detectar y resolver los diferentes ataques a medida que surgen. Esto puede significar la identificación del tráfico malicioso y el proceso de eliminación de malware, o a su vez considerar la idea de estar en contacto con tu proveedor de seguridad administrado. De esta manera, la mitigación es una planificación eficaz para que sean conscientes de su capacidad con el fin de combatir las amenazas con los recursos existentes.

Spread Spectrum es basado por los estándares 802.11b (IEEE), este trabaja con una banda de 2.4Ghz mediante un espectro de radio frecuencia ,el cual es totalmente libre debido a el manejo de la señal por DSSS manteniendo velocidades de transmisión hasta de 11Mbps, existen soluciones conocidas como indoors y outdoors, estas soluciones indoors están formadas básicamente con un Access point (hub inalámbrico – punto de acceso) este ofrece un servicio de conexión de forma inalámbrica hacia usuarios y estaciones de trabajo con placas PCI/PCMCIA Wireless, mediante una radio de 300 mts dependiendo del entorno en que se lo instale, a diferencia de las outdooes estas se deben tener que instalar bridges inalámbricos con una conexión building to building, y también se les puede conectar antenas de forma externa para así tener un mayor alcance, es importante

la protección de la red, en la figura 14 se observa el paso de información mediante una VPN.

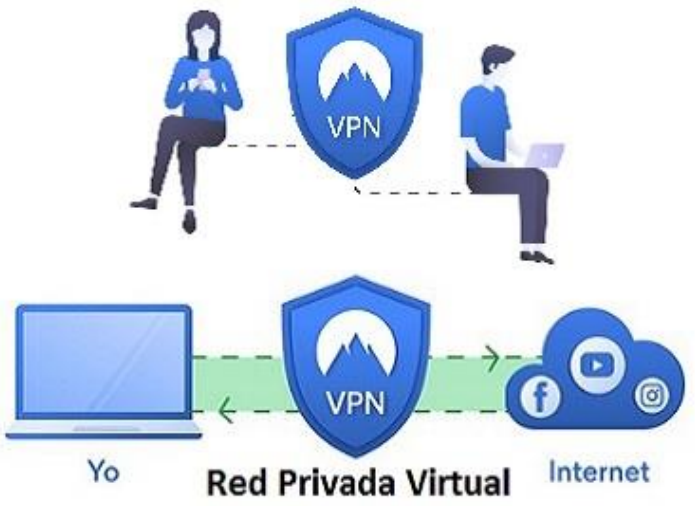


Ilustración 14.-Paso de información mediante una VPN.

En 1999 se aprobó el estándar 802.11b el cual, era una extensión del 802.11 para las WLAN de empresas, estas tienen una velocidad de 11 Mbps y maneja un alcance de hasta 100 metros, empleando consigo una banda de ICM con una frecuencia de 2.4 Ghz, pero en una modulación simple por radio digital acompañado de saltos de frecuencia es mejor utilizar una modulación lineal compleja.

El IEEE está trabajando en el estándar 802.11g capaz de poder alcanzar velocidades dobles de hasta 22Mbps, compitiendo con otros estándares, prometiendo velocidades más elevadas pero que son incompatibles con equipos de 802.11b que a su vez ya se encuentran instalados, es importante conocer que pueden coexistir hacia un mismo entorno por el motivo de que las bandas de las frecuencias que se llegan a usar son distintas.

2.1.5 MODELOS DE ANÁLISIS DE BLOQUES

2.1.5.1 COMPONENTES DE UN SISTEMA DE 2.4 GHZ EN LA ANTENA DEL PORTAHACK

Esta banda es considerada una de las más antigua, todos los **routers** que se encuentran en el mercado la incorporan, y se dispersa desde los 2.412 MHz hasta los 2.472 MHz, a su vez maneja canales que se subdividen en 13 canales, y cada

uno se compone de 20 MHz los cuales se solapan unos a otros. Posteriormente se añadió el canal 14 el cual quedaba alejada del espectro de frecuencias del Wi-Fi de 2.4 GHz.

Ilustración 15.- Componentes de un sistema de 2.4 GHz

Este aparato cuenta con una aplicación el cual permite el cálculo de la longitud de antena óptima de esta manera permite ingresar cualquier frecuencia específica mostrando los resultados en unidades **métricas** e **imperiales**, a su vez permite cambiar los tipos de ondas desde un apartado de listas establecidos como divisores que incluyen ondas completas, cuartos de donde y medias de ondas, siendo útiles para poder elegir una antena con una excelente señal de recepción y transmisión, es importante añadir que las necesidades de poder seleccionar una antena es que esta se pueda llegar a sintonizar y adaptar, de lo contrario la transmisión y recepción no sería tan optima y en ciertas circunstancias se desajusta al momento de transmitir en altas potencias llegando a dañar el equipo, existe la posibilidad de llegar a añadir una antena propia.

La aplicación de calculadora de antena va más allá, al calcular y mostrar en términos cuánto se debe ampliar cualquier antena telescópica predefinida, lo que es de mucha ayuda al realizar trabajos de campo y tener que recurrir a cualquier antena que haya incluido en el kit, tomar en cuenta que es necesario la tarjeta microSD insertada en el Portapack, el cual, debe contar con un archivo de texto simple con las antenas

que utilizas en /WHIPCALC/ANTENNAS.TXT, en la figura 16 Se muestran los tipos de antenas que maneja el portahack para sus diferentes estudios.

Ilustración 16.- Antenas que utiliza el PortaPack H2

El portahack es un dispositivo de software definido de radio (SDR, por sus siglas en inglés) es un aparato electrónico de bajo costo pero de alta calidad, es un transceptor de radio que capaz de sintonizar y transmitir señales de radio entre una frecuencia de 1 MHz a 6 GHz, esta característica lo hace ideal para los estudios y proyectos que se deseen implementar, incluyendo la recepción y transmisión de señales de radioaficionado, el poder explorar cada una de bandas de frecuencia a su alcance, control e investigación de seguridad y el desarrollo de protocolos de radio, maneja un código abierto, lo que significa que su hardware y software son libres de usar, tomando en cuenta que existe una gran comunidad de desarrolladores que han sido capaces de utilizar y realizas grandes proyectos con este aparato, debido al uso practico de conectarlo hacia el computador a través de un puerto USB.

Es importante recalcar que en caso de ser estudiado mediante otro dispositivo debemos usar otro software, como SDR o GNU Radio, o SDRANGEL, estos softwares permiten la configuración y control en las funciones del dispositivo, de esta manera es permitido poder ampliar variedad de aplicaciones de señales de radioaficionado.

Arquitectura del firmware

El microcontrolador es de doble núcleo LPC4320 de HackRF One este a su vez cuenta con recursos limitados para realizar tareas de radio definidas por software. Las configuraciones de cada aplicación tienden a guardarse en los archivos .ini correspondientes en la carpeta /SETTINGS, si se instala una tarjeta SD formateada, también se guardará en un archivo .ini actualizado cada vez que se cierra la aplicación, también permite la eliminación de forma segura del archivo .ini correspondiente y se creará un nuevo archivo automáticamente cuando se ejecute la aplicación posteriormente. Alternativamente también se pueden eliminar líneas individuales en el archivo para restablecer solo un subconjunto de las configuraciones de la aplicación, y para fines de depuración, tomar en cuenta que se pueden llegar a encontrar varias configuraciones adicionales en el archivo .ini pero estas no se pueden configurar en la propia aplicación, a continuación en la figura 17 se muestras los archivos guardados luego del ingreso de la tarjeta SD

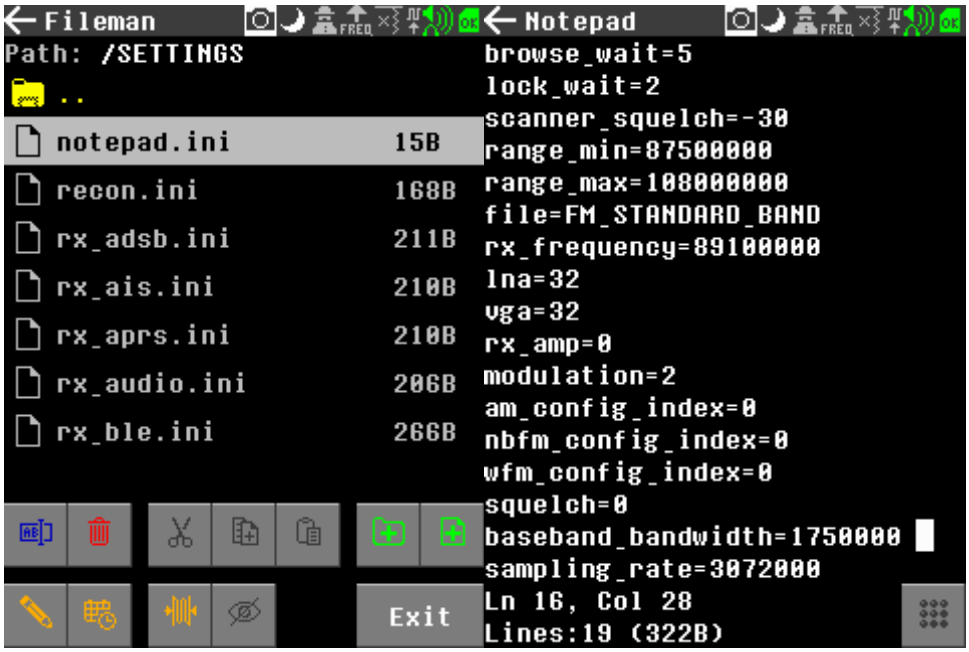


Ilustración 17.-Ventana de archivos guardados en un tarjeta SD en el PortaPack H2

DIVISIÓN DEL TRABAJO

Existen dos núcleos en el LPC4320:

- Cortex-M4F, este bloque se encarga de realizar el procesamiento de señales de banda base.

- Cortex-M0, este bloque se encarga de todas las tareas y su interfaz de usuario con el procesamiento de paquetes/señales simples.

El firmware Cortex-M4F maneja tres subprocesos de ChibiOS, enumerados con órdenes de prioridad decreciente:

- Banda base: esta banda es enlazada con el buffer de muestras de banda base y a su vez permite realizar el proceso para recuperar audios y paquetes.
- RSSI: permite la recepción de los buffers de muestras de RSSI (indicación de intensidad de señal recibida) mediante el cual este se procesa para generar métricas visuales, a su vez pueden utilizarse en el futuro para poder activar capturas de señales con el fin de proporcionar un control automático de ganancia (AGC) del receptor para ciertos modos del receptor.
- Predeterminado: el hilo ejecutado dentro de main () que recibe eventos de los otros hilos y mensajes del núcleo M0 (UI).

