

Pruebas de seguridad a nivel de radio (Espectro 915 MHz), en dispositivos LPWA (LoRa)

Michael Alejandro Rojas Giraldo

Informe final de trabajo de grado presentado como requisito parcial para optar al título de
Magíster en Seguridad de la Información

Director (a):

(M.Sc) Luis Carlos Correa Ortiz

Seguridad De La Informacion

Grupo de Investigación y Desarrollo en Informática y Telecomunicaciones

Universidad de Manizales

Facultad de Ciencias e Ingeniería

Maestría En Seguridad De La Informacion

Manizales, 2024

Resumen

Debido a la evolución de nuevas tecnologías inalámbricas que ayuden a solucionar problemas cotidianos de transporte de información a largas distancias y a la vez que requieran bajos consumos energéticos, se busca estudiar posibles falencias de seguridad de la información en dispositivos LPWA (LoRa), tecnología utilizada en aplicaciones de Internet de las Cosas (IoT). Tomando como componente fundamental la transmisión de radio en capas inferiores del modelo OSI, capturando información a base de un monitor que detecta y captura los datos dentro de una topología básica de comunicación, utilizando un hardware básico, que permita validar si es posible identificar amenazas y vulnerabilidades que pueden comprometer la integridad, disponibilidad y confidencialidad de los datos transmitidos.

Palabras claves: LPWA, LoRa, IoT, OSI, vulnerabilidades, transporte, seguridad de la información.

Abstract

Due to the evolution of new wireless technologies that help to solve everyday problems of information transport over long distances and at the same time require low energy consumption, it is sought to study possible information security weaknesses in LPWA (LoRa) devices, a technology used in Internet of Things (IoT) applications. Taking as a fundamental component the radio transmission in lower layers of the OSI model, capturing information based on a monitor that detects and captures the data within a basic communication topology, using basic hardware, which allows to validate if it is possible to identify threats and vulnerabilities that can compromise the integrity, availability and confidentiality of the transmitted data.

Keywords: LPWA, LoRa, IoT, OSI, Vulnerabilities, Transport, Information security

Contenido

	Pág.
1. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN Y SU JUSTIFICACIÓN.....	11
1.1 DESCRIPCIÓN DEL ÁREA PROBLEMÁTICA	11
1.2 FORMULACIÓN DEL PROBLEMA	13
1.3 JUSTIFICACIÓN	13
2. OBJETIVOS.....	16
2.1 OBJETIVO GENERAL.....	16
2.2 OBJETIVOS ESPECÍFICOS	16
3. ANTECEDENTES.....	18
4. REFERENTE NORMATIVO Y LEGAL.....	25
5. REFERENTE TEÓRICO	26
5.1 INTRODUCCIÓN.....	26
5.2 TECNOLOGÍA LoRa.....	26
5.2.1 <i>Detalle de la tecnología LoRa y su funcionamiento</i>	27
5.2.2 <i>Explicación del protocolo LoRa y su papel en la seguridad de las comunicaciones</i>	28
5.3 MODELO DE AMENAZAS EN DISPOSITIVOS LoRa.....	30
5.3.1 <i>Identificación de posibles amenazas a la seguridad en dispositivos LoRa</i>	30
5.3.2 <i>Análisis de escenarios de ataque y debilidades potenciales en la implementación de dispositivos LoRa</i>	32
5.4 VULNERABILIDADES CONOCIDAS EN DISPOSITIVOS LoRa.....	34
5.4.1 <i>Exploración de vulnerabilidades documentadas en dispositivos LoRa</i>	35
5.4.2 <i>Casos de estudio sobre incidentes de seguridad que han afectado dispositivos LoRa</i>	38
5.5 TECNOLOGÍAS EMERGENTES EN SEGURIDAD DE LA INFORMACIÓN EN DISPOSITIVOS LoRa.....	40
5.5.1 <i>Blockchain</i>	41
5.5.2 <i>Inteligencia Artificial (IA)</i>	42
5.5.3 <i>Computación Cuántica</i>	44
5.5.4 <i>Redes definidas por software (SDN)</i>	45
5.5.5 <i>Internet de las cosas (IoT) seguro</i>	47
6. METODOLOGÍA.....	49
6.1 ENFOQUE METODOLÓGICO	49
6.1.1 <i>Análisis Descriptivo de vulnerabilidades</i>	49
6.2 TIPO DE ESTUDIO	50
6.3 PROCEDIMIENTO.....	50
6.3.1 <i>Fase 1: Análisis modelo captura de tráfico LoRa</i>	51
6.3.2 <i>Fase 2: Análisis de vulnerabilidades</i>	51
6.3.3 <i>Fase 3: Formulación de acciones o estrategias para minimizar las vulnerabilidades identificadas</i> ...	51
7. RESULTADOS	53

7.1	FASE 1: ANÁLISIS MODELO CAPTURA DE TRÁFICO LoRA.....	53
7.1.1	<i>Topología</i>	53
7.1.2	<i>Configuración de la placa de desarrollo Heltec LoRa 32:</i>	55
7.1.3	<i>Programando el módulo Heltec (Receptor)</i>	55
7.1.4	<i>Programando el módulo Heltec (Transmisor)</i>	59
7.1.5	<i>Programando el módulo CatWAN USB Stick (Sniffer)</i>	64
7.2	FASE 2: ANÁLISIS DE VULNERABILIDADES	70
7.2.1	<i>Interferencia o jamming</i>	72
7.2.1.1	<i>Pruebas spreading factor (SF) 7:</i>	75
7.2.1.2	<i>Pruebas spreading factor (SF) 9:</i>	81
7.2.1.3	<i>Pruebas spreading factor (SF) 12:</i>	85
7.2.2	<i>Spoofing o suplantación</i>	90
7.2.3	<i>Repetición</i>	94
8.	CONCLUSIONES	98
9.	RECOMENDACIONES	103
9.1	VULNERABILIDADES FISICAS.....	104
9.2	CIFRADO.....	104
9.3	AUTENTICACIÓN	104
9.4	DETECCIÓN DE INTRUSIONES.....	104
9.5	JAMMING	105
9.6	SPOOFING	105
9.7	EVALUACIÓN COMPARATIVA: LoRA VS. OTRAS TECNOLOGÍAS DE IOT EN EL CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN	106
9.7.1	<i>LoRa</i>	106
9.7.2	<i>NB-IoT</i>	107
9.7.3	<i>Sigfox</i>	107
9.7.4	<i>Wi-Fi</i>	109
9.7.5	<i>Bluetooth</i>	110
10.	REFERENCIAS	114

Lista de figuras

	Pág.
Figura 5-1.....	35
Figura 7-1.....	54
Figura 7-2.....	56
Figura 7-3.....	56
Figura 7-4.....	57
Figura 7-5.....	59
Figura 7-6.....	61
Figura 7-7.....	62
Figura 7-8.....	65
Figura 7-9.....	67
Figura 7-10.....	68
Figura 7-11.....	70
Figura 7-12.....	72
Figura 7-13.....	73
Figura 7-14.....	74
Figura 7-15.....	74
Figura 7-16.....	76
Figura 7-17.....	77
Figura 7-18.....	77
Figura 7-19.....	78
Figura 7-20.....	79
Figura 7-21.....	80
Figura 7-22.....	80
Figura 7-23.....	81
Figura 7-24.....	82
Figura 7-25.....	83
Figura 7-26.....	83
Figura 7-27.....	84
Figura 7-28.....	85
Figura 7-29.....	86
Figura 7-30.....	86
Figura 7-31.....	97
Figura 7-32.....	88
Figura 7-33.....	88
Figura 7-34.....	89
Figura 7-35.....	90
Figura 7-36.....	91
Figura 7-37.....	95
Figura 7-38.....	96

Lista de tablas

	Pág.
Tabla 1	21

Nota: Si su trabajo así lo requiere, puede incluir la lista de cuadros. Estas listas deben ser generadas de forma automática utilizando las opciones que proporciona el software de procesamiento de texto. Todas las tablas deben estar nombradas en el texto, para describirlas se sugiere emplear la herramienta de referencia cruzada (para textos editados en Microsoft Word).

Lista de símbolos y abreviaturas

Esta sección se incluyen símbolos generales (con letras latinas y griegas), subíndices, superíndices y abreviaturas. Sólo se deben incluir las listas de símbolos que se utilicen. Cada una de estas listas debe estar ubicada en orden alfabético de acuerdo con la primera letra del símbolo. Su uso es frecuente en Ingeniería, en otras áreas de conocimiento puede ser opcional.

Símbolos con letras latinas

Símbolo	Término	Unidad SI	Definición
A	Área	m^2	$\iint dx dy$
A_{BET}	Área interna del sólido	$\frac{m^2}{g}$	ver DIN ISO 9277
A_g	Área transversal de la fase gaseosa	m^2	Ec. 3.2
A_s	Área transversal de la carga a granel	m^2	Ec. 3.6
a	Coficiente	1	Tabla 3-1

Símbolos con letras griegas

Símbolo	Término	Unidad SI	Definición
$\square_{\square\square\square}$	Factor de superficie	$\frac{m^2}{g}$	$(W_{F,waf})(A_{BET})$
\square_{\square}	Grado de formación del componente i	1	$\frac{m_j}{m_{bm\ \varrho}}$
\square	Wandhafbreibwinkel (Stahlblech)	1	Sección 3.2

Símbolo	Término	Unidad SI	Definición
□	Porosidad de la partícula	1	$1 - \frac{\rho_s}{\rho_w}$
□	mittlere Bettneigungswinkel (Stürzen)	1	Figura 3-1

Subíndices

Subíndice	Término
bm	Materia orgánica
DR	Dubinín-Radushkevich
E	Experimental

Superíndices

Superíndice	Término
n	Exponente, potencia

Abreviaturas

Abreviatura	Término
1.LT	Primera ley de la termodinámica
DF	Dimension fundamental
RFF	Racimos de fruta fresca

1. Planteamiento del problema de investigación y su justificación

1.1 Descripción del área problemática

En la era digital actual, la creciente interconexión de dispositivos y sistemas ha llevado a un aumento exponencial en la cantidad de datos que se transmiten y almacenan a través de redes inalámbricas. La tecnología LoRa (Long Range) ha emergido como una solución líder en la comunicación de larga distancia y bajo consumo de energía para aplicaciones de Internet de las Cosas (IoT, por sus siglas en inglés).

Sin embargo, con la proliferación de dispositivos LoRa y la transmisión de datos críticos, la seguridad de la información en las redes LoRa se convierte en un aspecto esencial que merece una atención especial.

Este trabajo se centra en la seguridad de la información en redes LoRa y su importancia en un contexto de IoT. El objetivo principal es analizar e identificar vulnerabilidades que sirvan como referencia para proteger la integridad, confidencialidad y disponibilidad de los datos transmitidos a través de tecnología LoRa. La seguridad de la información en redes LoRa se convierte en un componente crítico, ya que la información sensible y vital, como datos de telemetría, control de dispositivos y aplicaciones industriales, se transmite a través de estas redes.

El trabajo de investigación aborda los desafíos específicos relacionados con la seguridad de la información en tecnología LoRa, incluyendo el análisis de paquetes, modulación, anchos de banda y tasas de transmisión.

De igual forma también examina diferentes casos de uso realizados en laboratorio concretos de aplicaciones IoT basadas en LoRa, identificando las amenazas potenciales y los riesgos asociados a la seguridad de la información.

En resumen, este trabajo se enfoca en la seguridad de la información en redes LoRa y su papel crucial en el entorno de IoT. A medida que las aplicaciones IoT continúan creciendo y diversificándose, es fundamental comprender y abordar los desafíos de seguridad inherentes a la tecnología LoRa para garantizar la confiabilidad y la protección de los datos transmitidos en estas redes.

1.2 Formulación del problema

La pregunta de investigación que guía el desarrollo de esta tesis de maestría es:

¿Amenazas de seguridad de la información en redes LoRa (IoT), basado en tres categorías principales, interceptación de comunicaciones, manipulación de comunicaciones e interferencia, sobre un esquema básico de conectividad entre dos dispositivos?

1.3 Justificación

Este proyecto es novedoso ya que este tipo de tecnología a pesar de que se desarrolló en el 2015, su implementación en diferentes industrias a nivel mundial se dio desde el 2020, por eso es fundamental realizar validaciones de seguridad a este tipo de dispositivos buscando evidenciar si existen o no falencias en el mismo.

Realizando diferentes pruebas a nivel de comunicación de radio entre los dispositivos, Logística, edificios y ciudades inteligentes, agricultura, gestión de residuos, salud, monitorización, geolocalización, transportes, seguridad.

De este análisis se busca evaluar los riesgos asociados con las redes LoRa y cómo estos pueden impactar la seguridad y la confiabilidad de las comunicaciones en aplicaciones críticas, como la monitorización de dispositivos médicos, la gestión de ciudades inteligentes o la automatización industrial.

Este proceso de análisis implica la identificación de amenazas potenciales, como la interceptación de datos, la suplantación de dispositivos, los ataques de repetición y las posibles vulnerabilidades en la infraestructura de red. A continuación, se lleva a cabo una evaluación de riesgos para determinar el impacto y la probabilidad de que estas amenazas se materialicen.

Una vez identificadas las amenazas y evaluados los riesgos, se podrían desarrollar estrategias y contramedidas para mitigar los riesgos y fortalecer la seguridad en las redes LoRa. Esto podría incluir la implementación de encriptación de extremo a extremo, autenticación sólida de dispositivos, la gestión segura de claves y el monitoreo constante de la red en busca de actividades sospechosas.

Por esto este trabajo es relevante,

1. Crecimiento de IoT: El Internet de las Cosas (IoT) está en constante crecimiento, y las redes LoRa desempeñan un papel fundamental en la conectividad de dispositivos. Dado el aumento en la adopción de IoT, es esencial abordar las amenazas y vulnerabilidades en estas redes para garantizar la seguridad de datos y dispositivos.
2. Aplicaciones Críticas: Las redes LoRa se utilizan en una variedad de aplicaciones críticas, como la salud, la industria y la seguridad. Los fallos en la seguridad de estas aplicaciones pueden tener consecuencias graves, lo que destaca la importancia de un análisis de amenazas sólido.
3. Naturaleza Abierta de las Bandas de Frecuencia: Las redes LoRa operan en bandas de frecuencia no licenciadas, lo que las hace accesibles para cualquier persona. Esto significa

que los posibles atacantes tienen la capacidad de interferir con las comunicaciones, lo que resalta la necesidad de contramedidas efectivas.

4. **Privacidad y Confidencialidad:** Muchas aplicaciones IoT manejan datos sensibles. Proteger la privacidad y la confidencialidad de estos datos es esencial, y un análisis de amenazas ayuda a identificar riesgos relacionados con la exposición no autorizada de información.

5. **Concienciación sobre la Seguridad:** Realizar un análisis de amenazas fomenta la concienciación sobre la seguridad en el desarrollo y la implementación de sistemas LoRa. Esto promueve mejores prácticas de seguridad y la adopción de medidas proactivas para mitigar riesgos.

6. **Evolución de las Amenazas:** Las amenazas cibernéticas evolucionan constantemente. Un análisis de amenazas actualizado ayuda a mantenerse al día con las tácticas y técnicas de los atacantes y a adaptar las medidas de seguridad en consecuencia.

7. **Normativas y Cumplimiento:** En muchas regiones, existen regulaciones que requieren que las organizaciones protejan los datos y la privacidad. Un análisis de amenazas es fundamental para cumplir con estas regulaciones.

2. Objetivos

2.1 Objetivo general

El objetivo general de esta investigación consiste en: Realizar pruebas de seguridad a nivel de radio (Espectro 915 Mhz), en dispositivos LPWA (LoRa) del tipo IoT, con el fin de evaluar la seguridad de los dispositivos, comprendiendo todos los parámetros de radio y así intentar encontrar problemas como podrían ser comunicación en texto claro, claves débiles, vulnerabilidades en protocolo, jamming, spoofing o suplantación, ataques de repetición.

2.2 Objetivos específicos

- Interceptar la señal LoRa a nivel de radiofrecuencia, utilizaremos un monitor que detecta y captura los datos para realizar la adquisición de esta, teniendo claridad que debemos pasar por varias fases hasta que podamos capturar y analizar los datos.

- Identificar vulnerabilidades a nivel de espectro como sería el ataque de interferencia o jamming, buscando interrumpir la comunicación entre los dispositivos LoRa comprometiendo la disponibilidad de los datos.

- Analizar vulnerabilidades a nivel de comunicación capa física buscando explotar la técnica de suplantación o spoofing, creando un tercer dispositivo que envíe datos al equipo receptor de forma falsa, comprometiendo la disponibilidad, integridad y confidencialidad de los datos.

- Identificar vulnerabilidades a nivel de comunicación capa física buscando explotar la técnica de repetición, capturando y retransmitiendo los datos originales del sistema LoRa comprometiendo así la disponibilidad, integridad y confidencialidad de los datos.

3. Antecedentes

En el contexto de las redes IoT en el sector de las telecomunicaciones, se ha llevado a cabo una serie de investigaciones para comprender uno de los desafíos más complejos en este sector, el cual es la transmisión de datos de forma efectiva y segura. En particular, en las redes LoRa, es esencial debido a que tienen características de funcionamiento a largas distancias, bajos consumos energéticos y topología simple. Ante este reto, diversos estudios han explorado estrategias y técnicas para abordar el problema de la seguridad de la información en este tipo de red. En este apartado se identifican estudios recientes que han abordado esta problemática en el sector telecomunicaciones.

En primer lugar, el estudio de Aras, Small, Ramachandran, Delbruel, Joosen y Hughes (2017), se enfoca en el análisis y demostración de cómo es posible llevar a cabo ataques de interferencia selectiva en redes LoRa utilizando hardware comúnmente disponible. LoRa es una tecnología de comunicación inalámbrica utilizada en aplicaciones de Internet de las Cosas (IoT).

El estudio explora cómo un atacante podría aprovechar la naturaleza abierta y sin licencia de las bandas de frecuencia utilizadas por LoRa para realizar ataques de jamming selectivo. Estos ataques involucran la interrupción selectiva de transmisiones de datos, lo que puede tener graves implicaciones en aplicaciones críticas como la monitorización de dispositivos médicos o sistemas de seguridad.

Los investigadores demuestran que, con hardware relativamente asequible y software de radio definido por software, un atacante puede detectar y atacar de manera eficaz las señales LoRa, afectando la disponibilidad y la confiabilidad de la red. Esto destaca la importancia de considerar

la seguridad de las comunicaciones LoRa y la necesidad de implementar contramedidas para proteger estas redes contra ataques de interferencia.

Esta investigación subraya la necesidad de abordar la seguridad en las redes LoRa y desarrollar estrategias para mitigar el riesgo de interferencia maliciosa en aplicaciones de IoT.

En segundo lugar, Ningning Hou, Xianjin Xia, Yuanqing Zheng. (2021) se centran en el análisis de las vulnerabilidades de la capa física (PHY) de la tecnología LoRa (Long Range) a los ataques de interferencia y propone contramedidas para mitigar estos riesgos.

Los autores investigan cómo las redes LoRa, que se utilizan ampliamente en aplicaciones de Internet de las Cosas (IoT) debido a su alcance extendido y bajo consumo de energía, son susceptibles a ataques de interferencia. Estos ataques, conocidos como "jamming," pueden interrumpir la comunicación al saturar la banda de frecuencia con ruido, lo que puede tener un impacto negativo en aplicaciones críticas.

El estudio revela que la capa PHY de LoRa está particularmente expuesta a este tipo de ataques, y los autores proponen contramedidas que incluyen cambios en la configuración de las redes LoRa para dificultar la ejecución exitosa de ataques de jamming. Además, se exploran enfoques de modulación más robustos y técnicas de diversidad para mejorar la resistencia de las comunicaciones LoRa a la interferencia.

En tercer lugar, N. Torres, P. Pinto and S. I. Lopes (2022) realizaron un estudio para la identificación y explotación de vulnerabilidades en la capa física (PHY) de las redes LoRaWAN utilizadas en aplicaciones de Internet de las Cosas (IoT). La investigación revela cómo ciertas

debilidades en la capa PHY de LoRaWAN pueden ser aprovechadas por un atacante para comprometer la seguridad y la confidencialidad de las comunicaciones en estas redes.

Los autores demuestran que, mediante el uso de técnicas de radio definido por software (SDR) y equipamiento de bajo costo, un atacante puede llevar a cabo ataques de interferencia y escucha pasiva en las comunicaciones LoRaWAN. Esto significa que un atacante podría potencialmente detectar y decodificar paquetes de datos transmitidos a través de estas redes, lo que podría exponer información sensible.

El artículo destaca la importancia de abordar estas vulnerabilidades en la capa PHY de LoRaWAN y resalta la necesidad de implementar medidas de seguridad adicionales para proteger las comunicaciones en redes IoT. Además, se enfatiza la importancia de la concienciación sobre la seguridad y la necesidad de considerar estos riesgos al diseñar aplicaciones y sistemas basados en LoRaWAN.

En cuarto lugar, A N. BENKAHLA, B. BELGACEM and M. FRIKHA. (2018) desarrollaron un enfoque novedoso para realizar un análisis de seguridad específico en relación con el "duty cycle" mejorado en redes LoRaWAN. El "duty cycle" se refiere al tiempo durante el cual un dispositivo puede transmitir en una red LoRaWAN, y es una limitación crucial para evitar congestiones en la red y garantizar un uso equitativo del espectro radioeléctrico.

Los autores investigan cómo las implementaciones mejoradas del "duty cycle" pueden influir en la seguridad de las redes LoRaWAN y si pueden introducir vulnerabilidades o riesgos adicionales. El análisis se centra en entender cómo los ajustes en el "duty cycle" podrían afectar la confidencialidad y la integridad de los datos transmitidos en la red, además de considerar posibles implicaciones en términos de seguridad y privacidad.

El estudio busca identificar y abordar posibles amenazas y debilidades relacionadas con la configuración de "duty cycle" mejorado. Esto es especialmente relevante ya que, en un entorno de Internet de las Cosas (IoT), la seguridad de la información es crítica para proteger datos sensibles y garantizar el funcionamiento fiable de los dispositivos conectados.

En quinto lugar, J. Xing, L. Hou, K. Zhang and K. Zheng (2019) destacaron la importancia de la autenticación de claves como solución a los ataques de repetición, se centra en el desarrollo y propuesta de un esquema mejorado de gestión segura de claves para sistemas LoRa (Long Range). La tecnología LoRa se utiliza ampliamente en aplicaciones de Internet de las Cosas (IoT) debido a su alcance extendido y bajo consumo de energía, pero la seguridad en estas redes es de suma importancia.

El artículo aborda específicamente la gestión de claves, que es crucial para garantizar la seguridad de las comunicaciones en las redes LoRa. La gestión adecuada de claves criptográficas es esencial para proteger la confidencialidad e integridad de los datos transmitidos.

El enfoque principal del estudio es la mejora de la seguridad en la gestión de claves en redes LoRa. Los autores proponen un esquema que aborda desafíos como la distribución segura de claves entre dispositivos y la renovación periódica de claves para reducir el riesgo de exposición. Además, se enfatiza la importancia de considerar la escalabilidad y la eficiencia en la implementación de este esquema, ya que las redes LoRa a menudo involucran un gran número de dispositivos.

En sexto lugar, K. C. Wiklundh (2019) se enfoca en analizar la tecnología LoRa (Long Range) en el contexto de Internet de las Cosas (IoT) y su vulnerabilidad a interferencias. LoRa es

una tecnología de comunicación inalámbrica que se ha vuelto esencial en aplicaciones IoT debido a su capacidad de proporcionar conexiones de larga distancia con un bajo consumo de energía.

El estudio explora cómo, a pesar de las ventajas de LoRa, su operación en bandas de frecuencia no licenciadas lo hace susceptible a interferencias. Las interferencias pueden ser causadas por diversos factores, como otros dispositivos inalámbricos, condiciones climáticas adversas o incluso ataques deliberados.

El artículo destaca la importancia de comprender las vulnerabilidades de LoRa a la interferencia y cómo estas pueden afectar la confiabilidad de las comunicaciones en aplicaciones IoT críticas. Además, se enfatiza la necesidad de desarrollar estrategias para mitigar el impacto de las interferencias, como el uso de técnicas de corrección de errores, el ajuste de la potencia de transmisión y la implementación de técnicas de modulación más robustas.

En séptimo lugar, T. Perković, J. Šabić, K. Zovko and P. Šolić, (2023) analizaron el comportamiento de ataque llamado "replay attack" (ataque de repetición) en dispositivos vestibles que utilizan la tecnología LoRaWAN. LoRaWAN es una tecnología de comunicación inalámbrica de largo alcance ampliamente utilizada en dispositivos IoT, y los dispositivos vestibles son ejemplos comunes de aplicaciones de IoT.

