UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TELECOMUNICACIONES

COMPONENTE PRÁCTICO DE EXAMEN COMPLEXIVO

INGENIERO EN TELECOMUNICACIONES

ANÁLISIS DE DETECCIÓN Y LOCALIZACIÓN DE DISPOSITIVOS NO AUTORIZADOS MEDIANTE ESCANEO DE RADIOFRECUENCIA Y HARDWARE ESPECIALIZADO

AUTOR:

HEIDY YUDITH CRUZ BERNABE

TUTOR SUGERIDO:

ING. FERNANDO CHAMBA MACAS

LA LIBERTAD- ECUADOR

2024

TRIBUNAL DE SUSTENTACION

PhD. Ronald Rovira Jurado

DIRECTOR DE LA CARRERA

Ing. Carlos Andrade Caicho

DOCENTE ESPECIALISTA

Ing. Fernando Chamba Macas

DOCENTE TUTOR

Ing. Luis Amaya Fariño

DOCENTE GUIA UIC

Ing. Corina Gonzabay De La A

SECRETARIA

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 Cruz Bernabe Heidy Yudith, como requerimiento para la obtención del título de Ingeniero en Telecomunicaciones.

La Libertad, a los 06 días del mes de Diciembre del año 2024

Ing. Fernando Chamba Macas

TUTOR

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Fernando Chamba Macas**

DECLARO QUE:

El trabajo de Titulación, Análisis de Detección y Localización de Dispositivo No Autorizado mediante Escaneo de Radiofrecuencia y Hardware Especializado 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 06 días del mes de Diciembre del año 2024

Ing. Fernando Chamba Macas

TUTOR

CERTIFICACION DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Análisis de Detección y Localización de Dispositivo No Autorizado mediante Escaneo de Radiofrecuencia y Hardware Especializado, presentado por la estudiante, Cruz Bernabe Heidy Yudith fue enviado al sistema anti plagio, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS

Cruz_Heidy_Tesina

5%

Textos sospechosos

Similitudes

2% Idiomas no reconocidos

2% Textos potencialmente generados por la IA

Nombre del documento: Cruz Heidy Tesina.docx
ID del documento: 72ddf5ad9626d6a7c8237cddd323e1845ee97864
Tamaño del documento original: 3.33 MB
Autores: []

Depositante: FERNANDO VINICIO CHAMBA MACAS
Fecha de depósito: 2/12/2024
Tipo de carga: interface
fecha de fin de análisis: 2/12/2024

Número de palabras: 16.039
Número de caracteres: 104.459

Ubicación de las similitudes en el documento:

Ing. Fernando Chamba Macas

TUTOR

AUTORIZACIÓN

Yo, **Cruz Bernabe Heidy Yudith**

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.

Cedo los derechos en línea patrimoniales del trabajo de titulación con fines de difusión pública, 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.

La Libertad, a los 06 días del mes de Diciembre del año 2024

Heidy Yudith Cruz Bernabe

AUTOR

DEDICATORIA

El presente trabajo de titulación va dedicado a mis padres, Omar Cruz y Shirley Bernabe, que siempre están brindándome su apoyo y son el pilar fundamental de mi vida. Además, su motivación me impulsa a superarme en cada etapa de mi vida profesional.

A mi esposo, German Rodríguez, y mi hijo, Gael Rodríguez, por ser la razón de mi superación día a día y por darme su apoyo y amor incondicional en todo momento.

A mi hermano, Juan Cruz, por estar siempre a mi lado, apoyándome con sus palabras de inspiración, las cuales fueron de gran ayuda en este proceso de aprendizaje.

A mis tíos, tías, abuelos y abuelas que aún están en mi vida, y a quienes me cuidan desde el cielo, este logro es para ustedes, con mucho amor.

Heidy Yudith Cruz Bernabe

AGRADECIMIENTO

Primeramente, agradezco a nuestro Señor Jesús por ser mi guía en el transcurso de la vida y por permitirme tener una familia maravillosa que siempre me brinda su apoyo incondicional.

A mis padres, por estar siempre a mi lado, a pesar de las adversidades que se presentaron durante mi carrera universitaria.

A mi esposo y a mi hijo, quienes son parte fundamental en este proceso de aprendizaje, ya que me inspiran a seguir luchando por mis sueños.

A mis compañeros, por el apoyo mutuo y por no rendirnos fácilmente, aprendiendo a convivir junto a los docentes, quienes fueron parte importante en nuestra formación y nos dejaron grandes enseñanzas en cada clase impartida.

Heidy Yudith Cruz Bernabe

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo tiene como objetivo principal analizar y localizar dispositivos no autorizados con el Detect Protect 1206i y el Narda SRM-3006 para el escaneo y análisis de radiofrecuencia, para esto se realizan prácticas de campo en el laboratorio de electrónica y telecomunicaciones, creando un escenario que simule la presencia de dispositivos no autorizados con el fin de detectar las señales con tecnología GSM, Bluetooth y Wi-Fi.

Las metodologías empleadas en este proyecto son la investigación bibliográfica, destinada a comprender los conceptos y las funcionalidades de cada una de las tecnologías antes mencionadas, también es importante conocer las especificaciones técnicas del Detect Protect 1206i y el Narda SRM-3006; y la experimental, en la que se configuran los módulos GSM SIM808 y Bluetooth HC-05 para simular dispositivos no autorizados los mismos que emiten señales para comprobar el funcionamiento del equipo Detect Protect 1206i.

En la primera práctica se hace uso del módulo SIM808, se identifica y examina la señal GSM con los dispositivos Detect Protect 1206i y Narda SRM-3006, los resultados obtenidos es que la señal opera en frecuencia de 850 MHz y se observó un aumento en la intensidad de la señal cuando se acercaba al dispositivo emisor.

En la segunda práctica se utiliza el módulo HC-05, encargado de emitir señales Bluetooth. Se detecta de manera correcta la señal con el Detect Protect 1206i y se registra en el Narda SRM-3006 la señal con rango de frecuencia de 2.402-2.48 GHz obteniendo la intensidad máxima en 2.46 GHz.

En la tercera práctica se detecta la señal Wi-Fi mediante la configuración de un dispositivo móvil simulando el equipo de espionaje en las bandas de 2,4 GHz con el uso del Narda SRM-3006 se detectan picos en el espectro que corresponden a canales activos, confirmando la capacidad del equipo para monitorear tecnologías inalámbricas en tiempo real.

Palabras Clave: Señales, Detección, Radiofrecuencia, Análisis.

ABSTRACT

The main objective of this work is to analyze and locate unauthorized devices using Detect Protect 1206i and the Narda SRM-3006 for radiofrequency scanning and analysis. To achieve this, field practices are carried out in the electronics and telecommunications laboratory, creating a scenario that simulates the presence of unauthorized devices to detect signals using GSM, Bluetooth, and Wi-Fi technologies.

The methodologies used in this project are bibliographic research, aimed at understanding the concepts and functionalities of each of the aforementioned technologies, and it is also important to know the technical specifications of the Detect Protect 1206i and the Narda SRM-3006; and the experimental methodology, in which the GSM SIM808 and Bluetooth HC-05 modules are configured to simulate unauthorized devices that emit signals to verify the operation of the Detect Protect 1206i..

In the first practice, the SIM808 module is used, the GSM signal is identified and examined with the Detect Protect 1206i and Narda SRM-3006 devices, the results obtained are that the signal operates at 850 MHz frequency and an increase in signal strength was observed when approaching the transmitting device.

In the second practice, the HC-05 module is used, which is responsible for emitting Bluetooth signals. The signal is correctly detected with the Detect Protect 1206i, and the Narda SRM-3006 registers the signal within a frequency range of 2.402–2.48 GHz, with the maximum intensity observed at 2.46 GHz.

In the third practice, the Wi-Fi signal is detected by configuring a mobile device simulating the spying equipment in the 2.4 GHz bands with the use of the Narda SRM-3006, peaks in the spectrum corresponding to active channels are detected, confirming the equipment's ability to monitor wireless technologies in real time.

Keywords: Signals, Detection, Radio Frequency, Analysis.

INTRODUCCIÓN

En esta época, el término de las telecomunicaciones es indispensable en la vida de las personas ya que permite la conexión entre individuos, así como también el intercambio de datos en diferentes tecnologías. Al aumentar el número de dispositivos inalámbricos, existe el riesgo de que se vinculen dispositivos no autorizados, por esta razón es importante mantener segura la comunicación [1].

El presente trabajo de investigación tiene como finalidad identificar las señales de radio que emiten las diferentes tecnologías inalámbricas GSM, Bluetooth y Wi-Fi, haciendo uso del dispositivo Detect Protect 1206i, para detectar señales de radio con diferentes frecuencias, además ayuda a localizar la fuente que emiten estas señales y verificar la ubicación del equipo de espionaje.

Las prácticas se realizan en el laboratorio de electrónica y telecomunicaciones, creando un escenario de pruebas en el que se colocan dispositivos que simulan los equipos no autorizados, también se llevó a cabo una revisión bibliográfica de términos necesarios para entender el propósito de la investigación, los resultados de cada práctica no solo sirvieron para entender la parte teórica de las tecnologías analizadas, sino que también se crearon guías practicas dirigidas a los estudiantes de telecomunicaciones.

La importancia de este trabajo radica en el uso del equipo Detect Protect 1206i que permite detectar las señales e intensidad de esta, también se usa el equipo Narda SRM-3006 para analizar la señal y confirmar el rango de frecuencia que se ubica la señal emitida, estos dos equipos se complementan para entender de manera detallada la señal de cada tecnología.

CAPITULO I

1. Generalidades de la Propuesta

1.1 Objetivos

Objetivo General

Analizar y localizar dispositivos no autorizados con el Detect Protect 1206i y el Narda SRM-3006 para el escaneo y análisis de señales con tecnologías GSM, Bluetooth y Wi-Fi.

Objetivos Específicos

- Programar los equipos necesarios para crear el escenario de pruebas.
- Utilizar el Detect Protect 1206i para detectar señales de las tecnologías GSM, Bluetooth y Wi-Fi.
- Evaluar las señales detectadas utilizando el Narda SRM-3006.
- Crear guías prácticas con el uso del Detect Protect 1206i dirigido a los estudiantes.

1.2 Metodología

Investigación Bibliográfica

En el transcurso del proyecto se hizo uso de la metodología de investigación bibliográfica para comprender ciertos términos necesarios para llevar a cabo el trabajo, temas como conceptos y funcionalidades de cada una de las tecnologías antes mencionadas, también es importante conocer los manuales técnicos que presentan los equipos utilizados en este trabajo en este caso el Detect Protect 1206i y el Narda SRM-3006.

Investigación Experimental

La investigación experimental se realiza en el laboratorio de electrónica y telecomunicaciones usando dispositivos que simulan el acceso de dispositivos no autorizados, dispositivos emisores como el módulo GSM SIM808 y el módulo Bluetooth HC05, los mismos que emiten señales para comprobar el funcionamiento del equipo Detect Protect 1206i asegurando que trabaja de manera correcta en cuanto a la detección visual y sonora, así mismo el equipo Narda SRM-3006 se

configuró de manera adecuada para analizar estas señales, los resultados se realizan de manera individual de cada tecnología, considerando términos de intensidad de señal, frecuencia e intensidad de la señal.

Los resultados de las pruebas experimentales facilitan la percepción de las capacidades y limitaciones de los equipos de detección, se identifican patrones específicos en las señales producidas que facilitan su análisis y clasificación, este procedimiento posibilita la validación de los procesos de detección.

1.3 Resultados Esperados

- Escenario de pruebas utilizando dispositivos que simulan la presencia de dispositivos no autorizados.
- Análisis de las señales GSM, Bluetooth y Wi-Fi, utilizando el Detect Protect 1206i y el Narda SRM-3006.
- Informe detallado que incluye comparaciones entre los resultados teóricos y las señales detectadas en el entorno de pruebas.
- Material educativo práctico que pueda ser utilizado por otros estudiantes o investigadores para comprender y operar el equipo de escaneo de señales.

1.4 Contexto y Justificación

1.4.1 Importancia de las Señales de Radio en Telecomunicaciones

Las señales de radiofrecuencia es un término muy utilizado en las telecomunicaciones, hace referencia a la trasmisión inalámbrica de datos a largas distancias, este tipo de comunicación ha progresado de manera favorable para la interacción de las personas.

La telefonía móvil, la conexión a internet y televisión son distintos servicios que requieren procesar y detectar señales, evolucionando en tecnología y conectividad a nivel mundial, estos servicios toman en cuenta la calidad, seguridad de datos, infraestructuras e innovación de la tecnología, mejorando los sistemas de comunicación actuales.

Hoy en día usar dispositivos inalámbricos presenta varios desafíos a cumplir como la protección de privacidad de datos sensibles, con la aparición de equipos de espionaje y técnicas de encriptación es importante contar con equipos que ayuden a detectar estas anomalías que se presentan en el medio.

Uno de los dispositivos que se recomienda utilizar es el Detect Protect 1206i que fue presentado en la sociedad para detectar señales de radio con diferentes frecuencias, siendo útil para muchos exploradores o profesionales en seguridad de datos, además ayuda a localizar la fuente que emiten estas señales y verificar la ubicación del equipo de espionaje [2].

1.4.2 Justificación del Uso del Equipo Detect Protect 1206i

La protección de la información y las comunicaciones ha adquirido importancia en sectores tan diversos como el corporativo y el gubernamental, la detección y el control de transmisiones no autorizadas se han vuelto necesarios, las tecnologías inalámbricas como Wi-Fi, Bluetooth y las redes móviles están en aumento, lo que facilita el uso de las telecomunicaciones modernas.

El Detect Protect 1206i está sujeto a la regulación en Ecuador por dos leyes, la primera es la Ley orgánica de telecomunicaciones que establece que el equipo puede ser utilizado en todo momento siempre y cuando cumpla con las normas establecidas por la Agencia de Regulación y Control de las Telecomunicaciones y la segunda es la Ley de protección de datos personales que brinda seguridad en lo que respecta a la vida privada de la persona. [3]

CAPITULO II

2. Fundamentación Teórica

2.1 Comunicación

La comunicación es la representación donde el emisor y receptor transmiten información a través de un medio, manejando un lenguaje o algún tipo de sistema de códigos [4], en el área de las telecomunicaciones esta comunicación se orienta a la transmisión de datos por medio de tecnologías que verifiquen la llegada de la información de manera rápida y precisa, este proceso no solo funciona con la interacción de personas, sino que también puede compartir información entre dispositivos.

Cuando se habla de un tema tecnológico, la comunicación se distribuye en varios componentes necesarios como el medio en que se transmiten los datos, los protocolos de comunicación que se utilizan, así como los equipos de enlaces. Dichos componentes permiten transportar la información de manera correcta y segura para que sea aplicada en diversos campos.

2.2 Tipos de Comunicación

Los tipos de comunicaciones se clasifican de acuerdo con el medio en que se propaga la información y el alcance que este brinda. Existen dos tipos: el primero es por medio de un cable físico, también llamado alámbrica, en el cual se recurre al cable coaxial y la fibra óptica. De esta manera, se hace posible la transmisión de señales con mayor velocidad. El segundo tipo es la comunicación inalámbrica, que, en vez de usar cables, emplea la propagación de ondas electromagnéticas que se transmiten por antenas.

En las telecomunicaciones, el tipo de comunicación se emplea tomando en cuenta la amplitud, donde se utilizan tecnologías de corto alcance como Wi-Fi y Bluetooth para transmitir datos en redes locales, la otra tecnología es de larga distancia como GSM, que brinda cobertura en zonas más extensas [5].

2.3 Tecnologías de Comunicación

Las tecnologías de comunicación han progresado para simplificar la difusión de datos a través de diferentes canales, estas tecnologías comprenden alternativas alámbricas, como la fibra óptica que proporcionan velocidad y estabilidad elevadas y alternativas inalámbricas como GSM, Wi-Fi y Bluetooth que proporcionan versatilidad y movilidad a los usuarios, cada tecnología se crea para cubrir requerimientos particulares desde la comunicación individual hasta la vinculación de dispositivos en el Internet de las Cosas (IoT).