El firmware Cortex-M0 consta con un solo hilo, el predeterminado, esta espera eventos señalados por interrupciones y mensajes recibidos desde el núcleo M4 (banda base).

2.6.2. Modelado y Simulación de Ataques a la red

Una amenaza es considerada como cualquier método utilizado por partes no autorizadas para acceder a información, redes y aplicaciones sensibles. Algunas de estas amenazas incluyen virus informáticos, botnets, ataques hacia aplicaciones y fraudes de phishing. Estas representan riesgos habituales que las empresas deben anticipar mediante técnicas de modelado de amenazas tales como:

Ransomware:

El **ransomware** es un tipo de malware, su diseñado es utilizado en el cifrado con el objetivo del ataque para pagar un rescate, en su primera presentación en el sistema, es capaz de cifrar los archivos del usuario exigiendo un pago a cambio de la clave de descifrado. Los ataques de ransomware han llegado hasta el punto de detener grandes empresas y afectar gravemente la continuidad de un negocio.

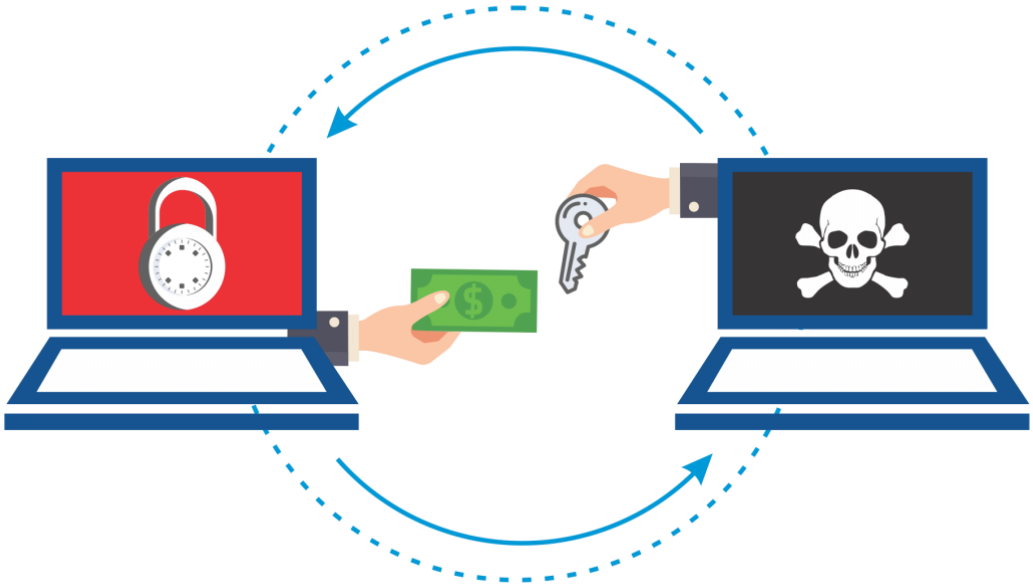


Ilustración 18.- Representación de Ransomware

Malware

El malware, abreviatura de software malicioso, es considerado una categoría de amenazas de ciberseguridad el cual incluyen amenazas entre ellas: virus informáticos, spyware y adware, es una amenaza muy común para atacar tanto a empresas, como a varias personas. Las empresas pueden llegar a utilizar el modelado de amenazas con la finalidad de asegurarse de que sus firewalls estén preparados, y de esta manera, se minimicen las vulnerabilidades o firmas de malware.

Ataques DDoS

También conocida como (denegación de servicio distribuida) es un método para atacar sitios web y aplicaciones web mediante varias solicitudes, que tienden a, sobrecargan los servidores. La mayoría de estos ataques llegan a ser impulsados por millones de bots y son indistinguibles de los usuarios que intentan acceder al sitio, por ende, es importante que las empresas pueden modelar sus planes de defensa para evitar que esto suceda, estas empresas pueden utilizar software de protección DDoS y software de monitoreo de red mejorando su capacidad de detectar ataques DDoS para equilibrar las cargas y restringir el acceso al tráfico de visitantes malintencionados.

Phishing

El phishing es un método que nos permite obtener información de usuarios a través de comunicaciones el cual pueden llegar hacer fraudulentas y a su vez son dirigidas directamente a las personas, a menudo este proceso se llega a realizar a través de correos electrónicos disfrazados como provenientes de una fuente legítima.

El phishing permite obtener acceso a información confidencial o aplicaciones privilegiadas, es importante que las empresas puedan prevenir este tipo de delito cibernético mediante un software de seguridad de correo electrónico para el filtrado y la identificación, en la figura 19 Se muestra una gráfica de la manera más común en donde se transmiten los ataques a la red.

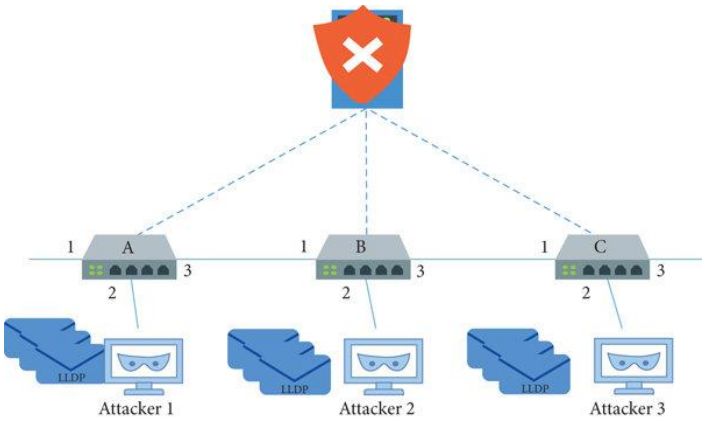


Ilustración 19.- Pishing

Las amenazas cibernéticas y las preocupaciones en la actualidad siguen siendo un problema muy grave en donde se han visto envuelto diferentes empresas, causándole grandes pérdidas y muchas de estas tendencias de ataques continúan siguen previstas existiendo nuevos problemas de seguridad de red e innovaciones en materia de delitos cibernéticos.

2.7. Estado del arte

2.7.1. Que es el Estado del arte

El estado del arte es considerado como el conjunto de saberes ante el desarrollo que se ha conseguido en diferentes áreas de investigación, por ello , su función se basa en la recaudación de información de fuentes que han sido verificadas y hacen referencia a el tema de indagación de esta manera, así se logra evitar a el autor la repetición de dicha investigación ya realizada, debido a que muchas veces esta tipo de información es distorsionada causando desconformidad al momento de poner en práctica el informe receptado . Sus inicios se remontan en los años ochenta de los países anglosajones, en este, se comenzó a utilizar dentro cada una de las investigaciones con el nombre de "state of the art", dicho nombre fue traducido al español, sin embargo, varios autores e instituciones han considerado desaprobar esta traducción y han sugerido términos como estado de la técnica y estado de la cuestión, entre otros términos que han sido rechazados, en la figura 20 se muestra el gran paso de la sociedad acompañado de las nuevas tecnologías que han sido implementadas hoy en día como medios útiles y diarios al momento de realizar un trabajo

Ilustración 20.- Nuevas Tecnologías utilizadas en la sociedad

Un estado del arte se escribe mediante un sinnúmero de pasos empezando por realizar un estado del arte el cual consiste en seleccionar un tema el cual se va a realizar una investigación, una vez ya definido dicho tema, se empieza con la exploración de varias fuentes relaciones a el tema, estas información puede ser

tomada de texto o videos y a su vez pueden ser escritas, siempre y cuando se tome en consideración citar ,es decir, nombrar quien escribió el tema o agregar su fuente bibliográfica correspondiente , estas fuentes se puede categorizar de diferentes formas o por periodos temporales , de esta manera, estas fuentes son evaluadas y analizadas mediante contrastes el cual pueda tener varios autores que han ido argumentos parte del texto.

De esta forma, no sólo se sopesará la bibliografía, debido a que mostrará el punto de vista de otro autor sumando o acotando lo ya investigado. Entre las recomendaciones que se debe tomar en cuenta al momento de llegar a escribir un estado del arte es que no se realice una lista de las fuentes, sino que se llegue a crear un texto que las integre y se presenten a partir de las propias palabras del investigador. Para ello, el autor del trabajo investigativo debe tener conocimiento del tema a tratar, así como los autores y sus fuentes. Finalmente, otra recomendación para escribir un estado del arte es leer otros artículos de estados del arte.

Estado del arte en el mundo de las telecomunicaciones

El mundo de las telecomunicaciones ha cambiado y ha evolucionado a grandes pasos, de acuerdo con Humberto Medina, "las empresas de Telecomunicaciones y de Tecnología han evolucionado de forma exponencial". Tiempo atrás solo se contaba con equipos básicos ya sea la radio, televisión y este se visualizaba a blanco y negro, también se encontraban teléfonos fijos, tal así que solo existía una forma de comunicación entre las personas, este era un teléfono que iba conectado con cable, luego de ello, llegó la televisión a color, y posteriormente a mediados de los 90´s empezaron a llegar los primeros teléfonos móviles a diferentes países, cabe recalcar que no son de fácil acceso debido a sus costos elevados y las altas tarifas de servicios.

Sin embargo, hoy en día el teléfono es considerado un medio necesario para la sociedad, por lo tanto, la mayoría de la población tiene uno a su alcance y el mercado de tarifas ha crecido y evolucionado por ello, han ofrecido diversas operadoras de comunicaciones que son asequibles para cualquier persona, contando con los servicios móviles llamadas, mensajes (SMS) y datos, la logística digital es

considerado como un tema de competitividad el cual ha brindado resultados muy favorable para todos, esta ha sido habilidad para dirigir el flujo de materiales, ya sea productos o información tecnológica y de marketing para un cliente final y satisfecho, fundamental para que las telecomunicaciones , conlleve a cambios por las comunicaciones y la digitalización de trabajos realizados.

2.7.2. Estudios Específicos con PortaPack H2

El Portapack radio debido a que está definida por software HackRF este utiliza el HackRF acompañada con una batería de manera portátil, a su vez posee una pequeña pantalla táctil LCD y una rueda de control utilizada para controlar el firmware HackRF personalizado, incluyendo un receptor de audio, decodificadores digitales y transmisores, mediante el Portapack ya no es necesario una PC para recibir o transmitir en el HackRF.