En un ataque de repetición, un atacante intercepta y registra datos transmitidos legítimamente por un dispositivo y luego retransmite esos datos en un momento posterior. Esto puede tener consecuencias graves, especialmente en dispositivos vestibles que pueden estar monitoreando la salud o la seguridad de las personas. Por ejemplo, un ataque de repetición en un dispositivo de seguimiento de la salud podría dar lecturas falsas que podrían afectar la toma de decisiones médicas.

El estudio investiga cómo es posible llevar a cabo este tipo de ataque en dispositivos vestibles LoRaWAN y cuáles son las implicaciones en términos de seguridad y privacidad. Los investigadores analizan los mecanismos de seguridad en LoRaWAN y cómo pueden ser vulnerables a estos ataques.

El artículo concluye destacando la importancia de abordar esta amenaza y de implementar medidas de seguridad adicionales, como la autenticación fuerte y la protección contra ataques de repetición en dispositivos vestibles LoRaWAN.

En octavo lugar, M. M. R. Monjur, J. Heacock, R. Sun and Q. Yu (2021) exploraron los factores que influyen en la creación de un marco de análisis de ataques específicamente diseñado para aplicaciones de fabricación avanzada que utilizan la tecnología LoRaWAN.

El estudio reconoce que, si bien LoRaWAN es valioso en el contexto de la fabricación avanzada y la automatización industrial, también puede ser vulnerable a ataques cibernéticos. Estos ataques pueden tener graves implicaciones en términos de seguridad, confiabilidad y privacidad de los sistemas de fabricación.

El marco de análisis propuesto tiene como objetivo identificar y evaluar los posibles ataques que podrían dirigirse a las redes LoRaWAN en entornos de fabricación avanzada. Esto incluye la evaluación de amenazas como la suplantación de dispositivos, ataques de repetición y la manipulación de datos. Además, el marco busca proporcionar pautas y contramedidas para mitigar estos ataques y proteger los sistemas de fabricación avanzada.

Por último, J. Ren and K. Xu, (2022) realizaron su estudio que se centra en la simulación y análisis de la capacidad de la señal de modulación LoRa (Long Range) para resistir interferencias.

El estudio se enfoca en evaluar la robustez de la señal LoRa en condiciones de interferencia. Esto es esencial, ya que las interferencias pueden ser causadas por diversos factores, como dispositivos inalámbricos cercanos, condiciones atmosféricas adversas o interferencias maliciosas.

El artículo utiliza simulaciones para analizar cómo la señal LoRa responde a diferentes tipos de interferencia y cómo se ve afectada su calidad y capacidad de transmisión. Además, se exploran estrategias para mejorar la resistencia a la interferencia, como ajustes en los parámetros de la modulación y la utilización de técnicas de corrección de errores.

4. Referente normativo y legal

Tanto en Europa, el Instituto Europeo de Normas de Telecomunicaciones (ETSI), como en los Estados Unidos, la Comisión Federal de Comunicaciones (FCC) crea estas normas (LoRa Documentation). Estas normas establecen los parámetros técnicos y operativos que deben seguir las redes LoRa, incluyendo aspectos como la potencia de transmisión, la frecuencia de operación y los protocolos de seguridad.

Además de estas normas técnicas, también existen leyes y regulaciones que pueden afectar a las redes LoRa. Por ejemplo, las leyes de privacidad y protección de datos pueden requerir que los operadores de redes LoRa tomen medidas para proteger los datos transmitidos a través de sus redes. Esto puede incluir la encriptación de los datos, la implementación de medidas de seguridad robustas y la obtención del consentimiento de los usuarios antes de recoger o utilizar sus datos.

5. Referente teórico

5.1 Introducción

Las redes LoRa (Long Range) son tecnologías inalámbricas de banda estrecha que permiten la comunicación de largo alcance y baja potencia, diseñadas para aplicaciones de Internet de las cosas (IoT). Al investigar las vulnerabilidades de seguridad en redes LoRa, es fundamental comprender el contexto teórico que rodea esta tecnología y las posibles amenazas que enfrenta.

5.2 Tecnología LoRa

LoRa es una tecnología de comunicación inalámbrica de baja potencia y largo alcance. Utiliza modulación de frecuencia ensanchada (FSK) para transmitir datos a velocidades de hasta 50 kbps. LoRa es una tecnología popular para aplicaciones de IoT, como la monitorización y seguimiento de activos y la automatización del hogar.

Sin embargo, LoRa también es una tecnología vulnerable a una serie de amenazas que pueden comprometer la seguridad de la información. Estas amenazas pueden ser de naturaleza física o lógica. Dentro de las amenazas físicas están el vandalismo, robo o destrucción, dentro de las lógicas las cuales son las de nuestro interés están ataques de jamming, ataques de spoofing, ataques de cifrado, de denegación de servicio, entre otras. (Alonso-Martín, A., Díaz-Lázaro, J. M., García-Martín, J., & Sánchez-Rodríguez, J. M. (2022)).

5.2.1 Detalle de la tecnología LoRa y su funcionamiento

LoRa es una tecnología de comunicación inalámbrica que utiliza el espectro radioeléctrico de banda libre. La banda libre es un espectro de radiofrecuencia que no está asignado a ningún servicio específico. Esto permite a LoRa utilizar un ancho de banda amplio, lo que es necesario para lograr un largo alcance (LoRaWAN Specification, Release 1.1. LoRa Alliance, 2021).

LoRa utiliza modulación de frecuencia ensanchada (FSK) para transmitir datos. La modulación de frecuencia ensanchada es una técnica de modulación que utiliza un ancho de banda mayor que el ancho de banda de la señal modulada. Esto permite a LoRa transmitir datos a velocidades relativamente bajas, pero con un alto rango, tiene una serie de características que la hacen adecuada para aplicaciones de IoT:

Bajo consumo de energía, LoRa es una tecnología de baja potencia, lo que la hace ideal para dispositivos IoT con baterías de larga duración.

Largo alcance, LoRa puede alcanzar un alcance de hasta 15 km en condiciones ideales.

Espectro radioeléctrico de banda libre, LoRa utiliza el espectro radioeléctrico de banda libre, lo que la hace una tecnología rentable.

El funcionamiento de LoRa se puede dividir en dos fases:

Transmisión: En la fase de transmisión, el dispositivo LoRa envía datos a una puerta de enlace LoRa, la puerta de enlace LoRa recibe los datos y los envía a la red.

Recepción: En la fase de recepción, la puerta de enlace LoRa recibe datos de la red y los envía al dispositivo LoRa, el dispositivo LoRa recibe los datos y los procesa.

La fase de transmisión se realiza de la siguiente manera:

El dispositivo LoRa genera una señal portadora, la señal portadora se modula con los datos que se van a transmitir, la señal modulada se transmite por el aire.

La fase de recepción se realiza de la siguiente manera:

La puerta de enlace LoRa recibe la señal transmitida por el aire, la señal recibida se demodula para recuperar los datos, los datos se envían a la red (The LoRaWAN specification: A comprehensive guide. Semtech Corporation, 2022).

LoRa es una tecnología de comunicación inalámbrica de baja potencia y largo alcance que es adecuada para aplicaciones de IoT. LoRa tiene una serie de características que la hacen atractiva para los desarrolladores de aplicaciones IoT, como el bajo consumo de energía, el largo alcance y el uso del espectro radioeléctrico de banda libre (LoRa: A low-power, wide-area network technology for the Internet of Things. IEEE Communications Magazine, vol. 55, no. 1, pp. 18-25, 2017).

5.2.2 Explicación del protocolo LoRa y su papel en la seguridad de las comunicaciones

LoRa ofrece una serie de medidas de seguridad para proteger los datos transmitidos, incluidas las siguientes:

Cifrado, los datos transmitidos por LoRa están cifrados utilizando el algoritmo de cifrado AES-128, AES-128 es un algoritmo de cifrado por bloques, esto significa que los datos se dividen en bloques de 128 bits antes de ser cifrados, el algoritmo AES-128 utiliza una clave de 128 bits para cifrar los bloques de datos.

El algoritmo AES-128 consta de 10 rondas. En cada ronda, el bloque de datos se cifra utilizando una combinación de operaciones lógicas, aritméticas y de desplazamiento. La clave de 128 bits se utiliza para controlar las operaciones de cifrado (Advanced Encryption Standard (AES). National Institute of Standards and Technology, 2023).

Autenticación, los dispositivos LoRa se autentican entre sí utilizando el protocolo de autenticación de clave pública (PKI), la autenticación PKI es un método de autenticación muy seguro esto se debe a que la PKI utiliza la criptografía de clave pública para establecer la confianza entre las partes.

La criptografía de clave pública utiliza dos claves, una clave pública y una clave privada, la clave pública se puede distribuir libremente, mientras que la clave privada se debe mantener en secreto. Para verificar la validez de un certificado digital, el servidor de autenticación utiliza la clave pública del emisor del certificado, el servidor de autenticación cifra un mensaje con la clave pública del emisor del certificado. Si el destinatario del mensaje puede descifrarlo con su clave privada, entonces el certificado digital es válido (Public Key Infrastructure (PKI). National Institute of Standards and Technology, 2023).

Integridad, los datos transmitidos por LoRa están protegidos contra la manipulación utilizando el algoritmo de integridad de mensajes (MIC), es una función matemática que se utiliza para calcular un valor de resumen de un mensaje, el valor de resumen se puede utilizar para verificar la integridad del mensaje, es decir, para garantizar que el mensaje no se haya modificado desde que se creó (Cryptography and Network Security: Principles and Practice. William Stallings, 2023).

5.3 Modelo de Amenazas en Dispositivos LoRa

Las amenazas a la seguridad de los dispositivos LoRa pueden clasificarse en cuatro categorías principales: interceptación de comunicaciones, manipulación de comunicaciones, acceso a dispositivos y sistemas, e interferencia con la red (White Oak Security, s.f.2).

La interceptación de comunicaciones se refiere a la posibilidad de que las comunicaciones de LoRa sean interceptadas y monitoreadas por partes no autorizadas, lo que podría exponer datos sensibles o propiedad intelectual. La manipulación de comunicaciones implica que los atacantes podrían inyectar datos falsos o interrumpir la red. El acceso a dispositivos y sistemas se refiere a la posibilidad de que los atacantes obtengan acceso a los dispositivos y sistemas conectados a la red LoRa. Por último, la interferencia con la red se refiere a la posibilidad de que los atacantes interrumpan la red, ya sea bloqueando las señales de radio o inundando la red con tráfico no deseado.

5.3.1 Identificación de posibles amenazas a la seguridad en dispositivos LoRa

Los dispositivos de comunicación de largo alcance (LoRa) han ganado popularidad en aplicaciones de Internet de las Cosas (IoT) debido a su eficiencia energética y capacidad para transmitir datos a larga distancia. Sin embargo, como cualquier tecnología, los dispositivos LoRa también enfrentan amenazas de seguridad que deben abordarse para garantizar la integridad y confidencialidad de los datos transmitidos. Algunas de las posibles amenazas a la seguridad en dispositivos LoRa y cómo mitigarlas.

Intercepción de datos: Los mensajes enviados por dispositivos LoRa pueden ser interceptados por atacantes. Esto podría comprometer la privacidad de los datos transmitidos, especialmente si se trata de información sensible. Para mitigar esta amenaza, se recomienda utilizar cifrado de extremo a extremo y autenticación sólida.

Repetición de mensajes: Los atacantes pueden capturar y retransmitir mensajes LoRa, lo que podría llevar a la repetición de comandos o la manipulación de datos. Para evitar esto, se deben implementar mecanismos de autenticación y control de secuencia para detectar y descartar mensajes duplicados.

Ataques de denegación de servicio (DoS): Los dispositivos LoRa pueden ser víctimas de ataques DoS, donde un atacante sobrecarga la red con tráfico falso o solicitudes excesivas. Esto podría afectar la disponibilidad de la red. Para mitigar esto, se deben implementar límites de tasa y monitoreo constante.

Suplantación de identidad: Los atacantes pueden falsificar la identidad de un dispositivo LoRa legítimo para acceder a la red o enviar mensajes maliciosos. La autenticación basada en claves y la gestión adecuada de certificados son esenciales para prevenir la suplantación de identidad.

Ataques físicos: Los dispositivos LoRa pueden ser vulnerables a ataques físicos, como manipulación de hardware o robo. Se deben implementar medidas de seguridad física, como encapsulamiento resistente y protección contra manipulaciones.

En resumen, la seguridad en dispositivos LoRa es crucial para garantizar la confiabilidad de las comunicaciones IoT. Al implementar prácticas sólidas de seguridad, como cifrado, autenticación y monitoreo constante, podemos mitigar estas amenazas y proteger la integridad de

nuestros datos. (6 clases de ciberamenazas a las que se enfrentan los dispositivos IoT – Bussines Insider – 2021)

5.3.2 Análisis de escenarios de ataque y debilidades potenciales en la implementación de dispositivos LoRa

Los atacantes pueden explotar una serie de vulnerabilidades en los dispositivos LoRa para llevar a cabo ataques contra la integridad, la confidencialidad o la disponibilidad de los datos.

Ataques contra la integridad, son aquellos que pueden modificar los datos transmitidos por los dispositivos LoRa. Los atacantes pueden utilizar estos ataques para manipular el comportamiento de un sistema o para robar información confidencial.

Un ejemplo de ataque contra la integridad es el ataque de suplantación de identidad. En este ataque, el atacante se hace pasar por un dispositivo legítimo para enviar datos falsos. Los datos falsos pueden utilizarse para manipular el comportamiento de un sistema, como por ejemplo, para activar un interruptor o para cambiar la configuración de un dispositivo.

Otro ejemplo de ataque contra la integridad es el ataque de denegación de servicio. En este ataque, el atacante sobrecarga el dispositivo con tráfico de datos, lo que impide que el dispositivo transmita datos legítimos. Los ataques de denegación de servicio pueden utilizarse para interrumpir el funcionamiento de un sistema o para impedir que los dispositivos LoRa transmitan datos críticos.

Ataques contra la confidencialidad, son aquellos que pueden revelar datos confidenciales transmitidos por los dispositivos LoRa. Los atacantes pueden utilizar estos ataques para robar información confidencial, como contraseñas o datos personales.

Un ejemplo de ataque contra la confidencialidad es el ataque de escucha. En este ataque, el atacante intercepta el tráfico de datos entre un dispositivo LoRa y un servidor. Los datos interceptados pueden utilizarse para robar información confidencial, como contraseñas o datos personales.

Otro ejemplo de ataque contra la confidencialidad es el ataque de fuerza bruta. En este ataque, el atacante intenta adivinar la contraseña de un dispositivo LoRa mediante un proceso de prueba y error.

Ataques contra la disponibilidad, son aquellos que pueden impedir que un dispositivo LoRa transmita datos. Los atacantes pueden utilizar estos ataques para interrumpir el funcionamiento de un sistema o para impedir que los dispositivos LoRa transmitan datos críticos.

Un ejemplo de ataque contra la disponibilidad es el ataque de denegación de servicio. En este ataque, el atacante sobrecarga el dispositivo con tráfico de datos, lo que impide que el dispositivo transmita datos legítimos.

Otro ejemplo de ataque contra la disponibilidad es el ataque de jamming. En este ataque, el atacante utiliza un transmisor de radio para interferir con la señal de radio del dispositivo LoRa.

Debilidades potenciales, además de los escenarios de ataque mencionados anteriormente, existen una serie de debilidades potenciales en la implementación de dispositivos LoRa que pueden ser explotadas por los atacantes.

Una debilidad potencial es la fragilidad del cifrado. El cifrado utilizado en LoRa es relativamente débil y puede ser descifrado por atacantes con los recursos adecuados.

Otra debilidad potencial es la falta de autenticación. Los dispositivos LoRa no se autentican de forma predeterminada, lo que significa que cualquier dispositivo puede conectarse a una red LoRa.

Una tercera debilidad potencial es la falta de protección de la identidad. Los dispositivos LoRa no protegen la identidad de los dispositivos, lo que significa que los atacantes pueden rastrear el tráfico de datos de un dispositivo LoRa.

5.4 Vulnerabilidades Conocidas en Dispositivos LoRa

como toda tecnología, los dispositivos LoRa no están exentos de riesgos de seguridad, por eso se debe revisar desde un enfoque técnico las características de los mismos.

La especificación de LoRa se ha mantenido cerrada y restringida a los fabricantes de chips LoRa. Sin embargo, las características del protocolo fueron determinadas mediante la ingeniería inversa de las señales intercambiadas por Matthew Knight y Balint Seeber. Esta investigación resultó en la creación de un módulo de GNU Radio (`gr-lora`) cuyo código fuente se puede descargar libremente desde GitHub.

5.4.1 Exploración de vulnerabilidades documentadas en dispositivos LoRa

LoRa es un protocolo de capa física inalámbrico privativo diseñado por Semtech para trabajar en las bandas ICM de 900 MHz (la frecuencia exacta depende de la región). En la Unión Europea, la frecuencia de trabajo es de 868 MHz. Las bandas ICM están compartidas por múltiples tecnologías de comunicaciones, que están sujetas a restricciones legales, como la potencia máxima permitida o el ciclo de trabajo (entre el 0,1% y el 1%). Estas restricciones limitan la duración y la frecuencia de las transmisiones de LoRa, lo que puede provocar intervalos de varios segundos entre tramas.

Para mejorar la inmunidad a la interferencia, LoRa utiliza una modulación de espectro ensanchado denominada CSS (Chirp Spread Spectrum). En esta modulación, la información digital se codifica como diferentes rotaciones de rampas de frecuencia dentro de los límites de cada canal. Estas rotaciones se denominan "chirps". Figura 5-1

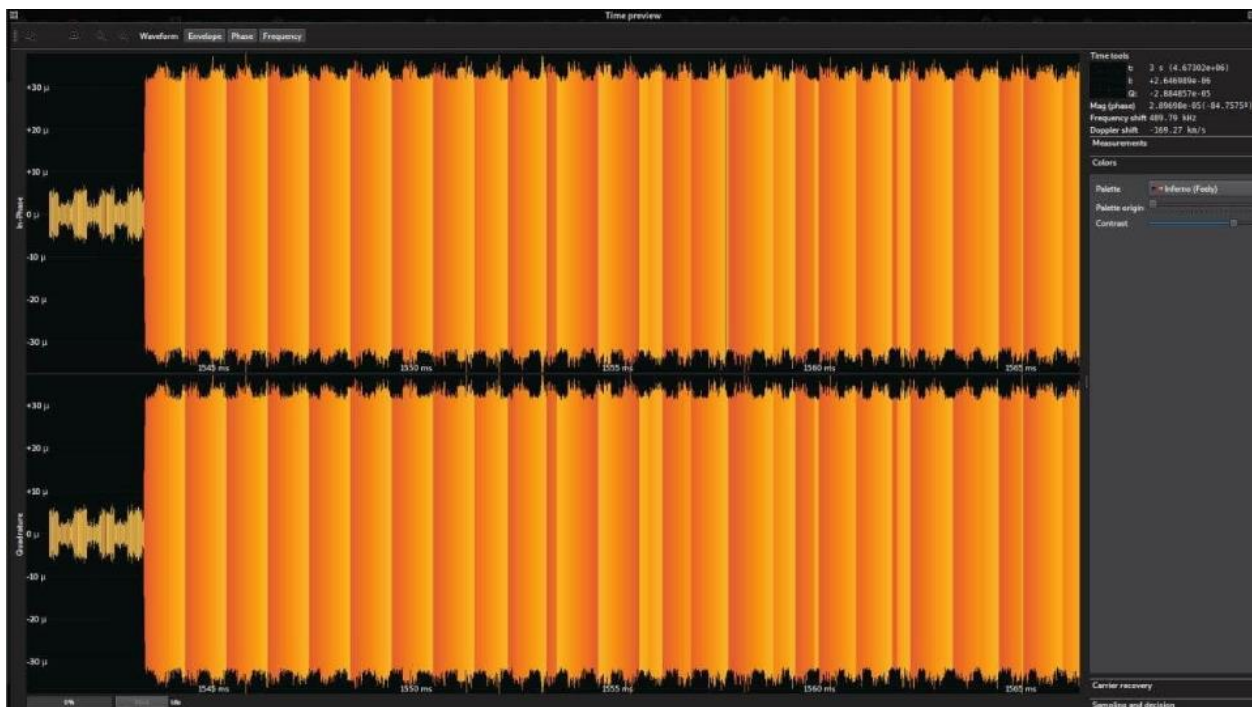


Figura 5-1: Rafaga LoRa.

En la Unión Europea (región ITU-1), la banda de 868 se divide en 10 canales LoRa, con anchos de 125 y 250 kHz para comunicaciones ascendentes (nodo-pasarela) y de 125 kHz solo para canales descendentes (pasarela-nodo). Siendo fijo el ancho de estos canales, la tasa de bits transmitida se controla ajustando dos parámetros: el spreading factor (SF) y el chirp rate (CR). Estos parámetros son en realidad sinónimos de “bits por símbolo” (que acepta valores entre 7 y 12) y “tasa de símbolos” respectivamente. Además, estos parámetros no son independientes, ya que la tasa de símbolos se calcula a partir de los bits por símbolo dividiendo el ancho de banda del canal por $2SF$. Es decir, incrementar el SF en una unidad (un bit) duplica la cantidad de símbolos que se pueden codificar y, al mismo tiempo, reduce la cantidad de chirps que se envían a la mitad.

En la práctica, como la cantidad de bits por unidad de tiempo es producto del CR por el SF, y como para un aumento lineal del SF se produce una disminución exponencial del CR, lo que sucede es que para mayores SF se obtienen menores tasas de transmisión de información. Esto permite ajustar la velocidad de envío de información en función de factores como la contención del canal, ruido, etcétera. (Ciberseguridad en LoRa – Gonzalo Carracedo – 2020)

De cara a aumentar la resiliencia de la transmisión, la información es transformada en varios pasos antes de ser enviada al medio. En particular:

Los símbolos se ordenan en código Gray (de forma que la confusión de un símbolo con el adyacente sólo impacte en un bit)

La información es aleatorizada aplicando un XOR bit a bit a la misma junto una secuencia de whitening, la cual no se corresponde con ninguna de las documentadas por Semtech. Esta secuencia de whitening fue derivada experimentalmente por Knight y Seeber (2016).

Los bits son reordenados con un entrelazador diagonal cuya descripción precisa tampoco aparece en las patentes de Semtech. El algoritmo de entrelazamiento también fue descifrado experimentalmente por Knight y Seeber (2016).

Se dota de redundancia a la información mediante el empleo de códigos Hamming de tasas variables de $4/5$, $4/6$, $4/7$ y $4/8$, con ordenaciones de bit no estándares.

El resultado de estas transformaciones (debido a los bits de paridad introducidos por los códigos Hamming) es una tasa de envío más reducida pero mayor robustez contra ruido e interferencias.

Una vez que el receptor ha sido capaz de sincronizarse con el preámbulo de una ráfaga y descodificar la información contenida en él, el resultado es una trama LoRa PHY con la siguiente estructura:

Preámbulo	Cabecera (4/8)	Payload (4/N)	CRC (opcional)
-----------	----------------	---------------	----------------

Donde la cabecera tiene una tasa de codificación fija de $4/8$ (mayor redundancia posible) e incluye información como el tamaño del payload, la tasa de codificación del payload y si hay un CRC presente o no. Es en este payload donde se incluyen las tramas LoRaWAN (tramas MAC).

5.4.2 Casos de estudio sobre incidentes de seguridad que han afectado dispositivos LoRa

Análisis de los casos de estudio más relevantes sobre incidentes de seguridad que han afectado dispositivos LoRa. El análisis se centra en las vulnerabilidades que se han explotado en estos incidentes y en las medidas de mitigación que se han adoptado para abordarlas.

Caso de estudio 1: Vulnerabilidad de suplantación de identidad en dispositivos LoRa de Semtech

En 2019, investigadores de seguridad de la empresa IOActive descubrieron una vulnerabilidad de suplantación de identidad en dispositivos LoRa de Semtech. Esta vulnerabilidad permitía a los atacantes tomar el control de un dispositivo LoRa sin autenticarse previamente.

La vulnerabilidad se encontraba en el protocolo de autenticación OTAA utilizado por LoRaWAN. El protocolo OTAA utiliza un procedimiento de desafío-respuesta para autenticar los dispositivos LoRa. En este procedimiento, el dispositivo LoRa genera un desafío aleatorio y lo envía al servidor de autenticación. El servidor de autenticación responde con una respuesta, que el dispositivo LoRa debe verificar.

La vulnerabilidad se encontraba en el proceso de generación del desafío aleatorio. El desafío aleatorio se generaba utilizando una función criptográfica débil, que podía ser predicha por los atacantes. Los atacantes podían utilizar esta vulnerabilidad para generar un desafío aleatorio que el dispositivo LoRa aceptaría como válido.

Una vez que el atacante tenía control del dispositivo LoRa, podía utilizarlo para enviar datos falsos o para interrumpir el funcionamiento del dispositivo.