En años recientes, los avances en las tecnologías de comunicación han propiciado progresos como el 5G [6], que promete velocidades de alta velocidad y una latencia reducida y las redes de área amplia de baja potencia (LPWAN), creadas para aplicaciones de IoT en áreas como la agricultura y la industria.

2.4 Tecnologías de Comunicación Inalámbrica

Las tecnologías de comunicación inalámbrica permiten la transmisión de datos inalámbricos, utilizando ondas de radio, microondas, o infrarrojas entre las más comunes están Wi-Fi, Bluetooth y redes GSM, la conectividad moderna depende de estas tecnologías, que facilitan la comunicación en tiempo real entre dispositivos [7].

Además de su versatilidad, las tecnologías inalámbricas resultan imprescindibles en usos contemporáneos como el Internet de las cosas (IoT) y la comunicación en tiempo real, el aumento en la necesidad de soluciones ha impulsado la creación de normas y protocolos que aseguran interoperabilidad, eficacia y protección en las conexiones como WPA3 para Wi-Fi y BLE para dispositivos de consumo reducido.

2.5 Telefonía Móvil

La tecnología móvil es una de las más empleadas a nivel global, facilitando la transmisión de voz, datos y contenidos multimedia mediante redes inalámbricas [8], desde sus comienzos con GSM ha progresado hacia tecnologías más sofisticadas como 3G, 4G y 5G, proporcionando velocidades y capacidades de conexión superiores, estas redes están formadas por varios componentes como

estaciones base, controladores de red y centros de conmutación, que complementan la infraestructura para ofrecer cobertura y calidad de servicio.

2.5.1 Tecnología GSM

La tecnología GSM es una red de telefonía móvil utilizada en la vida diaria por individuos de diferentes edades en todo el mundo, la capacidad y funciones que brinda esta tecnología hace que su uso sea indispensable en la vida cotidiana de las personas [9].

2.5.1.1 Principios de Funcionamiento

La red GSM sirve para la comunicación móvil su uso hace posible la trasmisión de datos y voz a través de redes móviles, esta tecnología admite que diferentes usuarios accedan a un mismo canal de frecuencia de acuerdo al periodo de tiempo asignado por cada registro de llamada, se emplea la modulación por diferencia de fase conocida como PSK que permite la transmisión de datos digitales haciendo uso de tarjetas SIM que sirven como asociación y certificación de usuarios [10].

La tecnología GSM utiliza distintas bandas de frecuencias de acuerdo con la zona geográfica que se encuentre el usuario, en Europa se utilizan de 900 a 1800 MHz y en Estados Unidos se usa la frecuencia de 1900 MHZ, esto quiere decir que los dispositivos GSM no serán compatibles en las distintas naciones del mundo.

2.5.1.2 Arquitectura de la red GSM

La arquitectura GSM está compuesta por los siguientes elementos [11]:

- **Estación móvil:** Cada teléfono representa una estación móvil.
- **Tarjeta SIM:** El primer paso para que la estación funcione es el uso de la tarjeta SIM en la que se guarda información necesaria del equipo, usuario y el operador de red.
- **IMEI:** Todos los dispositivos o estaciones móviles cuentan con un IMEI, que es un identificador único que lo distingue del identificador de la tarjeta SIM.

- **Estación base:** En esta etapa opera la tarjeta SIM, permitiendo que la estación base detecte quién está llevando a cabo la comunicación mediante ondas de radiofrecuencia.
- **Controlador de estaciones base:** El controlador conecta a las estaciones base, optimizando que exista una buena comunicación.
- **Centro de conmutación:** Esta es la fase final, en la que los controladores están enlazados al centro de conmutación por medio del operador de teléfono, en esta etapa se realiza la recolección de datos y se confirma la identidad de las tarjetas SIM que requieran acceso a los servicios.

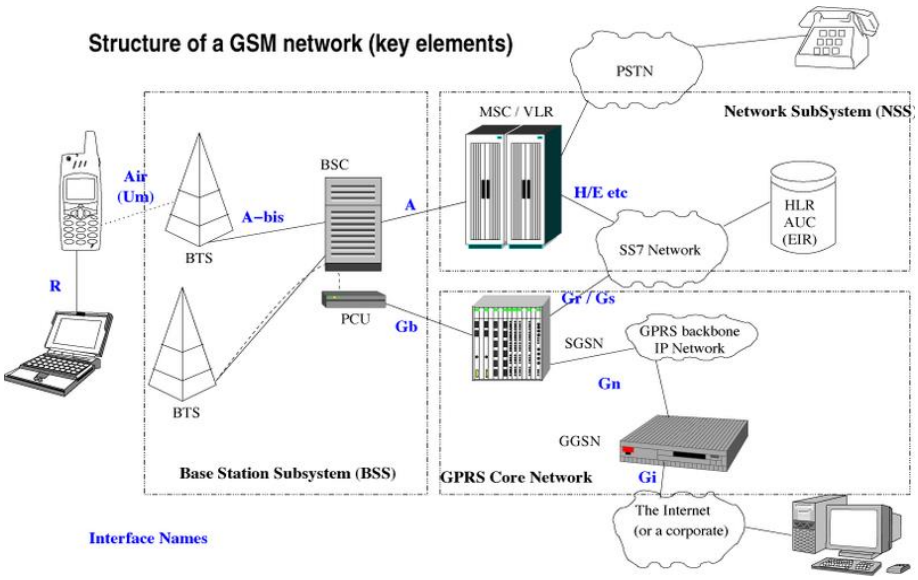


Ilustración 1 Arquitectura de la tecnología GSM Fuente [12]

2.6 Tecnología de Corto Alcance

Las tecnologías de corto alcance son sistemas de comunicación sin cables diseñados para crear conexiones entre aparatos que están en una cercanía cercana, usualmente en un rango de 100 metros [13]. Estas tecnologías se distinguen por emplear bandas de frecuencia sin licencia, tales como 2.4 GHz y 5 GHz, lo que las convierte en económicas y accesibles para una variedad de usos.

2.6.1 Bluetooth

En sus inicios, la tecnología Bluetooth era la más empleada para intercambiar datos entre dispositivos a poca distancia; esta red facilita la

transmisión de fotos y música, hoy en día ha progresado y permite realizar más actividades como sistema de manos libres en automóviles, auriculares inalámbricos, entre otros dispositivos [9].

2.6.1.1 Principios de Funcionamiento

El funcionamiento de la tecnología Bluetooth requiere el uso del espectro que trabaja a una frecuencia de 2.4 GHz, se usa para transmisión de información a una distancia de 100 metros, esto de acuerdo al dispositivo que se esté empleando, esta tecnología emplea el método de salto de frecuencia, es decir, que la señal va a cambiar continuamente en las distintas frecuencias dentro del rango de espectro que se le ha asignado, esto va a permitir la disminución de interferencias que se presenten en el medio [14].

2.6.1.2 Perfiles de Bluetooth y sus Aplicaciones

Cuando se habla de perfiles Bluetooth, se hace referencia a un conjunto de protocolos o normas que permiten a esta tecnología llevar a cabo tareas específicas. Existen varios perfiles de Bluetooth, los cuales se describen a continuación [15]:

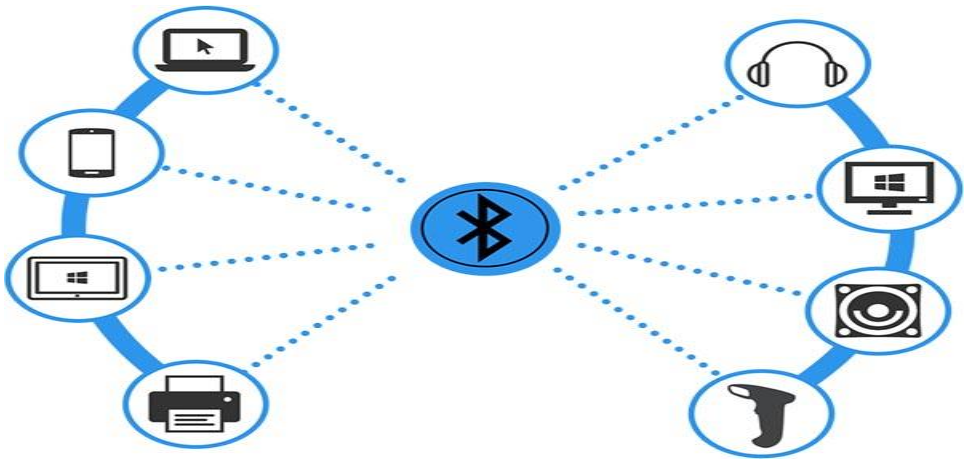


Ilustración 2 Perfiles de Bluetooth. Fuente [16]

- **Perfil de Distribución de Audio Avanzada (A2DP):** Este perfil garantiza el envío de información como archivos multimedia entre distintos dispositivos.

- **Perfil de Transferencia de Archivos (FTP):** El perfil de transferencia de archivo tiene el mismo objetivo que el perfil anterior sin embargo el usuario puede compartir archivos de forma remota.
- **Perfil de Identificación de Dispositivo (DIP):** A diferencia de los otros perfiles, el perfil de identificación de dispositivo permite la exigencia de reconectar dispositivos al momento de realizar la descarga de controladores.
- **Perfil Manos Libres (HFP):** Tiene la función de ejecutar llamadas inalámbricas como las utilizadas en sistemas de comunicación de manos libres de vehículos modernos.

2.6.2 Wi-Fi

La tecnología Wi-Fi es reconocida como la tecnología inalámbrica más usada en la vida diaria de las personas ya sea en la casa, en el lugar de trabajo o en centros comerciales, su uso es tan habitual que resulta casi imposible no reconocer a alguien que esté utilizando un teléfono inteligente sin estar en conexión con internet [9].

2.6.2.1 Principios de Funcionamiento

La tecnología inalámbrica Wi-Fi trabaja con el estándar IEEE.802.11 este estándar facilita la comunicación entre distintos dispositivos en redes locales, por medio de ondas de radio frecuencia, normalmente las bandas de frecuencia que emplea esta tecnología son de 2.4 GHz y 5 GHz, posibilitando el enlace por medio de puntos de acceso de múltiples dispositivos a internet [17].

Wi-Fi cuenta con protocolos de seguridad como es el caso de WPA2 y WPA3 que sirven para mantener protegidas las conexiones haciendo uso de la autenticación y cifrado de los datos, esto permite que otros dispositivos no autorizados se conecten a la red, también administra el acceso compartido al espectro, permitiendo que varios dispositivos operen al mismo tiempo sin que exista mucha interferencia.

2.6.2.2 Estándares y Protocolos Wi-Fi

Los estándares facilitan la conectividad de dispositivos cuando se utilizan protocolos compartidos, lo que garantiza una buena conexión, a partir de 1997 esta tecnología ha tenido un progreso, mejorando su velocidad, estabilidad y latencia que son términos importantes para tener una red en condiciones adecuadas [18].

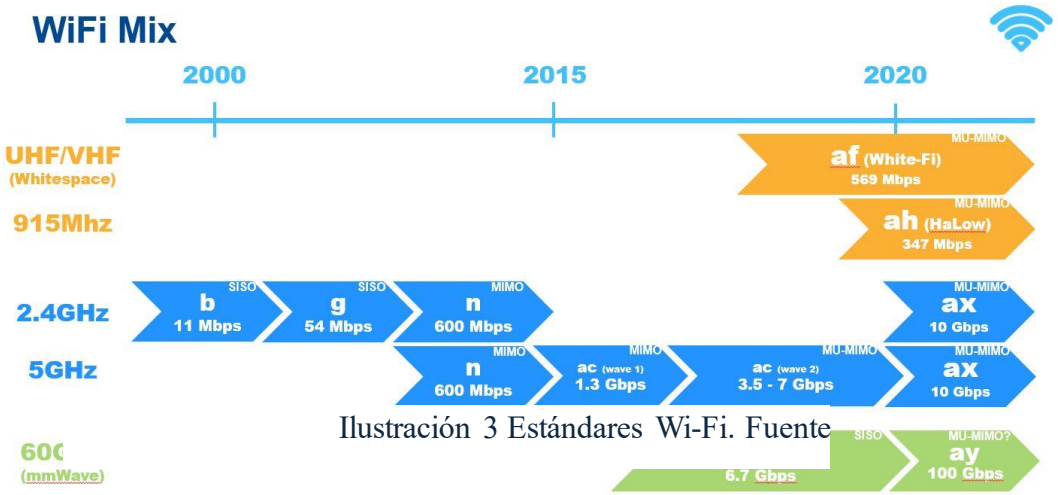


Ilustración 3 Estándares Wi-Fi. Fuente [19]

Wi-Fi cuenta con diversas clases el Wi-Fi 1 opera con 2 Mbps, Wi-Fi 5 y Wi-Fi 6 trabajaron con velocidades mejoradas que iban de 600 Mbps y 1.73 Gbps, la clase Wi-Fi 6e alcanzó 9.6 Gbps, obteniendo una eficiencia superior y finalmente Wi-Fi 7 que se cree que para este año alcance hasta 40 Gbps que tenga un rendimiento avanzado en las aplicaciones.

Tabla 1 Estándares Wi-Fi Fuente Otero. E

ESTANDAR	NOMBRE COMERCIAL	AÑO DE LANZAMIENTO	PRINCIPALES MEJORAS
IEEE 802.11	Wi-Fi 1	1997	Implementación de conexión inalámbrica básica, alcanzando 2 Mbps en 2,4 GHz.
IEEE 802.11ª	Wi-Fi 2	1999	Velocidad máxima de 54 Mbps en 5 GHz,

			mejorando su desempeño en lugares poco poblados.
IEEE802.11b	Wi-Fi 3	1999	Alcance mejorado y mayor confiabilidad, con velocidades de hasta 11 Mbps en 2.4 GHz.
IEEE802.11g	Wi-Fi 4	2003	Velocidades de 54 Mbps en 2,4 GHz, retrocompatibilidad con dispositivos IEEE 802.11b.
IEEE 802.11n	Wi-Fi 5	2009	Se empleó la técnica MIMO que alcanzó una velocidad de 600 Mbps con una cobertura de 2.4 y 5 GHz.
IEEE802.11ac	Wi-Fi 6	2014	Se logró obtener 1.73 Gbps mediante el incremento de flujos espaciales, logrando un mayor ancho de banda.
IEEE802.11ax	Wi-Fi 6e	2019	Se implementa el uso de OFDMS, con una velocidad de 9.6 GHz y una mayor eficiencia espectral.
IEEE802.11be	Wi-Fi 7	Prevista 2024	Se pretende alcanzar una velocidad de 40 Gbps con poca latencia y que aumente su eficiencia.

2.7 Espionaje Industrial o Corporativo

El espionaje industrial o corporativo se caracteriza por la adquisición ilícita de datos sensibles o estratégicos de una compañía, con la finalidad de conseguir ventajas competitivas en el mercado [20]. Este fenómeno, que impacta a corporaciones de grandes y pequeñas empresas, puede abarcar el hurto de secretos comerciales, datos económicos, tácticas de marketing, avances tecnológicos y cualquier información valiosa que brinde un beneficio financiero.

Las estrategias de espionaje empresarial han progresado conforme la tecnología progresa, hoy en día este tipo de acciones abarca tanto técnicas convencionales, como la infiltración de trabajadores, como técnicas tecnológicas de vanguardia, el hackeo, la ingeniería social y la utilización de dispositivos de escucha.

2.8 Surgimiento del Espionaje Industrial

El espionaje industrial se originó en los primeros sistemas económicos fundamentados en la rivalidad por el dominio de mercados y tecnologías, desde la Revolución Industrial, cuando las compañías empezaron a confiar en las innovaciones tecnológicas para ganar competitividad, el espionaje se transformó en un recurso empleado para sobrepasar a los competidores, un caso histórico destacado es la sustracción de secretos de producción de seda china, lo que facilitó a Europa la competencia en el sector textil [21].