Ilustración 21.- PortaPack H2 vista de la tarjeta y con su carcasa

CAPTURAR Y REPRODUCIR

Una de las opciones por la que se destaca el Portapack es aquella que nos permite realizar capturas y a su vez poder reproducir las señales inalámbricas como las de los mandos que se encuentran a distancia en banda ISM. Para la creación de la captura debemos entrar en el menú “Captura”, configurar la frecuencia del mando,

pulsar el botón rojo “R”, el cual es el que nos permite realizar la grabación y luego pulsar la tecla del mando a distancia, es importante detener la grabación para poder guardarla en la tarjeta SD, luego ir al menú Replay, de esta manera, seleccionaremos el archivo el cual acabamos de grabar y pulsar play, así, se transmitirá por aire la misma señal.

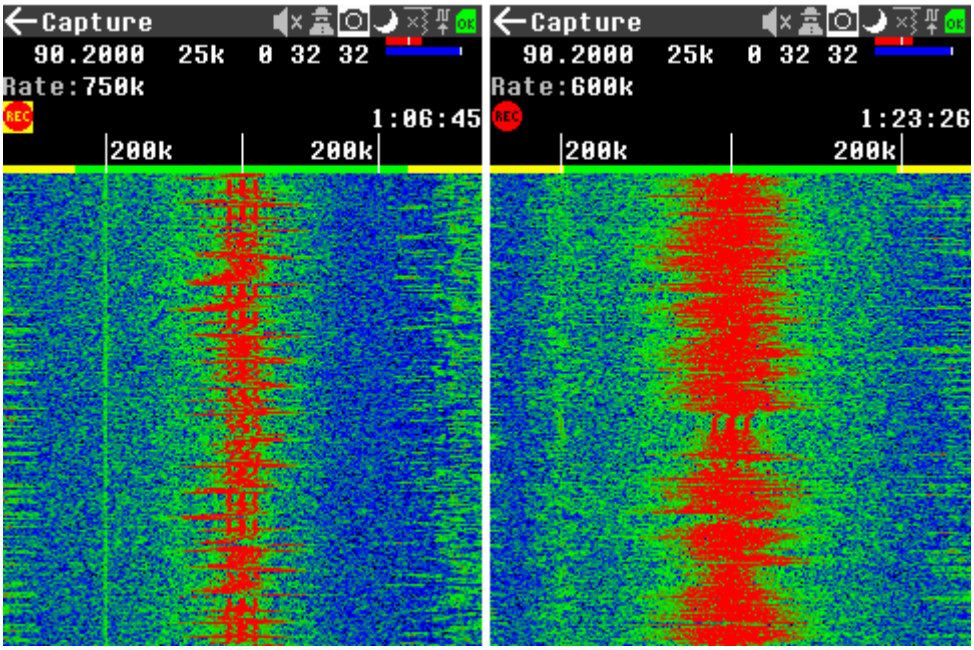


Ilustración 22.- Captura de señales inalámbricas

Transmisor de micrófono Portapack

Micrófono TX

El micrófono está compuesto por un conector de audio con una medida de 3,5 mm, por ende, este Portapack se puede utilizar como un dispositivo similar a el walkie talkie estándar con función Push to Talk o también como activado por voz, de esta manera, con un micrófono conectado hacia el conector del audio, y manteniendo presionado el botón derecho para pulsar y hablar, cabe recalcar que si es necesario, se pueden llegar habilitar múltiples opciones de tonos CTCSS, así como tonos que parecen habilitar la transmisión a auriculares inalámbricos, en la figura 23 se muestran las pruebas del audio con la version incluida del Portapack.

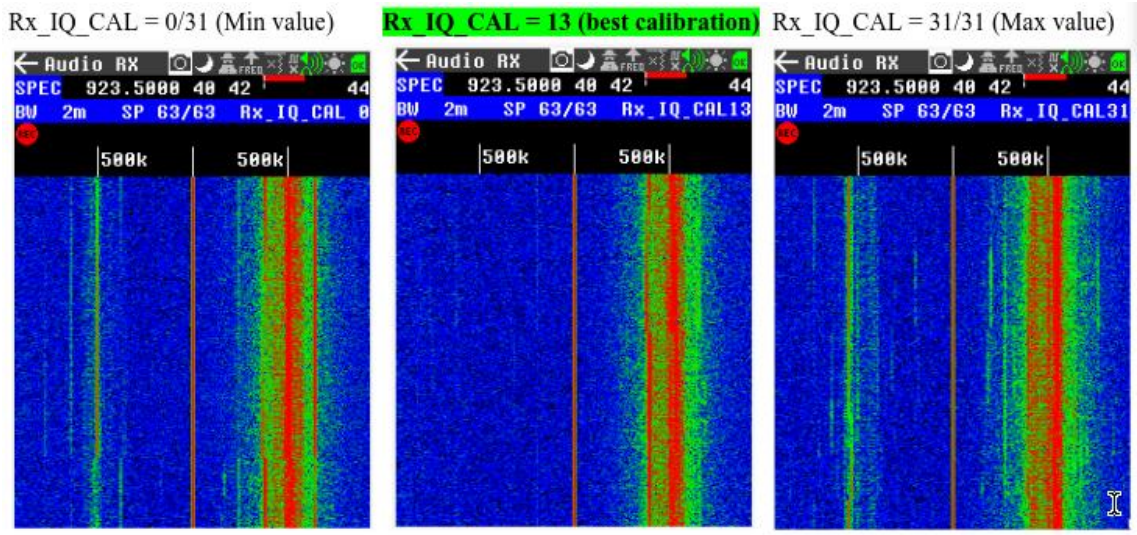


Ilustración 23.- Pruebas del audio

Otros transmisores

Se han realizado pruebas en función SSTV usando un software de decodificación RTL-SDR y SSTV, mediante estos modos de radioaficionado disponibles para transmitir incluyen APRS y código Morse, también cuenta con un transmisor OOK el cual es genérico y a su vez se puede programar con datos personalizados, de este modo, puede resultar muy necesario para experimentar con llaveros sencillos y cosas como interruptores de automatización para el hogar, es importante tomar en cuenta que existen numerosos modos de transmisión el cual pueden llegar hacer implementados de manera ilegal y en muchos países podrían causar serios problemas, por esa razón existe un bloqueador de señal, el cual es conectado con el Portapack hacia una carga ficticia colocando un RTL-SDR y antena cerca. Tomar en cuenta que algunas de las placas Portapack que se encuentra a la venta en el mercado pueden constar con un generador de reloj TCXO de 10 MHz de ppm bajo, y cuando está integrado, es conectado en paralelo hacia el conector de puerto CLK_in externo de HackRF. Entonces, en ese caso, esa señal de reloj PP interna siempre estará presente en el conector SMA CLK_in, y es recomendable no conectar ningún otro generador de señal externo allí (a menos que desmonte el Portapack de HackRF), porque de lo contrario, conectará dos generadores de señal de reloj en paralelo -el incorporado al externo-, dañando ese circuito IC de reloj TCXO de Portapack.

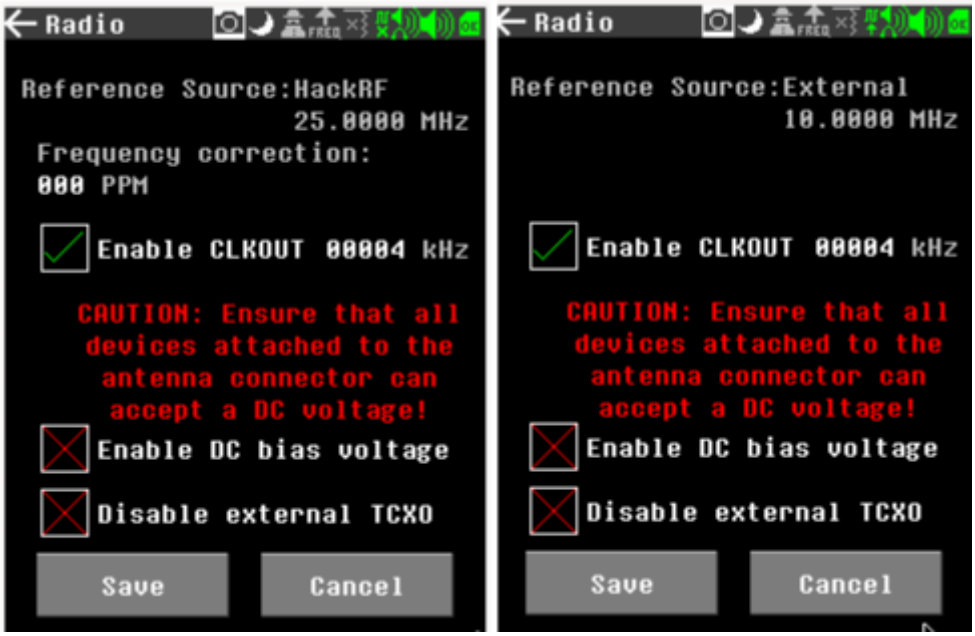


Ilustración 24.- Pruebas en función SSTV

Receptores

El ítem de receptores permite conectar los altavoces al conector de audio de 3,5 mm del Portapack, para poder escuchar fácilmente las señales de audio NFM y WFM estándar. El ancho de banda que se muestra es tan extenso como las señales, por lo que puede ser un poco difícil explorar las bandas de frecuencia arrojadas, por ende, se recomendó tener a la mano primero una lista de frecuencias. Es importante destacar la memoria personal, el cual se encuentra dividida por tres páginas, dichas paginas pueden ser cambiadas con el codificador y desplazadas desde el inicio del área p.mem por ende se muestra en la columna izquierda, en la parte inferior se observa el tamaño actual de la estructura data_t (esto es lo que persistimos en p.mem) con la suma de comprobación almacenada actualmente (se calcula a partir de los primeros 252 bytes del área p.mem cuando se realizan cambios en la configuración y luego se escribe en los últimos 4 bytes de p.mem), tomar en cuenta que la versión de configuración almacenada no se encuentra por separado, pero se puede ver como los primeros 4 bytes del área p.mem, tal y como se muestra en la figura 25.