Medidas de mitigación, Semtech publicó una actualización de firmware para abordar esta vulnerabilidad. La actualización de firmware modifica el proceso de generación del desafío aleatorio para utilizar una función criptográfica más fuerte.

Caso de estudio 2: Vulnerabilidad de seguridad en dispositivos LoRa de Aclara Networks

En 2020, investigadores de seguridad de la empresa NCC Group descubrieron una vulnerabilidad de seguridad en dispositivos LoRa de Aclara Networks. Esta vulnerabilidad permitía a los atacantes interceptar y descifrar los datos transmitidos por los dispositivos LoRa.

La vulnerabilidad se encontraba en el cifrado utilizado por LoRaWAN. LoRaWAN utiliza el cifrado AES-128 para proteger los datos transmitidos por los dispositivos LoRa. Sin embargo, la implementación del cifrado AES-128 en los dispositivos LoRa de Aclara Networks era defectuosa.

La vulnerabilidad permitía a los atacantes realizar un ataque de fuerza bruta para descifrar los datos transmitidos por los dispositivos LoRa.

Medidas de mitigación, Aclara Networks publicó una actualización de firmware para abordar esta vulnerabilidad. La actualización de firmware corrige el defecto en la implementación del cifrado AES-128.

Caso de estudio 3: Vulnerabilidad de seguridad en dispositivos LoRa de ChirpStack

En 2021, investigadores de seguridad de la empresa Red Hat descubrieron una vulnerabilidad de seguridad en dispositivos LoRa de ChirpStack. Esta vulnerabilidad permitía a los atacantes tomar el control de una red LoRaWAN.

La vulnerabilidad se encontraba en el servidor de autenticación de ChirpStack. El servidor de autenticación de ChirpStack utiliza una base de datos para almacenar las claves de cifrado de los dispositivos LoRa.

La vulnerabilidad permitía a los atacantes acceder a la base de datos de claves de cifrado. Una vez que los atacantes tenían acceso a la base de datos, podían utilizar las claves de cifrado para tomar el control de la red LoRaWAN.

Medidas de mitigación, ChirpStack publicó una actualización de firmware para abordar esta vulnerabilidad. La actualización de firmware modifica el acceso a la base de datos de claves de cifrado para hacerlo más seguro.

5.5 Tecnologías emergentes en seguridad de la información en dispositivos LoRa

La proliferación de dispositivos LoRa (Long Range) en diversos sectores, como la agricultura inteligente, edificios inteligentes, submetering, medida de energía, generación de energía solar, monitorización de agua, gas, consumos, las ciudades inteligentes y la industria 4.0, ha impulsado la necesidad de robustecer la seguridad de la información que estos dispositivos manejan.

Este artículo, desde una perspectiva de investigación académica, analiza las tecnologías emergentes que pueden contribuir a mejorar la seguridad de la información en dispositivos LoRa.

Tecnologías emergentes:

5.5.1 Blockchain

Facilita la implementación de mecanismos de control de acceso más seguros (Pastorino, 2022).

- Distribución y Disponibilidad:
 - En una red blockchain, cada nodo almacena una copia exacta de la cadena de bloques.
 - Esto garantiza la disponibilidad de la información en todo momento.
 - Aunque un atacante quisiera provocar una denegación de servicio, basta con que al menos un nodo esté operativo para que la información esté disponible.
- Registro Consensuado e Integridad:
 - Todos los nodos contienen la misma información, lo que hace casi imposible alterarla.
 - Para modificar la información en la blockchain, un atacante debería cambiar la cadena completa en al menos el 51% de los nodos.
- Inmutabilidad y Vinculación de Bloques:
 - Cada bloque está matemáticamente vinculado al siguiente.
 - Una vez que se añade un bloque a la cadena, se vuelve inalterable.
 - Si se modifica un bloque, su relación con la cadena se rompe.
- Certificación y Autenticidad:
 - Cada nodo utiliza certificados y firmas digitales para verificar la información y validar transacciones.
 - Esto asegura la autenticidad de los datos almacenados en la blockchain.
- Blockchain como un Escribano:
 - Podemos pensar en la blockchain como un escribano digital.
 - Un medio para certificar y validar cualquier tipo de información.
 - Un registro confiable, descentralizado y resistente a la manipulación de datos.
- Comparación con Modelos Centralizados:

- En la actualidad, confiamos nuestra información a empresas centralizadas como Google o Facebook.
- La blockchain ofrece una alternativa donde la información no se puede perder, modificar o eliminar.
- Es un cambio significativo en la forma en que manejamos y protegemos nuestros datos.

5.5.2 Inteligencia Artificial (IA)

La inteligencia artificial está siendo ampliamente adoptada en diversas industrias para mejorar la eficiencia y productividad, sustituyendo tareas manuales con automatización. En la salud, se aplica en tratamientos personalizados y descubrimiento de medicamentos, mientras que en el comercio, se utiliza para ofrecer recomendaciones a los clientes y prevenir la pérdida de clientes mediante estrategias proactivas.

En el campo de la seguridad de la información, la inteligencia artificial está siendo cada vez más utilizada para abordar los desafíos asociados con los ataques informáticos cada vez más sofisticados. El aumento de dispositivos de usuario final, servicios en la nube y redes de datos complejas ha complicado la labor de los especialistas en seguridad informática. Como respuesta, se están implementando sistemas basados en inteligencia artificial para hacer frente a esta situación.

La inteligencia artificial ofrece una mejora significativa en comparación con los sistemas de seguridad convencionales, los cuales se basan en reglas predefinidas y patrones conocidos para identificar posibles amenazas. Sin embargo, debido a la continua evolución de las técnicas de los cibercriminales, estas medidas pueden resultar insuficientes contra amenazas más avanzadas. La

IA, por otro lado, es capaz de analizar grandes volúmenes de datos en tiempo real y reconocer patrones asociados con comportamientos sospechosos, lo que le permite detectar posibles ataques incluso antes de que se materialicen. Esto permite tomar medidas inmediatas, como bloquear ciertos tipos de paquetes o archivos, y alertar a los especialistas en ciberseguridad para que tomen las acciones necesarias.

La inteligencia artificial en seguridad informática también ofrece la capacidad de automatizar tareas repetitivas, como el envío de notificaciones, el análisis de registros de acceso y actividades de usuarios, la revisión de eventos en dispositivos, la generación de reportes, y la validación de datos de usuarios en instituciones bancarias, entre otros protocolos de seguridad y auditoría. Esta automatización libera tiempo y recursos de los equipos de seguridad, permitiéndoles concentrarse en tareas más complejas y críticas, como el análisis de amenazas y la respuesta a incidentes, lo que mejora su eficiencia.

El uso de inteligencia artificial puede ayudar a los especialistas en seguridad informática a combatir la fatiga por exceso de alarmas, causada por la proliferación de dispositivos conectados a la red, como los dispositivos IoT, el aumento de sistemas en la nube y el incremento de teletrabajadores. Esta situación lleva a la generación de numerosas alertas, muchas de las cuales son redundantes o difíciles de entender, lo que disminuye la capacidad de los equipos de seguridad para detectar amenazas. La IA puede detectar patrones de comportamiento anómalos y automatizar tareas repetitivas, reduciendo así el riesgo asociado con la falta de atención a las alertas o su clasificación incorrecta como falsos positivos (Robayo, 2023).

5.5.3 Computacion Cuantica

Aunque la computación cuántica aún está en proceso de evolución, se vislumbran importantes y revolucionarios impactos en el ámbito de la ciberseguridad. Sin embargo, estas ventajas también traen consigo nuevas amenazas de seguridad que requerirán un enfoque diferente en cuanto a la encriptación de datos.

Aunque las computadoras cuánticas actuales no pueden descifrar la mayoría de los métodos de encriptación actuales, es crucial anticiparse a estas amenazas y encontrar soluciones desde ahora. La adopción de un enfoque de defensa en profundidad, con múltiples capas de protección, será esencial para abordar las amenazas cuánticas, similar a cómo se manejan otras vulnerabilidades de seguridad.

Algunas organizaciones ya están trabajando en soluciones de encriptación cuánticamente seguras para prepararse para las amenazas del futuro. Sin embargo, la concienciación sobre este tema entre los usuarios es crucial. Además de implementar capas de seguridad cuántica, será necesario formar a profesionales capaces de utilizar esta tecnología de manera segura y mitigar los riesgos de seguridad asociados. Aunque la situación aún está en sus primeras etapas, es importante comenzar a abordar esta problemática cuanto antes.

Uno de los principales enfoques en la seguridad de la computación cuántica es el criptográfico, donde se están desarrollando avances en cifrado "seguro cuántico". El Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) está evaluando 69 nuevos métodos potenciales de "criptografía poscuántica". Además, se está desarrollando Quantum Key Distribution (QKD) para transferir claves cuánticas de manera segura entre dos puntos finales, utilizando propiedades físicas, anteriormente solo posible a través de fibra óptica.

Las organizaciones ahora pueden elegir el nivel de preparación cuántica que desean, agregando criptografía QKD o PQC según sea necesario para la seguridad de sus comunicaciones. Sin embargo, es crucial que las organizaciones comprendan que la criptografía es solo una parte de la seguridad general. Deben repensar sus esquemas de seguridad y considerar factores como la concienciación sobre seguridad, las vulnerabilidades de software y el acceso interno a los datos, ya que el mejor cifrado no protegerá contra todas las posibles amenazas (Micucci, 2023).

5.5.4 Redes definidas por software (SDN)

Este tipo de soluciones permiten detectar y prevenir ataques de forma más efectiva, aborda la necesidad de una arquitectura de seguridad eficaz para las redes LoRaWAN (Long Range Wide Area Network) utilizando SDN (Software-Defined Networking). Este tipo de redes, ampliamente utilizadas en aplicaciones de Internet de las Cosas (IoT), enfrentan desafíos significativos en cuanto a la seguridad debido a su naturaleza inalámbrica y su amplia cobertura geográfica.

El texto comienza contextualizando la importancia de las redes LoRaWAN en el panorama actual de la IoT. Estas redes se utilizan para conectar dispositivos remotos con la infraestructura de la red, permitiendo la transmisión de datos de manera eficiente y económica. Sin embargo, debido a su naturaleza inalámbrica y su exposición a diversos tipos de ataques, la seguridad en las redes LoRaWAN es una preocupación creciente para la industria y la investigación en seguridad informática.

Una arquitectura de seguridad basada en SDN podría abordar eficazmente los desafíos de seguridad en las redes LoRaWAN. SDN es un enfoque de red que separa el plano de control del plano de datos, lo que permite una gestión centralizada y dinámica de la red. Al implementar SDN en redes LoRaWAN, mejora la seguridad mediante la centralización y la gestión dinámica de las políticas de seguridad.

Los componentes clave de la arquitectura de seguridad propuesta, esto incluye el controlador SDN, que actúa como el cerebro de la red, supervisando y controlando el tráfico de datos. También se mencionan los dispositivos de red LoRaWAN, como las estaciones base y los dispositivos finales, que son gestionados por el controlador SDN. Además, se destaca la importancia de implementar mecanismos de autenticación y cifrado para garantizar la confidencialidad e integridad de los datos transmitidos a través de la red LoRaWAN.

Los beneficios potenciales de la arquitectura de seguridad SDN para las redes LoRaWAN, estos incluyen una gestión centralizada y eficiente de las políticas de seguridad, la capacidad de adaptarse dinámicamente a las amenazas emergentes y una mayor visibilidad y control sobre el tráfico de datos en la red.

Además de los aspectos técnicos como los desafíos y las consideraciones prácticas asociadas con la implementación de la arquitectura propuesta. Por ejemplo, se discuten los requisitos de rendimiento y escalabilidad, así como los posibles impactos en la latencia y el consumo de energía de los dispositivos LoRaWAN (Kim et al., 2022).

5.5.5 Internet de las cosas (IoT) seguro

El IoT seguro permite crear dispositivos LoRa más seguros y confiables, ofrece un análisis exhaustivo sobre la seguridad en las redes LoRaWAN (Long Range Wide Area Network). Estas redes, ampliamente utilizadas en aplicaciones de Internet de las Cosas (IoT) debido a su capacidad para proporcionar conectividad de largo alcance con bajo consumo de energía, presentan desafíos significativos en cuanto a la seguridad debido a su naturaleza inalámbrica y su amplia cobertura geográfica.

Una introducción detallada sobre el contexto y la importancia de las redes LoRaWAN en el panorama actual de la IoT. Se resaltan sus ventajas, como su capacidad para conectar dispositivos remotos en áreas geográficamente dispersas y su eficiencia energética, lo que las convierte en una opción atractiva para una amplia gama de aplicaciones, desde la agricultura hasta la monitorización ambiental.

Sin embargo, a pesar de sus beneficios, las redes LoRaWAN enfrentan desafíos significativos en cuanto a la seguridad. Estos desafíos incluyen vulnerabilidades específicas de la tecnología LoRaWAN, como la falta de autenticación mutua entre los dispositivos finales y la red, la exposición a ataques de denegación de servicio (DoS) y la necesidad de garantizar la confidencialidad e integridad de los datos transmitidos.

Se tiene una revisión exhaustiva de las técnicas y mecanismos de seguridad propuestos para abordar estos desafíos en las redes LoRaWAN. Se describen en detalle los diferentes enfoques de seguridad, desde la autenticación y el cifrado de extremo a extremo hasta la gestión de claves y la detección de intrusiones. Además, se analizan los estándares y protocolos de seguridad

relevantes para las redes LoRaWAN, como el estándar LoRaWAN Regional Parameters Specification y el protocolo MAC (Media Access Control) de LoRaWAN.

Las áreas de investigación y desarrollo futuro en seguridad para las redes LoRaWAN. Se identifican oportunidades para mejorar la resistencia a ataques específicos, como ataques de denegación de servicio y ataques de falsificación de identidad, así como para desarrollar soluciones de seguridad más eficientes y escalables.

Además de abordar aspectos técnicos, analiza consideraciones prácticas y de implementación relacionadas con la seguridad en las redes LoRaWAN. Se discuten temas como la gestión de claves, la actualización de firmware y la monitorización de la seguridad, así como la importancia de la colaboración entre la industria, la academia y los organismos de normalización para promover mejores prácticas de seguridad en el ecosistema de la IoT (Alcaraz et al., 2022).

6. Metodología

6.1 Enfoque metodológico

El objetivo es identificar y analizar las vulnerabilidades de seguridad en las comunicaciones entre dispositivos LoRa, este proyecto de investigación se centra en un análisis descriptivo de las posibles vulnerabilidades de seguridad en las comunicaciones entre dispositivos LoRa. La investigación es descriptiva porque busca presentar un panorama detallado de los factores que pueden causar la pérdida de comunicación y datos en un enlace LoRa, describiendo las variables observadas.

6.1.1 Análisis Descriptivo de vulnerabilidades

En esta tesis se realizó, en primer lugar, un análisis exploratorio de las posibles vulnerabilidades en el transporte de datos en una comunicación LoRa para identificar variables que puedan ser afectadas, tales como: espectro, paquetes, autenticación, spreading factor, ancho de banda, etc. Este análisis permitió comprender las características de la comunicación LoRa a nivel de capa de transporte.

6.2 Tipo de estudio

Esta investigación se desarrolla desde el paradigma cuantitativo de tipo correlacional, dado que busca comprender y determinar la interacción-incidencia entre las diversas variables y grupos de variables que intervienen dentro de la comunicación de un sistema LoRa. Asimismo, es de tipo explicativo, porque tiene como objetivo identificar las variables que permitan acceder a un ataque en el cual se pueda poner en riesgo algún pilar de la seguridad de la información, como los son, confidencialidad, integridad y disponibilidad.

Este estudio, en particular, permitió la identificación y clasificación de las posibles fuentes de ataque vulnerabilidades en un sistema de comunicación entre dos dispositivos LoRa. Esta información es esencial para desarrollar estrategias o medidas de mitigación que puedan ayudar para que la comunicación entre dispositivos LoRa conserve la integridad, disponibilidad y confidencialidad.

6.3 Procedimiento

Esta investigación se desarrolló en tres fases: análisis modelo captura de tráfico en sistema de comunicación de dos dispositivos LoRa; análisis de vulnerabilidades; y formulación de acciones o estrategias para minimizar las vulnerabilidades identificadas.

6.3.1 Fase 1: Análisis modelo captura de tráfico LoRa

Se inició con la comprensión de las políticas, protocolos, espectro radioelectrico y dispositivos para lograr entender el funcionamiento del sistema de comunicación entre dispositivos Lora, como tambien el dispositivo que nos permite monitorear el trafico de la red, esta fase es fundamental para determinar el modelo de pruebas de vulnerabilidades que se busca ejecutar.

6.3.2 Fase 2: Análisis de vulnerabilidades

Durante esta etapa del proceso investigativo se busca que las pruebas se ajusten a los requerimientos técnicos iniciales del sistema de comunicación LoRa, con acciones como agrupar factores comunes que ayuden a desarrollar un buen laboratorio de pruebas.

6.3.3 Fase 3: Formulación de acciones o estrategias para minimizar las vulnerabilidades identificadas

Dentro de la metodología de esta investigación, una vez obtenidos y analizados los resultados, se procedió con la formulación de estrategias basadas en los hallazgos. Esta fase es esencial para traducir los conocimientos derivados de fase anterior.

7. Resultados

7.1 Fase 1: Análisis modelo captura de tráfico LoRa

Primero vamos a usar unos dispositivos simples para enviar, recibir y capturar tráfico de radio LoRa, decodificar paquetes, así como el funcionamiento de las redes, descripción general de varios ataques que son posibles contra esta tecnología.

7.1.1 Topología

Para poder simular los escenarios de prueba vulnerabilidades en redes LoRa, vamos a utilizar tres componentes, un módulo para enviar información, otro para recibir y la última una placa sniffer para capturar tráfico LoRa.

Heltec LoRa 32, Una placa de desarrollo ESP32 LoRa (<https://heltec.org/project/wifi-lora-32/>). Las placas ESP32 son de bajo costo, bajo consumo y microcontrolador (MCU de 32 bits de doble núcleo, núcleo ULP, con chip de nodo LoRa SX1276/SX1278). Los Heltec pueden funcionar en modo unidireccional (una unidad emisora y otra receptora), bidireccional (intercambio en ambos sentidos para cada dispositivo) o bien en multidifusión (un mensaje es recibido por todos los dispositivos que estén en su rango de alcance).

CatWAN, es una USB stick open source compatible con LoRa and LoRaWAN (<https://electroniccats.com/store/catwan-usb-stick/>). Está programado con una imagen de

firmware especial que lo convierte en un rastreador de LoRa fácil de usar. Puede capturar pasivamente los intercambios de datos entre dos dispositivos LoRa.

Tenemos dos placas Heltec, vamos a utilizar una transmitir y otra para recibir y luego hacer que se comuniquen entre sí usando LoRa, configuraremos el stick CatWAN como sniffer para capturar el tráfico LoRa. Como se observa en la Figura 7-1.

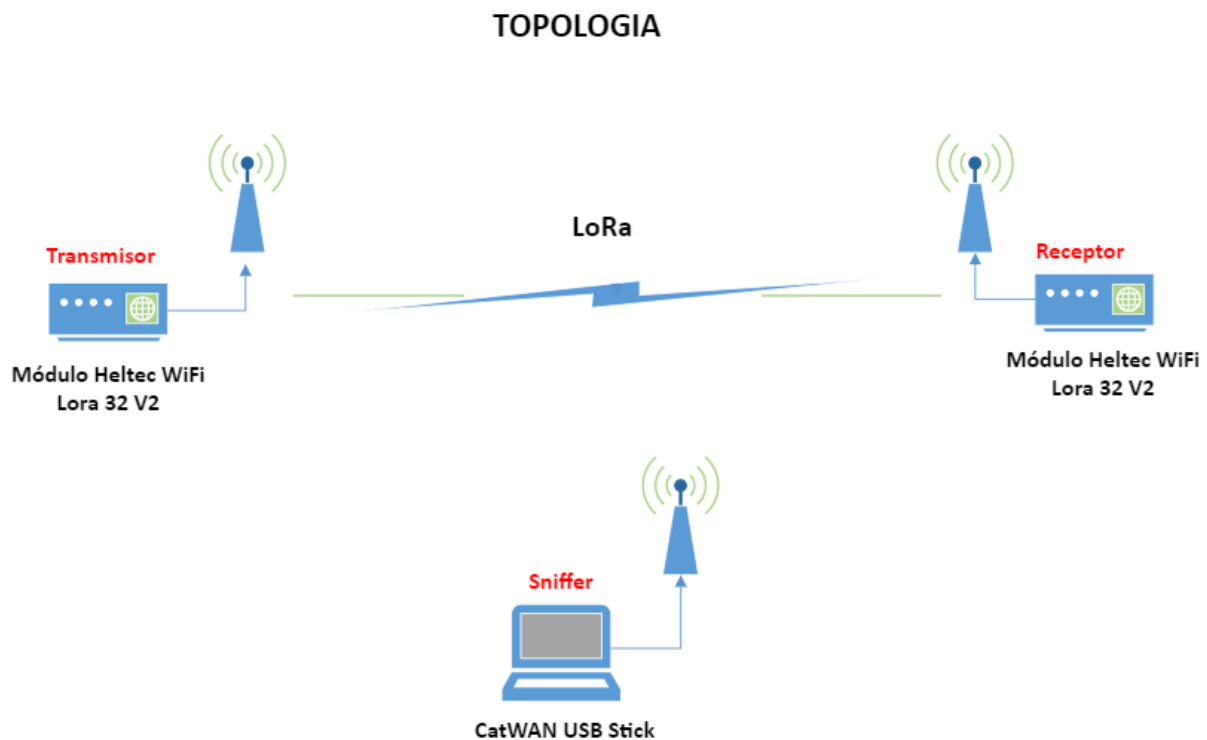


Figura 7-1: Topología.

7.1.2 Configuración de la placa de desarrollo Heltec LoRa 32:

Comenzaremos programando la placa Heltec usando el IDE de Arduino, instalando el IDE y agregando las bibliotecas de Heltec para Arduino-ESP32. Esto nos permitirá programar placas ESP32, como el Heltec LoRa, utilizando el IDE de Arduino. Para realizar la instalación debemos: Clic en File – Preferences – Settings, luego hacer Click en Additional Boards Manager URLs button, Agregue la siguiente URL en la lista: https://github.com/Heltec-Aaron-Lee/WiFi_Kit_series/releases/download/0.0.7/package_heltec_esp32_index.json

Click en OK. Posteriormente hacer Click en Tools - Board - Boards Manager. Buscar la opción Heltec ESP32, Click en instalar la version complete es Heltec ESP32 Series Dev-boards by Heltec Automation 0.0.6. El proximo paso es instalar la libreria Heltec ESP32, vamos a ir al menú principal y hacer Click en la opción Sketch - Include Library - Manage Libraries en el recuadro de buscar escribir “Heltec ESP32” hacer Cclick en instalar la versión Heltec ESP32 Dev-Boards by Heltec Automation option 1.1.5.

7.1.3 Programando el módulo Heltec (Receptor)

Para programar el módulo Heltec, lo primero que debemos hacer es conectar la antena al módulo, esto es muy importante ya que sin ella podríamos dañar el mismo, lo segundo es conectarlo a un puerto USB de nuestro computador. (Figura 7-2).

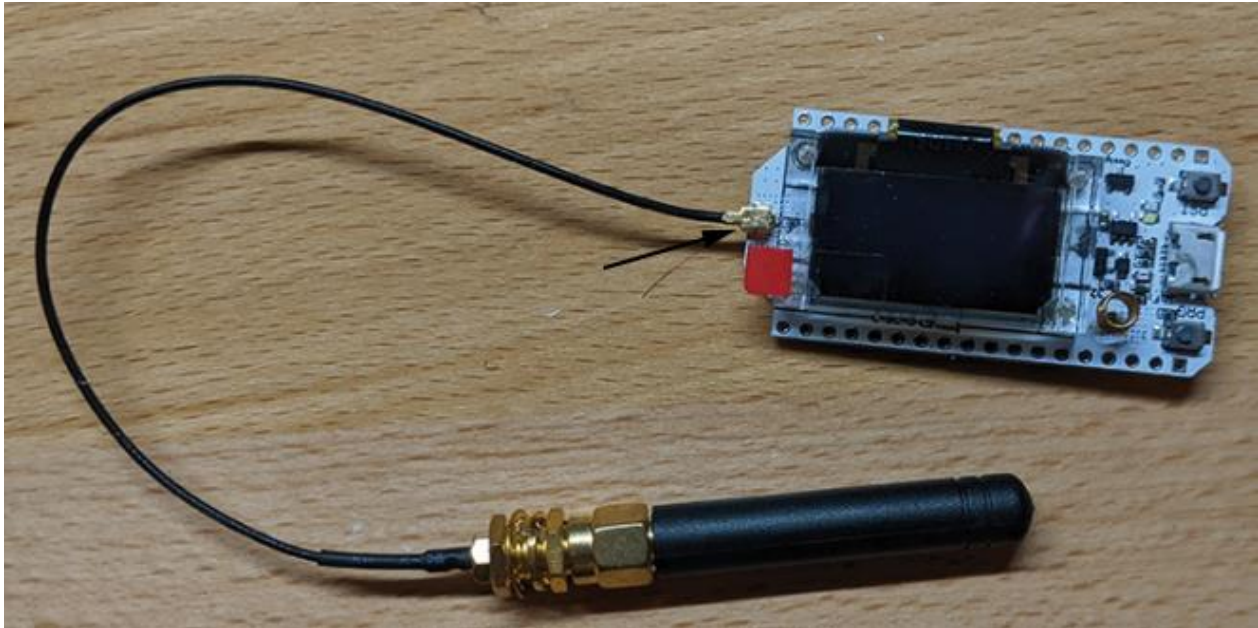


Figura 7-2: Heltec Wi-Fi LoRa 32 (V2) ESP32 SX1278 con soporte Wi-Fi, BLE, LoRa, y LoRaWAN.