En la era digital, este término aumentó de manera rápida, la digitalización y la interconexión de datos a escala global han facilitado la obtención de datos sensibles a través de medios digitales, haciendo que el espionaje sea una actividad de menor costo y sea más difícil de detectar.

2.9 Principios de Ataque

Los principios del ataque en el sector de espionaje industrial se basan en la identificación, acceso y adquisición de datos sensibles mediante diferentes estrategias [22]:

- Identificación y recolección de datos iniciales: Los cibernéticos evalúan el escenario que quieren atacar, empezando por verificar el área de interés

como también conocer los datos de la persona encargada de la misma, también toman en cuenta el tipo de tecnología que se está utilizando, todo esto para poder aplicar estrategias de cómo intervenir en la red.

- Infiltración y entrada no permitida: Una vez verificada la identificación y recolección de datos, se llega a la etapa de infiltración para lo cual el atacante usa técnicas de hackeo para entrar al sistema y obtener de manera rápida la información.
- Análisis y aplicación de la información: La última etapa es el análisis que realizan los atacantes con la información recolectada por lo cual se favorecen de la misma para usos malintencionados.

2.10 Hardware Especializado en Escaneo de Radiofrecuencia

El escaneo de radiofrecuencia es importante en el análisis y detección de dispositivos no autorizados, como pueden ser micrófonos, cámaras o transmisores ocultos que operan en diferentes frecuencias como GSM, Bluetooth y Wi-Fi, para lograr esto se emplean herramientas especializadas como el Detect Protect 1206i y el Narda que facilitan la localización de señales emitidas por estos dispositivos.

2.10.1 Tipos de Dispositivos de Escaneo de Señales de Radiofrecuencias

En el mercado, existen diferentes tipos de dispositivos que se utilizan para el escaneo y monitoreo de señales de radiofrecuencia, estos se dividen principalmente en dos categorías que son:

- Detectores de Radiofrecuencias

Los detectores de radiofrecuencias son herramientas portátiles diseñadas para captar emisiones de radiofrecuencia en un rango amplio de frecuencias, estos dispositivos, como el Detect Protect 1206i, están equipados con antenas y circuitos especializados para detectar señales de hasta 6 GHz [23], abarcando las bandas más comunes usadas por dispositivos como cámaras inalámbricas y micrófonos espía. Sus características incluyen:

- Sensibilidad: Capacidad para detectar señales de baja potencia.
- Indicación visual y auditiva: Medidores de nivel de señal para guiar la localización del dispositivo.

- ❖ Portabilidad: Generalmente son dispositivos compactos, diseñados para uso móvil.

- Analizadores de espectro

Son dispositivos que ayudan a analizar el espectro en el campo electromagnético de una señal, para verificar la potencia y frecuencia en la que se encuentra la misma, facilitando el trabajo de conocer y realizar el análisis de estos patrones [24].

2.10.2 Detect Protect 1206i

El Detect Protect 1206i es un equipo que tiene la función de identificar señales ocultas y proteger a los sistemas de vigilancia, este dispositivo tiene la capacidad de detectar señales que emplean protocolos de bluetooth y Wi-Fi a largas distancias, a diferencia de otros equipos se les complica captar las señales debido a su baja potencia de emisión y al tipo de modulación que se utilice [25], el dispositivo cuenta con antenas que operan a frecuencias de 2.4 y 5 GHz lo que facilita detectar y localizar estas señales con una gran precisión.

Ilustración 4 Detect Protect 1206i [26]

En la tabla se presentan las especificaciones técnicas de Detect Protect 1206i.

Tabla 2 Especificaciones Técnicas del Detect Protect 1206i

Especificaciones Técnicas del Protect 1206i

Gama de Frecuencias	Antena 1: 50-12000 MHz; Antena 2: 2.4-2.48 GHz; 4.9-5.875 GHz
Potencia	Dos pilas AAA (2xLR03)
Dimensiones	Sin antenas: 120x70x16 mm Con antenas: 210x70x16 mm
Consumo actual	Hasta 30 mA
Duración de la operación	Hasta 20 horas
Indicaciones	Antena activa, batería baja, modo, identificación, atenuador, demodulación secundaria.
Antena Micro-Pointer	
Gama de Frecuencias	2-12 GHz
Tipo	Conjunto logarítmico-periódico
Nombre	LPDA-12
Dimensiones	53x84x9 mm
Conector	SMA Macho

2.10.3 Narda SRM-3006

El NARDA SRM-3006 es un instrumento de medición especializado en campos electromagnéticos, con un rango de operación que abarca frecuencias desde 9 kHz hasta 6 GHz [27], este equipo emplea una antena de tres ejes para captar de manera precisa diversos parámetros, tales como la intensidad de campo electromagnético, la intensidad de campo magnético y la densidad de potencia.

Ilustración 5 Narda SRM-3006 [28]

En la siguiente tabla se detallan las especificaciones técnicas más importantes que presenta este equipo.

Tabla 3 Especificaciones Técnicas del Narda SRM-3006

Especificaciones Técnicas del Narda SRM-3006	
Rango de frecuencia	9 KHz – 6 GHz
Tipo de medición	Campo eléctrico
Rango dinámico	70 dB
Resolución de ancho de banda	1 Hz – 3 Hz
Precisión de medición	2 dB
Receptividad	-170 dBm/Hz
Tipo de operación	LTE - FDD/TDD, UMTS y 5G.
Sistema de comunicación	USB y Ethernet
Sistema de comunicación	4 horas

2.11 Técnicas de Detección de Dispositivos

Las técnicas de detección de dispositivos no autorizados juegan un papel importante en la seguridad de la red, a continuación, se detallan los principios necesarios y técnicas de escaneo que se usan para diferenciar entre señales legítimas y falsas.

2.11.1 Principios de Detección de Radiofrecuencia

La detección de dispositivos a través de radiofrecuencia utiliza señales emitidas por dispositivos que utilizan una variedad de tecnologías de comunicación, como GSM, Wi-Fi y Bluetooth, para identificar y analizar estos dispositivos. Los receptores sintonizados a las frecuencias de interés se utilizan en los sistemas de detección de radiofrecuencia para capturar y procesar las señales que pueden provenir de dispositivos electrónicos [29].

Uno de los principios importantes es la medición de parámetros de señal como frecuencia, potencia de señal, tiempo de llegada para poder encontrar y clasificar los equipos dependiendo de las características del espectro de radiofrecuencia.

2.11.2 Métodos de Escaneo de Radiofrecuencia

Los principales procedimientos de escaneo de radiofrecuencia son:

- **Escaneo activo:** En este procedimiento, el sistema de detección envía señales sonoras y se espera un tiempo prolongado para que los dispositivos cercanos respondan, lo que resulta beneficioso para identificar dispositivos que reaccionan rápidamente a las peticiones de comunicación [30].
- **Escaneo pasivo:** El sistema va a detectar las señales que los otros dispositivos van a estar emitiendo sin la necesidad de pedir nada para la identificación de dispositivos en modo de escucha o enviar señales de manera pasiva, su funcionamiento es óptimo [30].
- **Escaneo direccional:** Se hace uso de antenas direccionales y se emplea el escaneo pasivo para que sea fácil encontrar la fuente de la señal lo que permite conocer la ubicación exacta del dispositivo que emite la señal [30].

2.11.3 Identificación de Señales Legítimas vs. No Legítimas

Las señales legítimas o autorizadas provienen de equipos electrónicos como routers, teléfonos, cámaras o algún otro equipo de comunicación que trabaje dentro de las regulaciones permitidas, por otro lado, están las señales no legítimas o no autorizadas que son generadas por dispositivos de espionaje que intentan operar fuera del rango de frecuencias [31].

Para entender cómo se propaga una señal en el espectro de frecuencias es necesario conocer los patrones y huellas espectrales, siendo esta la identificación que cada dispositivo, para verificar el ancho de banda y potencia que el dispositivo genere dependiendo de la tecnología de transmisión que se use.

2.12 Dispositivos No Autorizados en Redes Empresariales

2.12.1 Módulo GSM SIM 808

Esta tarjeta de comunicación inalámbrica destaca por su diseño ultra compacto y su amplia compatibilidad, ya que puede utilizarse con cualquier modelo de Arduino en formato Uno, su diseño se basa en el módulo SIM808 GSM, lo que le permite ofrecer funciones de comunicación mediante GPRS [32].

.

Ilustración 6 Módulo GSM [33]

La configuración y el control de la tarjeta se realizan a través de UART utilizando comandos AT. Para comenzar a utilizarla, basta con conectarla al microcontrolador deseado, como Arduino, y enviar los comandos AT necesarios.

Tabla 4 Especificaciones Técnicas del Módulo GSM

Especificaciones Técnicas del Módulo GSM	
Voltaje de alimentación externo	5-12V DC
Voltaje de Funcionamiento	V
Consumo de Corriente en Modo de Suspensión	1.5mA
Compatibilidad de Batería RTC	3V CR1220
Antena GSM	conector SMA
Frecuencias GSM/GPRS Soportadas	850/900/1800/1900 MHz

Velocidad Máxima de Datos GPRS	Descarga: 85.6 Kbps, Carga: 42.8 Kbps

2.12.2 Módulo Bluetooth HC-05

El módulo Bluetooth HC-05 ofrece una solución sencilla para establecer comunicación inalámbrica entre proyectos basados en Arduino y dispositivos como smartphones, celulares o computadoras personales [34], funciona como un puerto serial, lo que permite transmitir datos de manera transparente para el programador, conectándose directamente a los pines seriales del microcontrolador.

Ilustración 7 Módulo Bluetooth HC-05 [35]

Permite configurar todos sus parámetros a través de comandos AT, la placa incluye un regulador integrado de 3.3V, lo que posibilita alimentarlo con un rango de voltaje entre 3.6V y 6V. Este módulo es una herramienta versátil y práctica para proyectos en áreas como robótica, domótica y control remoto.

Tabla 5 Especificaciones Técnicas del Módulo Bluetooth

Especificaciones Técnicas del Módulo Bluetooth	
Voltaje de operación	3.6V - 6V DC
Consumo corriente	50mA
Frecuencia	Banda ISM 2.4GHz
Modulación	GFSK (Gaussian Frequency Shift Keying)
Sensibilidad	-84dBm a 0.1% VER

Interface comunicación	Serial TTL
Velocidad de transmisión	1200bps hasta 1.3Mbps

2.12.3 Teléfonos Redmi

Los teléfonos móviles de la marca Redmi pertenecen a los teléfonos fabricados por Xiaomi, estos dispositivos tienen un precio accesible para los usuarios y desde su aparición en el mercado, son conocidos por las diferentes características que poseen. Resaltando estos dispositivos como gama media cubriendo las necesidades de los usuarios, dependiendo del modelo del teléfono varían las características.

Ilustración 8 Teléfono Redmi [36]

A continuación, se exponen las características más habituales de los teléfonos Redmi.

Tabla 6 Especificaciones Técnicas del Teléfono Redmi

Especificaciones Técnicas del Teléfono Redmi	
Pantalla	LCD 6,74" HD + 90 Hz
Procesador	Helio G85
Cámara	8 MP f/2.0
Batería	5.000mA, Carga rápida 18W
Almacenamiento/RAM	4 / 6 / 8 GB y 128 / 256 GB
Sistema operativo	MIUI 14, Android 13

Conectividad	4G/5G, Wi-Fi, Bluetooth 5.0

CAPITULO III

3. Escaneo y Comparativa de Señales en las Tecnologías GSM, Bluetooth y Wi-Fi.

3.1 Introducción

La detección y análisis de señales inalámbricas, como GSM, Bluetooth y Wi-Fi, es importante en la gestión de redes y la seguridad de la información en ambientes de alta conectividad, la variedad de protocolos y frecuencias utilizadas en estas tecnologías plantea el desafío de contar con equipos y procedimientos específicos que permitan la correcta identificación, comparación y monitoreo de cada tipo de señal mediante este capítulo se explorará las distinciones funcionales y matizadas en la recepción de señales dentro de estas tres modalidades mediante el uso de los equipos Detect Protect 1206i y Narda SRM-3006, las herramientas de monitoreo de redes también se utilizan en diversas industrias para identificar posibles vulnerabilidades o dispositivos no aprobados en instalaciones críticas.

3.1.1 Objetivos del Capítulo

- Presentar una descripción general de las diferencias técnicas en la captura de señales GSM, Bluetooth y Wi-Fi
- Detallar los pasos necesarios para configurar y ajustar el Detect Protect 1206i para un correcto escaneo
- Comparar los resultados obtenidos de los equipos Narda SRM-3006 y Detect Protect 1206i

3.1.2 Importancia de la Implementación Práctica

La capacidad de detectar y analizar diferentes señales es necesaria en un mundo donde las comunicaciones inalámbricas han evolucionado, un escaneo adecuado de estas señales permite identificar patrones de uso como

posibles interferencias e incluso brechas de seguridad, mejorando la eficiencia y la confiabilidad de las redes inalámbricas mediante una configuración adecuada y un ajuste preciso de los equipos se maximiza la capacidad de los ingenieros para obtener información útil y procesable.

La implementación del escaneo de señales es vital para detectar:

- Dispositivos no autorizados
- Interferencias maliciosas o espionaje

3.1.3 Procedimiento General para el Escaneo

Preparación del Equipo de Escaneo

Seleccionar el equipo adecuado para el escaneo en función de las señales que se desean detectar. En este procedimiento se utilizarán los dos equipos mencionados, puesto que son adecuados para utilizarlos en la detección de señales GSM, Bluetooth y Wi-Fi. También se debe de tener en cuenta que los equipos deben de estar en buen estado, con baterías cargadas y actualizado si el equipo lo requiere.

Selección de Antenas en el Detect Protect 1206i

En este equipo se debe seleccionar la antena correcta dependiendo de la frecuencia y tipo de señal que se desea detectar. El rango de frecuencia que escanea la antena uno es de 50 a 12000 MHz y en la antena 2 escanea un rango de frecuencia de 2.4 a 5 GHz. Como se van a emplear frecuencias bajas que es el caso de GSM se hará uso de la antena uno mientras que para frecuencias más altas como Bluetooth y Wi-Fi que trabajan en frecuencia de 2.4 GHz se utilizará la antena 2.

Configuración Inicial de los Equipos

Para realizar una detección con el equipo Detect Protect 1206i se deben conocer los botones y controles del equipo, como se mencionan a continuación:

- **(POWER):** Permite encender y apagar el equipo mediante el interruptor.
- **(ANT1/ANT2):** Selección alterna entre las dos antenas disponibles, sabiendo que el botón ANT1 cubre el rango de frecuencia amplio (50-12.000 MHz) mientras que el botón ANT2 es especializado en frecuencias de 2.4 GHz y 5 GHz.

- **(MODE):** Diferentes modos de operación del equipo como el modo sonido permite que el equipo emita alertas audibles al detectar una señal, el modo vibración permite que el equipo vibre al detectar señales y por último el modo mixto combina las alertas sonoras y vibración
- **(CORR):** La función de este botón es clasificar, permitiendo identificar transmisores de FM y utiliza impulsos sonoros de prueba.
- **(ATT):** Ajusta la sensibilidad del dispositivo ayudando a reducir la intensidad de las señales cercanas en el caso del botón (ATT+) va a aumentar la atenuación lo que reduce la sensibilidad del dispositivo ignorando las señales más débiles y enfocándose en las señales fuertes o cercanas sin interferencias y el botón (ATT-) va a disminuir la atenuación lo que incrementa la sensibilidad del dispositivo permitiendo detectar señales más débiles y de mayor alcance.
- **(IDENTIFICATION LED):** Identificación del protocolo según el color:
  Bluetooth indicador azul
  Wi-Fi indicador verde
  GSM indicador rojo
  DECT indicador naranja
- **(DEMODULATION):** Muestra fluctuaciones que indican la presencia de señales moduladas y es útil para analizar la naturaleza de la señal detectada.