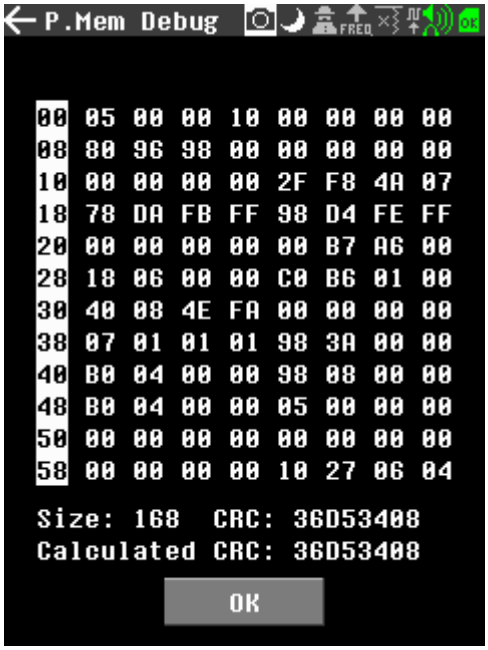


Ilustración 25.- ítem de receptores

Recepción de audio WFM y NFM con el Portapack.

También han probado la recepción ADS-B con LNA ADS-B, y la conexión en T del HackRF se pueden ser habilitados fácilmente en el Portapack seleccionados con el inductor y el símbolo del rayo en la parte superior derecha, de esta manera, con la conexión en T han recibido señales de aeronaves.

Ilustración 26.- Recepción de audio

Contenido de la tarjeta SD los recursos del Portapack

La tarjeta SD proporciona varios recursos de memorias y estos a su vez son capaces de adaptar a cada usuario. Los detalles técnicos de la tarjeta se proporcionan como parte de la descarga estándar correspondiente al firmware. A continuación, se mostrarán las carpetas de la tarjeta SD el cual contienen información específica del uso y su aplicación (varias de estas carpetas se encuentran incluidas en el archivo de imagen de la misma tarjeta SD y algunas han sido creadas posteriormente por el firmware o por los usuarios):

Ilustración 27.- Contenido de la tarjeta SD de los recursos del Portapack

- **ADSB:** En la carpeta ADBS se encuentran bases de datos correspondientes a aerolíneas, IACO y es donde se ve establece el mapa mundial, para generar este mapa es importante consultar con el dispositivo
- **AIS:** Se encuentra la base de datos AIS.
- **APLICACIONES:** contiene aplicaciones "externas", muchas veces por las actualizaciones se tienden a mover varias aplicaciones de la ROM flash del firmware a archivos externos (con extensión. ppma) que están almacenados en la tarjeta SD, con el objetivo de tener espacio en la ROM Mayhem y de esta manera tener aplicaciones y funciones acorde a lo que uno desee usar.

- **APRS:** contiene archivos de registro de la aplicación APRS-RX.
- **AUDIO:** se encuentran grabaciones de audio (WAV) de la aplicación Audio.

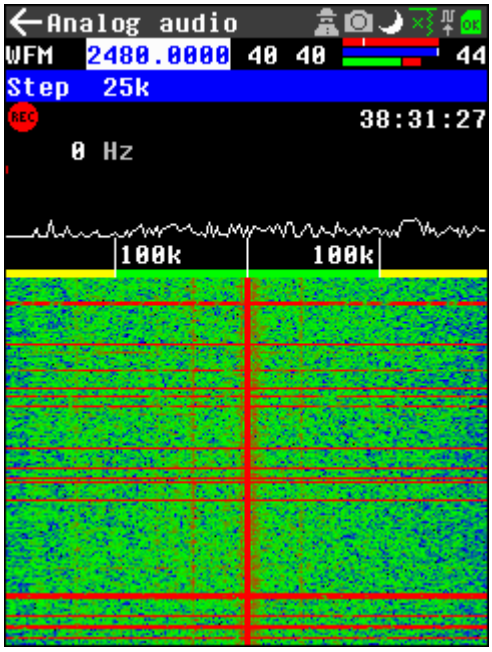


Ilustración 28.- Grabaciones de audio (WAV)

- **BLERX:** encontraremos archivos de registro de la aplicación BLE-RX.
- **BLETX:** contiene archivos para el aplicativo BLE-TX.
- **CAPTURAS:** Contiene archivos de captura IQ (C16/C8 y sus archivos TXT de metadatos)
- **DEBUG:** contiene varios archivos de los registros que han sido depurados.
- **FIRMWARE:** en esta función se puede colocar los archivos bin y a su vez que estos se puedan usar para actualizar el firmware de Portapack sin una computadora.
- **FREQMAN:** recepta los archivos de base de datos FreqMan, el cual se suma a las listas de frecuencias y pueden cargarse a través varias aplicaciones, de esta manera, pueden editar y ver mediante la aplicación FreqMan.

    - **Frecuencias fijas en las aplicaciones:** este bloque de frecuencias fijas es importante resaltar que en ciertas aplicaciones los rangos de frecuencia se encuentran fijados en la aplicación, por lo tanto, no es permitido seleccionar desde las listas de FREQMAN. Entre los ejemplos son "AIS" y TPMS. (En ciertos casos, el archivo de configuración .ini puede ser modificado manualmente para cambiar la frecuencia con otras configuraciones que no se logra configurar al momento de ejecutar la aplicación en sí).

- **GPS:** este archivo contiene la información generada por las simulaciones de la aplicación que se encuentran guardadas en la tarjeta SD
- **REGISTROS:** contiene los archivos de registro para algunas aplicaciones como ADSB, POCSAG, ERT, etc.
- **LOOKINGGLASS:** En esta carpeta encontraremos varios archivos de texto, estos son utilizados sirve en la aplicación LOOKINGGLASS y consta de un listado de rangos con su respectivo escaneo de frecuencia y una descripción. Es importante conoce que esta aplicación solo puede mantener rangos con un tamaño mínimo de 240 MHz. Además, el rango es capaz de comenzar desde 10 MHz el cual es la frecuencia operativa mínima nominal de HackRF y este se debe tener en cuenta al momento de planificar el rango de frecuencia indicado.
- **LISTA DE REPRODUCCIÓN:** contiene los archivos en listado de reproducción (PPL) para la aplicación Replay.
- **REMOTES:** contiene archivos remotos (REM) el cual, sirven para las aplicaciones Remote y TouchTune.
- **MUESTRAS:** Tiene un ejemplo de varias configuraciones para el uso en la aplicación OOK TX
- **CAPTURAS DE PANTALLA:** Se registran las capturas de pantalla (SCR) tomadas en el dispositivo.

- **CONFIGURACIÓN:** contiene la configuración de todas las aplicaciones, si se tiene un problema con una aplicación, es importante eliminar su archivo de configuración y de esta manera poder restaurar los valores predeterminados (También se puede almacenar un archivo de "lista negra" esto es de forma opcional bajo su propio directorio (que incluye una lista de aplicaciones que se encuentran en uso).
- **SPECTRUM:** registra imágenes BMP para la aplicación Spectrum Painter.
- **SPLASH:** registra archivos BMP de la pantalla de presentación personalizada, sin embargo, el archivo de la imagen de presentación actualmente activo debe encontrarse en el directorio raíz y llamarse "splash.bmp").
- **SSTV:** Tiene algunas imágenes estándar para utilizarse en la aplicación SSTV.
- **WAV:** Tiene archivos de sonido que sirven en la aplicación SoundBoard.
- **WHIPCALC:** Maneja la información sobre ciertos cálculos que realizan ciertas aplicaciones.

Dentro del contenido de la tarjeta SD se le permite instalar y editar aplicaciones mediante USB desde la computadora a través de la aplicación "SD over USB" (SD sobre USB), o a su vez se puede extraer la tarjeta SD física del Portapack y conectarla hacia la computadora. Tener cuidado al reinstalar la tarjeta SD en el Portapack, ya que puede caerse dentro del dispositivo y requerir que se desarme la carcasa para recuperarla.

Ilustración 29.- Contenido de la tarjeta SD que le permite instalar y editar aplicaciones mediante USB

JAMMER

También es conocido como bloqueador o inhibidor, un jammer es un dispositivo electrónico el cual, permite la transmisión de señales en un mismo rango de frecuencia, es utilizado en las redes móviles celulares y equipos de posicionamiento global (GPS), bluetooth, WIFI entre otras, como tal , este dispositivo es capaz de generar interferencias y mala recepción de las señales pero de una manera intencional provocando actos delictivos.

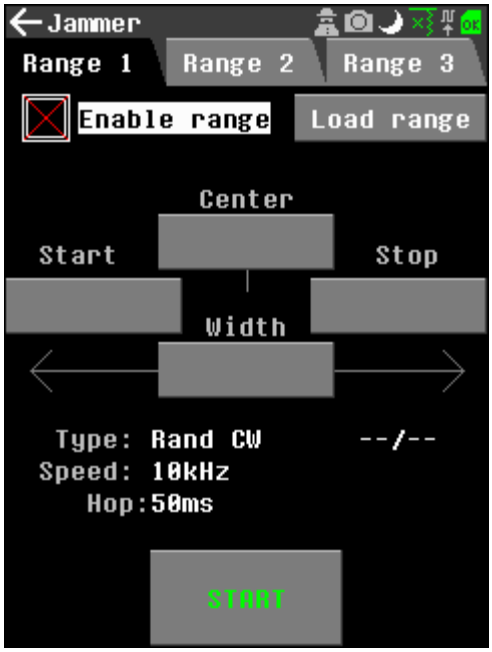


Ilustración 30.- Jammer

Por lo general, los bloqueadores de señal tienen como objetivo ser indetectables, los usuarios tienden a experimentar efectos negativos, y aparentemente inofensivos, ya sea una mala recepción de la señal que los deja incomunicados.

Características de los jammer

Los equipos bloqueadores o también conocido como inhibidores de señales se encuentran en diferente presentación tanto en forma y tamaño, que incluyen:

- Dispositivos compactos y portátiles, similares los teléfonos móviles.
- Su forma es muy parecida a los routers.
- Otra de sus presentaciones es que tiende a ser similar a un maletín para obtener un mayor rango de cobertura de la señal.

La gran mayoría de los equipos utilizados para la interferencia de las señales cuentan con tres componentes principales para su funcionamiento, tales como:

- Una antena que vaya conectada al dispositivo.
- Una fuente de alimentación o una batería.

- Un circuito electrónico que debe estar compuesto por un oscilador, sintonizador de frecuencia, controlado por voltaje, generador de ruido y el amplificador de radiofrecuencia (RF).