En la aplicación Arduino IDE, seleccionamos en el menú principal, Tools – Board - WiFi LoRa 32 (V2), como se muestra en la figura 7-3.

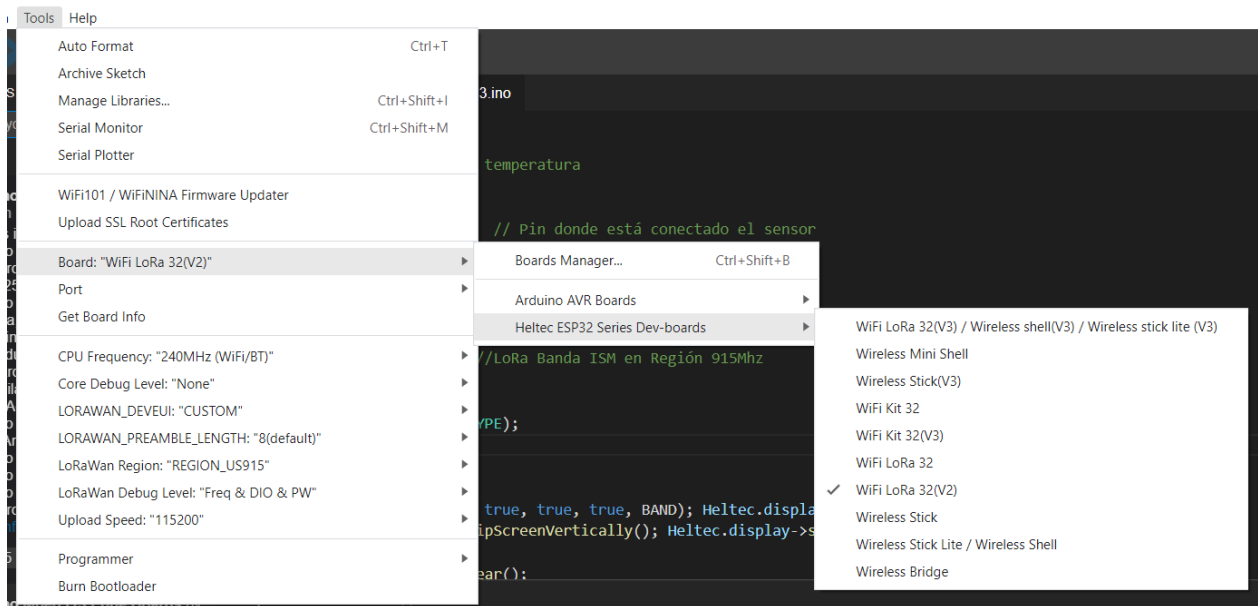


Figura 7-3: Arduino IDE: WiFi LoRa 32(V2).

Vamos a utilizar uno de los ejemplos que se tienen en Arduino IDE, en el menú principal, File – Examples – Heltec ESP32Dev Boards – LoRa – LoRaReceiver, como se muestra en la figura 7-4. Este nos ayudara como elemento que permitira recibir todos los mensajes. Al utilizar este código estamos buscando realizar pruebas más reales, sin alterar nada del mismo.

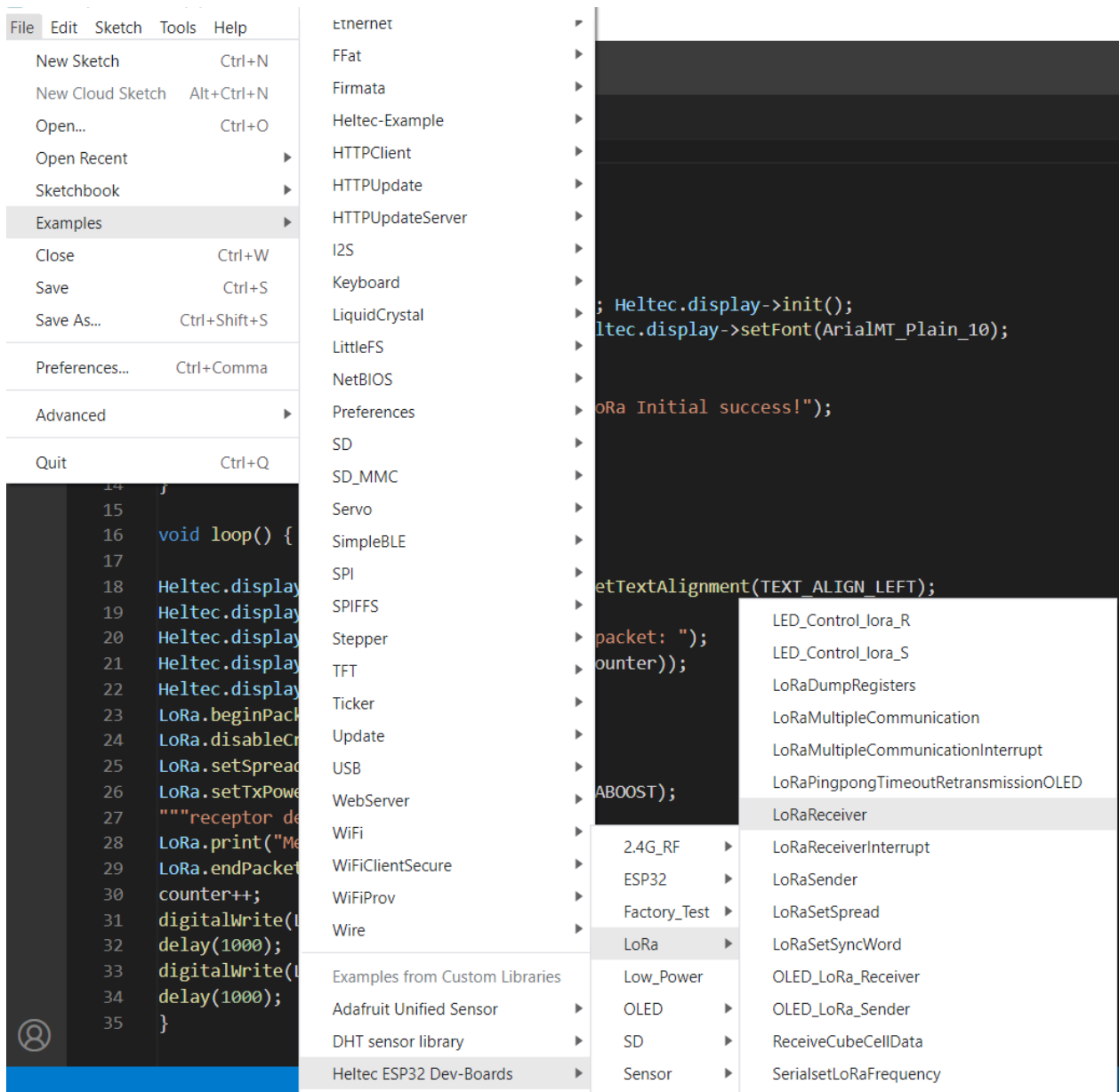


Figura 7-4: Arduino IDE: LoRaReceiver.

El código es:

```
/*
  Check the new incoming messages, and print via serialin 115200 baud rate.

  by Aaron.Lee from HelTec AutoMation, ChengDu, China
  成都惠利特自动化科技有限公司
  www.heltec.cn

  this project also reealss in GitHub:
  https://github.com/Heltec-Aaron-Lee/WiFi_Kit_series
*/

#include "heltec.h"

#define BAND    433E6 //you can set band here directly,e.g. 868E6,915E6
void setup() {
  //WIFI Kit series V1 not support Vext control
  Heltec.begin(true /*DisplayEnable Enable*/, true /*Heltec.LoRa Disable*/, true
/*Serial Enable*/, true /*PABOOST Enable*/, BAND /*long BAND*/);
}

void loop() {
  // try to parse packet
  int packetSize = LoRa.parsePacket();
  if (packetSize) {
    // received a packet
    Serial.print("Received packet ");
    // read packet
    while (LoRa.available()) {
      Serial.print((char)LoRa.read());
    }
    // print RSSI of packet
    Serial.print(" with RSSI ");
    Serial.println(LoRa.packetRssi());
  }
}
```

7.1.4 Programando el módulo Heltec (Transmisor)

Ahora necesitamos configurar el módulo transmisor, vamos al menú principal, File – New Sketch, como se muestra en la Figura 7-5

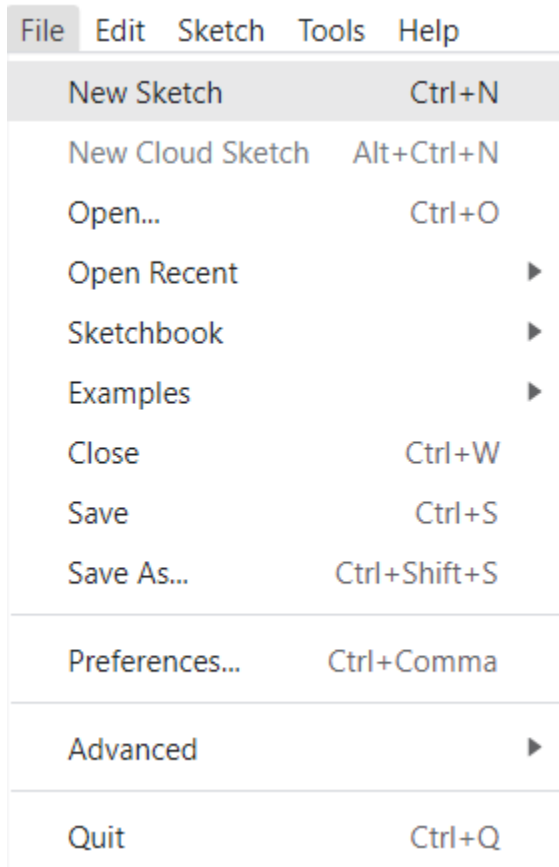


Figura 7-5: Arduino IDE: Sketch

El código que vamos a utilizar es:

```
#include "heltec.h"
#define BAND 915E6
String packet;
unsigned int counter = 0;

void setup() {
```

```
Heltec.begin(true, true, true, true, BAND); Heltec.display->init();
Heltec.display->flipScreenVertically(); Heltec.display-
>setFont(ArialMT_Plain_10);
delay(1500);
Heltec.display->clear();
Heltec.display->drawString(0, 0, "Heltec.LoRa Initial success!");
Heltec.display->display();
delay(1000);
}

void loop() {

Heltec.display->clear(); Heltec.display->setTextAlignment(TEXT_ALIGN_LEFT);
Heltec.display->setFont(ArialMT_Plain_10);
Heltec.display->drawString(0, 0, "Sending packet: ");
Heltec.display->drawString(90, 0, String(counter));
Heltec.display->display();
LoRa.beginPacket();
LoRa.disableCrc();
LoRa.setSpreadingFactor(7);
LoRa.setTxPower(20, RF_PACONFIG_PASELECT_PABOOST);
//receptor de sensor y envío de dato
LoRa.print("Medida sensor"+String(counter));
LoRa.endPacket();
counter++;
digitalWrite(LED, HIGH);
delay(1000);
digitalWrite(LED, LOW);
delay(1000);
}
```

En primer lugar, se tienen las bibliotecas Heltec, que contienen funciones para interactuar con la pantalla OLED de la placa y el nodo LoRa SX1278, en nuestro caso estamos usando la versión estadounidense de LoRa, con la frecuencia de 915 MHz, como prueba inicial vamos con unos parámetros de potencia de transmisión de 20 (TX Power) y Spreading Factor de 7, buscando el mayor alcance posible, como la mejor tasa de transmisión. Figura 7-6

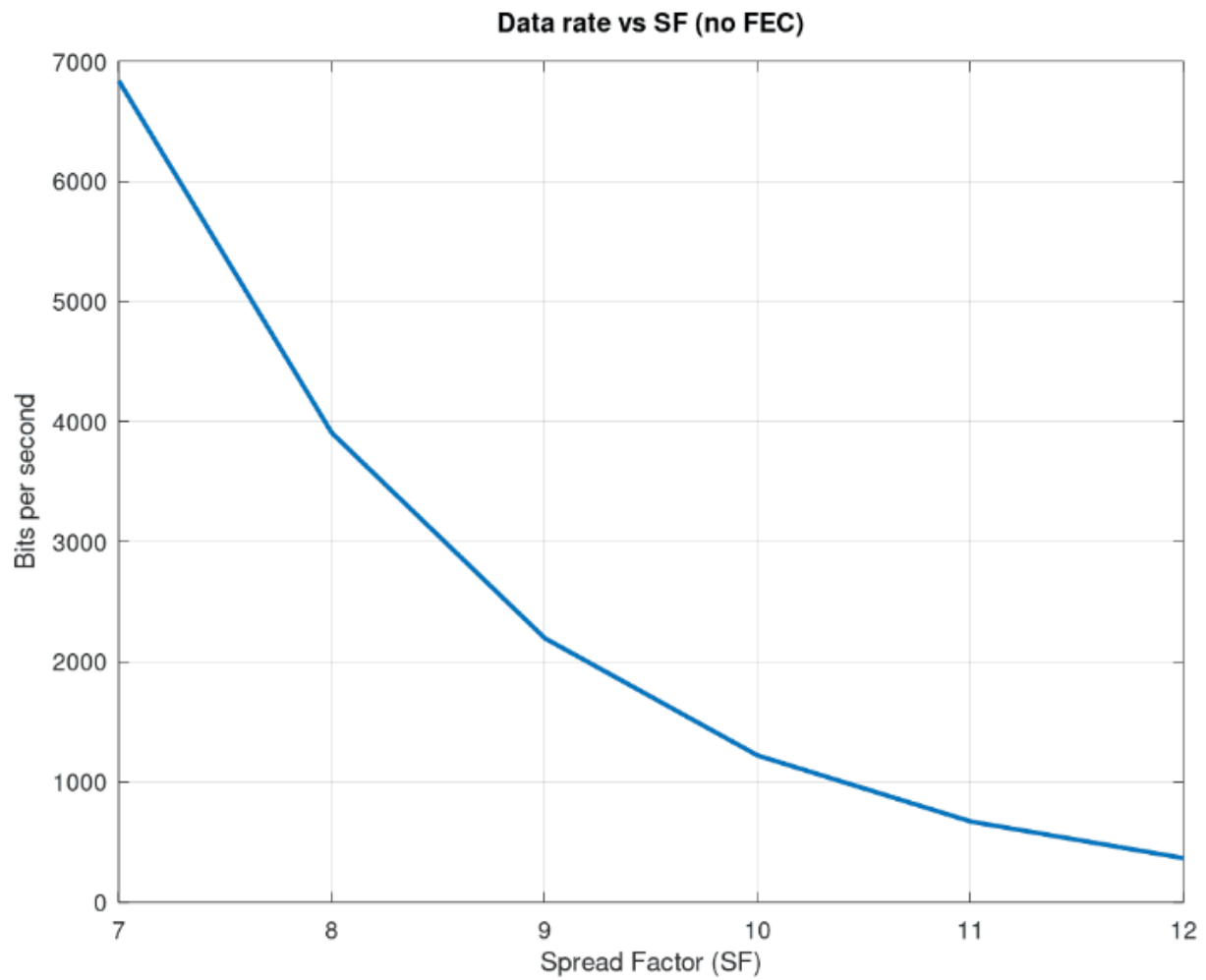


Figura 7-6: Bits por segundo en función del spreading factor.

También necesitamos capturar alguna variable para poder transmitir, en nuestro caso vamos a utilizar un sensor de temperatura, el cual podemos programar para que nos entregue valores en grados Centígrados o Fahrenheit, como lo muestra la Figura 7-7.

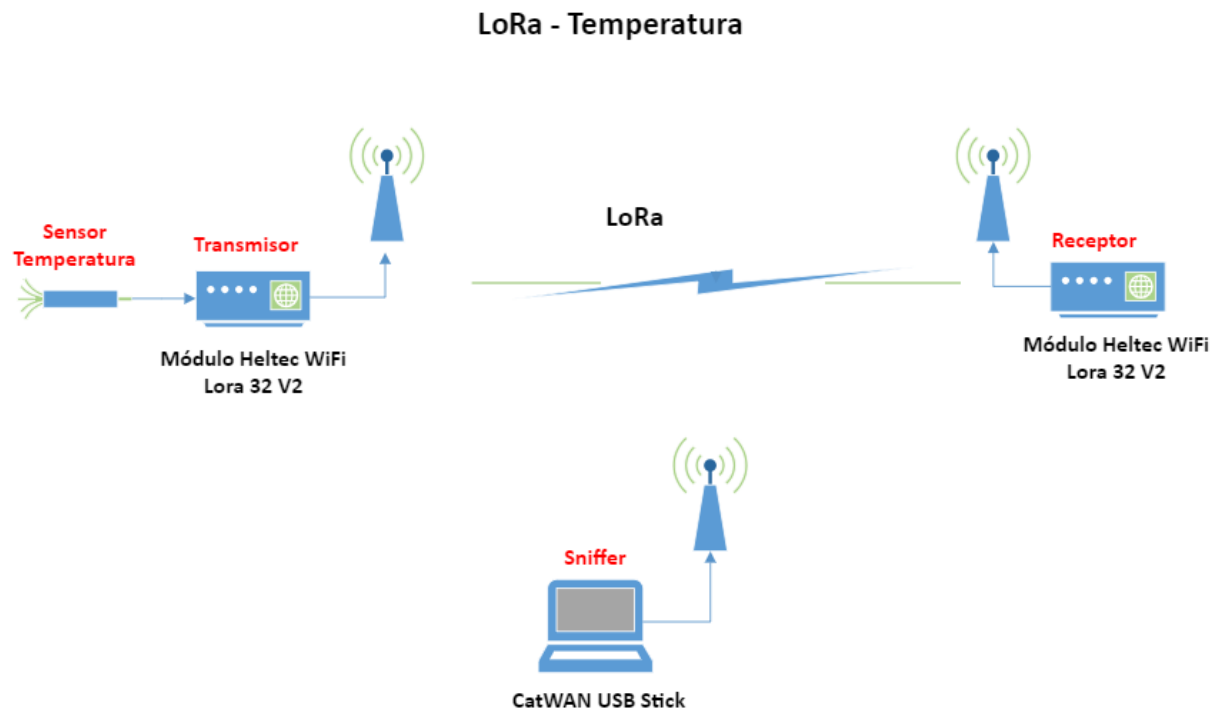


Figura 7-7: Diagrama conexión LoRa – Sensor de temperatura

Por tanto el código final que vamos a utilizar es:

```
#include <heltec.h>

//libreria de sensor temperatura
#include "DHT.h"

#define DHTPIN 13    // Pin donde está conectado el sensor

#define DHTTYPE DHT11 // Descomentar si se usa el DHT 11

//libreria heltec para envio datos lora
#include "heltec.h"
#define BAND 915E6 //LoRa Banda ISM en Región 915Mhz

DHT dht(DHTPIN, DHTTYPE);

void setup() {
```

```
    Heltec.begin(true, true, true, true, BAND); Heltec.display->init();
    Heltec.display->flipScreenVertically(); Heltec.display-
>setFont(ArialMT_Plain_10);
    delay(1500);
    Heltec.display->clear();
    Heltec.display->drawString(0, 0, "Heltec.LoRa Initial success!");
    Heltec.display->display();
    delay(1000);

    Serial.begin(9600);
    Serial.println("Iniciando...");
    dht.begin();
}
void loop() {
    delay(2000);
    float h = dht.readHumidity(); //Leemos la Humedad
    float t = dht.readTemperature(); //Leemos la temperatura en grados Celsius
    float f = dht.readTemperature(true); //Leemos la temperatura en grados
Fahrenheit
    //-----Enviamos las lecturas por el puerto serial-----
    Serial.print("Humedad ");
    Serial.print(h);
    Serial.print(" %t");
    Serial.print("Temperatura: ");
    Serial.print(t);
    Serial.print(" *C ");
    Serial.print(f);
    Serial.println(" *F");

    Heltec.display->clear();
    Heltec.display->setTextAlignment(TEXT_ALIGN_LEFT);
    Heltec.display->setFont(ArialMT_Plain_10);
    Heltec.display->drawString(0, 0, "Sending packet: ");
    Heltec.display->drawString(90, 0, String(t));
    Heltec.display->display();
    LoRa.beginPacket(); //Start the sequence of sending a packet.
    LoRa.disableCrc(); //Enable or disable CRC usage, by default a CRC is not used.
    LoRa.setSpreadingFactor(7); //Change the spreading factor of the radio. spreading
factor, defaults to 7 , Supported values are between 6 and 12. If a spreading
factor of 6 is set, implicit header mode must be used to transmit and receive
packets
    //cuanto te "esparces" en el tiempo, transmitir mas despacio, SF7 a SF12 de menor
a mayor esparcimiento
```

```
LoRa.setTxPower(20, RF_PACONFIG_PASELECT_PABOOST); //Change the TX power of the
radio. Supported values are 2 to 20 for PA_OUTPUT_PA_BOOST_PIN, and 0 to 14 for
PA_OUTPUT_RFO_PIN

//receptor de sensor y envío de dato
LoRa.print("Medida sensor en celsius "+String(t));
LoRa.endPacket(); //End the sequence of sending a packet

digitalWrite(LED, HIGH);
delay(1000);
digitalWrite(LED, LOW);
delay(1000);
}
```

Con este código buscamos capturar una variable análoga como lo es la temperatura y transmitirlo por medio de LoRa, la gran ventaja de este es que nos permite cambiar valores fundamentales para un buen funcionamiento a nivel de radio e interferencias, buscando garantizar que el mensaje pueda ser transportado sin ningún tipo de cambio.

7.1.5 Programando el módulo CatWAN USB Stick (Sniffer)

Ahora necesitamos configurar el módulo transmisor, vamos al menú principal, File – New Sketch, como se muestra en la Figura 7-8

Ahora vamos a configurar el dispositivo que nos permitirá capturar este tráfico LoRa. El modulo USB CatWAN (Figura 4-8) utiliza un chip RFM95 y puede configurarlo dinámicamente para que utilice 868 MHz (para la Unión Europea) o 915 MHz (para los Estados Unidos).



Figure 7-8: CatWAN USB stick, compatible with LoRa and LoRaWAN, es basado en el RFM95 transceiver.

Después de conectar el dispositivo a la computadora, se presione rápidamente el botón de reinicio dos veces, inmediatamente nos mostrara una unidad de almacenamiento USB llamada USBSTICK en el Explorador de archivos de Windows, descargamos e instalamos la última versión de CircuitPython de Adafruit así: https://circuitpython.org/board/catwan_usbstick/. CircuitPython es una herramienta fácil y abierta con lenguaje fuente basado en MicroPython, una versión de Python optimizada para microcontroladores, vamos a utilizar la versión 4.1.0.

CatWAN utiliza un microcontrolador SAMD21, que tiene un gestor de arranque que nos permite de forma fácil flashear código en él, utiliza el formato de flasheo USB de Microsoft (UF2), que es un formato de archivo adecuado para flashear microcontroladores en unidades flash extraíbles, esto nos permite arrastrar y soltar el archivo UF2 de Radio alcance al dispositivo de almacenamiento USBSTICK.

Esta acción hace automáticamente un flash del Boot-Loader, el dispositivo se reinicia y cambia el nombre de la unidad a CIRCUITPY, adicionalmente se requieren dos bibliotecas de CircuitPython: Adafruit CircuitPython RFM9x y Adafruit CircuitPython BusDevice. Las podemos encontrar en https://github.com/adafruit/Adafruit_CircuitPython_RFM9x/releases y https://github.com/adafruit/Adafruit_CircuitPython_BusDevice/releases.