En el caso del NARDA SRM-3006 para detectar y analizar dispositivos no autorizados, se detallan los pasos de configuración:

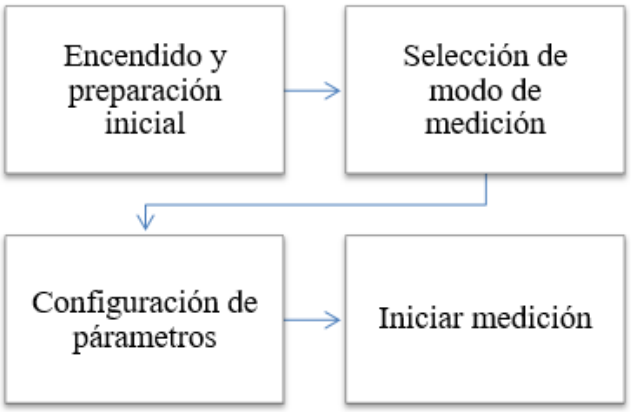


Ilustración 9 Pasos de configuración Narda SRM-3006.
Fuente [Autor]

1. **Encendido y Recomendación Inicial:** Presiona el botón de encendido hasta que el SRM-3006 se encienda, es necesario confirmar que la batería está suficientemente cargada y conectar la antena que se utilizará dentro del rango de frecuencia deseado.
2. **Selección del Modo de Medición:** El equipo tiene varias funciones, pero en este caso se va a utilizar el análisis de espectro accediendo al menú principal y seleccionando el botón Spectrum.
3. **Configuración de Parámetros de Medición:** El parámetro principal que se debe establecer es el rango de frecuencia presionando el botón FREQ y así ajustar la frecuencia mínima o máxima, aunque también se puede ajustar la frecuencia central y el ancho de banda.
4. **Iniciar la Medición**: Para dar inicio al barrido, el equipo utiliza la opción START visualizando el monitoreo del espectro por consiguiente, utiliza el botón HOLD para pausar el monitoreo cuando se encuentra actividad continua en el rango de frecuencia analizado.

Escenario de Simulación

El escenario de simulación se ha situado en el laboratorio de electrónica de la Facultad de Sistemas y Telecomunicaciones un espacio elegido por sus mínimas interferencias lo que garantiza la precisión en la práctica. En este escenario los módulos se configuran simulando un dispositivo no autorizado oculto en el entorno es decir los módulos se colocan en un lugar específico del área de práctica preferiblemente fuera de la vista directa con el objetivo de recrear cómo un dispositivo podría permanecer oculto en un entorno real mientras mantienen una conexión activa en la red.

Ilustración 10 Escenario de simulación

3.2 Detección de Dispositivo No Autorizado con Tecnología GSM

Objetivo de la práctica: Simular un dispositivo no autorizado con tecnología GSM mediante el módulo SIM808 y realizar su respectiva detección utilizando el equipo Detect Protect 1206i y el SRM-3006.

3.2.1 Rol de la Detección de Dispositivos GSM No Autorizado en el Marco de Seguridad

La inseguridad causada por dispositivos GSM no autorizados es una preocupación importante, especialmente en los dominios de telecomunicaciones y seguridad, entre otros campos sensibles a la seguridad.

GSM, en su uso final, tiene una aplicación más amplia en teléfonos móviles, sistemas de telecomunicaciones, monitoreo y dispositivos remotos. Pero esta tecnología también puede verse afectada por dotaciones no autorizadas y malintencionadas.

Una de las razones más importantes que existe para detectar dispositivos GSM no autorizados es:

- **Seguridad de la información:** Por ejemplo, algunos teléfonos celulares o módulos de comunicación pueden ser espías y podrían servir para recopilar y enviar información crucial incrustada en una ubicación controlada o

secreta en ausencia de o en contra de personal autorizado y capacitado que trabaja en tales áreas y asignar dispositivos.

3.2.2 Revisión Teórica

Principios básicos de la Tecnología GSM

Al hablar sobre el Sistema Global para Comunicaciones Móviles, se hace referencia a la tecnología de comunicación ampliamente utilizada en redes móviles sabiendo que operan en bandas de frecuencia de 850 MHz y 1900 MHz caracterizándose por su modulación digital y su capacidad de soportar comunicaciones de voz y datos.

GSM utiliza modulación GMSK durante la transmisión de datos por lo cual la transmisión es eficiente y la utilización del espectro óptima además vale la pena mencionar que se utilizan ráfagas de señal que se pueden ver en el análisis espectral siendo de gran utilidad al momento de detectar.

Dispositivos GSM No Autorizado

Cualquier equipo GSM que no haya sido autorizado por las autoridades competentes o cuyo uso esté excluido en una zona restringida específica se denomina dispositivo GSM no autorizados tales como teléfonos móviles, módulos de comunicación (por ejemplo, SIM900, SIM808) y micrófono GSM (MICRO 785) entre otros dispositivos capaces de conectarse a redes GSM con el propósito de que los usuarios puedan realizar y recibir llamadas, además de enviar y recibir mensajes de texto en bandas de frecuencia GSM.

Existen algunos módulos de comunicación que soportan protocolos GSM, pero el SIM808 es de gran importancia en la práctica para la simulación de dispositivos no autorizados siendo factible por su tamaño pequeño al momento de ocultarse aumentando el riesgo de utilización no autorizada de los módulos.

Principios de Detección de Señales de Radiofrecuencia

Los dispositivos GSM se basan en la detección de señales de RF y la localización de dispositivos como estos individuos en el rango de frecuencia en el

que operan. Es posible detectar señales GSM solo empleando equipos que puedan escanear estas bandas de frecuencia e investigar las propiedades de la señal.

El análisis espectral significa escanear bandas de frecuencia específica en busca de sus cambios en el nivel de señal que indica alguna actividad continua, en las señales GSM se envían intermitentemente debido a su modulación formando algunos patrones específicos en el espectro y el reconocimiento de estos picos hace posible identificar los dispositivos que están actualmente en uso. Además la intensidad de la señal que se mide en dBm va a indicar la intensidad que está emitiendo el dispositivo.

Equipos de Detección

- **Detect Protect 1206i:** Equipo que permite la detección rápida en transmisiones de radiofrecuencia en áreas determinadas siendo capaz de captar señales de dispositivos GSM en el rango de frecuencia adecuado mediante la intensidad de la señal detectada.
- **SRM-3006:** Analizador de espectro portátil que permite un análisis detallado de las señales de radiofrecuencia permitiendo visualizar la frecuencia, intensidad y patrón de modulación de la señal lo que es útil para identificar y confirmar la presencia de dispositivos GSM mediante un análisis en tiempo real del espectro.

3.2.3 Configuración del Módulo GSM

Antes de iniciar con la configuración se debe ubicar y conectar la antena GSM en el puerto correspondiente del módulo. El módulo SIM808 requiere de una alimentación estable de 5V. Por consiguiente, se debe colocar el chip de la operadora móvil en la ranura correspondiente del módulo, como se muestra en la siguiente ilustración.

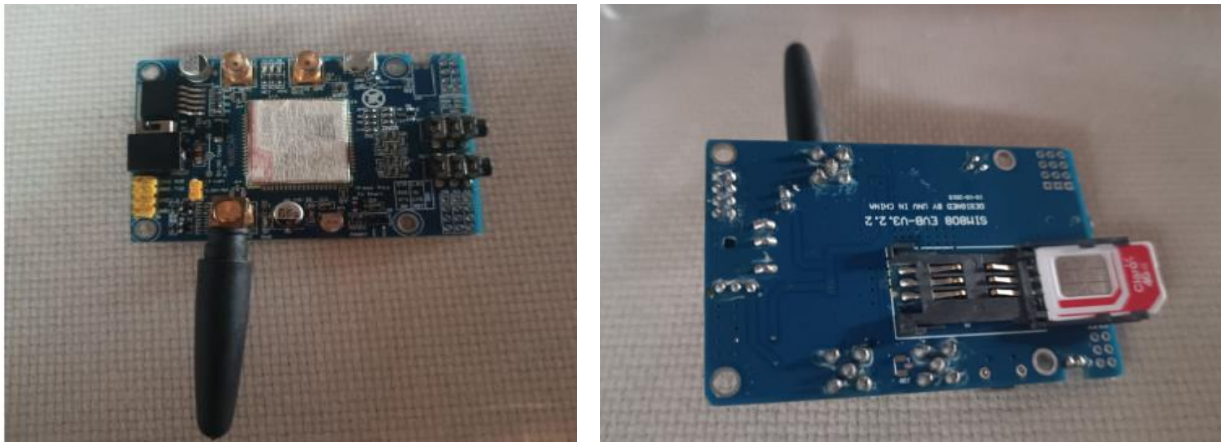


Ilustración 11 Conexión de Antena GSM y Chip de Operadora en el Módulo SIM808. Fuente [Autor]

En la configuración del módulo SIM808, el uso de un Arduino Uno facilita la comunicación y el control del módulo, es por eso por lo que en esta práctica también se necesita de un ARDUINO UNO como se muestra en la siguiente ilustración.

Ilustración 12 Configuración del Módulo SIM808 con Arduino Uno para Comunicación y Control. Fuente [Autor]

En la siguiente tabla se detalla las conexiones de comunicación entre el módulo SIM808 y el Arduino Uno.

Tabla 7 Conexiones de comunicación Fuente [Autor]

Módulo SIM808	Arduino Uno
GND	GND
Tx	Pin 7
Rx	Pin 8

La conexión final entre el módulo SIM808 y el Arduino Uno permite establecer una comunicación eficiente para el envío y recepción de datos a través de la red móvil, esta configuración asegura una alimentación estable para el módulo y una comunicación adecuada entre ambos dispositivos, permitiendo que el Arduino Uno controle y monitorice el módulo SIM808.

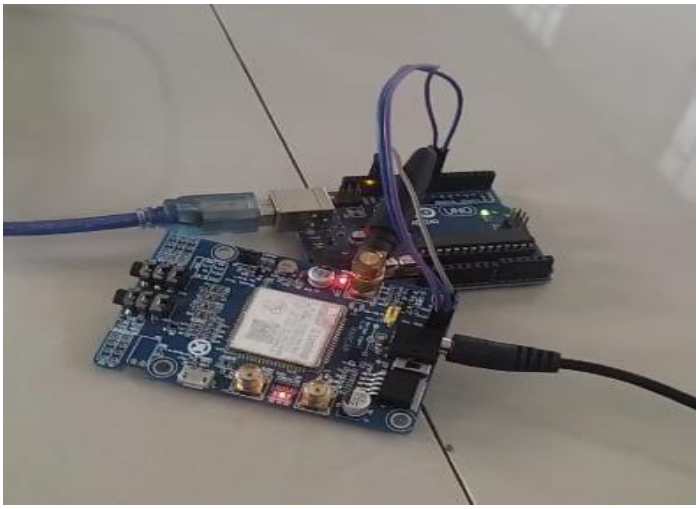


Ilustración 13 Conexión entre el Módulo SIM808 y Arduino Uno. Fuente [Autor]

Una vez establecida la conexión física entre el módulo SIM808 y el Arduino Uno, el siguiente paso es programar el Arduino utilizando el software de Arduino IDE, el código debe ser cargado en el Arduino para configurar y controlar el módulo SIM808, permitiéndole interactuar con la red móvil para enviar y recibir mensajes, realizar llamadas, este proceso implica la programación de comandos AT específicos para el funcionamiento del módulo, así como la gestión de la comunicación serial entre el Arduino y el SIM808.

Ilustración 14 Configuración del Código en Arduino IDE para Control del Módulo SIM808 Fuente [Autor]

Configuración del SIM808 para Emisión Constante

La red consiste en enviar mensajes de texto a teléfonos móviles configurando el módulo SIM808. En esta práctica es útil este tipo de tráfico que soporta la red para destino de detección.

Alternativamente, si la tarjeta SIM tiene acceso a datos, se activa una conexión GPRS que mantiene una comunicación constante, para ello se utilizan comandos AT, como AT+CGATT=1 para activar GPRS y AT+CIPSTAR para iniciar una conexión TCP o UDP.

Control y Monitoreo con Arduino

Se da la posibilidad a la tarjeta Arduino Uno para enviar los comandos AT que inician las actividades del SIM808, lo que incluye el envío de mensaje mediante SMS en tiempos determinados, estos comandos estarán programados en la tarjeta Arduino para controlar el módulo SIM808 y realizar la transmisión de mensajes de forma automática.

3.2.4 Procedimiento de Detección con el Detect Protect 1206i

Preparación del Equipo

Antes de iniciar con la detección, es de importancia preparar el equipo apropiadamente. El Detect Protect 1206i debe estar en buenas condiciones operativas y tener todos sus accesorios necesarios. Se recomienda familiarizarse con los controles y funciones, en específico:

- El interruptor de encendido.
- El control de sensibilidad (Att+, Att-).
- La barra de luces Led que indica la intensidad de la señal detectada.

Además, es recomendable revisar que el equipo esté completamente cargado para evitar interrupciones al momento de realizar la prueba.

Encendido y Configuración Inicial

1. Enciende el Detect Protect 1206i moviendo el interruptor a la posición de encendido.
2. Configura el modo de detección de radiofrecuencia haciendo uso del modo sonido y como es detección de tecnología GSM enciendes la antena de barra (ANT1).
3. El ajuste de sensibilidad inicial debe estar bajo (ATT-) para captar ciertas señales a cierta distancia sin saturar el detector.

Después de completar los pasos anteriores, se inicia con una detección preliminar en el área donde se ha ocultado el dispositivo. Sosteniendo el Detect Protect 1206i de manera que la antena se encuentre orientada hacia adelante y a una altura estable (cerca del pecho). Se inicia el recorrido de manera lenta en diferentes direcciones prestando atención a los indicadores LED y la intensidad de la señal detectada.

Al momento que el Detect Protect 1206i detecta la señal GSM, es necesario observar tanto la barra de intensidad como el LED de color.

Ilustración 15 Detección de la señal GSM

Resultados de Detección

Teniendo en cuenta que la barra de la intensidad de la señal no es constante y el LED rojo por su parte se enciende constantemente por lo cual se establece que la señal de tecnología GSM se encuentra operativa en los límites de lo razonable del lugar de prueba mediante un dispositivo que hace uso de esta tecnología de comunicación.

Al inicio de la detección se encienden de uno a dos LEDs indicando que se presencia una señal débil, a medida que se sigue el recorrido en la dirección correcta va a existir un aumento en la barra de intensidad, encendiendo de 3 a 5 LEDs haciendo referencia a que se aproxima a la señal y posteriormente cuando se visualiza entre 6 a 8 LEDs encendidos la señal se encuentra muy cerca.

En la siguiente tabla se detallan los resultados obtenidos en la detección de la señal GSM.

Tabla 8 Resultados de Detección GSM

Escenario	Barra de Intensidad	Color de LED	Interpretación
Lejos de la fuente	1 a 2 LEDs encendidos	Ninguno o Verde, azul/rojo	La señal detectada es débil o se detecta una señal de otra tecnología.
Aproximadamente	3 a 5 LEDs encendidos	Rojo	La señal GSM es más fuerte, aproximándose al dispositivo.
Muy cerca	6 a 8 LEDs encendidos	Rojo	Alta intensidad GSM, se reduce la sensibilidad para localizar la fuente exacta.

3.2.5 Procedimiento del Análisis con Narda SRM-3006

Preparación del Equipo

Antes de iniciar con el análisis, es de importancia preparar el equipo apropiadamente, el Narda SRM-3006 debe estar en buen estado de funcionamiento y comprobar que esté cargado, además se debe ubicar la antena de manera correcta, se enciende el equipo y se espera hasta que se inicie completamente. Selecciona el modo Spectrum Analysis (Análisis de espectro) para visualizar el espectro de frecuencia.