Los equipos de mano logran interrumpir las señales en un rango de hasta 30 metros, mientras que equipos de mayor tamaño con más potencia, logran neutralizar las señales en un rango de hasta 1,6 kilómetros.

Ilustración 31.- Equipos de mano que logran interrumpir las señales

Aplicaciones del jammer en telecomunicaciones

Existe varios equipos inhibidores de señal, de tal manera, el espectro de las comunicaciones es bastante amplio debido a los diferentes tipos de bandas, es por ellos que los bloqueadores se centran en los espectros de rango de señal más comunes de los equipos, como son:

Teléfonos móviles

Invaden las frecuencias DCS, GSM, GPRS, 2G, 3G y 4G, y anulan las comunicaciones de audio, y videos por internet y transmisión de datos. (“¿Qué es un jammer y cómo protegerte de él? - Ubícalo®”)

Equipos GPS

Encontramos varias bandas de comunicación de los equipos GPS, sin embargo, las más utilizadas es la L1, debido a que, es utilizada en dispositivos GPS. Los

bloqueadores tienden a neutralizar las señales del GPS, de esta manera, impiden determinar la ubicación exacta de las unidades vehiculares.

Ilustración 32.- Simulador de GPS

Dispositivos: wifi, bluetooth o cámaras inalámbricas

Bloquean las señales en bandas 2,4 Ghz y 5 Ghz, por lo tanto, evitan la comunicación en los equipos de uso comercial y doméstico, entre ellas:

- Router
- Decodificadores de televisión
- Computadoras
- Micrófonos inalámbricos
- Cámaras

Equipos Walkie talkie

Causan Perturbación en las señales de frecuencias de los equipos de comunicación punto a punto, debido que no tienen restricciones legales.

Instalaciones de radiofrecuencia

Se utilizan para impedir la comunicación en bandas de frecuencia, aunque estas, son muy selectivas del tipo VIP, y son utilizadas por equipos técnicos de comunicación, entre los que se encuentran: ("¿Qué es un jammer y cómo protegerte de él? - Ubícalo®")

- Radares
- Telecomunicaciones por microondas
- Mando de vehículos
- Mandos automatizados de equipos especiales (robótica).

Ataques realizados mediante el uso de un jammer

Antecedentes

Durante la Segunda Guerra Mundial, en los periodos hacia la invasión a Sicilia en 1943, ante las fuerzas aliadas y lideradas por los Estados Unidos desarrollaron un Jammer, el cual consistía en un bloqueador para contrarrestar los sistemas de radares antiaéreos de los alemanes.

Este eficaz invento de lo denomino "Alfombra, fue diseñado por el ingeniero eléctrico estadounidense William Rambo dándole uso a amplificadores y osciladores de ultra frecuencia con el objetivo de anular completamente las señales de los radares.

En la actualidad, el desarrollo de los sistemas de comunicación ha crecido exponencialmente y han evolucionado, formando parte del eje central en el mundo de las telecomunicaciones.

Entre los proyectos que han realizado se encuentre el desarrollo de un dispositivo Jammer con el objetivo de bloquear una señal móvil GSM, este proyecto consistía en desarrollar un dispositivo electrónico que pueda interferir señales de varios operadores móviles en distintos lugares donde no está permitido el uso de celulares que han operado en la banda GSM, presentaron a su vez un diseño por etapas de practica de dicho dispositivo y desarrollando la aplicación generando consigo su respectiva función dependiendo del área de cobertura.

3 CAPÍTULO III

3.1 METODOLOGÍA

3.1.1 HERRAMIENTAS Y EQUIPOS UTILIZADOS

3.1.1.1 PORTAHACK H2

El HackRF One es una herramienta de análisis de Radiofrecuencias portátil, este portahack cuenta con dos versiones la H1 y H2, ambos dispositivos cumplen con las mismas funciones, la única diferencia es que el ultimo presenta mejoras en el acabo físico, como la pantalla y los comandos. EL HackRF (la placa que se encuentra debajo del Portapack) mantiene la capacidad de poder enviar y recibir ondas de radio mediante un amplio rango de frecuencias, a continuación, estas son algunas de sus especificaciones:

- Transceptor: Half-duplex
- Frecuencia de funcionamiento: 1 MHz a 6 GHz
- Frecuencias de muestreo: 2 a 20 Msps (cuadratura)
- Resolución: 8 bits
- Potencia máxima de TX (es posible consultar una medición empírica):
    - 10 a 2150 MHz: 5 a 15 dBm, va aumentando mientras disminuye la frecuencia
    - 2150 a 2750 MHz: 13 a 15 dBm
    - 2750 a 4000 MHz: 0 a 5 dBm, va aumentando mientras disminuye la frecuencia
    - 4000 a 6000 MHz: -10 a 0 dBm, va aumentando mientras disminuye la frecuencia
- Potencia máxima de recepción: -5 dBm. Cabe recalcar que si este llega a superar los -5 dBm, existe la posibilidad de daños permanentes, por ende,

solo es aceptable de manera segura hasta 10 dBm con su amplificador de recepción frontal deshabilitado.

- CLKOUT/CLKIN: onda cuadrada de 10 MHz (0 V a 3 V es considerado para una carga de alta impedancia)

MENU PRINCIPAL

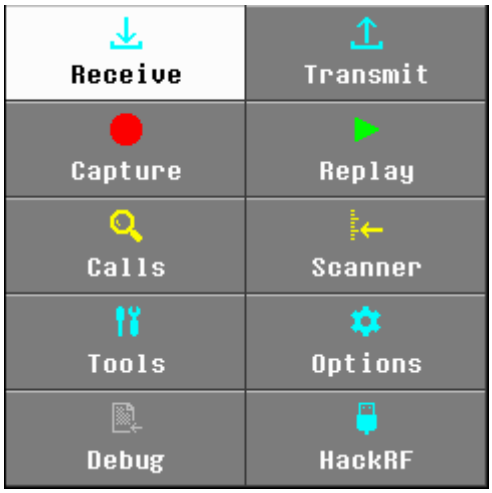


Ilustración 33.- Menú Principal de PortaPack H2

Recibir	*Aplicaciones del receptor*
Transmitir	*Aplicaciones de transmisión*
Captura	*Permitir la grabación o 'captura' de RF para facilitar los análisis o las diferentes reproducciones de ataques*
Repetición	*Transmitir un archivo de captura de RF previamente grabado*
Llamadas	*Detecta todo tipo de señales dentro de un ancho de banda específico, semejante a la función 'Close Call' en los escáneres*
Escáner	*Recorre una lista de frecuencias que se encuentran predefinidas ya se mediante un silenciamiento (señal detectada)*
Herramientas	*Incluye listas de administradores mediante frecuencias dadas en la tarjeta SD, administradores de archivos, visores*

	de archivos WAV, borrado de tarjetas SD y la calculadora de longitud de la antena.
Opciones	*En este apartado se configura el tono de audio, el radio y la configuración de interfaz para el usuario, ya sea, el reloj, la fecha y hora y la calibración de pantalla táctil*
Depurar	*Protege el uso de la memoria hasta la información de la tarjeta SD y codificadores.*
Hacker RF	*Esta opción permite usarlo desde un dispositivo host USB (por ejemplo, la computadora)*

Tabla 6.- Funciones que tiene el PortaPack H2

Aplicaciones del portahack

En la opción de recepción encontramos aplicaciones que nos permite receptar datos para el desarrollo de la investigación, a continuación en la figura 34 se muestran los bloques de las diferentes aplicaciones.

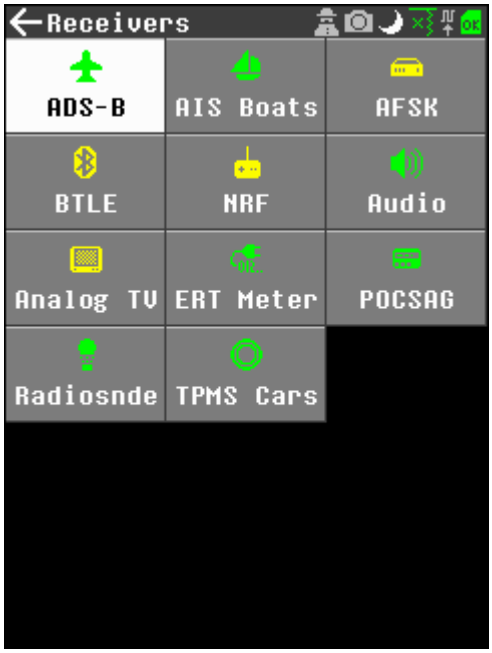


Ilustración 34.- Aplicaciones en la Función de Recibir Señales

Vigilancia dependiente automática por radiodifusión (ADS-B)

Con esta aplicación se pueden recibir señales de ADS-B en tiempo real, es muy útil para el control del tráfico aéreo, su funcionamiento es mediante la selección de la

aeronave, este recibe la señal, de esta manera, nos permitirá visualizar más a detalles su paso, es importante cargar un mapa en la tarjeta SD para que pueda ser visto desde allí , el ADS-B tiene un rango de 978 a 1090 MHz, e incluso si se conecta la antena corta que viene dentro del paquete se recibirá una señal ADS-B cuando el preamplificador de recepción esté habilitado

AFSK

Si bien esta aplicación se encuentra marcada como beta, dicho receptor mantiene un flujo constante y es independiente de la frecuencia a su vez, tiene otra configuración del modem, por lo tanto, se requiere de mayor estudio y de otros componente, por tal motivo no funciona.

Embarcaciones AIS

El sistema de identificación automática (AIS) Consiste en la visualización del seguimiento, el cual es de gran utilidad en los buques de navegación marítima. El receptor AIS Portapack permite la decodificación de la información el cual, es procedente de los buques y estaciones base en dos frecuencias VHF seleccionables: 161,975 MHz (canal 87B) o 162,025 MHz (canal 88B), a su vez se pueden añadir más frecuencias a la tarjeta SD

Decodificador para NRF24L01

NRF es un transceptor patentado, entre sus características destaca el bajo consumo y coste en el rango de 2,4 GHz producido por Nordic Semiconductor, es utilizado principalmente para los mandos a distancia, ya sea teclados o ratones y, en general, para comunicaciones de bajo consumo, a su vez se visualiza como nFR24L01 y otros transceptores un tanto baratos similares entre los aficionados a la electrónica, es popular en el control por radio de minidrones.