Los instalamos usando `adafruitcircuitpython-rfm9x-4.x-mpy-1.1.6.zip` y `adafruit-circuitpython-bus-device-4.xmpy-4.0.0.zip`. El número 4.x se refiere a la versión de CircuitPython, debemos asegurarnos de que estas instalaciones corresponden con la versión instalada, debemos descomprimirlos y transferir los archivos. mpy a la unidad CIRCUITPY, tener muy en cuenta que este método necesita que los archivos. mpy estén en el directorio de la biblioteca de bus, como se muestra en la Figura 7-9. Los archivos de la biblioteca se colocan dentro del directorio lib, y hay un archivo subdirectorio `adafruit_bus_device` para los módulos I2C y SPI. El archivo `code.py` que creará reside en el directorio superior (raíz) de la unidad de volumen USB.

```
G:\>dir /s
Volume in drive G is CIRCUITPY
Volume Serial Number is 2821-0000

Directory of G:\

01/01/2000  12:00 AM    <DIR>          .fseventsd
01/01/2000  12:00 AM             0 .metadata_never_index
01/01/2000  12:00 AM             0 .Trashes
01/01/2000  12:00 AM    <DIR>          lib
01/01/2000  12:00 AM             92 boot_out.txt
09/04/2019  02:31 AM      1,044 code.py
                4 File(s)          1,136 bytes

Directory of G:\.fseventsd

01/01/2000  12:00 AM    <DIR>          .
01/01/2000  12:00 AM    <DIR>          ..
01/01/2000  12:00 AM             0 no_log
                1 File(s)           0 bytes

Directory of G:\lib

01/01/2000  12:00 AM    <DIR>          .
01/01/2000  12:00 AM    <DIR>          ..
08/26/2019  01:07 AM      8,741 adafruit_rfm9x.mpy
08/27/2019  11:58 PM    <DIR>          adafruit_bus_device
                1 File(s)          8,741 bytes

Directory of G:\lib\adafruit_bus_device

08/28/2019  12:43 AM    <DIR>          .
08/28/2019  12:43 AM    <DIR>          ..
08/27/2019  11:58 PM      1,766 i2c_device.mpy
08/27/2019  11:58 PM      1,250 spi_device.mpy
08/27/2019  11:58 PM             0 __init__.py
                3 File(s)          3,016 bytes
```

Figure 7-9: CIRCUITPY estructura de directories.

A continuación, configuraremos el puerto serie utilizando PuTTY en Windows, porque ha funcionado mucho mejor que cualquier otro emulador de terminal basado en Windows que probamos, identificamos el puerto COM correcto en Windows así: Administrador de dispositivos, Puertos (COM y LPT) (Figura 7-10).

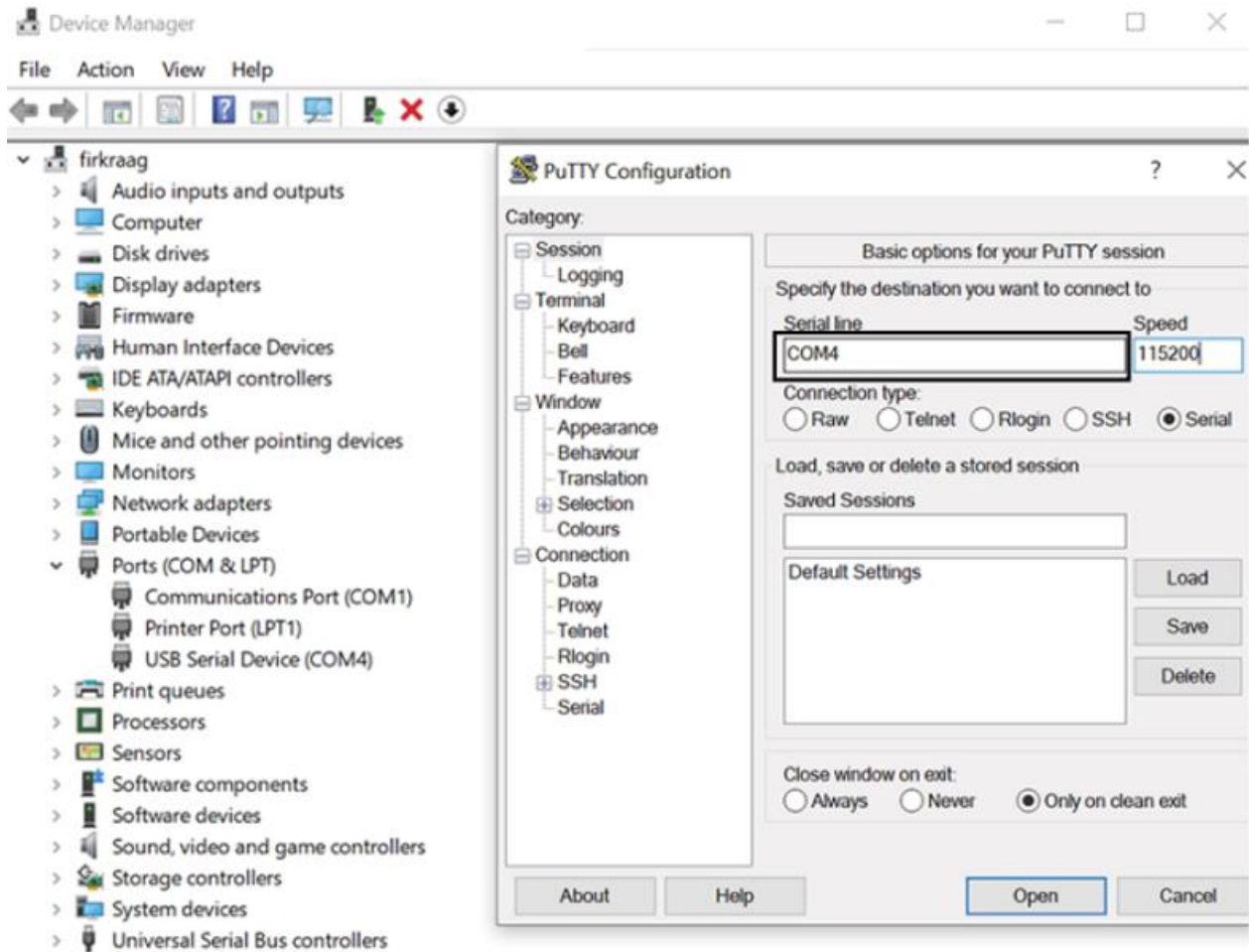


Figure 7-10: Configuración PuTTY CatWAN stick.

Ahora debemos desconectar y volver a conectar la memoria CatWAN en la computadora para identificar el puerto COM correcto, al hacerlo veremos que el puerto COM desaparece en el Administrador de dispositivos cuando lo desconectamos y vuelve a aparecer cuando lo conectamos, luego en la pestaña Session, elegimos Serie Line e introducimos el puerto COM correcto y cambiamos la velocidad en baudios a 115200.

Para escribir el código de CircuitPython, se recomienda utilizar el editor de MU (<https://codewith.mu/>). De lo contrario, los cambios en el variador CIRCUITPY es posible que no se guarde correctamente y en tiempo real, cuando abrimos MU por primera vez, debemos elegir el

modo Adafruit CircuitPython, también puede cambiar el modo más tarde usando el icono Modo en la barra de menús, inicie un nuevo archivo, ingrese el código de la Figura 7-11 y guarde el fichero en la unidad CIRCUITPY usando el botón nombre code.py. Tenga en cuenta que el nombre del archivo es importante, porque CircuitPython buscará un archivo de código llamado code.txt, code.py, main.txt o main.py en ese orden.

Cuando se guarde por primera vez el archivo code.py en la unidad y cada vez que se hagan cambios en el código a través del editor de MU, MU ejecutara automáticamente la versión del código en CatWAN, se puede supervisar esta ejecución mediante la consola serie con PuTTY. usando la consola, también puede presionar CTRL-C para interrumpir el programa o CTRL-D para volver a cargarlo.

```
import board
import busio
import digitalio
import adafruit_rfm9x
RADIO_FREQ_MHZ = 915.0
CS = digitalio.DigitalInOut(board.RFM9X_CS)
RESET = digitalio.DigitalInOut(board.RFM9X_RST)
spi = busio.SPI(board.SCK, MOSI=board.MOSI, MISO=board.MISO)
rfm9x = adafruit_rfm9x.RFM9x(spi, CS, RESET, RADIO_FREQ_MHZ)
rfm9x.spreading_factor = 7
print('Waiting for LoRa packets...')
i = 0
while True:
    packet = rfm9x.receive(timeout=1.0, keep_listening=True, with_header=True)
    if (i % 2) == 0:
        rfm9x.spreading_factor = 7
    else:
        rfm9x.spreading_factor = 11
    i = i + 1
    if packet is None:
        print('Nothing yet. Listening again...')
    else:
        print('Received (raw bytes): {}'.format(packet))
        try:
            packet_text = str(packet, 'ascii')
            print('Received (ASCII): {}'.format(packet_text))
        except UnicodeError:
            print('packet contains non-ASCII characters')
        rssi = rfm9x.rssi
        print('Received signal strength: {} dB'.format(rssi))
```

Figura 7-11: CircuitPython Código para CatWAN USB stick, LoRa sniffer

7.2 Fase 2: Análisis de vulnerabilidades

Las redes de comunicación LoRa (Long Range) son una tecnología emergente que permite la transmisión de datos a larga distancia con un bajo consumo de energía, lo que las hace ideales para aplicaciones de Internet de las Cosas (IoT). Sin embargo, como cualquier tecnología de

comunicación, las redes LoRa no están exentas de amenazas y vulnerabilidades que pueden comprometer la integridad, disponibilidad y confidencialidad de los datos transmitidos.

Una de las principales amenazas en las redes LoRa es la interferencia o jamming. Este tipo de ataque consiste en la emisión deliberada de señales de radiofrecuencia para interferir con las señales de comunicación de la red LoRa. Esta interferencia puede causar la pérdida de paquetes de datos o incluso la interrupción completa de la comunicación.

Otra amenaza común en las redes LoRa es el spoofing o suplantación. En este tipo de ataque, un actor malintencionado puede hacerse pasar por un nodo legítimo de la red y enviar datos falsos o maliciosos. Esto puede llevar a decisiones erróneas basadas en datos incorrectos, lo que puede tener consecuencias graves en aplicaciones críticas como el monitoreo del medio ambiente o la gestión de infraestructuras críticas.

Además, las redes LoRa también pueden ser vulnerables a ataques de repetición. En este tipo de ataque, un actor malintencionado captura y retransmite paquetes de datos legítimos. Esto puede causar una serie de problemas, desde el agotamiento de la batería hasta la ejecución repetida de acciones no deseadas.

7.2.1 Interferencia o jamming

Luego de tener la maqueta funcional con los dos módulos Heltec LoRa 32, uno para transmitir y el otro para recibir, la primera prueba a realizar es de interferencia, para ello incluimos un equipo adicional llamado, analizador de espectros y antenas de marca Anritsu referencia Cell Master MT8212B, con espectro de operación entre 100 kHz a 3000 MHz (espectro LoRa 915 MHz), como se muestra en la Figura 7-12.



Figura 7-12: Anritsu Cell Master MT8212B

Con este analizador de espectros buscamos identificar la señal portante en los 915 MHz, para poderla analizar e identificar sus características, como se muestra en la Figura 7-13.

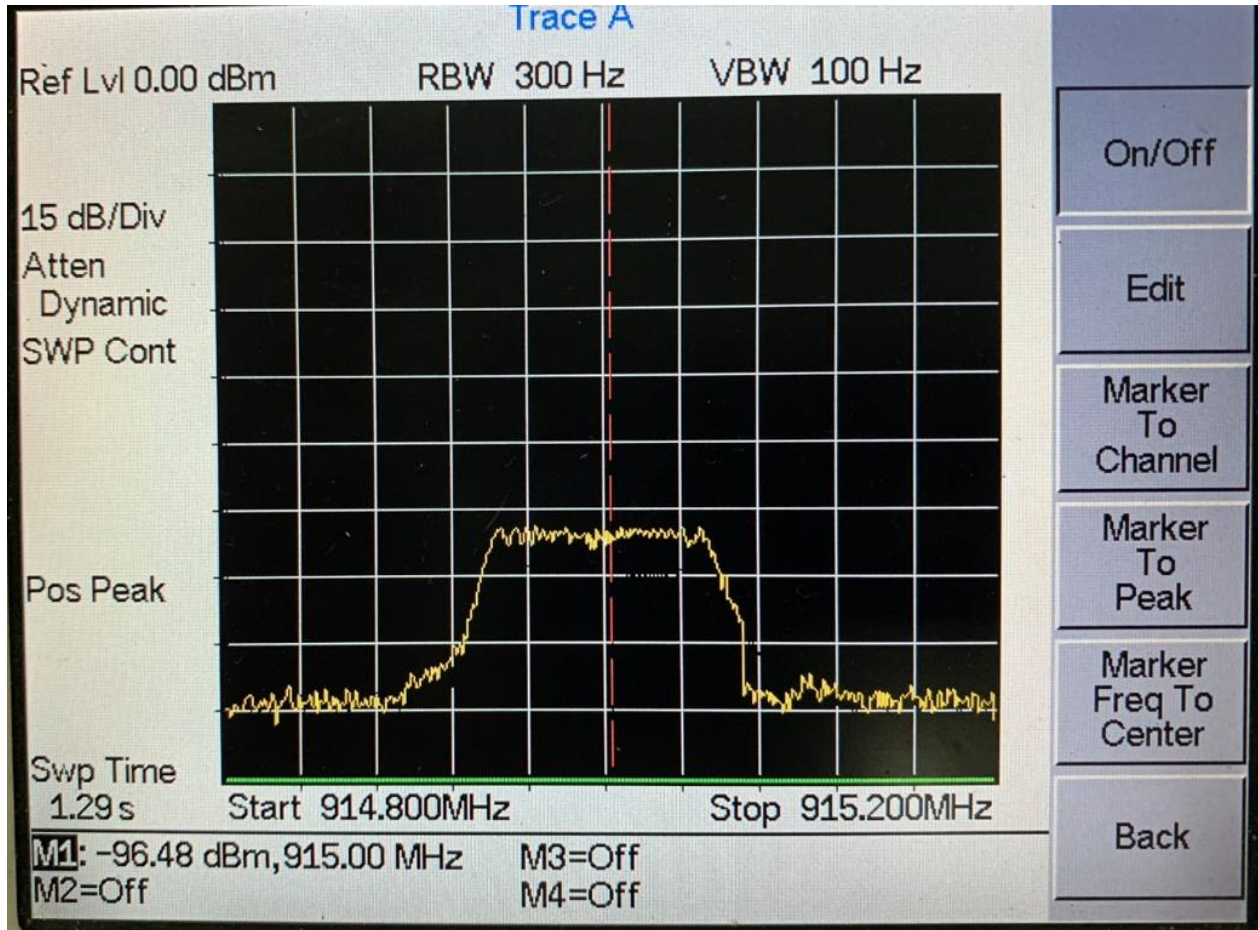


Figura 7-13: Anritsu, Espectro LoRa 915 MHz

Como se mencionó en la Fase 1, tenemos los módulos Heltec transmitiendo y recibiendo, teniendo como variable de captura un sensor de temperatura el cual nos muestra el resultado en grados centígrados, como se muestra en la figura 7-14 y 7-15.

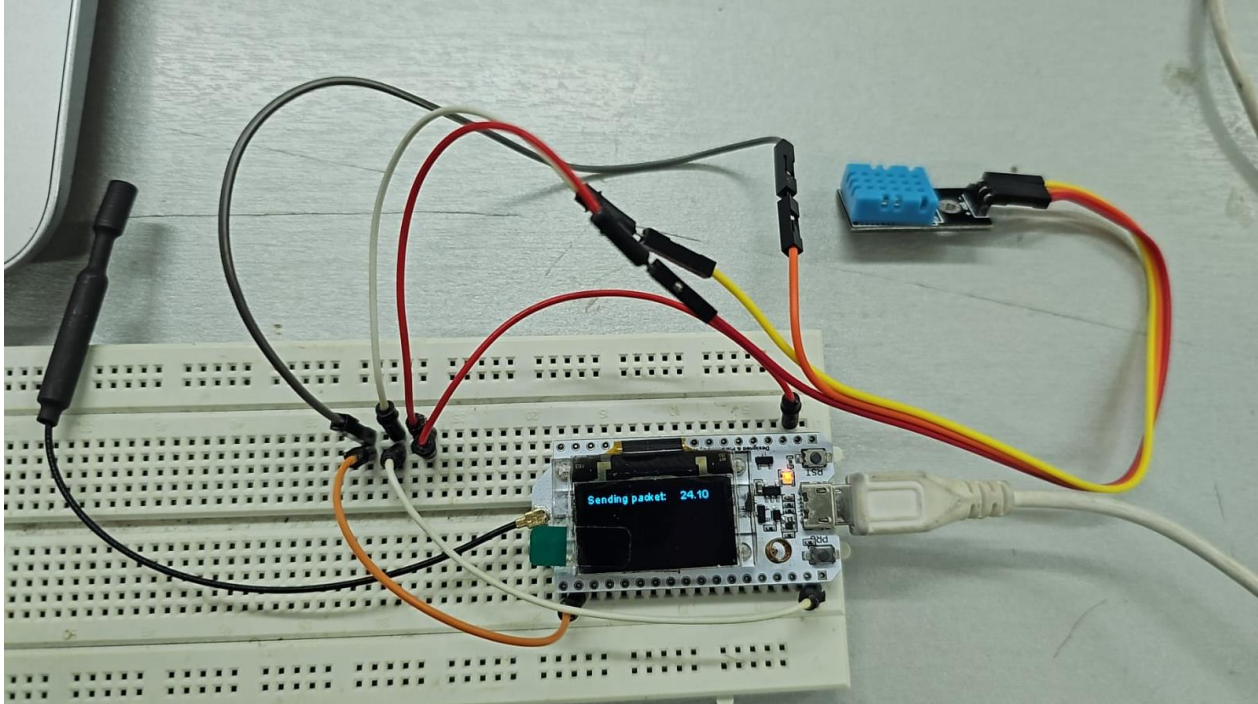


Figura 7-14: Modulo transmisor, sensor de temperatura

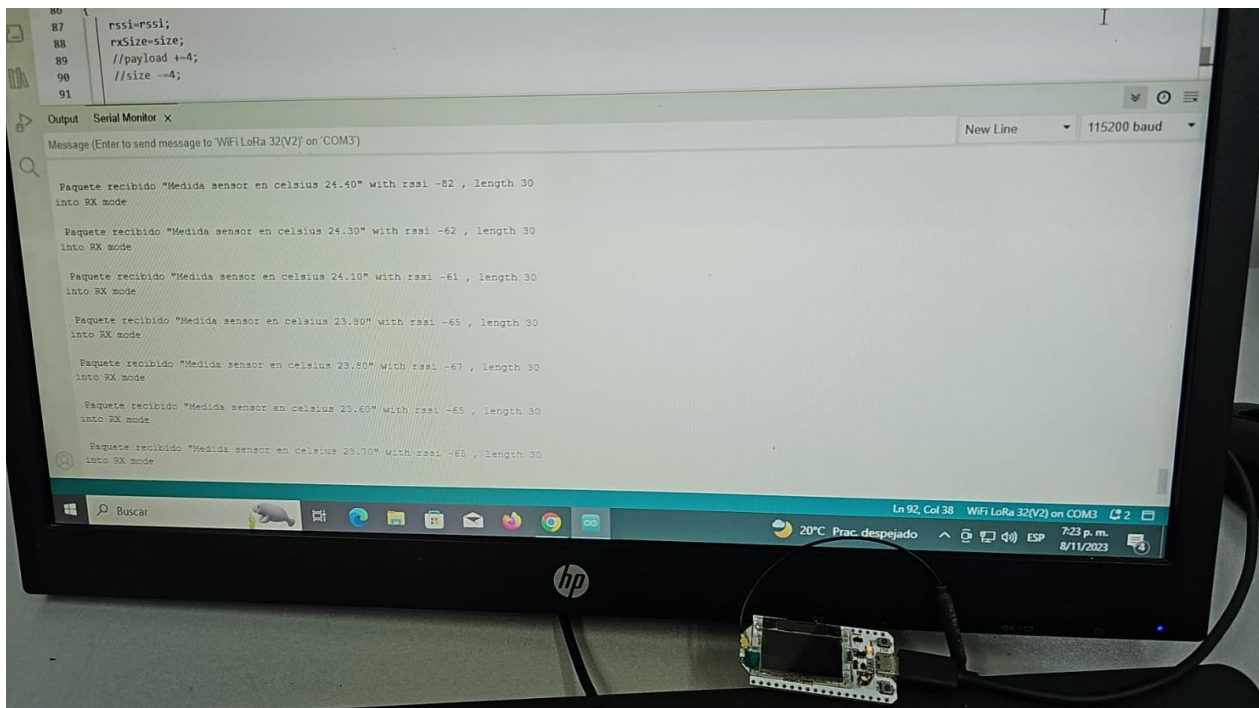


Figura 7-15: Modulo receptor, medidas de temperatura

Ahora con el módulo CatWAN stick buscamos hacer jamming transmitiendo una señal bajo la misma portadora de comunicación LoRa y variando el spreading factor. Como se ha mencionado el spreading factor, se podría traducir como factor de esparcimiento, para entenderlo podemos imaginar que estás en un bar y queremos hablar con un acompañante pero no nos oye por el ruido de la música y las demás personas en el sitio, aunque gritemos todo lo que podamos (potencia de transmisión), la solución para que nos escuche es hablar mucho más despacio, esto es lo que define este factor, cuanto nos “esparcimos” en el tiempo, los SF inician en 7, mínimo esparcimiento (mayor velocidad de transmisión, más expuesto a interferencias), al 12, máximo esparcimiento (menor velocidad de transmisión, menos expuesto a interferencias). Se realizaron tres pruebas con diferentes SF, utilizando el 7, 9 y 12.

7.2.1.1 Pruebas spreading factor (SF) 7:

Como lo hemos venido mencionado, tenemos dos módulos LoRa comunicándose de forma unidireccional transmitiendo datos de temperatura, un tercer equipo generando interferencia y un analizador de espectros para intentar observar los cambios de señal, en la figura 7-16 vemos el analizador de espectros capturando la señal LoRa.

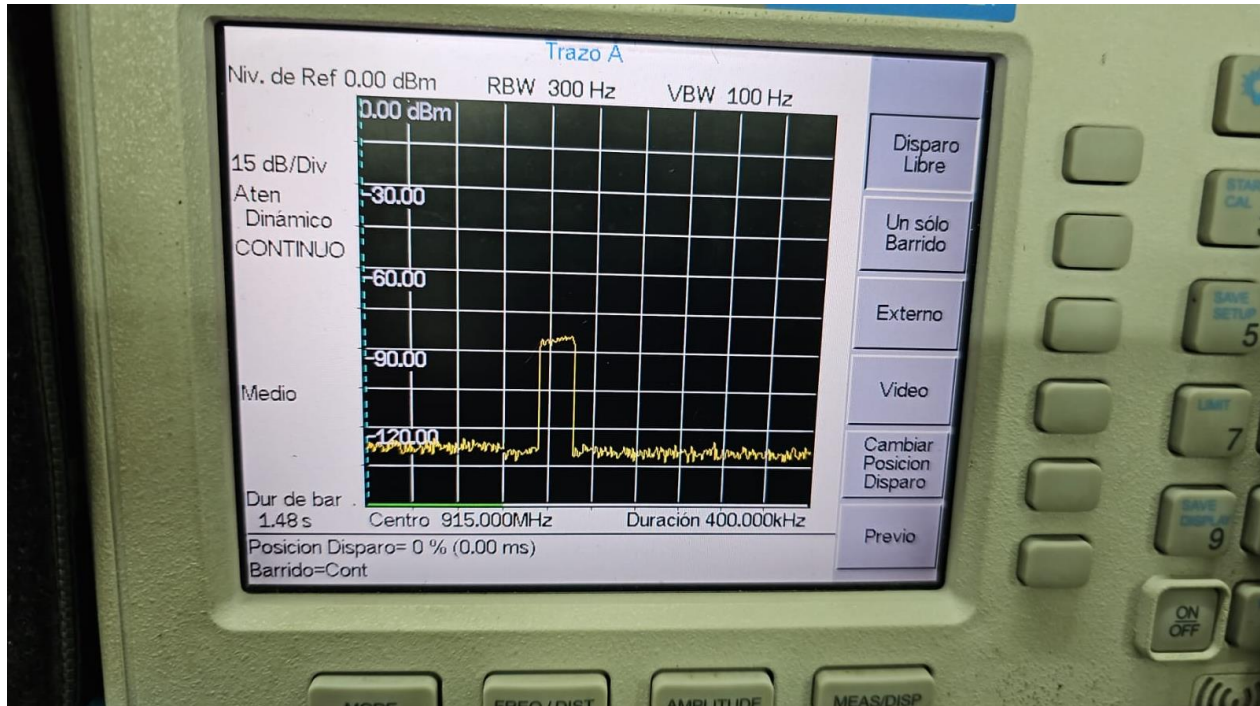


Figura 7-16: Espectro LoRa

Encendemos la interferencia y como lo observamos en las figuras 7-17, 7-18 y 7-19, se muestra un cambio en el espectro de la señal.