Selección del Rango de Frecuencia

Antes de iniciar el análisis es necesario configurar rangos importantes como la frecuencia mínima y máxima en la que trabaja la banda GSM:

Frecuencia mínima: 840 MHz

Frecuencia máxima: 855 MHz

Configuración de los Parámetros de Resolución

- RBW (Ancho de banda de resolución): En el menú de configuración del equipo se debe seleccionar el rango de ancho de banda de resolución de 100 KHz para coincidir con el canal de GSM, facilitando la visualización de cada salto de frecuencia.

- VBW (Ancho de banda de video): Configura el VBW para un valor adecuado que te permita suavizar la señal.

Análisis antes de Encontrar la Señal

Para proceder con el análisis se ubican las configuraciones mencionadas anteriormente y se visualiza la intensidad del campo eléctrico sin estar activo el dispositivo con la tecnología GSM.

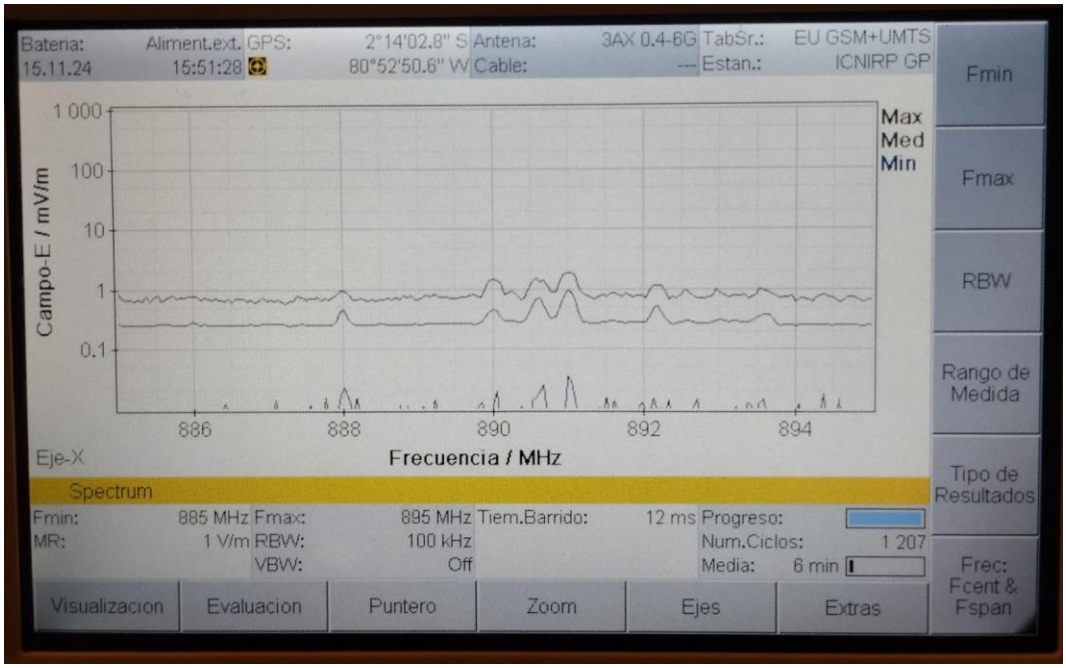


Ilustración 16 Visualización antes del Análisis de la señal GSM

Medición con el Narda SRM-3006

Ubica el dispositivo no autorizado a una distancia aproximada de 1 metro del equipo analizador SRM-3006 para captar una señal clara.

Verifica que el dispositivo esté emitiendo señales de manera continua en la banda GSM.

Selecciona el botón Hold puedes pausar el análisis al momento de visualizar un pico en el espectro.

En el menú debes seleccionar la opción de visualización de pico con el objetivo de listar los picos de frecuencia activos en el rango GSM.

Con el botón Save guarda la captura del espectro con el pico más alto para luego analizar los resultados.

Resultados de Análisis

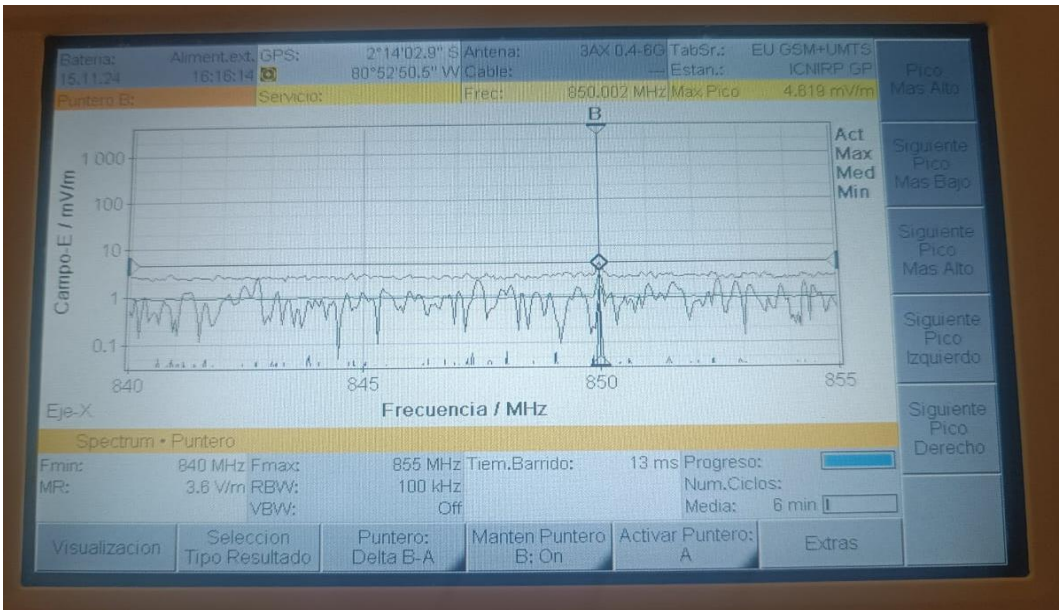


Ilustración 17 Resultados de Análisis GSM

Se registró un rango de frecuencia de 840 MHz a 855 MHz, este rango incluye parte de las bandas usadas en GSM en frecuencias bajas como 850 MHz.

El pico más alto identificado está en 850.0002 MHz lo que corresponde a una frecuencia típica de un canal en la banda GSM-850 haciendo referencia a que se detectó una portadora activa.

En términos de potencia se obtuvo un valor de 4.819 mV/m esta señal es relativamente fuerte y podría indicar la proximidad a una buena recepción de señal GSM.

3.2.6 Conclusiones de la Práctica

La programación basada en comandos AT del Arduino Uno conectado al módulo SIM808 permite enviar algunas señales GSM automatizadas, como enviar un mensaje de texto como si el dispositivo estuviera oculto.

El equipo detector es efectivo al momento de reconocer la señal siendo eficiente en la identificación del dispositivo con tecnología GSM lo cual lo conlleva a ser primordial en la detección de intrusos o monitoreo de señales no deseadas.

El analizador SRM-3006 proporcionó un mejor análisis espectral del dispositivo GSM activo en la frecuencia detectada.

La combinación de equipos permite cubrir tanto la detección aproximada de señales como el análisis detallado de señales GSM. El procedimiento es robusto en la detección de dispositivos GSM no autorizados en diversos entornos operativos y la medición de su intensidad de señal.

La práctica estableció una metodología clara y poco exigente que fue práctica para el control, detección y análisis de señales GSM y se espera que produzca resultados fiables que sean útiles en varios sectores como la seguridad de redes, monitoreo ambiental o auditorías de telecomunicaciones.

3.3 Detección de Dispositivo No Autorizado con Tecnología Bluetooth

Objetivo: Simular un dispositivo no autorizado mediante el módulo HC-05 y usando los equipos Detect Protect 1206i y Narda SRM-3006 detectar y analizar la fuente de la señal evaluando la efectividad de estos instrumentos en la identificación de dispositivos no autorizados.

3.3.1 Importancia de la Tecnología Bluetooth

La tecnología Bluetooth debido a su bajo costo, bajo consumo de energía y facilidad para la transferencia de datos en distancias cortas se ha convertido en un estándar de comunicación inalámbrico se encuentra en los dispositivos tales como teléfonos móviles, auriculares, computadoras y una amplia gama de dispositivos IoT, con el propósito de permitir conexiones rápidas y seguras, no obstante, su gran disponibilidad conlleva algunos inconvenientes, puesto que los dispositivos que tienen la capacidad de conexión Bluetooth pueden ser empleados de forma no autorizada recolectando información o interferiendo en sistemas críticos.

Un análisis rápido permite indicar que la detección y localización de las fuentes de emisión no permitidas puede ser crítico tanto en el área de seguridad como en el área de privacidad.

3.3.2 Revisión Teórica

Al momento de llevar a cabo una detección de señal Bluetooth no autorizado existen varios métodos teóricos y prácticos que permiten localizar la fuente de la señal, a continuación, se describen los métodos principales que pueden ser aplicados:

Detección de nivel de señal

La detección basada en el nivel de señal se centra en medir la intensidad de la señal de radiofrecuencia emitida por el dispositivo Bluetooth en cuestión sabiendo que la intensidad de la señal disminuye con la distancia lo cual permite estimar la proximidad de la fuente. Este método es útil para aproximaciones iniciales, aunque puede presentar limitaciones en áreas donde existen múltiples dispositivos o fuentes de interferencia.

Análisis de espectro

Visualiza y estudia la frecuencia de la señal detectada en un rango de frecuencias específicos induciendo a que esta técnica es útil para la detección de señales de Bluetooth además el análisis espectral permite identificar los picos de frecuencias vinculados a dispositivos Bluetooth activos en el área.

Reconocimiento de patrones de señal

Cada tecnología de transmisión tiene patrones específicos que pueden ser identificados mediante algoritmos o equipos especializados. En la tecnología Bluetooth se pueden reconocer patrones de pulso o modulación específica, que permiten diferenciar esta señal de las otras tecnologías presentes en el entorno.

3.3.3 Configuración del Módulo Bluetooth

Al configurar el módulo HC-05 como un dispositivo no autorizado se deben realizar conexiones físicas específicas entre el módulo y un microcontrolador, como el Arduino Uno. El módulo HC-05 se conecta a los pines de alimentación, transmisión y recepción del Arduino, permite establecer una comunicación serial que simule la presencia de un dispositivo Bluetooth activo, a nivel de software, el código en el entorno Arduino IDE debe programarse de manera que el módulo esté

en modo de enlace (o pairing) con otro dispositivo, replicando el comportamiento de un dispositivo Bluetooth desconocido.

Explicación de las conexiones físicas:

- Conexión de alimentación de 5V.
- Conexión a tierra (GND).
- El pin TX del módulo HC-05 va al pin RX del Arduino.
- El pin RX del módulo HC-05 va al pin TX del Arduino.

Una de las configuraciones que se busca en este entorno de simulación es imitar el funcionamiento de un espacio cerrado con el objetivo de comprobar la intensidad de la señal Bluetooth proveniente del módulo HC-05. Este tipo de entorno debería de reducir la interferencia de otros dispositivos Bluetooth y estar dispuestos de forma estratégica para permitir el análisis de la señal desde diferentes perspectivas.

En la realización de la práctica y una vez finalizados los pasos previos, se procede a la activación del módulo HC-05 para que emita señal Bluetooth, para la localización de esta se utilizan los equipos Detect Protect 1206i y Narda SRM-3006, quienes registran la información, siendo esta importante para la comparación entre ambos equipos en la intensidad de la fuente de la señal.

3.3.4 Procedimiento de Detección con el Detect Protect 1206i

Preparación del Equipo

Es de importancia que antes de comenzar cualquier proceso de detección asegurarse de que el dispositivo en este caso el Detect Protect 1206i este en perfectas condiciones de funcionamiento y tener todos los accesorios relevantes y se recomienda adquirir conocimiento sobre su control y alguna de las funciones fundamentales del equipo como:

- El interruptor de encendido.
- Los controles de sensibilidad (Att+ y Att-).
- La barra de indicadores LED que muestra la intensidad de la señal detectada.

Asimismo, se debe verificar que la batería esté completamente cargada para garantizar un uso continuo y evitar interrupciones durante la prueba.

Encendido y Configuración Inicial

- Encender el Detect Protect 1206i desplazando el interruptor hacia la posición de encendido.
- Para configurar el modo de detección de RF, es necesario activar el modo de sonido y, al tratarse de la detección de tecnología Bluetooth, encienda la antena de micro-pointer (ANT2).
- De manera general, es recomendable empezar el uso del equipo ajustando la sensibilidad a un nivel alto (ATT+) de modo que el detector no se sature con señales ambientales, pero que pueda recibir señales específicas a una distancia razonable.

Detección de la Señal Bluetooth

Al completar la configuración inicial se procede con una detección preliminar en el área donde podría estar oculto el dispositivo por lo cual el Detect Protect 1206i debe sostenerse con la antena orientada hacia adelante y a una altura estable aproximadamente a la altura del pecho se debe de realizar un recorrido lento y en distintas direcciones para así observar cuidadosamente los indicadores LED junto a la barra de intensidad de la señal detectada.

Ilustración 18 Detección de señal Bluetooth

Cuando el Protect 1206i identifica una señal Bluetooth, se debe prestar especial atención tanto a la barra de intensidad como al indicador LED correspondiente, lo que permitirá determinar la ubicación aproximada del dispositivo emisor.

Resultados de Detección

Al comenzar la detección, si se encienden entre uno y dos LED, esto indica que la señal es débil, a medida que se avanza en la dirección correcta, la barra de intensidad aumenta, entre tres y cinco LED encendidos significa que se está acercando a la señal, cuando se alcanzan entre seis y ocho LED encendidos, significa que la señal está muy cerca. En este punto la señal de tecnología Bluetooth se identifica como activada de manera significativa en el área de prueba.

A continuación, se muestra una tabla que sintetiza los resultados logrados durante el reconocimiento de la señal Bluetooth:

Tabla 9 Resultados de Detección Bluetooth

Escenario	Barra de intensidad	Color de LED	Interpretación
Lejos de la fuente	1 a 2 LEDs encendidos	Ninguno o Verde, azul/rojo	La señal es débil o se detecta una señal de otro tipo de tecnología.
A medida que se acerca	3 a 5 LEDs encendidos	Azul	La señal Bluetooth aumenta en intensidad a medida que se acerca al dispositivo.
Muy cerca	6 a 8 LEDs encendidos	Azul	La señal Bluetooth alcanza su máxima intensidad, reduciendo la capacidad para localizar la fuente exacta.
Ubicación exacta	1-2 LEDs encendidos o todos los LEDs encendidos	Azul	La señal ha sido identificada en la ubicación precisa.

3.3.5 Procedimiento para el Análisis con Narda SRM-3006

Preparación del Equipo

Antes de comenzar el análisis, es fundamental preparar adecuadamente el equipo verificando que se encuentre en perfecto estado de funcionamiento y que tenga carga suficiente para realizar el análisis, además la antena debe estar ajustada adecuadamente para ser encendido y se espera unos minutos que se inicie por completo. Luego se selecciona el botón (Spectrum) para poder observar el espectro de frecuencia.

Selección del Rango de Frecuencia

Antes de iniciar el análisis es necesario configurar rangos importantes como la frecuencia mínima y máxima en la que trabaja la banda Bluetooth:

Frecuencia mínima: 2.402 GHz

Frecuencia máxima: 2.480 GHz

Configuración de los Parámetros de Resolución

En la configuración del equipo se debe elegir un valor de 1 MHz para el ancho de banda de resolución ajustando el canal de la tecnología Bluetooth y facilitando la visualización de los cambios en la frecuencia.

Análisis antes de encontrar la Señal

Para realizar el análisis, se ajustan las configuraciones previamente indicadas y se observa la intensidad del campo eléctrico sin que el dispositivo con tecnología Bluetooth esté activo.