Con esta aplicación, puedes usar el Portapack para decodificar los datos enviados desde NRF24L01 y ver algunos mensajes de datos en 2,4 GHz, es importante conocer que en la actualidad solo admite el modo 250 KPS.

Televisión analógica

La aplicación de TV analógica actualmente solo admite PAL de banda ancha modulada en amplitud, debido a que, esta señal solía adoptarse ampliamente por varios trasmisiones de televisión, cabe recalcar que la aplicación reduce el tamaño de la imagen a 52 líneas x 128 de ancho para poder restar la sobrecarga del procesamiento y para que se ajuste a la pantalla del Portapack, aun no se admite la detección de las señales para la sincronización por esta razón , los fotogramas se encuentran desalineados tanto vertical como horizontal y tienden a desviarse con el tiempo, es importante acotar que solo se muestran imágenes a blanco y negro

Audio

La aplicación de audio es primordial pues es la forma de escuchar y ver las señales en detalle, estas se distribuyen en tres tipos de decodificadores para señales de audios moduladas con una vista de espectro de las señales, a su vez la interfaz de usuario nos permite realizar cambios en:

- **ESPECIFICACIÓN:** Muestra un espectro de señal recibida y a su vez permite la visualización de 10 MHz del espectro de RF, está centrado en una frecuencia configurable, con 5 MHz por encima de la frecuencia y 5 MHz por debajo.
- **AM:** graba y permite la demodulación de señales de RF el cual, son moduladas a través de un esquema de modulación de amplitud, esta aplicación permite demodular señales AM que sean de banda lateral doble (designación de la UIT: A3E), también, señales AM de banda lateral inferior y de banda lateral superior de banda lateral única (clasificación de la UIT: R2E, H3E, J3E).
- **NFM:** Decodificación de modulación de frecuencia de banda estrecha Clasificación ITU: FM3
- **WFM:** El receptor Wide FM es considerada una sub-aplicación de receptor de audio, tiene como objetivo demodular y grabar señales de RF moduladas que sirven para el bloque de modulación de frecuencia, es permitido

demodular señales Wide FM estéreo y mono que sean correspondientes a un archivo de un ancho de banda de 200 KHz.

Transmisor

Ilustración 35.- Aplicaciones del PortaPack en la Función de Transmisión

APRS TX

La aplicación TX hace referencia el sistema de informes automáticos de paquetes, este a su vez, permite él envió de mensajes en una frecuencia seleccionada, dicha aplicación desde su configuración autoriza del flujo APRS, cabe recalcar que la aplicación se encuentra solo en modo Beta, pero parece que envía mensajes en AFSK correctamente en el formato AX25 correcto.

La aplicación tiene configuraciones para:

- "Origen;" La dirección es seleccionada moviendo el cursor para el lado derecho de donde se encuentra la etiqueta y seleccionando su carácter alfanumérico necesario, de esta manera se escogen los campos y son almacenados en la SSID, esto se da tanto para origen y destino

- En el contenido de mensajes se puede añadir el "Campo de información" seleccionando el botón "Establecer", con un máximo de 30 caracteres, no el máximo típico de 67 o 256.
- la frecuencia primaria con el cursor para TX desde el teclado en pantalla, por ejemplo 144.800

BHT

Esta aplicación es usada solo en Francia puesto que nos permite el control del alumbrado público, este sistema fue fabricado por BH-Technologies, y es muy útil para los diferentes municipios franceses, su sistema permite el encendido y apagado de los sectores mediante la señal de radio en un rango de 31 a 32Mhz, este proyecto se basa en un protocolo de gestión remoto y solo es usado en ciertas ciudades europeas.

RDS

"RDS" significa "Sistema de datos de radio" esta aplicación trabaja en torno a las emisoras FM puesto que permite enviar más que una simple señal de audio ya sea analógica o por ondas, esto se da, por una onda subportado de 57 KHz, las estaciones son capaces de transmitir datos RDS de manera digital y para la recepción de estos datos es mediante un sintonizador FM. Esta tecnología es capaz de abrir toda una gama de funciones con el objetivo de brindarle una ayuda el oyente mediante la recepción de RDS, la información depende de lo que se desee transmitir y que a su vez se pueda captar en el dispositivo, es importante conocer que existe dos categorías: estática y dinámica.

La aplicación RDS consta con 4 pestañas: Nombre: Texto: Tiempo: Audio, los elementos claves a su vez puede ser editados con el mando del codificador, a continuación, se muestras los comandos.

- **Barra de título:** Se pueden editar y mostrar los elementos habituales.
- **Tipo de programa:** Existen 31 tipos de programas preestablecidos
- **ID del programa:** El ID del programa es un código hexadecimal de 4 caracteres que va desde 0000 hasta FFFF.

- **TP:** Casilla de verificación selecciona los envíos del Símbolo del Programa de Tráfico.

En la parte inferior de la página de la aplicación se encuentran las configuraciones relacionadas con la configuración de RF, que son:

- **Frecuencia:** Esta dependería del rango y la práctica que se desea emplear.
- **Tamaño de paso:** se encuentra a un lado de la frecuencia y permite seleccionar los tamaños del paso estándar.
- **Ganancia:** La configuración de ganancia se encuentra abajo del ítem de frecuencia y marcada (0-47) LNA(IF) y AMP 0=0db o 1=14dB.
- **Inicio:** Este botón permite iniciar la transmisión y si es presionada nuevamente detiene la transmisión.

Jammer

Esta aplicación permite la transmisión de diversas formas de audio con el objetivo de provocar una denegación en el servicio de dispositivos, esto puede incluir teléfonos inalámbricos, móviles, wifi, y otros dispositivos, varios usuarios han implementado la capacidad de interferencias y de esta manera han implementado en cada uno de sus proyectos, es importante conocer que dependerá de la configuración, potencia de la señal y la fuente de interferencia.

Varias veces el rango de interferencia tiende a bajar debido a la potencia de transmisión, este será dependiendo del orden entre pocos metros, aunque el uso de otros implementos como amplificadores y antenas han sido capaces de potenciar el aumento de fuerza de la señal.

Esta aplicación trae consigo tres pestañas para el rango 1, rango 2 y rango 3, estas se han habilitado por separado y han funcionado pero de una manera secuencia, es decir, del rango 1 al 2 y al 3, limitando su tiempo del escaneo para cada rango y su señal de interferencia que se está generando, el rango de interferencia mantiene un límite máximo de 24 MHz y el movimiento de la señal de interferencia mediante la banda se lleva a cabo en fragmentos de 1, tomar en cuenta, que la potencia de salida del Jammer se establece al máximo nivel posible, normalmente entre 5 y 10 dBm.

Morse

La aplicación Morse permite él envió de mensajes codificados en Morse ya sea en CW o FM. También hay mensajes de Foxhunt preconfigurados, pero no se consideran tan útiles debido a que en la mayoría de los países un indicativo debe ser parte del mensaje o debe ser enviado a través de intervalos regulares.

Ilustración 36.- Envió en Código Morse

Los elementos clave de la aplicación se seleccionan con el cursor y la perilla

- **Foxhunt:** esta casilla de verificación se habilita con las cadenas de mensajes preestablecidos (cuenta con 11 de ellas) son seleccionados en la misma línea, como "3 (MOS)".
- **Velocidad:** se selecciona la velocidad de transmisión, pero en palabras por minuto (10-45). Tomar en cuenta que la etiqueta debe ser “ppm” y no “wps”, porque si no es considerado como un error.
- **Tono:** Establece el tono para la transmisión FM (0-9999).
- **Modulación:** Establece en CW o FM.
- **Bucle:** Permite la configuración de repetición del mensaje tomando un valor de “Desactivado” o 6 configuraciones de tiempo de 5 segundos a 5 minutos.

- **Frecuencia:** Se selecciona la frecuencia en la que se desea operar, esta se almacena mediante una memoria persistente.
- **Tamaño de paso:** permite seleccionar los tamaños del paso estándar.
- **Desviación:** permite configurar la desviación de 1 kHz a 150 kHz.
- **Ganancia:** La configuración de ganancia se encuentra a bajo de la frecuencia y marcada (0-47) LNA(IF) y AMP 0=0db o 1=14dB.
- **Barra de progreso de la transmisión:** Esta barra indica el progreso de la transmisión, en función de la longitud del mensaje.

3.1.1.2 OTROS EQUIPOS Y SOFTWARE

3.1.2 PROCEDIMIENTO EXPERIMENTAL

PRÁCTICA 1: Captura de Tráfico de Red Durante un Ataque de Jamming Constante

Objetivo:

Capturar y analizar el tráfico de red para identificar patrones de pérdida de paquetes durante un ataque de jamming constante.

Configuración inicial:

1. Configuración del router

Se considera la configuración de un router, enfocados en el wifi, uno de los más importantes es el Canal para utilizar, en este caso se utiliza el canal 9, debido a que es un ataque constante.

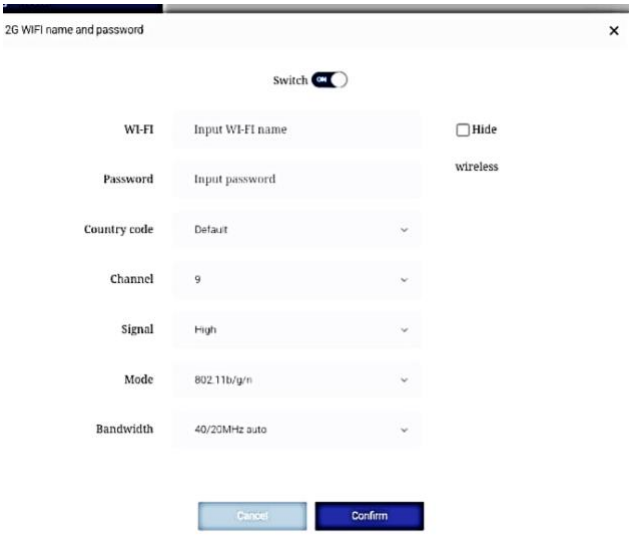


Ilustración 37.- Configuracion del Router

2. Conexión de dispositivos portátiles que puedan utilizar wifi, especialmente la frecuencia seleccionada y para denotar el ataque se realiza actividades normales, como transmisión de video o descarga de archivos.
3. Configuración de Wireshark en la laptop para capturar todo el tráfico de la red. Se escoge la captura de todo el trafico de la red Wifi y el funcionamiento se denota en los paquetes enviados y recibidos.