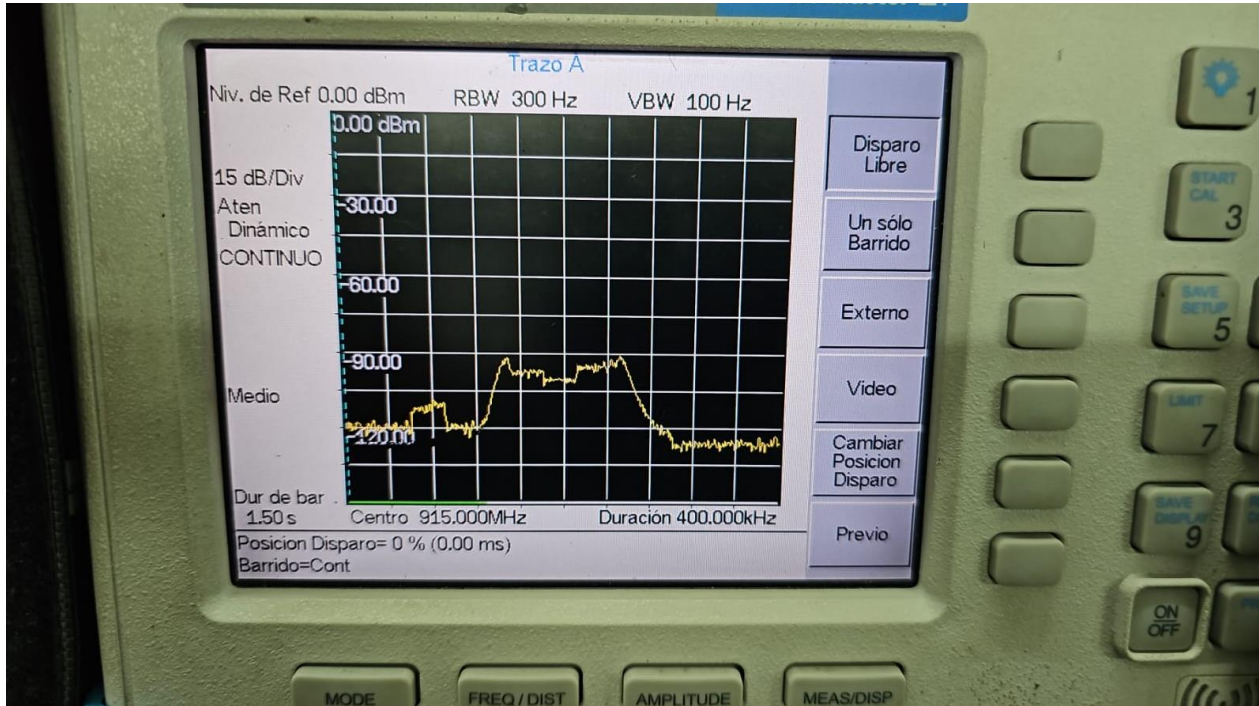


Figura 7-17: Espectro LoRa, cambios en inicio de portadora

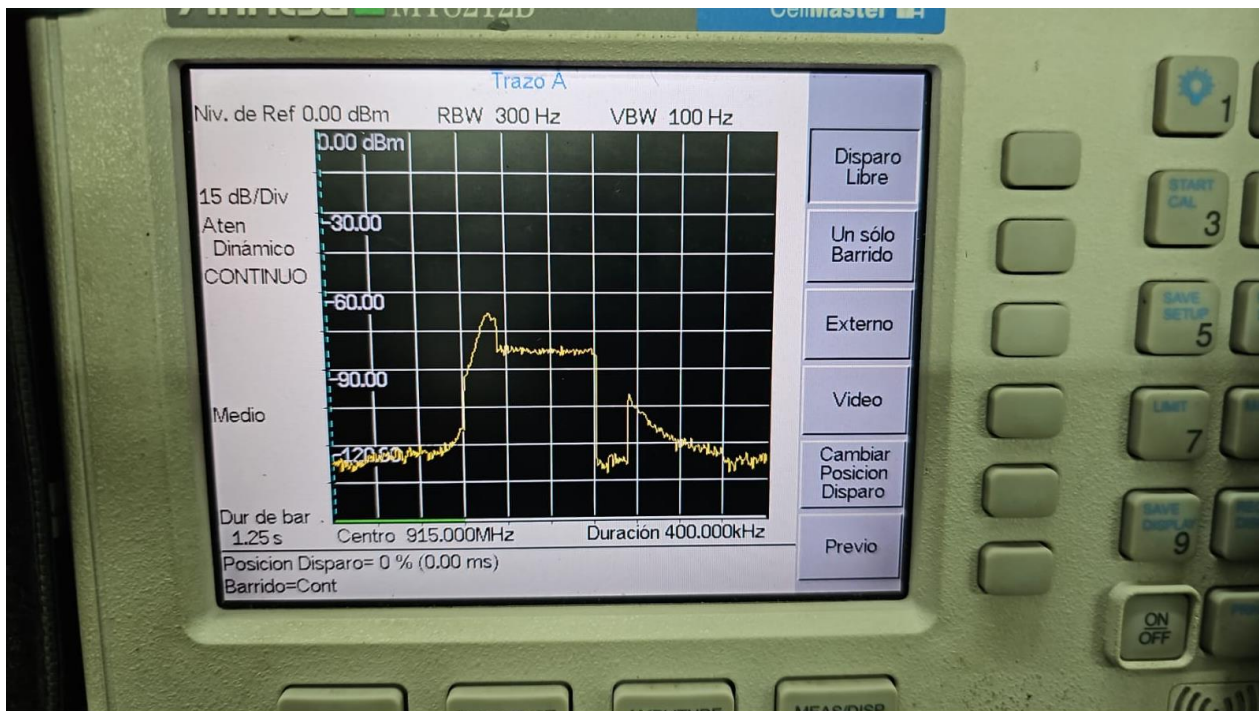


Figura 7-18: Espectro LoRa, cambios en medio de portadora

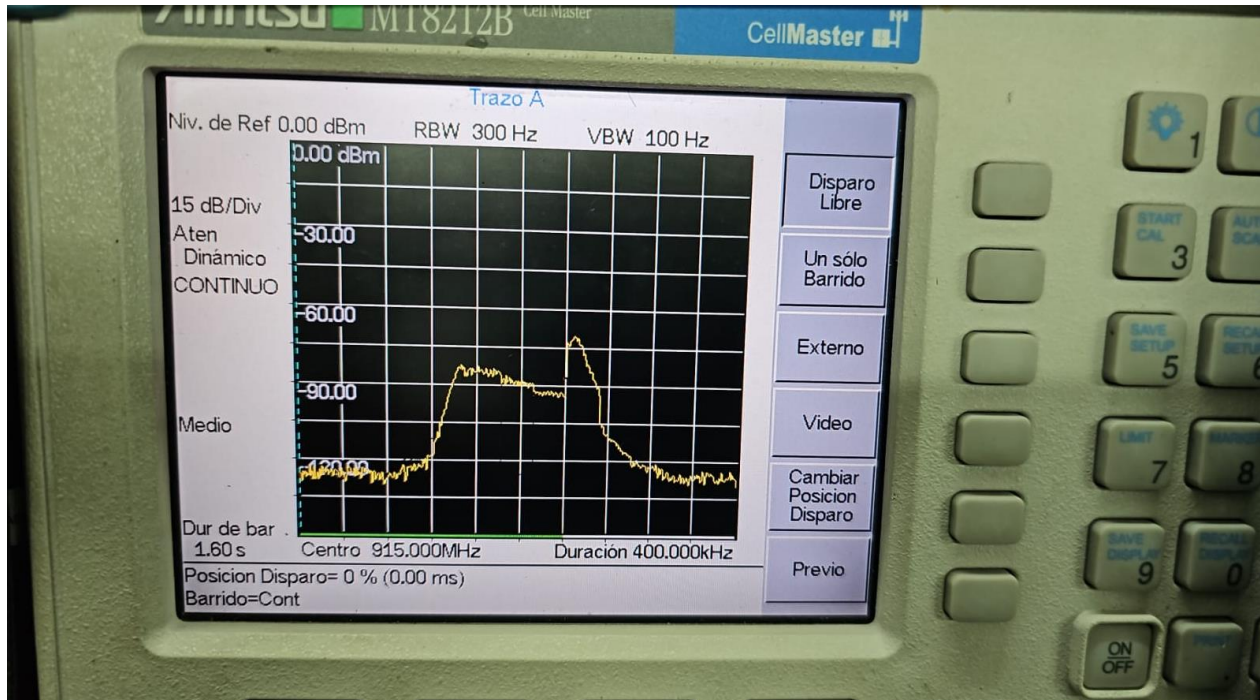


Figura 7-19: Espectro LoRa, cambios en final de portadora

El resultado de la inyección de interferencia es la pérdida total de la comunicación entre los dispositivos LoRa las figuras 7-20, 7-21 y 7-22 muestran desde que se transmite la información hasta la recepción de la misma y la no posibilidad decodificación del mensaje.

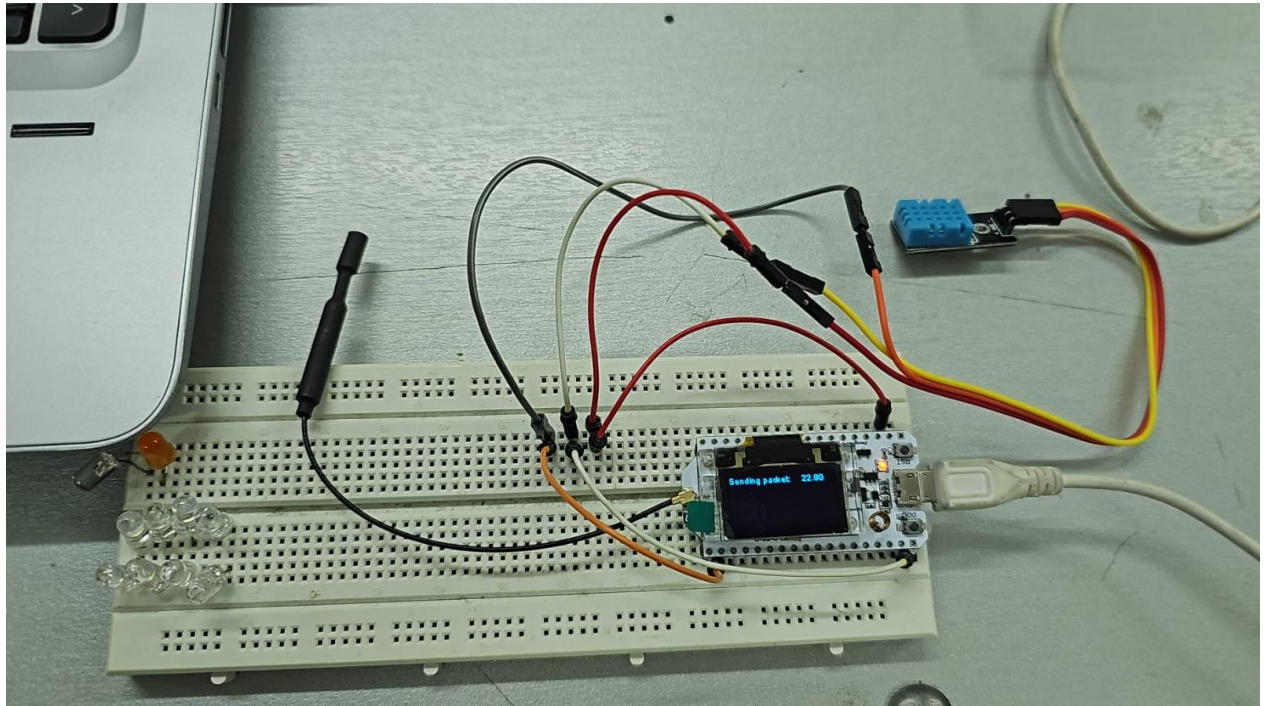


Figura 7-20: Transmision LoRa, temperatura



Figura 7-21: Modulo CatWAN, inyección interferencia

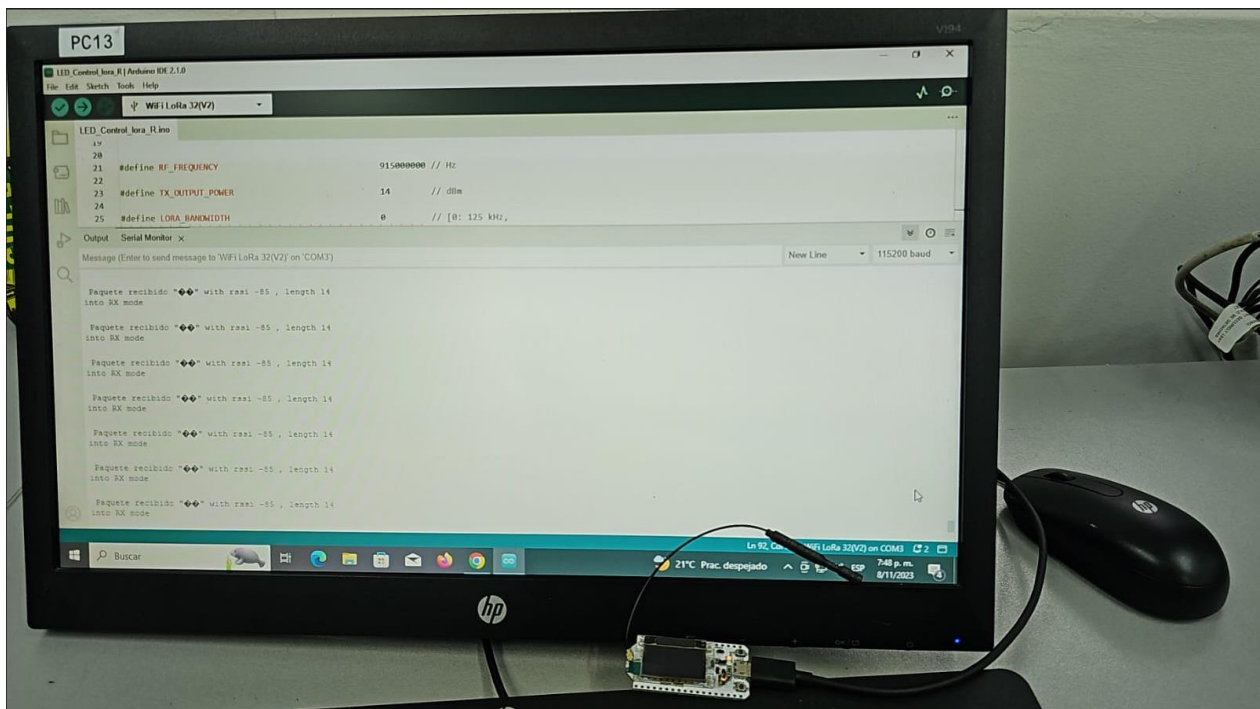
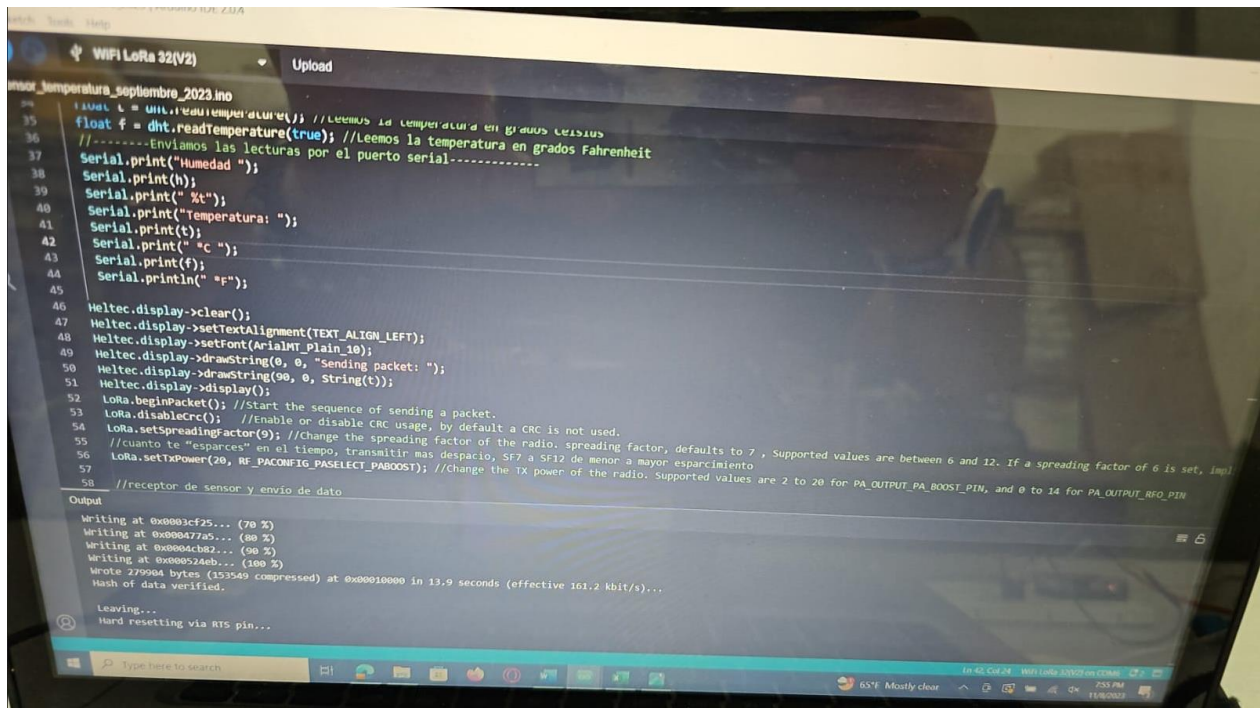


Figura 7-22: Modulo LoRa receptor, mensaje interferido

7.2.1.2 Pruebas spreading factor (SF) 9:

Para intentar evitar el ataque de jamming vamos a empezar a aumentar el spreading factor (hablar más despacio), por tanto, la siguiente prueba se realizará con un factor de 9, tenemos el mismo laboratorio de pruebas, en el emisor LoRa cambiamos la configuración, como se muestra en la figura 7-23.



```
34 float t = util.readTemperature(); //Leemos la temperatura en grados Celsius
35 float f = dht.readTemperature(true); //Leemos la temperatura en grados Fahrenheit
36 //-----Enviamos las lecturas por el puerto serial-----
37 Serial.print("Humedad ");
38 Serial.print(h);
39 Serial.print(" %t");
40 Serial.print("Temperatura: ");
41 Serial.print(t);
42 Serial.print(" °C ");
43 Serial.print(f);
44 Serial.println(" °F");
45
46 Heltec.display->clear();
47 Heltec.display->setTextAlignment(TEXT_ALIGN_LEFT);
48 Heltec.display->setFont(ArialMT_Plain_10);
49 Heltec.display->drawString(0, 0, "Sending packet: ");
50 Heltec.display->drawString(90, 0, String(t));
51 Heltec.display->display();
52 LoRa.beginPacket(); //Start the sequence of sending a packet.
53 LoRa.disableCrc(); //Enable or disable CRC usage, by default a CRC is not used.
54 LoRa.setSpreadingFactor(9); //Change the spreading factor of the radio. spreading factor, defaults to 7, Supported values are between 6 and 12. If a spreading factor of 6 is set, Imp
55 //cuanto te "esparces" en el tiempo, transmitir más despacio, SF7 a SF12 de menor a mayor esparcimiento
56 LoRa.setTxPower(20, RF_PA_CONFIG_PASELECT_PABOOST); //Change the TX power of the radio. Supported values are 2 to 20 for PA_OUTPUT_PA_BOOST_PIN, and 0 to 14 for PA_OUTPUT_RFO_PIN
57 //receptor de sensor y envío de dato
58
Output
Writing at 0x0000cf25... (70 %)
Writing at 0x00004725... (80 %)
Writing at 0x00004c82... (90 %)
Writing at 0x0000524b... (100 %)
Wrote 279904 bytes (153549 compressed) at 0x00010000 in 13.9 seconds (effective 161.2 kbit/s)...
Hash of data verified.
Leaving...
Hard resetting via RTS pin...
```

Figura 7-23: Código Modulo LoRa transmisor (SF 9)

Iniciamos con una captura de la portadora con el analizador de espectros, como se identifica en la figura 7-24.

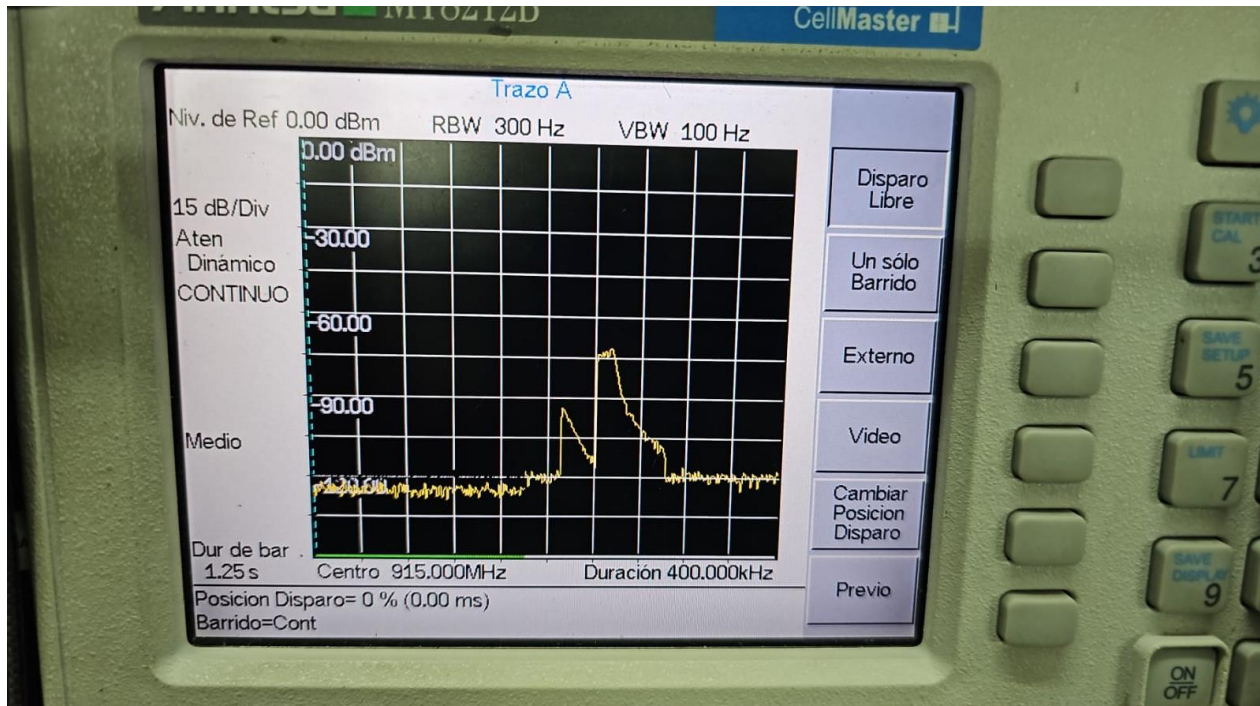


Figura 7-24: Portadora Lora SF 9

Encendemos el módulo CatWAN iniciamos la interferencia o jamming y como se muestra en las figuras 7-25, 7-26 y 7-27, hay una deformación de la señal.