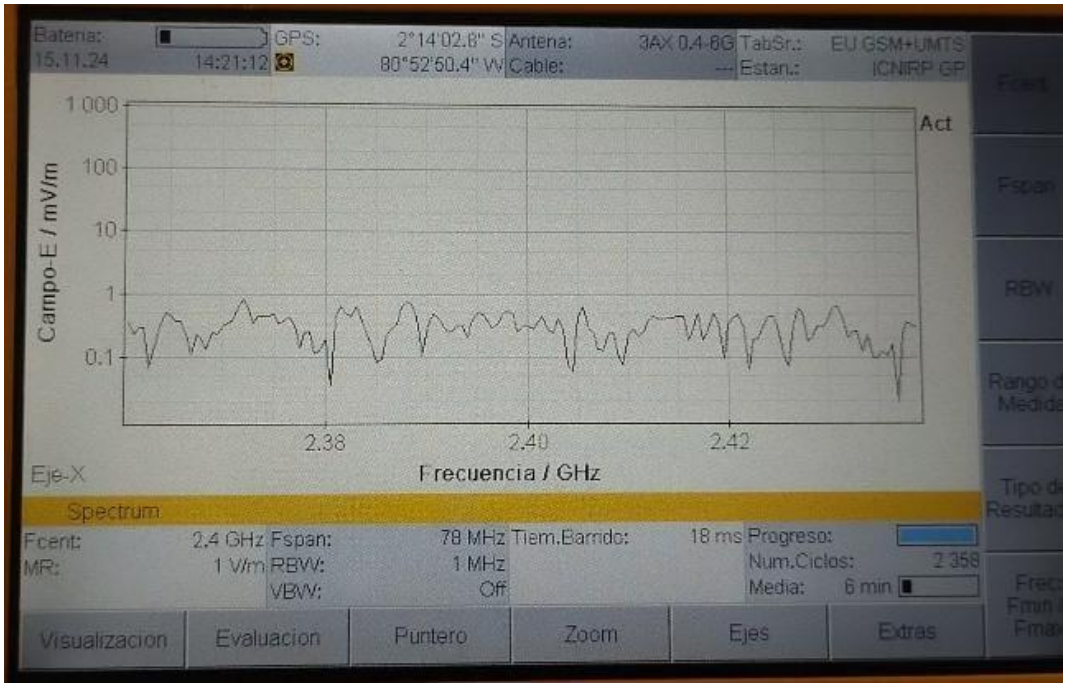


Ilustración 19 Visualización antes de analizar la señal Bluetooth

Medición con el equipo Narda SRM-3006

Ubica el dispositivo no autorizado a una distancia aproximada de 1 metro del equipo analizador SRM-3006 para captar una señal clara.

Verifica que el dispositivo esté emitiendo señales de manera continua en la banda de frecuencia de 2.4 GHz.

Selecciona el botón Hold para pausar el análisis al momento de visualizar un pico en el espectro.

En el menú debes seleccionar la opción de visualización de pico con el objetivo de listar los picos de frecuencia activos en el rango del bluetooth.

Con el botón Save guarda la captura del espectro con el pico más alto para luego analizar los resultados.

Resultados de Análisis

La frecuencia en la que se detecta el máximo nivel de campo eléctrico es de 2.46 GHz como lo indica el puntero B en la ilustración 20. El rango medido abarca el espectro completo de la banda ISM (Industrial, Scientific, and Medical) donde opera Bluetooth.

El nivel de intensidad medido es de 65.84 mV/m lo cual representa la mayor potencia detectada en ese rango de frecuencia.

Se presentan 3 curvas: máxima, media y mínima. Estas indican el comportamiento del nivel de señal en el tiempo. La curva máxima resalta los picos de intensidad en el rango analizado, mientras que la curva media sugiere que, aunque hay picos de actividad el nivel promedio no es muy alto lo que puede indicar transmisiones intermitentes o de baja potencia.

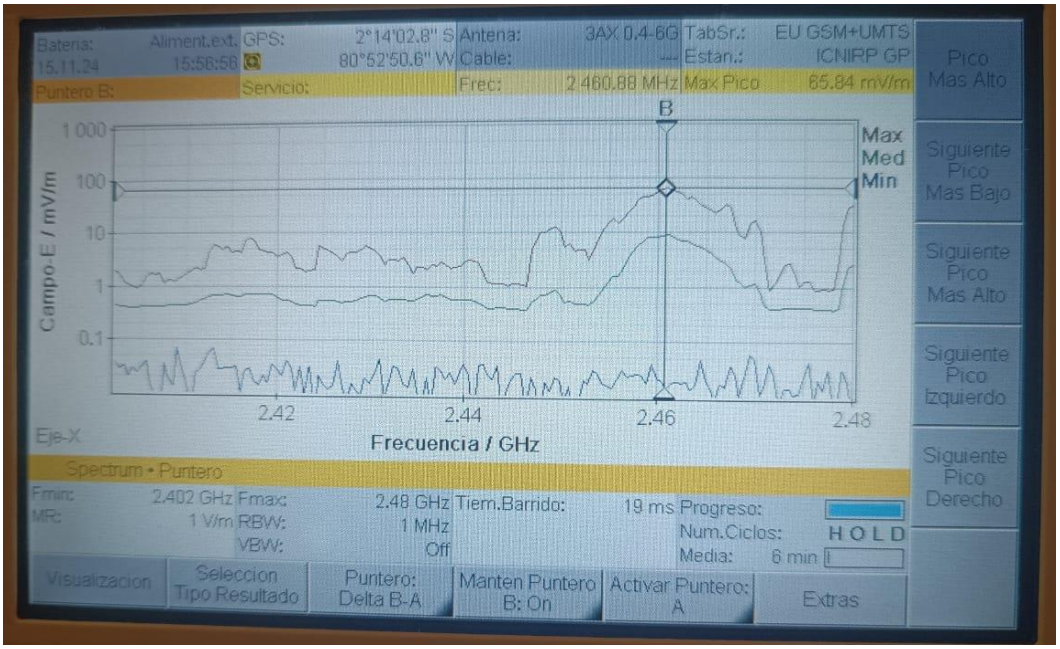


Ilustración 20 Resultados de Análisis Bluetooth

3.3.6 Conclusiones de la Práctica

Para una buena detección y localización de un dispositivo no autorizado en este caso con tecnología bluetooth fue importante combinar ambos equipos ya que su precisión funcional permitió obtener resultados de manera rápida y analizada.

El Detect Protect 1206i es eficiente en las primeras etapas de escaneo en busca de la presencia de una señal Bluetooth por consiguiente el analizador Narda SRM3006, proporciona la última verificación precisa, particularmente en entornos donde la interferencia puede distorsionar los resultados.

3.4 Detección de Dispositivo No Autorizado con Tecnología Wi-Fi

Objetivo: Configurar un teléfono móvil que simule un dispositivo sospechoso oculto en la red Wi-Fi con el propósito de emitir señales que puedan ser detectadas y localizadas haciendo uso de herramientas de detección y análisis de señales de radiofrecuencia.

3.4.1 Importancia de la Tecnología Wi-Fi

La tecnología Wi-Fi es una de las innovaciones más influyentes en la era moderna debido a su capacidad de proporcionar conectividad inalámbrica a dispositivos electrónicos, su importancia radica en varios aspectos fundamentales:

- Permite a los usuarios conectar varios dispositivos sin el uso de cables físicos, lo que mejora la movilidad y flexibilidad de los usuarios con el uso de dispositivos como laptops, teléfonos inteligentes, tablets y dispositivos IoT.
- El acceso a la red de redes en el hogar o dentro de las empresas desempeña un papel significativo en la realización de actividades económicas en varias áreas como el comercio electrónico, los servicios de trabajo en línea.
- En la plataforma IoT, la tecnología Wi-Fi está destinada a interconectar varios dispositivos como sensores, cámaras de seguridad, electrodomésticos inteligentes y sistemas de automatización en el programa.
- Se encuentra al alcance de muchos usuarios y es más asequible a diferencia de otras soluciones de conectividad como las redes celulares priorizando resolver brechas digitales existentes y desplazar internet a sitios alejados o en vías de desarrollo.

3.4.2 Revisión Teórica

En la actualidad la tecnología Wi-Fi (Wireless Fidelity) es la más utilizada debido a su capacidad de conectividad a internet que permite el intercambio de información en tiempo real haciendo uso del protocolo IEEE 802.11.

Fundamentos Técnicos:

Frecuencias de operación

Entre las bandas de frecuencia más empleadas se encuentra la de 2.4 GHz que abarca un mayor alcance sin embargo pueden presentarse interferencias en el recorrido por otro lado se encuentra la banda de 5 GHz que ofrece velocidades más altas en comparación con la otra banda, pero teniendo un menor alcance.

Estándares IEEE 802.11

- 802.11b/g/n: Pertenecen a la banda de frecuencia de 2.4 GHz con velocidades de hasta 600 Mbps.
- 802.11ac: Este estándar incentivó el uso de la banda de frecuencias de 5 GHz y alcanzó velocidades de hasta 1 Gbps.
- Wi-Fi 6 (802.11ax): La ventaja de esta versión es que aumenta la capacidad, reduce la latencia y mejora la transmisión.

Ventajas de la Tecnología Wi-Fi

Wi-Fi es importante para el funcionamiento de múltiples sistemas debido a sus ventajas:

- Flexibilidad: Permite conexiones inalámbricas sin necesidad de infraestructura extensa de cables.
- Movilidad: Los usuarios pueden acceder a internet desde cualquier lugar dentro del rango de cobertura.
- Eficiencia: Soporta aplicaciones exigentes como streaming, teletrabajo y videollamadas.

Configuración del dispositivo no autorizado

Un Hospot oculto puede representar un punto de acceso no autorizado que alguien está usando para robar datos o interceptar comunicaciones. Para simular un Hospot oculto debe estar configurado de la siguiente manera:

- En configuración del teléfono buscas conexiones y debes activar Zona Wi-Fi portátil o Hospot móvil.
- Selecciona la opción punto de acceso móvil o configurar Hospot.
- En el apartado de establecer punto de acceso portátil cambia el nombre del SSID a un nombre sospechoso o genérico como: Network_Unk.

- Establece una contraseña para evitar conexiones no deseadas.
- Busca la opción que indica ocultar SSID y actívala para que el hospot no sea visible en los escaneos normales de redes Wi-Fi.
- Selecciona la banda de emisión sabiendo que en 2.4 GHz se tiene un mejor alcance y es compatible con más dispositivos mientras que en 5 GHz es más rápido y tiene menos interferencia, pero tiene menos alcance. Además, un canal menos común se encuentra en la banda de 2.4 GHz.
- Un hospot oculto será más fácil de rastrear si está generando tráfico en la red.

3.4.3 Procedimiento de Detección con el Detect Protect 1206i

Encendido y Configuración Inicial

- El Detect Protect 1206i debe estar encendido correctamente.
- Conecta la antena de medición micro-pointer a la entrada RF (ANT2) del protect 1206i.

Detección de la Señal Wi-Fi

Después de completar los pasos anteriores se inicia con una detección preliminar en el área donde se ha ocultado el dispositivo por lo tanto sosteniendo el Detect Protect 1206i con la antena orientada hacia adelante y a una altura estable (cerca del pecho) se inicia el recorrido de manera lenta en diferentes direcciones.

Al momento en que el Detect Protect 1206i detecta la señal Wi-Fi, es necesario observar tanto la barra de intensidad como el LED de color.

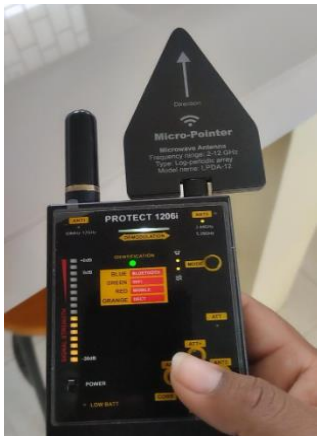


Ilustración 21 Detección de la señal Wi-Fi

Resultados de Detección

El LED verde permanece encendido de forma constante, indica que una señal de tecnología Wi-Fi está activa de manera notable en el área de prueba a través de un dispositivo que utiliza esta tecnología de comunicación.

Inicialmente la detección muestra entre uno y dos LEDs encendidos dando a entender que existe en el medio una señal débil a menudo que se avanza en la dirección correcta la barra de intensidad incrementa encendiendo de 3 a 5 LED por lo cual se da a entender que se está acercando a la fuente de la señal y posteriormente cuando se visualiza entre 6 a 8 LEDs encendidos la señal se encuentra muy cerca. Finalmente, cuando la barra de intensidad muestra todo el encendido se deduce que la fuente de la señal ha sido detectada.

En la siguiente tabla se detallan los resultados obtenidos en la detección de la señal Wi-Fi.

Tabla 10 Resultados de Detección Wi-Fi

Escenario	Barra de intensidad	Color de LED	Interpretación
Lejos de la fuente	1 a 2 LEDs encendidos	Ninguno o Verde, azul/rojo	La señal detectada es débil o se detecta una señal de otra tecnología.
Aproximadamente	3 a 5 LEDs encendidos	Verde	La señal Wi-Fi es más fuerte, aproximándose al dispositivo.

Muy cerca	6 a 8 LEDs encendidos	Verde	Alta intensidad Wi-Fi, se reduce la sensibilidad para localizar la fuente exacta.

3.4.4 Procedimiento del Análisis con Narda SRM-3006

Preparación del equipo

Antes de realizar algún análisis se debe de encender correctamente el equipo revisando con anterioridad que tenga suficiente batería para realizar la práctica y verificar si la antena está instalada correctamente y en una posición adecuada.

Selecciona el botón de encendido y espera mientras finaliza el proceso de inicio. Como es un análisis de señal se aplica el modo de analizador de espectro visualizado en el equipo como Spectrum.

Una vez seleccionado el modo de trabajo se ubica el rango de frecuencia como es tecnología Wi-Fi su rango de frecuencia mínimo será de 2.403 GHz con una frecuencia máxima de 2.482 GHz.

En el menú de configuración se selecciona el rango de ancho de banda a 1 MHz para captar la señal de Wi-Fi con suficiente detalle.

Procedimiento del Escaneo

- El dispositivo que emite la señal Wi-Fi debe de estar activo para así dar inicio al escaneo de la señal.
- En la pantalla del equipo se visualizará cómo el espectro se llena con señales captadas en tiempo real para luego identificar los picos más altos en la banda de frecuencia de 2.4 GHz correspondiente a canales activos de Wi-Fi.
- Para captar la señal se debe de pausar el escaneo haciendo uso del botón Hold y así poder obtener la intensidad de la señal.

Identificación de Señales y Parámetros Clave

Curso/Puntero: Se activa el puntero para luego ubicarlo en el pico más alto en la frecuencia central.

Campo E (mV/m): Se observa el valor del campo eléctrico asociado al pico más alto donde dicho valor indica la intensidad de la señal captada en esa frecuencia.

Resultados de Análisis

En la ilustración 22 se refleja actividad de alta intensidad en la frecuencia asociada al canal 13 de Wi-Fi para lo cual el nivel de campo eléctrico máximo es de 191.0 mV/m además que la ubicación del pico en la frecuencia de 2.4 GHz muestra que hay una transmisión activa en esa zona del espectro típica de un punto de acceso Wi-Fi o de dispositivos que comparten datos mediante esta tecnología.