Ejecución del ataque:

1. Configura PortaHack H2 en modo de jamming constante en el canal 9 (frecuencia 2.452 GHz).

Ilustración 38.- Configuracion del portapack h2

2. Inicia el ataque desde una distancia de 3 metros.

Captura de datos:

1. Monitorea el tráfico en Wireshark durante 5 minutos.

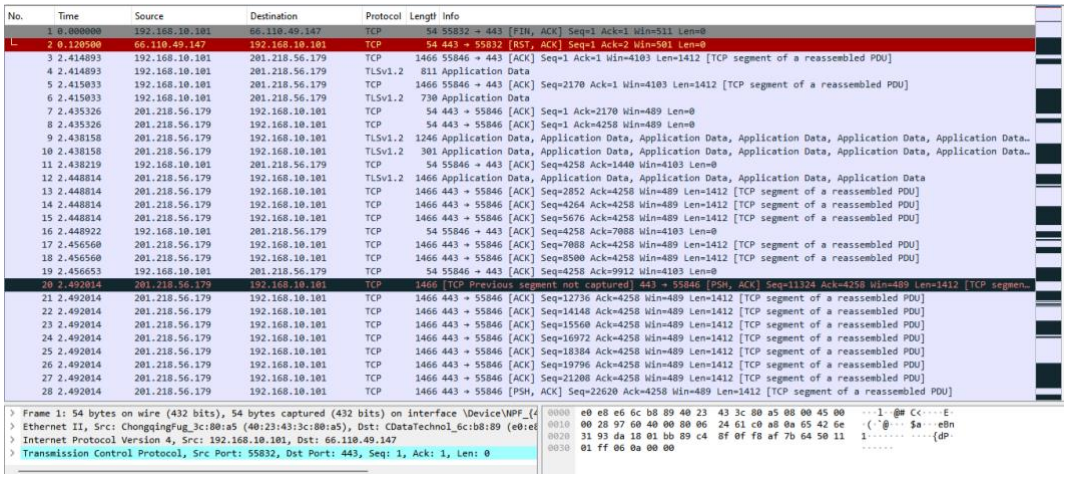


Ilustración 39.- Monitoreo en WireShark

2. Registra métricas como la cantidad de paquetes perdidos, retransmisiones y el tiempo de respuesta.

Análisis:

1. Revisa en Wireshark los gráficos de tráfico y filtros para identificar patrones, como caídas abruptas en la tasa de transferencia.

En las capturas se puede observar que durante el lapso que se estuvieron tomando capturas se obtuvo que existió una perdida de un 10.1% de datos, mientras que antes de ejecutar el ataque no existía perdida alguna.

Práctica 2: Análisis del Espectro RF Durante un Ataque Jump-Stay

Objetivo:

Visualizar los cambios en el espectro RF cuando el ataque de jamming utiliza la estrategia Jump-Stay (salto entre canales).

Pasos a seguir:

1. **Configuración inicial:**
    - Configura el router en modo de canal automático para permitir el uso de varios canales dentro de la banda de 2.4 GHz.
    - Conecta los dispositivos cliente y genera tráfico constante (por ejemplo, transmisión de video en YouTube).
    - Configura HackRF con SDRSharp para monitorear el espectro de frecuencias en tiempo real.
2. **Ejecución del ataque:**
    - Configura PortaHack H2 en modo Jump-Stay con intervalos de cambio de canal cada 2 segundos.
    - Inicia el ataque desde una distancia de 5 metros.
3. **Captura de datos:**
    - Observa en SDRSharp cómo se distribuye la interferencia en el espectro.
    - Registra la intensidad de señal en cada canal afectado.
4. **Análisis:**

- Identifica los canales más afectados y los patrones de salto.
- Documenta las frecuencias más vulnerables y la correlación con la actividad de los dispositivos cliente.

Práctica 3: Validación de un Sistema de Detección Basado en Latencia y Pérdida de Paquetes

Objetivo:

Probar un sistema de detección que identifique ataques de jamming basándose en métricas como latencia y pérdida de paquetes.

Pasos a seguir:

1. **Configuración inicial:**
   - Crea un script en Python que monitoree la latencia y pérdida de paquetes de la red usando la herramienta **Ping**.
   - Configura umbrales para generar alertas, por ejemplo:
     - Latencia > 100 ms.
     - Pérdida de paquetes > 10%.
   - Conecta un dispositivo cliente y genera tráfico constante.
2. **Ejecución del ataque:**
   - Configura PortaHack H2 en modo intermitente, alternando entre 10 segundos de ataque y 10 segundos de pausa.
   - Inicia el ataque desde una distancia de 5 metros.
3. **Captura de datos:**
   - Ejecuta el script en Python y deja que recolecte datos de latencia y pérdida de paquetes durante 5 minutos.
   - Registra las alertas generadas por el sistema.
4. **Análisis:**

- Compara las métricas registradas durante los períodos con y sin ataque.
- Valida si el sistema de detección es capaz de identificar los momentos exactos en los que ocurre el jamming.

Configuraciones Necesarias en el PortaPack H2

1. Hardware Necesario:

- **PortaPack H2**: Asegúrate de tener el dispositivo PortaPack H2 correctamente conectado al **HackRF One**, que es el hardware que habilita la capacidad de transmisión de señales en las frecuencias deseadas.
- **Antena**: Utiliza una antena adecuada para la frecuencia de 2.4 GHz (frecuencia de la banda Wi-Fi de 2.4 GHz). Asegúrate de que la antena esté orientada correctamente para maximizar el área de interferencia.

2. Configuración del PortaPack H2:

a) Iniciar el PortaPack H2:

- Conecta el **PortaPack H2** al **HackRF One**.
- Conecta ambos dispositivos a tu computadora a través de **USB**.
- Enciende el dispositivo y asegúrate de que esté correctamente reconocido por el software que usarás para configurar y monitorear el PortaPack H2 (como **CubicSDR** o **GNU Radio**).

b) Configuración de Jamming:

- En el **PortaPack H2**, accede al menú de **jamming** (puedes encontrarlo en la interfaz de PortaPack o en la aplicación que uses para controlarlo, como **CubicSDR**).
- Establece el **canal de Wi-Fi 6** en la frecuencia **2.437 GHz**. Este canal corresponde a la frecuencia utilizada por la mayoría de las redes Wi-Fi en la banda de 2.4 GHz.

- Configura el **modo de jamming constante**, donde el PortaPack H2 emitirá señales de interferencia en la misma frecuencia sin interrupciones.

c) Distancia del Ataque:

- Coloca el **PortaPack H2** a aproximadamente **3 metros** del router o del dispositivo objetivo, ya que esta distancia generará suficiente interferencia sin desbordar la capacidad de medición.
- Verifica que la señal de jamming esté suficientemente fuerte para interrumpir las conexiones sin que afecte demasiado a la visibilidad del análisis.

d) Configuración de Potencia de Transmisión:

- Ajusta la potencia de transmisión del PortaPack H2. Generalmente, en ataques de jamming, **una potencia de 20-30 dBm** es suficiente para generar interferencia en redes cercanas. Evita usar una potencia demasiado alta para prevenir daños al equipo o interferencia en otras redes.

1. Software Necesario:

- **Wireshark**: Para capturar el tráfico de red en la laptop.
    - **Instalación:** Descargado e instalado desde Wireshark.org.
    - **Configuración:** Inicia la captura en la interfaz de red Wi-Fi de la laptop que está conectada a la misma red que el dispositivo objetivo.
    - **Captura de tráfico:** Filtra el tráfico según el protocolo que quieras analizar, como tcp o icmp, y guarda los resultados en un archivo **.pcap** para análisis posterior.
- **CubicSDR** o **GNU Radio**: Para controlar y configurar el PortaPack H2.
    - **CubicSDR**: Un software gráfico que permite visualizar y controlar el PortaPack H2, disponible en CubicSDR.

- **GNU Radio**: Si prefieres una interfaz más avanzada, puedes usar GNU Radio para crear flujos de trabajo y controlar el PortaPack H2 a través de scripts.

2. Otros Dispositivos:

- **Laptop**: Donde ejecutarás Wireshark y el software para monitorear el tráfico de la red.
- **Smartphone**: Para realizar actividades normales (como navegar en la web, ver videos, o descargar archivos) que generen tráfico de red durante la prueba.
- **Router Wi-Fi**: El punto de acceso al que se conectarán tanto la laptop como el smartphone.

Pasos para Completar la Práctica:

1. **Conectar Dispositivos:**
   - Conecta la **laptop** y el **smartphone** al **router Wi-Fi**.
   - Asegúrate de que ambos dispositivos estén generando tráfico de red, como la transmisión de video, descarga de archivos, o navegación web.
2. **Configurar el PortaPack H2:**
   - Conecta el **PortaPack H2** al **HackRF One** y asegúrate de que esté alimentado correctamente.
   - Configura el PortaPack H2 en **modo jamming constante** a una frecuencia de **2.437 GHz** (canal 6).
   - Colócalo a una distancia de aproximadamente **3 metros** del router o del dispositivo objetivo.
3. **Capturar el Tráfico con Wireshark:**
   - Abre **Wireshark** en la laptop y selecciona la interfaz de red correcta (Wi-Fi).

- Inicia la captura de paquetes y deja que se capture el tráfico durante 5 minutos.
- Asegúrate de registrar el tráfico relevante, como la **pérdida de paquetes**, **retransmisiones**, y el **tiempo de respuesta**.

4. **Monitoreo y Análisis:**
   - Observa las métricas en Wireshark y anota cualquier anomalía, como un aumento en la **latencia**, **pérdida de paquetes**, o **retrasos**.
   - Guarda los resultados de la captura en un archivo **.pcap** para un análisis más profundo.
   - Revisa los **gráficos de tráfico** y las estadísticas de pérdida de paquetes o retransmisiones.
5. **Documentar los Resultados:**
   - Documenta los resultados de la prueba, incluyendo:
     - Las **condiciones previas** y **configuración** de los dispositivos.
     - **Métricas** observadas como **pérdida de paquetes**, **tiempo de respuesta**, y **retransmisiones**.

Gráficos de Wireshark que muestren cómo el ataque afectó el rendimiento de la red.

3.1.3 ANÁLISIS DE DATOS

Como parte del análisis, se creó un código que busca almacenar los datos y organizarlos en un arreglo ejecutable para comparar los cambios que sufre una red.