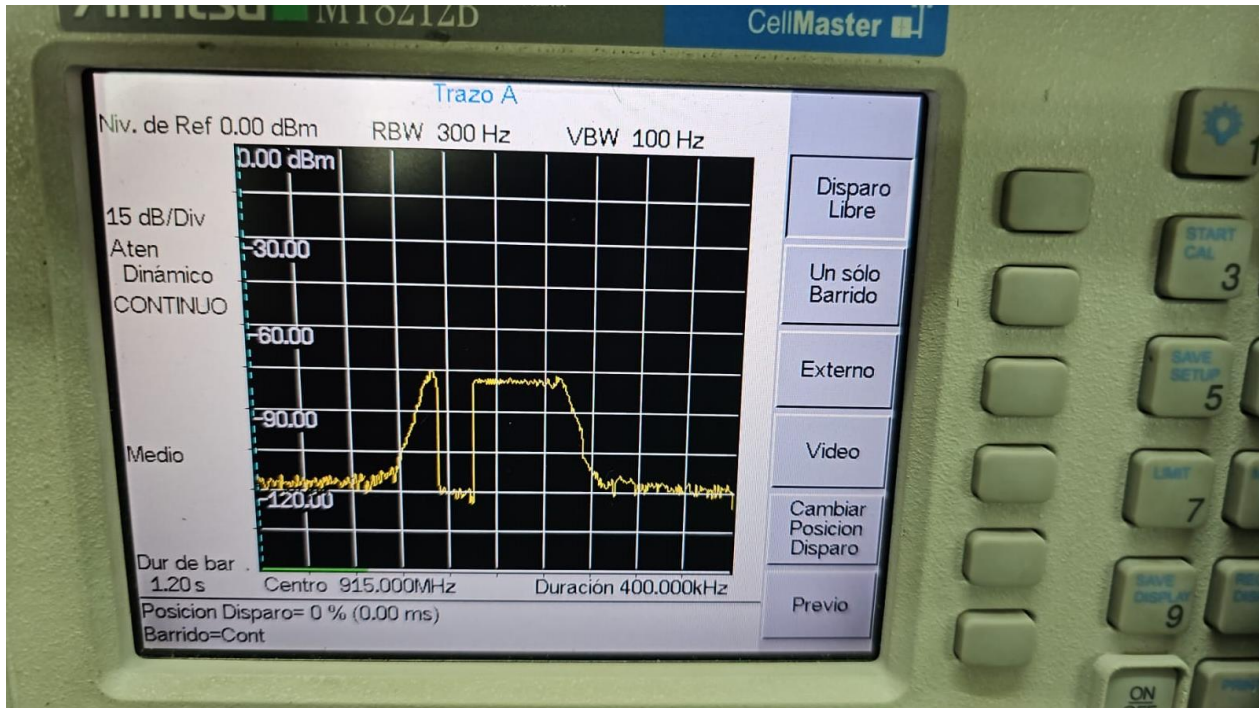


Figura 7-25: Espectro LoRa (SF9), cambios en inicial de portadora

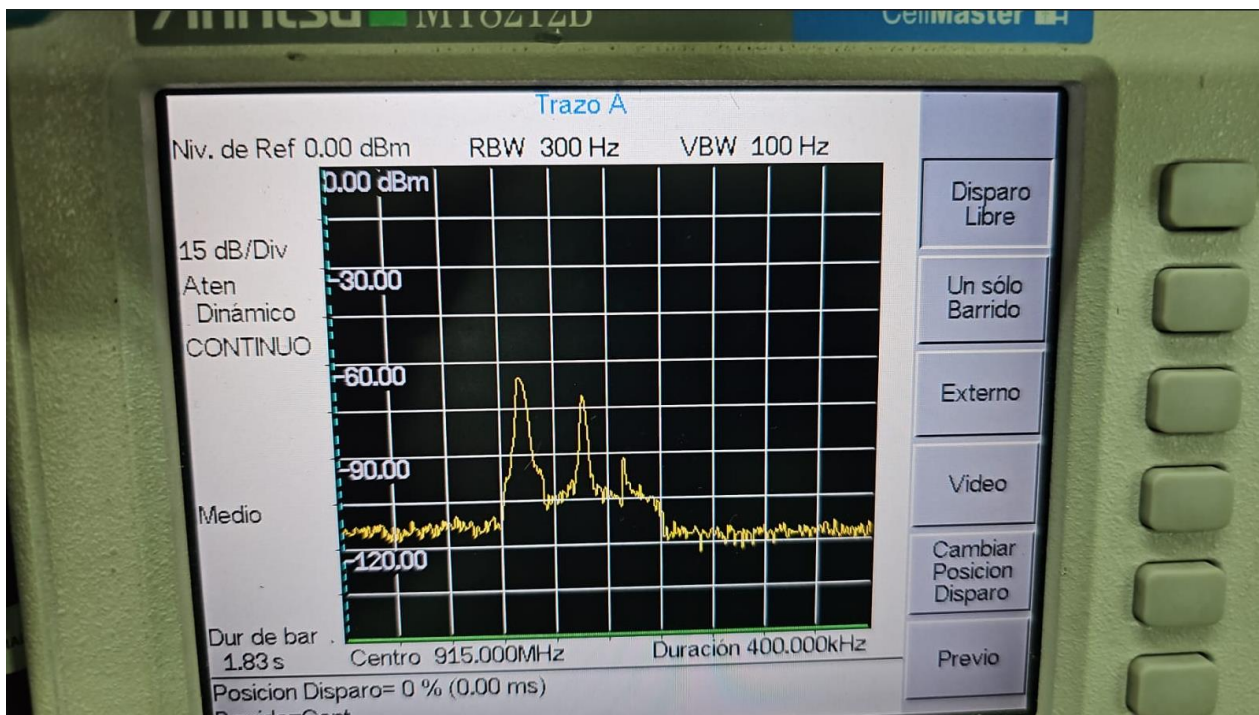


Figura 7-26: Espectro LoRa (SF9), cambios en medio de portadora

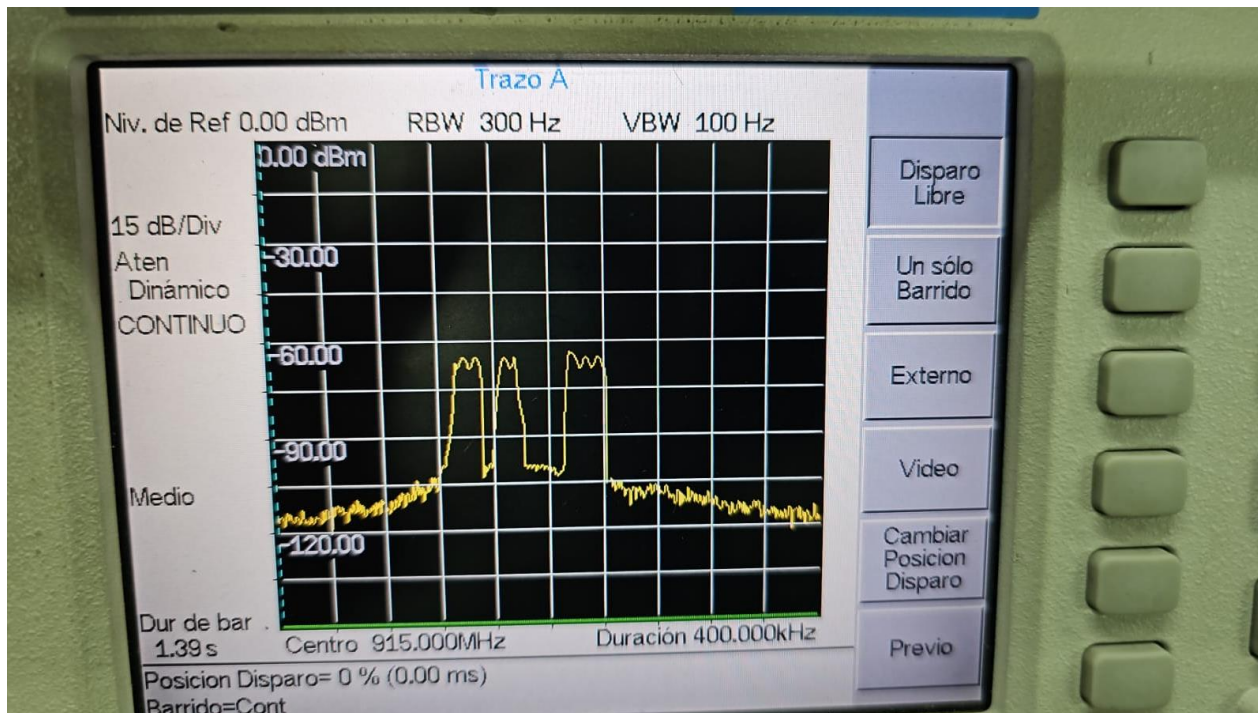


Figura 7-27: Espectro LoRa (SF9), cambios en final de portadora

Revisamos el mensaje decodificado en el módulo receptor LoRa, nuevamente observamos que el mensaje fue totalmente interferido evitando que los datos de temperatura enviados desde el transmisor LoRa sean identificados correctamente y no logremos observar el dato correcto, como se muestra en la figura 7-28.

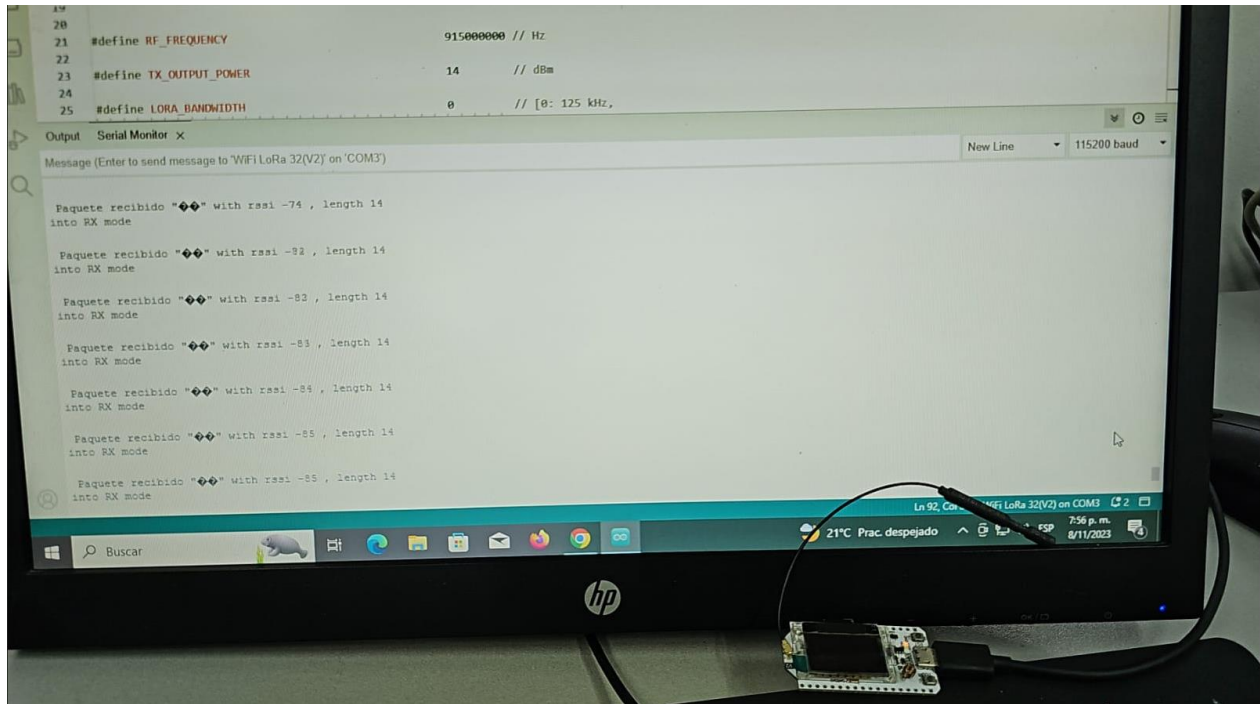


Figura 7-28: Modulo LoRa receptor, mensaje interferido (SF9)

7.2.1.3 Pruebas spreading factor (SF) 12:

Nuevamente para intentar evitar el ataque de jamming vamos a empezar a aumentar el spreading factor (hablar aún más despacio), por tanto, la siguiente prueba se realizará con un factor de 12, pero también aumentaremos el ancho de banda en espectro de la señal, utilizando 500 KHz, teniendo el mismo laboratorio de pruebas, en el emisor LoRa y en el receptor cambiamos la configuración, como se muestra en las figuras 7-29 y 7-30.

```

44 temperatura_2023.ino
45 Serial.println(" *F*");
46 Heltec.display->clear();
47 Heltec.display->setTextAlignment(TEXT_ALIGN_LEFT);
48 Heltec.display->setFont(ArialMT_Plain_10);
49 Heltec.display->drawString(0, 0, "Sending packet: ");
50 Heltec.display->drawString(90, 0, String(t));
51 Heltec.display->display();
52 LoRa.beginPacket(); //start the sequence of sending a packet.
53 LoRa.disableCrc(); //Enable or disable CRC usage, by default a CRC is not used.
54 LoRa.setSpreadingFactor(12); //Change the spreading factor of the radio. spreading factor, defaults to 7 , Supported values are between 6 and 12. If a spreading factor
55 //cuanto te "esparces" en el tiempo, transmitir mas despacio, SF7 a SF12 de menor a mayor esparcimiento
56 LoRa.setSignalBandwidth(500E3);
57 LoRa.setTxPower(20, RF_PACONFIG_PASELECT_PABOOST); //Change the TX power of the radio. Supported values are 2 to 20 for PA_OUTPUT_PA_BOOST_PIN, and 0 to 14 for PA_OUTPUT_
58 //receptor de sensor y envio de dato
59 LoRa.print("Medida sensor en celsius "+String(t));
60 LoRa.endPacket(); //End the sequence of sending a packet
61
62 digitalWrite(LED, HIGH);
63 delay(1000);
64 digitalWrite(LED, LOW);
65 delay(1000);
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
```

Iniciamos con una captura de la portadora con el analizador de espectros, como se identifica en la figura 7-31.

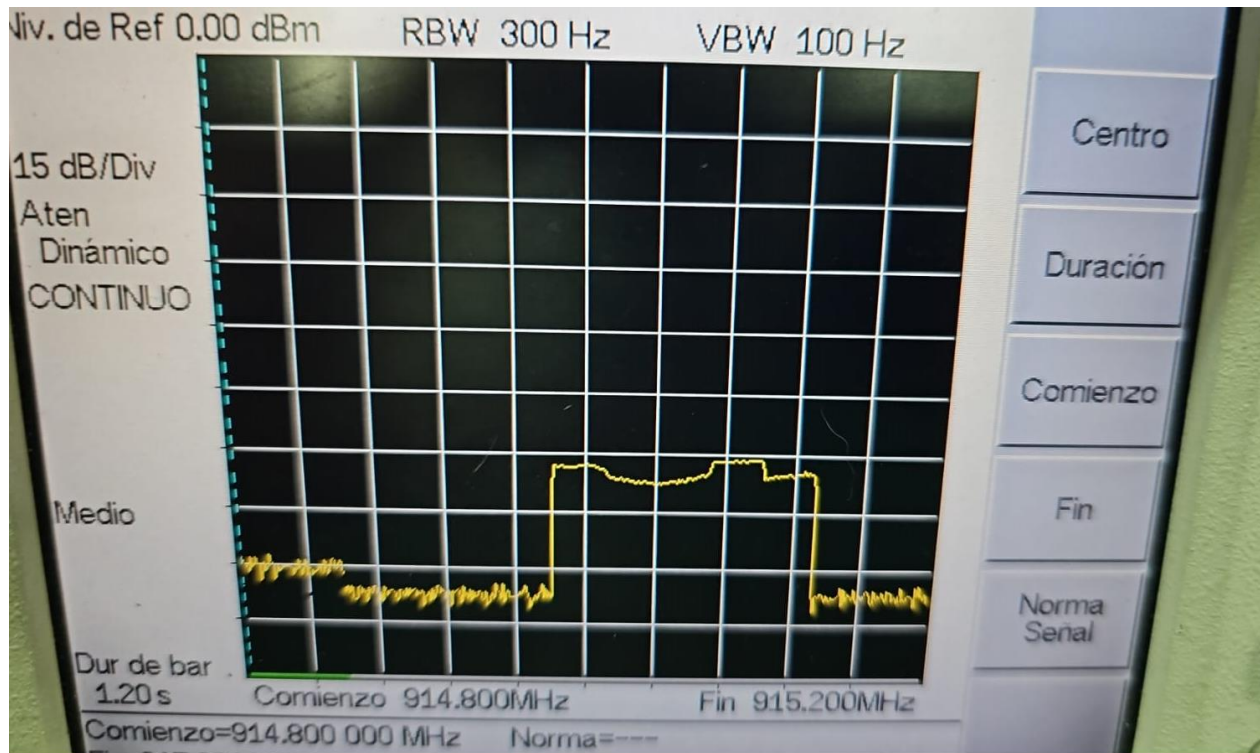


Figura 7-31: Portadora Lora SF 12 – BW 500 KHz

Encendemos el módulo CatWAN iniciamos la interferencia o jamming y como se muestra en las figuras 7-32 y 7-33, hay una deformación de la señal.

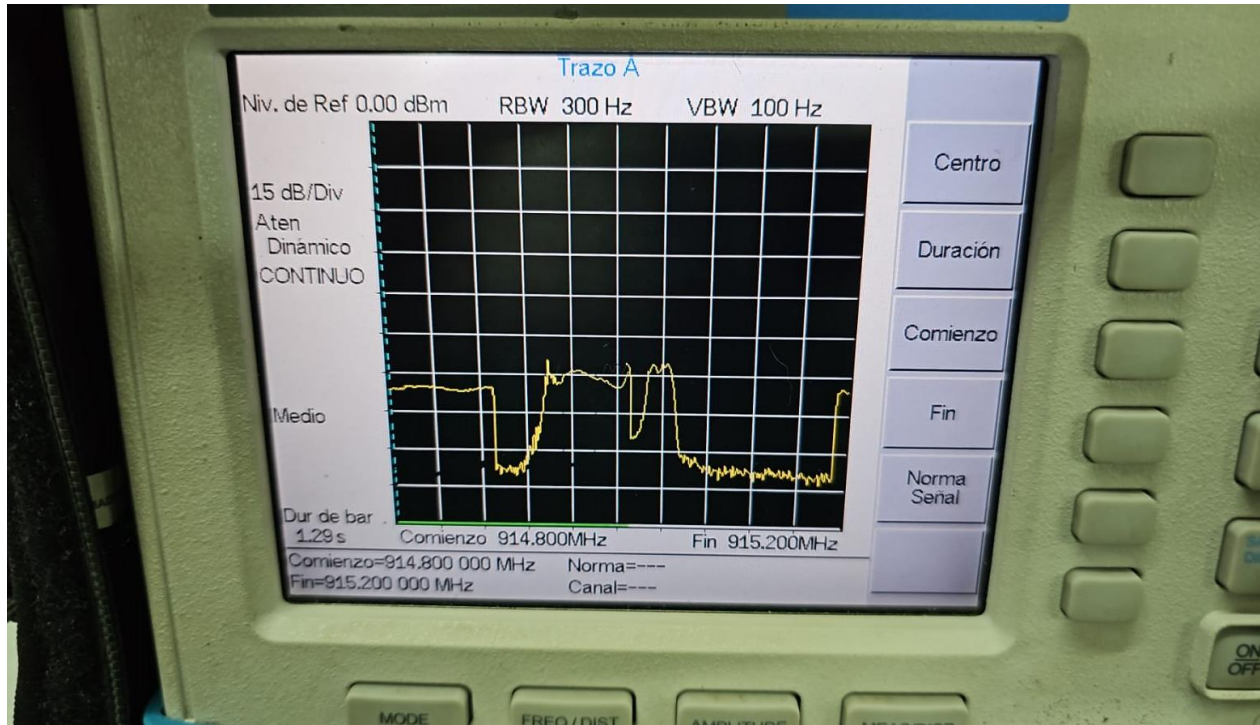


Figura 7-32: Espectro LoRa (SF12), cambios en medio de portadora

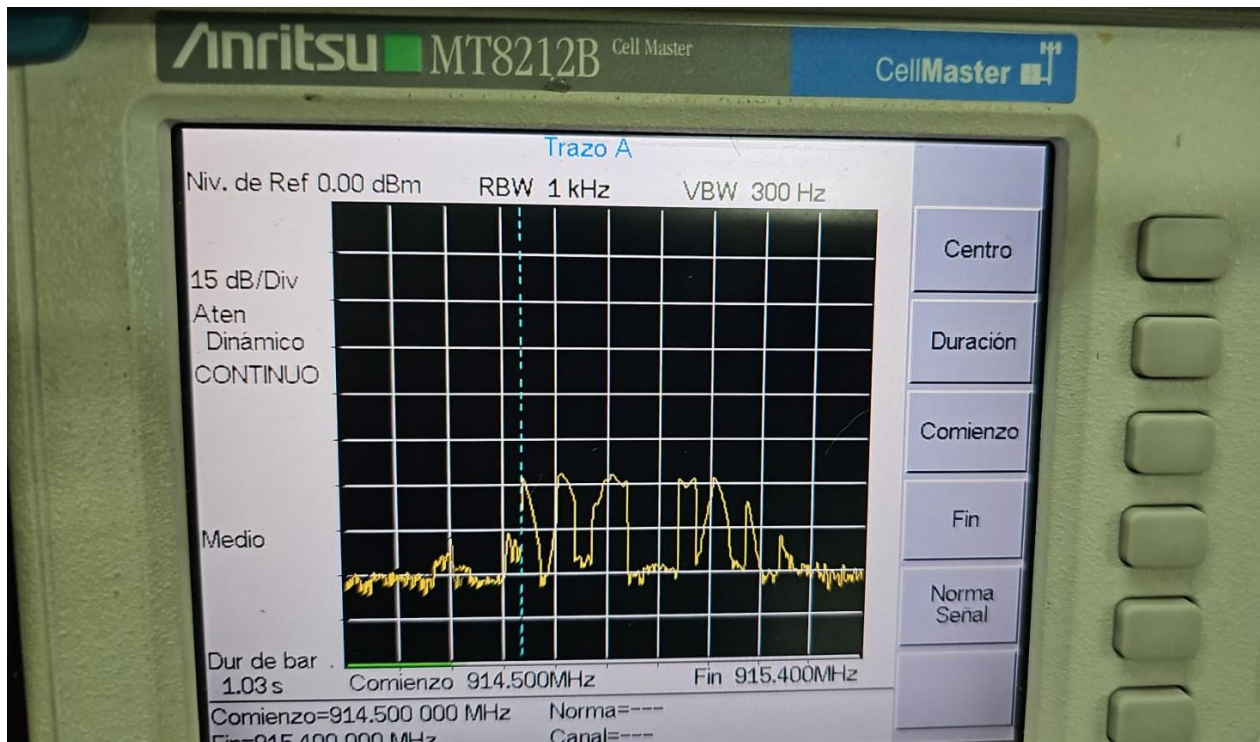
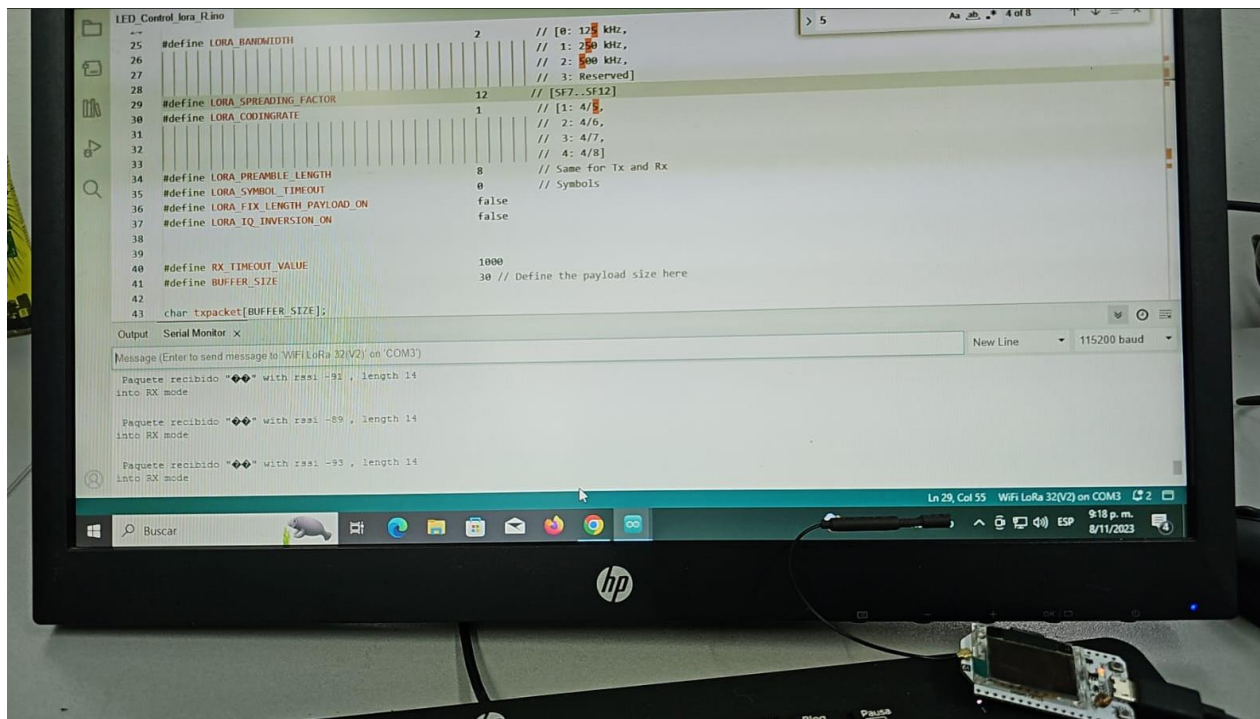


Figura 7-33: Espectro LoRa (SF12), cambios en espectro de portadora

Revisamos el mensaje decodificado en el módulo receptor LoRa, nuevamente observamos que el mensaje fue totalmente interferido evitando que los datos de temperatura enviados desde el transmisor LoRa sean identificados correctamente y no logremos observar el dato correcto, como se muestra en la figura 7-34.