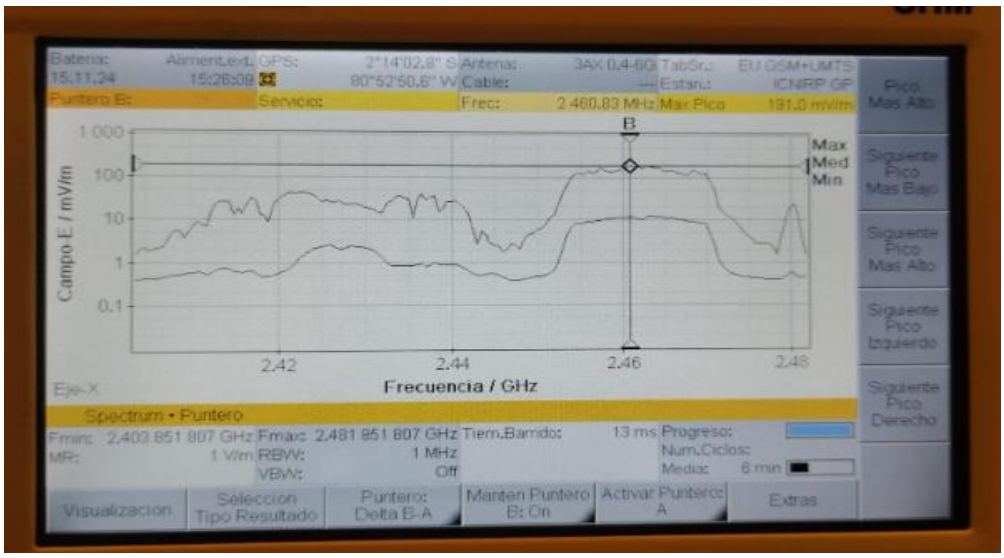


Ilustración 22 Resultados de Análisis de la señal Wi-Fi

3.4.4.1 Conclusión de la Práctica

El equipo Narda SRM-3006 permite identificar y analizar de manera precisa las señales Wi-Fi en la banda de 2.4 GHz, mostrando picos claros en el espectro que corresponden a canales activos, confirmando la capacidad del equipo para monitorear tecnologías inalámbricas en tiempo real.

La representación gráfica del espectro facilita la interpretación del comportamiento de la señal por lo cual identifica fácilmente la frecuencia con mayor actividad.

Comparación de ambos Equipos

El Detect Protect 1206i es una herramienta de gran importancia si se desea identificar la presencia de una señal de radio mediante su intensidad de señal que se visualiza sin embargo su precisión en los datos numéricos resulta menor en comparación con el analizador SRM-3006.

El SRM-3006 proporciona mayor precisión y detalles en la caracterización de la señal encontrada en la frecuencia de interés mostrando patrones de intensidad especialmente en la fase de confirmación de la ubicación.

El análisis de ambos equipos permite evaluar su complementariedad es decir el Detect Protect 1206i es ideal para una detección rápida y preliminar por consiguiente el Narda SR-3006 es adecuado para una confirmación detallada de la fuente de señal en la etapa final.

3.5 Conclusiones del Capitulo

El estudio de estas tres tecnologías sirvió para dar valor a los equipos Detect Protect 1206i y SRM-3006 para el análisis de dispositivos no autorizados. La práctica concluyó que el Protect 1206i es eficiente en la localización rápida y preliminar de señales GSM además de que el analizador Narda SRM3006 ofrece un análisis más preciso por lo cual permite identificar frecuencias específicas evaluando la intensidad de las señales en el espectro de 850 MHz.

En el caso de la tecnología Bluetooth, se demuestra que el Detect Protect 1206i y el Narda SRM-3006 son herramientas complementarias para la detección y análisis de señales. El Protect 1206i facilitó la identificación rápida de dispositivos no autorizados mediante su sensibilidad ajustable y un indicador visual específico para Bluetooth y con el Narda SRM-3006 se comprobó la existencia y valores de la señal detectada en el espacio.

La investigación realizada en base al escaneo de redes Wi-Fi evidencia la posibilidad de combinar aspectos prácticos y análisis detallados para evaluar la seguridad de las redes inalámbricas: el equipo Detect Protect 1206i con la antena micro pointer fue capaz de realizar de forma rápida la detección de la señal Wi-Fi en las bandas de 2.4 GHz y 5 GHz localizando el dispositivo funcional dentro del área y se completó el proceso con el analizador para proporcionar un análisis en profundidad de las características de las señales en relación, como su nivel de intensidad y su frecuencia central.

Desarrollo de material educativo

Ejercicio 1: Detección de señales de radio en el Laboratorio de Telecomunicaciones.

Objetivo general

Ejecutar un escaneo de señales para detectar diversas señales presentes en el laboratorio de telecomunicaciones empleando el dispositivo Detect Protect 1206i.

Objetivos específicos

- Enseñar a los estudiantes el procedimiento de la configuración del Detect Protect 1206i.
- Reconocer las señales de radio presentes en el laboratorio de Telecomunicaciones.
- Analizar los resultados obtenidos para establecer la eficiencia de las antenas del equipo.

Materiales

- Dispositivos emisores de señales
- Detect Protect 1206i

Marco teórico

Señales RF

Las señales Rf transmiten información a través de ondas de radiofrecuencia como microondas o láser, operan en diversas frecuencias dependiendo de la tecnología utilizada y el uso que se le quiera dar, la frecuencia es un término indispensable en este tema dado que se refiere al número de ciclos de una onda en segundos y se cuantifica en Hertz, estas señales poseen múltiples usos en el área de las telecomunicaciones.

Importancia de la detección de señales RF

El reconocimiento de señales de radiofrecuencia es una práctica necesaria en el campo de las telecomunicaciones por lo que permite:

- Medir la eficiencia y el alcance de las antenas en uso un entorno de prueba.
- Verificar las condiciones circundantes para el despliegue de dispositivos de comunicación.
- En el ámbito académico, estas prácticas permiten a los estudiantes visualizar la práctica de laboratorio en un escenario real donde existe una propagación de señal e incluso conocer los instrumentos de medición.

Detect Protect 1206i

El equipo Detect Protect 1206i cuenta con dos antenas, la antena de varilla que se identifica con el nombre de ANT1 que funciona para detectar señales de frecuencias en el rango de 50 MHz a 12 GHz y la antena Micro Pointer conocida como ANT2 para detectar altas frecuencias como señales de la tecnología Wi-Fi y Bluetooth que operan en el rango de 2.4 GHz y 5 GHz.

Modos de Indicación

Las partes del equipo pueden integrarse también de forma magistral, complementando cada uno de sus recursos con el sonido del equipo, la vibración y la luz que permiten interpretar visual y auditivamente la presencia de señales.

Procedimiento de la Práctica

1. Preparación del Equipo: Colocar el Detect Protect 1206i en la mano del estudiante que va a realizar la detección, verificar que tenga carga (LOW BATT) y encender el equipo (Power).
2. Selección del modo de canal: El equipo cuenta con dos canales, el primer canal se usa para detectar frecuencias de ancho de banda de 50-12000 MHz (ANT1) mientras que el segundo canal se utiliza solo para Bluetooth y Wi-Fi, es decir, 2.4 GHz a 5 GHz (ANT2).
3. Conexión de las Antenas: Se deben conectar sus respectivas antenas en el caso del puerto ANT1 se conecta la antena de varilla y para el puerto ANT2 se conecta la antena Micro Pointer.
4. Selección del modo de indicación: El equipo tiene 4 modos de indicación para este caso se va a emplear el modo de sonido.

5. Proceso de detección:

- Detección con ANT1: El estudiante debe de caminar por todo el área del laboratorio activando la antena 1 es decir 50-12000 MHz para abarcar una banda ancha de frecuencia.
- Detección con ANT2: El estudiante repite el procedimiento, pero esta vez cambia a ANT2 teniendo en cuenta que las frecuencias a detectar son de 2.4GHz a 5 GHz.

El modo de sonido permite que el altavoz del equipo produzca un sonido demodulado al encontrar una señal de radio.

6. Interpretación de resultados: El estudiante debe de registrar todas las señales encontradas en el laboratorio y diferenciar el alcance de las dos antenas.

Preguntas Teóricas

¿Qué son las señales de radio?

¿Por qué es importante realizar una detección de señales de radio dentro del laboratorio?

¿Mencione los tipos de antena que contiene el equipo y en qué rango de frecuencia operan?

¿Cuál es la diferencia que pudiste deducir entre las dos antenas con relación a la distancia?

Ejercicio 2: Detección de la fuente de un dispositivo de espionaje que emite señal de Bluetooth.

Objetivo general

Detectar la fuente de un dispositivo no autorizado con la simulación de un módulo Bluetooth HC05 como un equipo de espionaje haciendo uso del Detect Protect 1206i y el analizador Narda SRM-3006.

Objetivo específico

- Promover habilidades que faciliten la identificación y ubicación de dispositivos no autorizados que emitan señales a través del uso de instrumentos de escaneo de radiofrecuencia.
- Entender cómo operan y se utilizan los dispositivos de escaneo RF, como el módulo HC05, el Detect Protect 1206i y el analizador Narda SRM-3006.
- Utilizar métodos de localización para identificar físicamente los dispositivos no autorizados.

Materiales

- Módulo Bluetooth HC05
- Detect Protect 1206i
- Narda SRM-3006

1. Marco teórico

Tecnología Bluetooth

La tecnología Bluetooth es un medio de comunicación inalámbrica a corta distancia que permite la transmisión de información a través de ondas de radio de acuerdo con las bandas IMS.

- Esta tecnología trabaja en la frecuencia de 2,4 GHz y 2,485 GHz.
- Componentes eléctricos como auriculares, mouse, teclados son de uso en la vida cotidiana, sin embargo, existe la posibilidad de que se conecten a la red sin autorización.
- Los dispositivos que usan esta tecnología producen señales con baja potencia, lo que resulta casi imposible detectarlos cuando existe mucha interferencia de otras señales en el medio con dicha frecuencia.

2. Componentes usados en la práctica

Módulo Bluetooth HC05

El módulo Bluetooth HC05 tiene la función de enlazarse con otros dispositivos mediante la tecnología Bluetooth es utilizado para escanear señales en el área de pruebas como también realiza la detección de equipos cercanos considerando la posibilidad de que sean dispositivos no autorizados.

Detect Protect 1206i

El dispositivo Detect Protect 1206i es elaborado para satisfacer la necesidad de detectar señales de radiofrecuencia emitidas por dispositivos de diferentes tecnologías, en este caso la de Bluetooth, este equipo detecta señales de frecuencia que se encuentra dentro del rango de frecuencia de 50 MHz y 12 GHz, la misma que incluye a la frecuencia utilizada por la tecnología Bluetooth.

Narda SRM-3006

Este dispositivo es usado con mayor frecuencia para el análisis de señales que se desean detectar, cuenta con una interfaz gráfica que muestra a detalle los picos de señales que se encuentran en el medio y la del dispositivo que está emitiendo la señal no autorizada.

3. Importancia del ajuste de sensibilidad

En el dispositivo protect 1206i es indispensable ajustar la sensibilidad siendo esta la capacidad para detectar las señales que emiten señales con varias intensidades dependiendo de la distancia que se encuentre, la sensibilidad funciona de la siguiente manera, si se está en una sensibilidad máxima el equipo detectará señales débiles que se encuentren más lejanas, siendo esto un problema porque el dispositivo detectará muchas señales y se complica al identificar la fuente emisora.

Cuando se escanea con sensibilidad baja el dispositivo va a ignorar las señales débiles y captará las que se encuentren cerca del área, permitiendo así hallar de manera más eficiente la fuente del dispositivo que emite la señal.

4. Procedimiento de la práctica

a) Configuración de los equipos a utilizar

1. Módulo Bluetooth

Se debe configurar de manera correcta el módulo Bluetooth, es importante enlazar el dispositivo a una computadora para visualizar los dispositivos Bluetooth cercanos por medio de un adaptador bluetooth o un microcontrolador de Arduino, es recomendable ejecutar una búsqueda inicial para observar los dispositivos presentes en el entorno y verificar las señales de baja frecuencia.

2. **Detect Protect 1206i.**

Se inicia con un barrido en el área de pruebas para comprobar la sensibilidad de las señales que se presenta en el medio y conocer a detalle lo que indica la barra de intensidad, para esto es necesario ajustar la sensibilidad dependiendo del dispositivo que se desee encontrar, al comienzo se empieza con una sensibilidad alta para detectar señales débiles usando el botón ATT+ e irla ajustando cada vez que se acerque al dispositivo no autorizado.

3. **Narda SRM-3006**

En primer lugar, se prepara el equipo para realizar escaneos en las bandas de frecuencia necesarias, luego se ejecuta una captura preliminar para examinar el espectro presente en el entorno, luego se debe ajustar la sensibilidad de acuerdo con el ruido ambiental del lugar para prevenir anomalías y finalmente se establece la frecuencia central y el ancho de banda del escaneo en función de la fuente no autorizada.

b) Escaneo y detección de dispositivo no autorizado

1. Escaneo inicial con el Módulo Bluetooth

Realiza un barrido de dispositivos cercanos y anota los resultados obtenidos, considera la lista de dispositivos autorizados y los que no están en la lista, siendo estos los posibles dispositivos desconocidos que requieren un análisis con mayor interés.

2. Detección con el Protect 1206i

Usa la antena micro-pointer para detectar señales de Bluetooth, rastreando el origen de donde proviene esta señal no autorizada, hacer un barrido de manera lenta e ir observando el equipo cuando muestre la detección de la señal por medio

del indicador Led además es necesario ir regulando la sensibilidad esto evita que exista saturación.

3. Análisis con el Narda

Una vez que el protect 1206i detecte la señal no autorizada se hace uso del Narda SRM-3006 para obtener un mejor análisis por medio de su interfaz gráfica donde se da a conocer la frecuencia de la señal detectada, la potencia de esta y otros términos importantes.

5. Preguntas teóricas

¿Por qué es necesario ajustar la sensibilidad de los dispositivos en esta práctica?

¿Cómo afecta el ruido de fondo durante la ejecución de un barrido?

¿Qué nuevos conceptos aprendiste y por qué crees que son importantes para llevar a cabo esta práctica?

Describe tu análisis basándote en los resultados de la práctica.

Ejercicio 3: Detección y análisis de intensidad de un dispositivo con Tecnologia Wi-Fi

Objetivo general

Identificar y verificar la intensidad de una señal RF en el laboratorio de telecomunicaciones usando los dispositivos el Protect 1206i y el Narda 3006.

Objetivos específicos

- Elaborar un escenario de pruebas que permita identificar dispositivo RF que trabajan en la frecuencia de 2.4 GHz garantizando una adecuada emisión e identificación de señales en el laboratorio.
- Analizar la detección y sensibilidad del equipo Protect 1206i al medir la fuerza de la señal que el router TENDA emite a distintas distancias y direcciones empleando las antenas Ant1 y Ant2.
- Evaluar las variaciones de intensidad de señal registradas con las antenas del equipo Protect 1206i, estableciendo la efectividad de cada antena en función de la frecuencia y distancia.

Materiales

- Protect 1206i
- Narda 3006
- Router TENDA
- Antenas Ant1 y Ant2
- Cinta métrica

1. Marco Teórico

Al analizar una detección de señales RF se pueden presentar en el medio diferentes tipos señales entre las características que se pueden analizar es la de intensidad del equipo dependiendo de la distancia a la que se encuentre y frecuencia con la que opere.

El Detect Protect 1206i permite detectar las señales e intensidad de esta, mientras que el Narda SRM-3006 sirve para analizar la señal en el campo

electromagnético y confirmar el rango de frecuencia que se encuentra la señal emitida.

La mayoría de los routers trabajan en los rangos de frecuencias de 2.4 GHz y 5GHz en la tecnología Wi-Fi, al usar ambas antenas del equipo Detect Protect 1206i se puede sacar conclusiones de que señal se encuentra más cercana haciendo uso de la barra de intensidad del dispositivo.

2. Procedimiento de la práctica

a) Preparación del entorno del laboratorio

Ubica el router TENDA en una posición adecuada, es importante hacer las respectivas configuraciones del equipo para que esta emita señales de frecuencias de 2.4GHz y 5GHz.

Empieza a detectar las señales considerando distancias de 50cm, 1m y 2m del router observando la barra de intensidad en cada caso.

b) Mediciones iniciales

Para medir la intensidad de la señal desde donde está ubicado el router TENDA haz uso del Protect 1206i con la antena Ant1 y redacta los resultados obtenidos en cada distancia.

c) Comparación entre antenas

Realiza el mismo procedimiento antes mencionado pero esta vez con la antena Ant2 con la finalidad de analizar que ocurre en cada situación y como varia la intensidad de la señal.

d) Análisis de campo con el Narda SRM-3006

Una vez que se halla hecho el escaneo con el Detect Protect 1206i, se continua con el análisis de la señal mediante el Narda SRM 3006 para obtener la potencia que se muestra en cada escenario evaluado.