Codigo Phyton

```
import subprocess
import time
import re

# Configuración inicial
host = "192.168.10.1"  # Dirección IP del router u otro dispositivo en la red
```

```
threshold_latency = 100  # Latencia máxima permitida (ms)
threshold_loss = 10  # Pérdida de paquetes máxima permitida (%)
monitor_duration = 300  # Duración del monitoreo en segundos
interval = 1  # Intervalo entre pings (segundos)

def ping(host):
    """Ejecuta un comando ping y analiza los resultados."""
    try:
        # Ejecuta el comando ping
        output = subprocess.check_output(
            ["ping", "-n", "4", host],
            stderr=subprocess.STDOUT,
            universal_newlines=True
        )
        print("Resultado del comando ping:")
        print(output)  # Muestra el resultado para depuración
# Extraer latencia promedio (formato en español: "Media = XXms")
        latency_match = re.search(r"Media =(\d+)ms", output)
        latency = int(latency_match.group(1)) if latency_match else None

        # Extraer porcentaje de pérdida de paquetes (formato en español: "XX%
perdidos")
        loss_match = re.search(r"\((\d+)% perdidos", output)
        loss = int(loss_match.group(1)) if loss_match else 0

        return latency, loss
    except subprocess.CalledProcessError as e:
        print(f"[ERROR] El comando ping falló:\n{e.output}")
        return None, 100  # Asumir 100% de pérdida si falla
    except Exception as e:
        print(f"[ERROR] Ocurrió un error inesperado: {e}")
        return None, 100

def monitor_network():
    """Monitorea la red y detecta anomalías."""
    start_time = time.time()
    while time.time() - start_time < monitor_duration:
latency, loss = ping(host)
        if latency is not None and loss is not None:
            print(f"Latencia: {latency} ms | Pérdida de paquetes: {loss}%")

            # Detecta anomalías
            if latency > threshold_latency:
                print("[ALERTA] Latencia alta detectada.")
            if loss > threshold_loss:
                print("[ALERTA] Alta pérdida de paquetes detectada.")
        else:
```

```
        print("[ALERTA] No se pudo contactar al host. Verifique la conexión o la configuración.")

    time.sleep(interval)

# Ejecución del monitoreo
if __name__ == "__main__":
    print(f"Monitoreando la red durante {monitor_duration} segundos...")
    monitor_network()
```

Resultados del código en el espacio del programa y resultados en diagramas para su análisis.

```
Hora                Latencia (ms)  Pérdida (%)    Estado
============================================================
2024-12-20 05:34:57 4              0              OK
2024-12-20 05:35:01 9              0              OK
2024-12-20 05:35:05 5              0              OK
2024-12-20 05:35:09 4              0              OK
2024-12-20 05:35:14 4              0              OK
2024-12-20 05:35:18 5              0              OK
2024-12-20 05:35:22 24             0              OK
2024-12-20 05:35:26 6              0              OK
[ERROR] No se pudo enviar el correo: (535, b'5.7.8 Username and Password not accepted. For more information, go to\n5.7.8  https:
//support.google.com/mail/?p=BadCredentials e9e14a558f8ab-3c0e3f36354sm7948195ab.52 - gsmtp')
2024-12-20 05:35:30 900            0              Latencia Alta
[ERROR] No se pudo enviar el correo: (535, b'5.7.8 Username and Password not accepted. For more information, go to\n5.7.8  https:
//support.google.com/mail/?p=BadCredentials 8926c6da1cb9f-4e68bf676c6sm725178173.50 - gsmtp')
2024-12-20 05:35:44 432            0              Latencia Alta
2024-12-20 05:35:56 7              0              OK
2024-12-20 05:36:00 5              0              OK
2024-12-20 05:36:04 5              0              OK
```

Ilustración 40.- Captura de Datos del Código anterior

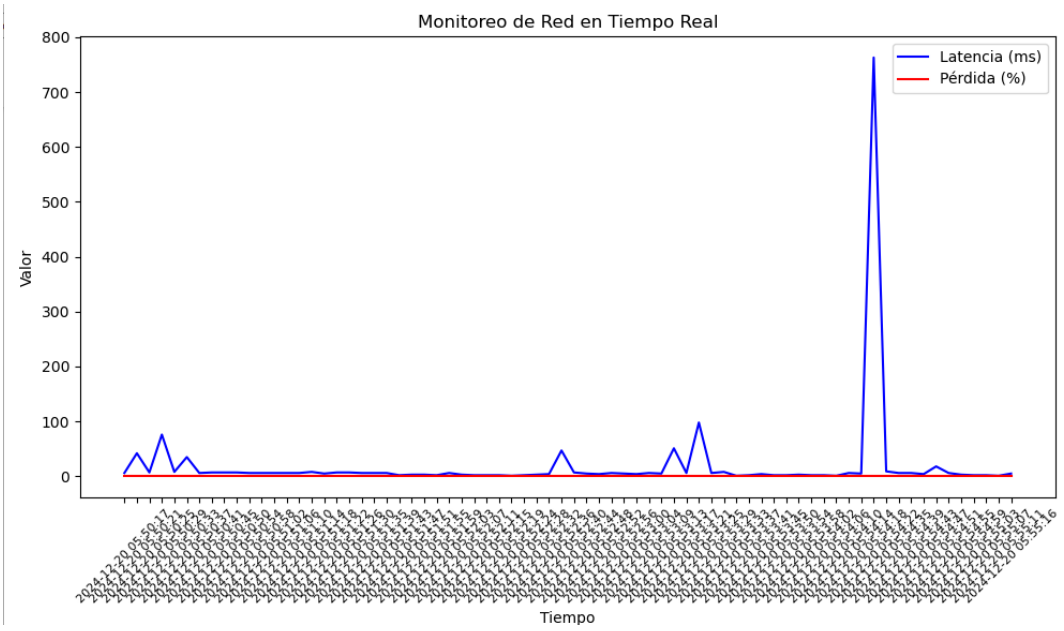


Ilustración 41.- Monitoreo de red en tiempo real

4 CAPITULO IV

4.1 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES.

El hecho de que se haya registrado una pérdida del 10.1% de los datos con el uso de un jammer, mientras que sin el jammer no hubo pérdida de datos, sugiere varios aspectos técnicos relevantes:

1. **Impacto de la interferencia**: La pérdida de datos en presencia de un jammer indica que la interferencia está afectando la capacidad del sistema para transmitir y recibir datos de manera eficiente. El jammer está generando ruido o señales que interfieren con las transmisiones legítimas, lo que puede resultar en errores de recepción o en la necesidad de retransmisiones, lo que contribuye a la pérdida de datos.

2. **Robustez del sistema ante interferencias**: La falta de pérdida de datos sin el jammer sugiere que el sistema es robusto y adecuado para operar en un entorno libre de interferencias. Sin embargo, la pérdida de datos cuando se introduce un jammer resalta una vulnerabilidad en la capacidad del sistema para manejar condiciones de interferencia. Este tipo de pruebas puede evidenciar que el sistema no tiene mecanismos de mitigación suficientes para contrarrestar el jamming.

3. **Eficiencia en la retransmisión y la corrección de errores**: Dependiendo del protocolo de comunicación utilizado, la pérdida de datos podría indicar una capacidad insuficiente para manejar errores o problemas causados por el jamming. La presencia de un jammer podría estar produciendo un número elevado de colisiones o fallos en la decodificación, lo que genera pérdidas de datos.

4. **Análisis de rendimiento bajo condiciones adversas**: Este tipo de prueba también ayuda a evaluar el rendimiento del sistema bajo condiciones de ataque o interferencia. Un análisis detallado de la frecuencia y la duración

de las pérdidas podría ofrecer insights sobre el impacto real del jammer en diferentes aspectos del rendimiento, como la tasa de datos o la latencia.

5. **Estrategias para mejorar la resistencia al jamming**: El resultado sugiere la necesidad de explorar estrategias que mejoren la resistencia del sistema al jamming, como el uso de esquemas de modulación más robustos, técnicas de detección y cancelación de interferencias, o la implementación de protocolos que prioricen la fiabilidad de las transmisiones en lugar de la velocidad.

En resumen, el análisis de la pérdida de datos con y sin jammer es fundamental para entender las debilidades del sistema ante interferencias y explorar soluciones para mejorar su desempeño en entornos ruidosos.

5 BIBLIOGRAFÍA

[1] J. M. Huidrovo, «Wi-Fi. Conectividad en todo lugar y momento-Asociacion de Autores Cientificos-Tecnicos y Academicos,» 11 2018. [En línea]. Available: https://www.acta.es/medios/articulos/informatica_y_computacion/035031.pdf. [Último acceso: 05 2022].

[2] F. Lopez Ortiz, «El estándar IEEE 802.11-Wireless LAN,» Septiembre 2019. [En línea]. Available: https://www.dit.upm.es/~david/tar/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf. [Último acceso: Julio 2022].

[3] T. Torres Israel, «UNIVERSIDAD NACIONAL DE CHIMBORAZO,» 27 Octubre 2021. [En línea]. Available: http://dspace.unach.edu.ec/handle/51000/8185.

[4] R. A. Gimenez, «Analisis de la Seguridad en Redes 802.11,» Marzo 2008. [En línea]. Available: https://www.securityartwork.es/wp-content/uploads/2008/10/seguridad-en-redes-80211.pdf. [Último acceso: Julio 2022].

[5] T. Unavarra, «Redes inalámbricas 802.11 y acceso al medio,» Enero 2019. [En línea]. Available: www.tlm.unavarra.es/~daniel/docencia/arss/arss09_10/slides/31y32-CSMA-CA.pdf. [Último acceso: Julio 2022].

[6] M. Fernandez, «CISCO, Wi-Fi 6E: La evolución del Wi-Fi estimula a renovar el modo de pensar la conectividad y manejar el espectro,» Agosto 2020. [En línea]. Available: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/smc-wifi6-evolution-latam-white-paper.pdf. [Último acceso: Julio 2022].

[7] Y. Huo, X. Dong, W. Xu y M. Yuen, «Co-Diseño Celular y Wi-Fi para equipos de usuario 5G,» IEEE Xplore, USA, 2018.

[8] B. Ayón Byron, «Beneficios de implementar una red con tecnología Mesh en la redes Inalambricas Universitarias,» *Publicaciones UCI*, pp. 185-195, 2020.

[9] J. Smith y M. Taylor, Wireless network security and spectrum analysis: Techniques for detecting jamming attacks., 2022.