Preguntas Teóricas

¿Qué importancia tiene la tecnología Wi-Fi?

¿Menciona dos ventajas de la tecnología Wi-Fi?

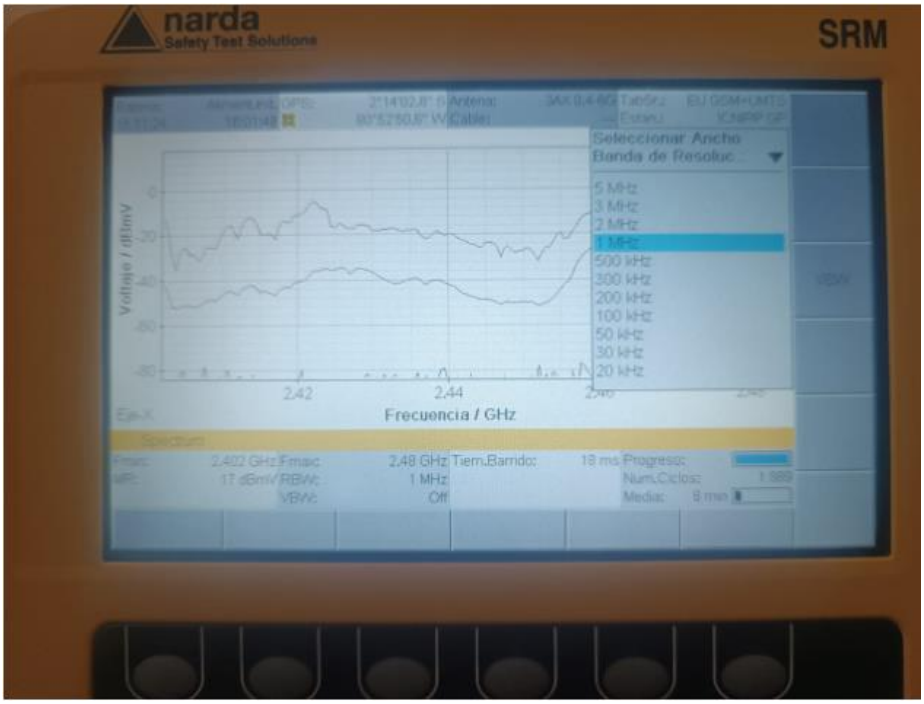
¿Cuál es la diferencia de los dos equipos aplicados al momento de realizar el escaneo?

Describe tu análisis de acuerdo con los resultados adquiridos.

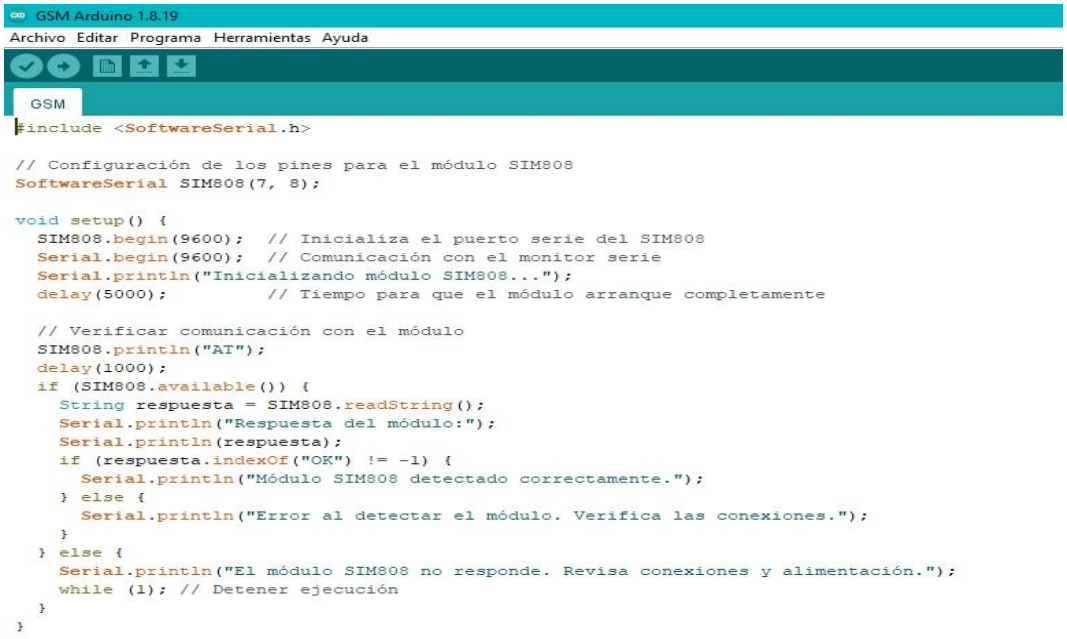
Anexos

Anexo 1 Análisis con el Narda

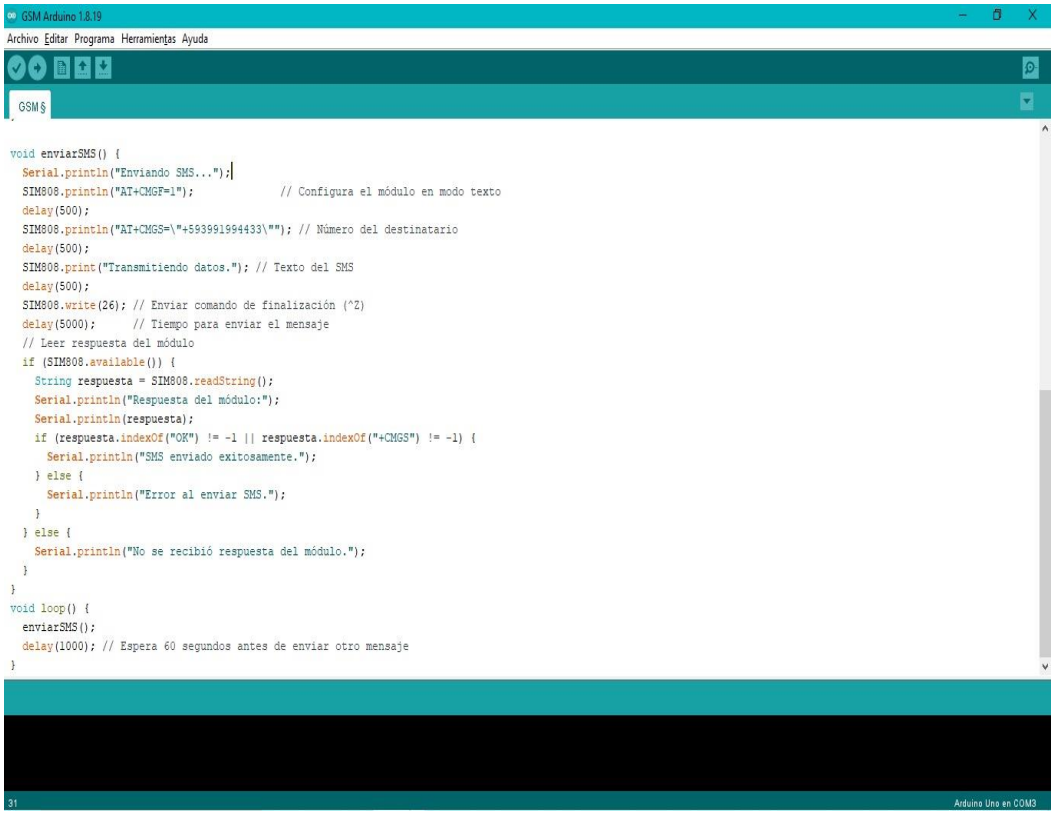
Anexo 2 Selección del Ancho de Banda de Resolución



Anexo 3 Configuración del módulo GSM parte 1



Anexo 4 Configuración del módulo GSM parte 2



Anexo 5 Configuración del módulo Bluetooth

Bluetooth Arduino 1.8.19

Archivo Editar Programa Herramientas Ayuda

Bluetooth

```
#include <SoftwareSerial.h>

// Configuración de los pines para el HC-05
SoftwareSerial BTSerial(10, 11); // RX, TX (Conecta TX del HC-05 al pin 10 y RX al pin 11)

void setup() {
  // Configuración de los puertos serie
  Serial.begin(9600);       // Comunicación con el monitor serie
  BTSerial.begin(9600);     // Comunicación con el HC-05
  Serial.println("Inicializando HC-05...");

  delay(1000); // Tiempo para que el módulo Bluetooth inicie

  // Configuración del HC-05 en modo texto
  BTSerial.print("AT+CMODE=1\r"); // Configura el HC-05 para ser detectable por cualquier dispositivo
  delay(1000);
}

void loop() {
  // Transmitir datos continuamente
  String mensaje = "Transmitiendo datos";
  BTSerial.println(mensaje); // Enviar datos por Bluetooth
  Serial.println("Enviado: " + mensaje); // Mostrar en el monitor serie
  delay(1000); // Enviar un mensaje cada segundo
}
```

Anexo 6 Selección de antena de barra ANT1 con modo de sonido

Anexo 7 Selección de antena micro pointer ANT2 sin modo

Bibliografías

[1] I. Moreno Carre, «Análisis integral de seguridad en dispositivos IoT,» Universitat Oberta de Catalunya, Catalunya, 2024.

[2] Sanju Mishraa , Rafid Sagbanb , Ali Yakoobc y Nikita Gandhi, «Inteligencia de enjambre en sistemas de detección de anomalías: una visión general,» *Revista internacional de informática y aplicaciones,* vol. 43, nº 2, pp. 109-118, 2023.

[3] G. R. Lanas y G. P. Cárdenas, «La protección de datos personales en el Ecuador,» *Revista internacional de cultura visual,* vol. 13, nº 2, pp. 1-16, 2023.

[4] P. Petrone, «Principios de la comunicación efectiva en una organización de salud,» *Revista Colombiana de Cirugía,* vol. 36, nº 2, pp. 188-192, 2021.

[5] L. Sagard, «Contribución de los sistemas de geolocalización y monitorización remota a los problemas sociales,» Universitat Politècnica de València, Valencia, 2022.

[6] T. Trapé, «Desempleo tecnológico y economía post-escasez: De Jeremy Rifkin al,» Universidad Nacional de Rosario, Rosario, 2022.

[7] A. Ruiz Canales y J. M. Molina Martínez, Automatización y telecontrol de sistemas de riego, España: Marcombo Ediciones tecnicas, 2020.

[8] A. F. Pasquel Cajas, Y. K. Ortega Rojas y V. Cajas Bravo, «La telefonía móvil: impacto en las actitudes culturales y conductas sociales de estudiantes universitarios,» *Revista cientifica INICC-PERU,* vol. 4, nº 2, pp. 55-65, 2021.

[9] E. J. Cedeño Marcillo, « Red Lan de datos y voz con tecnología inalámbrica para la empresa Polaca del cantón Santo Domingo de los Colorados.,» Universidad Laica Eloy Alfaro de Manabí, Manabí, 2022.

[10] I. A.-. Colón, J. C. Alonso, A. Ucero y C. Palacín, «Aplicación de tecnologías GSM/GPRS y acelerometría a la ecología espacial de la avutarda hubara,» *Asociación Española de ecología terrestre,* vol. 32, nº 2, pp. 2420-2425, 2023.

[11] J. L. Bustos, «¿Qué es la red GSM y cuál ha sido su trayectoria?,» KEEPCODING, Europa, 2024.

[12] Mrdesc, «sdrlatino,» 2013. [En línea]. Available: https://sdrlatino.wordpress.com/2013/06/28/introduccion-a-la-tecnologia-de-acceso-gsm/.

[13] C. G. Arreola Olivarría, M. T. Fernández Nista, J. J. Vales García y P. A. Sánchez Escobedo, «Factores asociados a las prácticas de enseñanza docentes con apoyo de las tecnologías de la información y comunicación,» *Educar,* vol. 15, nº 2, pp. 214-222, 2019.

[14] D. Mucientes San José, «Implementación de un entorno de comunicación Bluetooth basado en modulo Hc-05,» Unversidad de Valladolid, Valladolid, 2021.

[15] J. Jiménez, «Estos son los diferentes tipos de perfiles de Bluetooth y sus usos,» Redes Zone, Colombia, 2018.

[16] A. Bassi, «Intro a la tecnología Bluetooth,» Comunidad Goto Iot, España, 2021.

[17] k. K. Mero Suárez y P. L. Mosquera Delgado, «Análisis de equipos con banda de frecuencia de 2.4 Y 5.0 GHz para el mejamiento de cobertura Wi-Fi y la trama de datos en los espacios abiertos del cpmplejo universitario de la Universidad Estatal del Sur DE Manabí,» Universidad Estatal del Sur de Manabí, Manabí, 2018.

[18] E. Otero, «Todos los estándares y protocolos Wi-Fi: diferencias y ventajas de cada uno,» La vanguardia, Mexico, 2024.

[19] R. Tellas, «La evolución y el progreso de los estándares inalámbricos,» CPV MICRO, Guadalajara, 2018.

[20] R. E. Cotrina Roldan, «El espionaje Corporativo su incidencia en el funcionamiento interno de las empresas privadas del periodo 2007- 2013,» Universidad Provada del Norte, Trujillo, 2020.

[21] I. M. Gallardo Urbini, «Estrategia de Ciberseguridad Distribuida, aplicando el concepto de Operación de Inteligencia,» Universidad Nacional de La Plata, La plata, Argentina, 2022.

[22] M. A. Cano Olivares y R. Torres, «Caracterización de ataques multietapa en ejercicios capture The Flag,» *Revista política y estrategia,* vol. 141, nº 1, pp. 133-151, 2023.

[23] A. López Riera, «Aplicaciones avanzadas del principio superregenerativo a comunicaciones por radiofrecuencia,» Universitat Politècnica de Catalunya. , Catalunya, 2017.

[24] G. A. Montenegro y A. E. Marchesin, «Sistemas de identificación por radiofrecuencia (RF),» Nuevas Tecnologías, Buenos Aires, 2017.

[25] H. I. D. SL, «iProtect 1206i - Detector de Frecuencias Multibanda,» Espiamos, España, 2024.

[26] iProtect®, «Protect 1206i,» Tecnología de Shopify, España, 2024.

[27] J. Ilakovac, «Metode mjerenja 5G sustava (Doctoral dissertation, Josip Juraj Strossmayer University of Osijek.,» Department of Communications), 2024.

[28] J. G. Plaza Lucas, «Diseño de un prototipo generador de interferencias en la frecuencia de 2.4 GHZ para el desarrollo educativo de la facultad,» (Bachelor's thesis, La Libertad: Universidad Estatal Península de Santa Elena, 2023.).

[29] R. Alvarez Urdiales y A. García Villamar, «Diseño de un prototipo de sistema de prevención de accidentes para vehículos industriales mediante la tecnología de identificación por radiofrecuencia,» [Tesis de Maestría] Escuela Superior Politécnica del Litoral, 2018.

[30] D. Rodríguez Jorge, «Detectores de RF hasta 40 GHz basados en HEMTs de AlGaN/GaN.,» 2020.

[31] R. Pino Guzmán, «Propuesta de analizador de espectro óptico-heterodino.,» UNIVERSIDAD DE CANTABRIA, 20 03 2023.

[32] HeTPro., «SIM808 GSM GPRS Shield con Arduino UNO,» 2015.

[33] HeTPro., «SIM808 GPRS SIMCOM Quad band GSM shield,» 2015.

[34] A. Electronics, «MODULO BLUETOOTH HC-05,» 2024.

[35] DESTEC, «HC-05 Módulo Bluetooth [AA127],» 2024.

[36] Computron, «CELULAR XIAOMI 13C 4GB 128GB 6.7″ ANDROID 13 – NEGRO,» 2024.