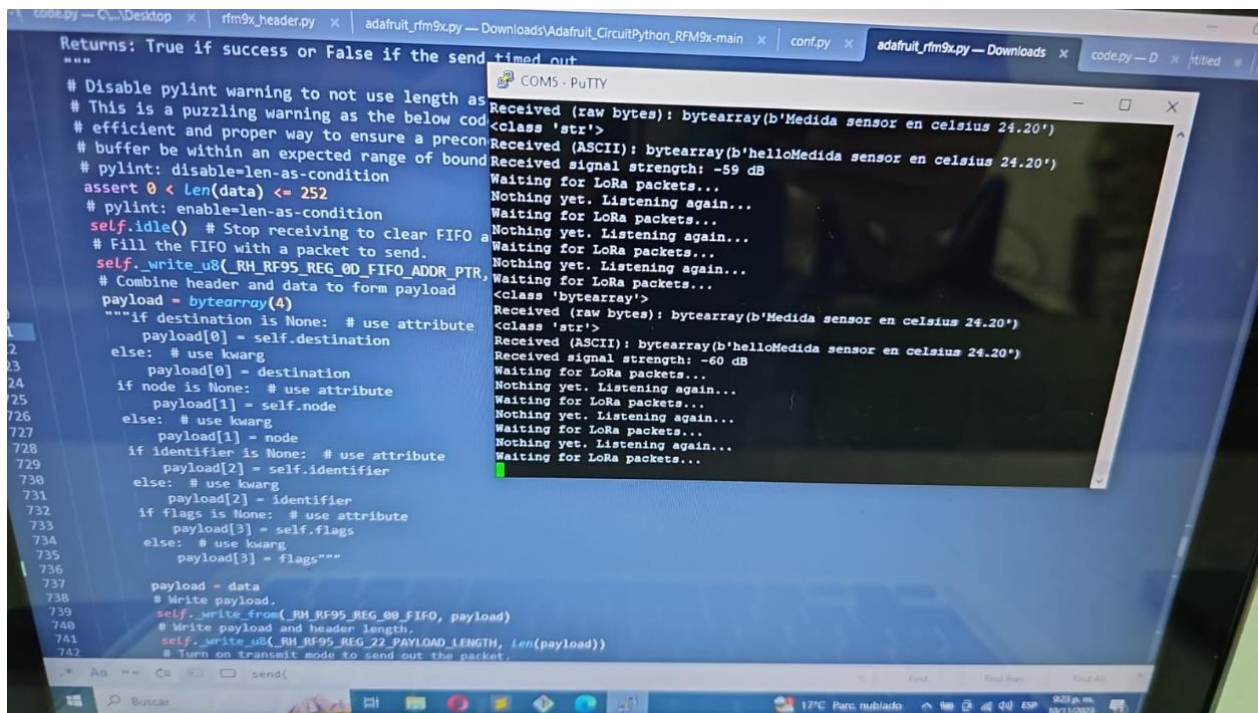
```
LED_Control_LoRa_Rx.ino
25 #define LORA_BANDWIDTH 2 // [0: 125 kHz,
26 // 1: 250 kHz,
27 // 2: 500 kHz,
28 // 3: Reserved]
29 #define LORA_SPREADING_FACTOR 12 // [SF7..SF12]
30 #define LORA_CODINGRATE 1 // [1: 4/5,
31 // 2: 4/6,
32 // 3: 4/7,
33 // 4: 4/8]
34 #define LORA_PREAMBLE_LENGTH 8 // Same for Tx and Rx
35 #define LORA_SYMBOL_TIMEOUT 0 // Symbols
36 #define LORA_FIX_LENGTH_PAYLOAD_ON false
37 #define LORA_TQ_INVERSION_ON false
38
39
40 #define RX_TIMEOUT_VALUE 1000
41 #define BUFFER_SIZE 30 // Define the payload size here
42
43 char txpacket[BUFFER_SIZE];
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
262
```

7.2.2 Spoofing o suplantación

El segundo ataque es el de spoofing o suplantación, este tipo de ataque, un dispositivo LoRa malintencionado puede hacerse pasar por un nodo legítimo de la red y enviar datos falsos o maliciosos.

Para este laboratorio vamos a utilizar el módulo CatWAN el cual trabajara como un sniffer que suplantara un nodo real LoRa

En la imagen 7-35 vemos el código que utilizamos para este laboratorio, como también el envío de información LoRa para que pueda ser recibida por un nodo LoRa receptor.



```

Returns: True if success or False if the send timed out
"""
# Disable pylint warning to not use length as
# This is a puzzling warning as the below code
# efficient and proper way to ensure a precond
# buffer be within an expected range of bound
# pylint: disable=len-as-condition
assert 0 < len(data) <= 252
# pylint: enable=len-as-condition
self.idle() # Stop receiving to clear FIFO a
# Fill the FIFO with a packet to send.
self._write_u8(_RH_RF95_REG_0D_FIFO_ADDR_PTR,
# Combine header and data to form payload
payload = bytearray(4)
"""if destination is None: # use attribute
    payload[0] = self.destination
else: # use kwargs
    payload[0] = destination
if node is None: # use attribute
    payload[1] = self.node
else: # use kwargs
    payload[1] = node
if identifier is None: # use attribute
    payload[2] = self.identifier
else: # use kwargs
    payload[2] = identifier
if flags is None: # use attribute
    payload[3] = self.flags
else: # use kwargs
    payload[3] = flags"""
payload = data
# Write payload.
self._write_from(_RH_RF95_REG_00_FIFO, payload)
# Write payload and header length.
self._write_u8(_RH_RF95_REG_72_PAYLOAD_LENGTH, len(payload))
# Turn on transmit mode to send out the packet.
send()

```

```

COM5 - PuTTY
Received (raw bytes): bytearray(b'Medida sensor en celsius 24.20')
<class 'str'>
Received (ASCII): bytearray(b'helloMedida sensor en celsius 24.20')
Received signal strength: -59 dB
Waiting for LoRa packets...
Nothing yet. Listening again...
Waiting for LoRa packets...
Nothing yet. Listening again...
Waiting for LoRa packets...
Nothing yet. Listening again...
Waiting for LoRa packets...
<class 'bytearray'>
Received (raw bytes): bytearray(b'Medida sensor en celsius 24.20')
<class 'str'>
Received (ASCII): bytearray(b'helloMedida sensor en celsius 24.20')
Received signal strength: -60 dB
Waiting for LoRa packets...
Nothing yet. Listening again...
Waiting for LoRa packets...
Nothing yet. Listening again...
Waiting for LoRa packets...
Nothing yet. Listening again...
Waiting for LoRa packets...

```

Figura 7-35: Modulo CatWAN spoofing

En el módulo receptor LoRa podemos observar este mismo mensaje con datos falsos de temperatura ya que no se tiene ningún sensor de temperatura conectado en el equipo CatWAN, en la imagen 7-36 vemos el mensaje.

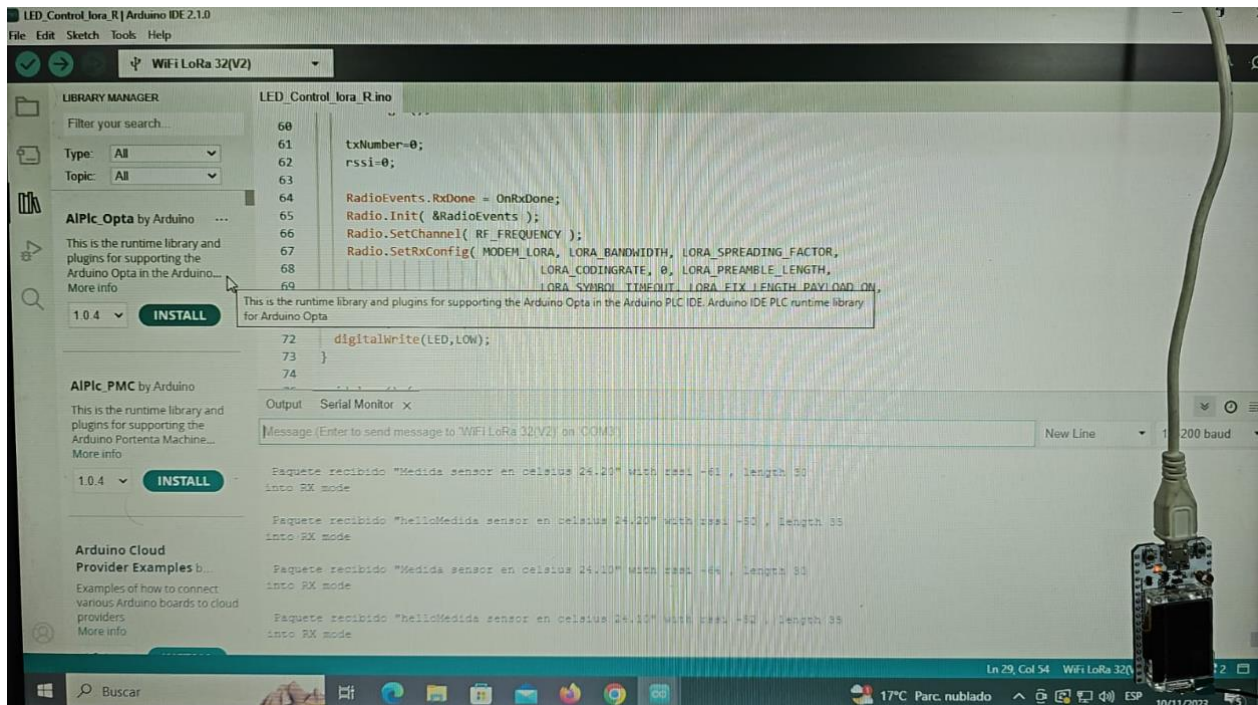


Figura 7-36: Modulo receptor LoRa

Siendo un poco mas precisos con el código,

```

import board
import busio
import digitalio
import adafruit_rfm9x

from array import array

RADIO_FREQ_MHZ = 915.0
CS = digitalio.DigitalInOut(board.RFM9X_CS)
RESET = digitalio.DigitalInOut(board.RFM9X_RST)
spi = busio.SPI(board.SCK, MOSI=board.MOSI, MISO=board.MISO)

```

```

rfm9x = adafruit_rfm9x.RFM9x(spi, CS, RESET, RADIO_FREQ_MHZ)
rfm9x.spreading_factor = 7
rfm9x.signal_bandwidth = 500000

while True:
    #prueba 2
    recieved_msg = ""
    print('Waiting for LoRa packets...')
    i = 0
    packet = rfm9x.receive(timeout=1.0, keep_listening=True, with_header=True)
    #rfm9x.spreading_factor =

    if packet is None:
        print('Nothing yet. Listening again...')
    else:
        #Recibió mensaje
        print(type(packet))
        print('Received (raw bytes): {0}'.format(packet))
        try:
            #Aquí se podrán guardar datos de recepción
            packet_text = str(packet, 'ascii')
            packet_text = "hello"+packet_text
            s = packet_text
            print(type(s))
            #encoded = s.encode('ascii')
            array = bytearray(s)

            rfm9x.send(array)
            print('Received (ASCII): {0}'.format(array))
        except UnicodeError:
            print('packet contains non-ASCII characters')
        rssi = rfm9x.rssi
        print('Received signal strength: {0} dB'.format(rssi))

```

Se modificó el método send de la librería rfm9x y el with_header=true, así:

```

def send(
    self,
    data: ReadableBuffer,
    *,
    keep_listening: bool = False,
    destination: Optional[int] = None,

```

```

node: Optional[int] = None,
identifier: Optional[int] = None,
flags: Optional[int] = None
) -> bool:
    """Send a string of data using the transmitter.
    You can only send 252 bytes at a time
    (limited by chip's FIFO size and appended headers).
    This appends a 4 byte header to be compatible with the RadioHead library.
    The header defaults to using the initialized attributes:
    (destination,node,identifier,flags)
    It may be temporarily overridden via the kwargs -
destination,node,identifier,flags.
    Values passed via kwargs do not alter the attribute settings.
    The keep_listening argument should be set to True if you want to start
listening
    automatically after the packet is sent. The default setting is False.

    Returns: True if success or False if the send timed out.
    """
    # Disable pylint warning to not use length as a check for zero.
    # This is a puzzling warning as the below code is clearly the most
    # efficient and proper way to ensure a precondition that the provided
    # buffer be within an expected range of bounds. Disable this check.
    # pylint: disable=len-as-condition
    assert 0 < len(data) <= 252
    # pylint: enable=len-as-condition
    self.idle() # Stop receiving to clear FIFO and keep it clear.
    # Fill the FIFO with a packet to send.
    self._write_u8(_RH_RF95_REG_0D_FIFO_ADDR_PTR, 0x00) # FIFO starts at 0.
    # Combine header and data to form payload

    payload = data
    # Write payload.
    self._write_from(_RH_RF95_REG_00_FIFO, payload)
    # Write payload and header length.
    self._write_u8(_RH_RF95_REG_22_PAYLOAD_LENGTH, len(payload))
    # Turn on transmit mode to send out the packet.
    self.transmit()
    # Wait for tx done interrupt with explicit polling (not ideal but
    # best that can be done right now without interrupts).
    timed_out = False
    if HAS_SUPERVISOR:

```

Se conserva el método payload para poder alterar el mensaje original

Para ello se debió precompilar el archivo `adafruit_rfm9x.py` para generar `adafruit_rfm9x.mpy` compatible con la versión de CircuitPython en el módulo CatWAN

```
daniel@DESKTOP-PNG1QVT MINGW64 ~/Downloads
$ ./mpy-cross.static-x64-windows-7.3.3.exe adafruit_rfm9x.py

daniel@DESKTOP-PNG1QVT MINGW64 ~/Downloads
$
```

7.2.3 Repetición

Como última prueba vamos a realizar el ataque de repetición, este tipo de ataque, un módulo malintencionado captura y retransmite paquetes de datos legítimos.

El laboratorio utiliza el módulo CatWAN como sniffer el cual captura la información del nodo transmisor LoRa y luego la retransmite agregándole información diferente para que el módulo receptor LoRa capture esta información, en la figura 7-37 vemos el código utilizado.

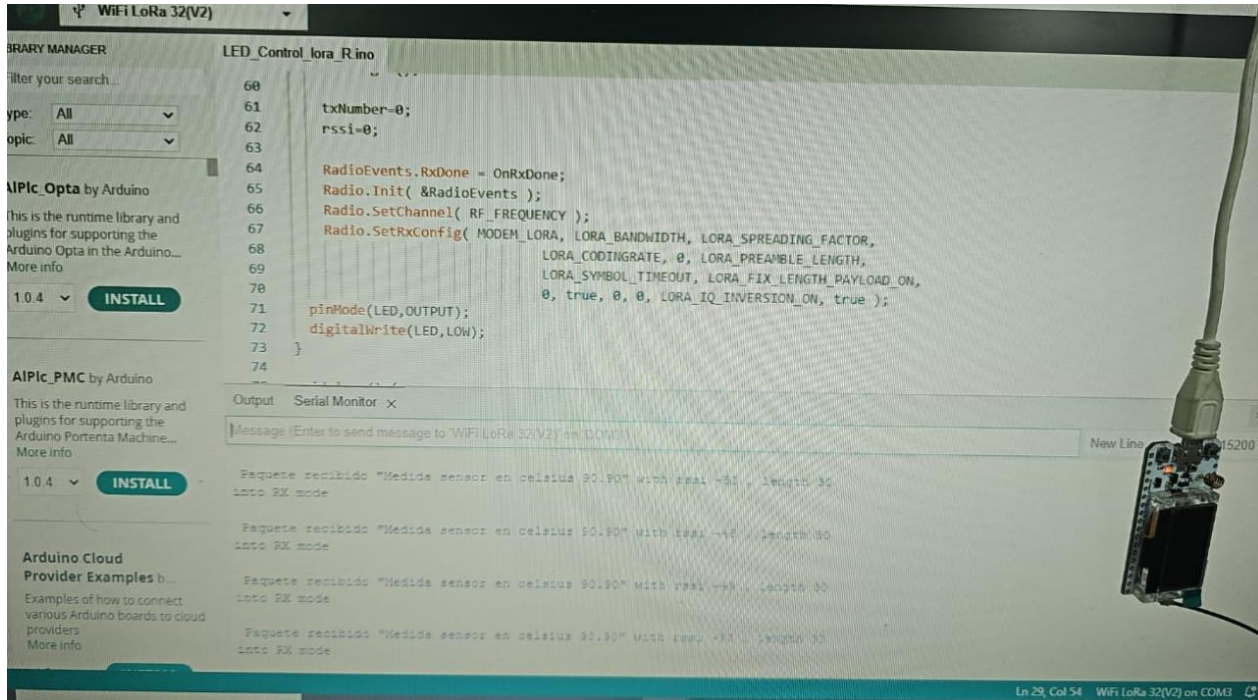


Figura 7-38: Modulo receptor LoRa Repetición

Finalmente, las redes LoRa también pueden ser susceptibles a ataques físicos. Dado que los nodos LoRa suelen estar ubicados en lugares remotos y accesibles, pueden ser objeto de vandalismo o robo. Además, un atacante podría intentar manipular físicamente los nodos para alterar su funcionamiento o extraer información sensible.

Para mitigar estas amenazas, es fundamental implementar medidas de seguridad adecuadas en las redes LoRa. Esto incluye el uso de técnicas criptográficas para garantizar la autenticidad e integridad de los datos transmitidos, así como mecanismos robustos para detectar y responder a posibles ataques. Además, es importante considerar la seguridad física de los nodos y utilizar técnicas como el blindaje o el alojamiento seguro para protegerlos contra ataques físicos.

En conclusión, aunque las redes LoRa ofrecen muchas ventajas para las aplicaciones IoT, también presentan una serie de amenazas que deben ser consideradas y gestionadas adecuadamente para garantizar una comunicación segura y confiable.

8. Conclusiones

Este estudio tuvo como objetivo establecer posibles factores que inciden en vulnerabilidades de seguridad en una comunicación LoRa en capa de transporte. Para alcanzarlo, se utilizaron dos dispositivos LoRa, uno de los cuales hacia funciones de emisión conectado a un sensor de temperatura y humedad, el segundo equipo hacia funciones de recepción para poder recibir los datos del sensor de temperatura y humedad, se incluyeron dos equipos adicionales los cuales fueron un módulo sniffer CatWAN el cual tiene la particularidad de poder monitorear el espectro LoRa, como también contener un chip LoRa para poder tener habilidades adicionales para capturar y transmitir mensajes de este tipo, el ultimo equipo es un analizador de espectros centrado principalmente en poder identificar el espectro radioeléctrico para así identificar la comunicación.

Una herramienta muy efectiva que se logro identificar a nivel comercial es la tarjeta CatWAN la cual fue determinante por su gran versatilidad, con la misma podíamos simular un nodo, como también un monitor de detección de señal en espectro y captura de tramas de información, esta tarjeta permitió ejecutar las pruebas de vulnerabilidades como fueron, jamming, spoofing y repetición.

El jamming, o bloqueo intencional de señales de comunicación, es un desafío crucial en entornos donde la seguridad de las comunicaciones es esencial. En el desarrollo del laboratorio se identifico que independientemente del spreading factor u el ancho de banda configurado en el establecimiento de la comunicación entre dispositivos LoRa se tuvo éxito en evitar la misma

afectando de forma crucial este tipo de solución., la interferencia permitía que el receptor no decodificara la información de forma correcta.

El jamming puede ser perpetrado por actores malintencionados con el fin de interrumpir la transmisión de datos, lo que podría tener consecuencias graves en aplicaciones críticas como sistemas de seguridad, redes de sensores y comunicaciones militares, es fundamental desarrollar y aplicar estrategias efectivas para prevenir y mitigar los efectos del jamming, dentro de ellas se pueden usar, diversificación de Frecuencias, al operar en múltiples frecuencias, los sistemas de comunicación pueden evitar ser completamente bloqueados por interferencias en una sola banda de frecuencia. Esta estrategia requiere el uso de técnicas de salto de frecuencia o frecuencias alternativas predefinidas, lo que dificulta considerablemente los intentos de jamming.

También se tiene la modulación espectral, al utilizar esquemas de modulación más complejos, como la modulación de espectro ensanchado (spread spectrum), las señales de comunicación se vuelven más difíciles de detectar y bloquear. Esto se debe a que la energía de la señal se distribuye en un ancho de banda mayor, lo que dificulta su interferencia efectiva.

La detección de Jamming, es fundamental para implementar contramedidas efectivas, el monitoreo continuo de la calidad de la señal, el análisis estadístico de patrones de interferencia y el uso de algoritmos de aprendizaje automático para identificar anomalías en el entorno de comunicación.

La incorporación redundancia y resiliencia, en los sistemas de comunicación, esto puede lograrse mediante la implementación de rutas de comunicación alternativas, el uso de técnicas de corrección de errores y la adopción de protocolos de comunicación que puedan adaptarse dinámicamente a las condiciones cambiantes del canal.

Las contramedidas adaptativas, pueden incluir la reconfiguración automática de parámetros de comunicación, el cambio de frecuencias o potencias de transmisión, o la alteración de patrones de modulación en respuesta a la interferencia detectada.

La colaboración entre nodos en una red de comunicación pueden cooperar para detectar y mitigar los efectos del jamming compartiendo información sobre la calidad de la señal, identificando nodos comprometidos y coordinando acciones para mantener la integridad de la red.

El spoofing, o suplantación de identidad, es una amenaza significativa en entornos de comunicación y redes, y su prevención requiere estrategias sólidas y multifacéticas. Dentro del desarrollo de pruebas utilizando el modulo CatWAN se identifico la suplantación del mismo dentro del sistema básico de comunicación LoRa, engañando el receptor permitiendo recibir datos de un tercer elemento, se presentan diversas estrategias para prevenir el spoofing:

La implementación de mecanismos de autenticación fuerte, como el uso de certificados digitales, tokens de seguridad o biometría, al verificar de manera más sólida la identidad de los usuarios o dispositivos que intentan acceder a la red. Estos métodos de autenticación pueden dificultar significativamente los intentos de suplantación de identidad.

La detección de patrones anómalos en el tráfico de la red, mediante el análisis de comportamientos y características inusuales, la implementación de sistemas de detección de intrusiones y análisis de comportamiento puede ayudar a identificar actividades sospechosas que podrían ser indicativas de spoofing.

La encriptación de comunicaciones, especialmente aquellas que involucran la transmisión de datos de identificación o credenciales de acceso, la utilización de protocolos de encriptación robustos

puede garantizar la confidencialidad y la integridad de la información transmitida, lo que dificulta la manipulación no autorizada de los datos.

El monitoreo activo y respuesta rápida de la red y la capacidad de respuesta rápida ante actividades sospechosas, la implementación de sistemas de monitoreo en tiempo real, junto con procedimientos de respuesta a incidentes bien definidos, puede ayudar a identificar y mitigar los intentos de suplantación de identidad antes de que causen un daño significativo.

En el ataque de repetición se identifico la captura de la información del sistema de comunicación LoRa, hay que tener muy presente que como fueron pruebas a nivel de capa física no se realizo cifrado de la información, por tanto desde el modulo CatWAN se lee la información del sistema de transmisión para luego retrasmitirla con la información deseada, este tipo de vulnerabilidad es muy sensible ya que se pierde confidencialidad e integridad.

9. Recomendaciones

Este estudio posee limitaciones que tienen que ser contempladas para la comprensión de los datos. En primer lugar, el estudio fue realizado con componentes comerciales y códigos comunes ejecutando un banco de laboratorio en el cual se tenían dos módulos LoRa, un sniffer, un analizador de espectros, un sensor de temperatura humedad y tres equipos de cómputo. En este sentido, los resultados tienen que generalizarse con cuidado a otras pruebas más direccionadas a equipos específicos con códigos más específicos, pues este estudio solo se realizó con estos equipos. En segundo lugar, los resultados no pueden abordarse desde una perspectiva de causalidad, a razón de que los datos del análisis son apartir de equipos funcionales en un entorno comercial o laboral.

Las vulnerabilidades identificadas en LoRa pueden clasificarse en dos categorías principales:

Vulnerabilidades físicas: Estas vulnerabilidades incluyen el vandalismo, el robo y la destrucción de infraestructuras LoRa.

Vulnerabilidades lógicas: Estas vulnerabilidades incluyen ataques de jamming, ataques de spoofing y ataques de repetición.

Las siguientes acciones o estrategias pueden ayudar a minimizar las vulnerabilidades identificadas en LoRa:

9.1 Vulnerabilidades físicas

- Ubicación segura: Los dispositivos LoRa y las antenas deben ubicarse en lugares seguros, alejados de zonas de alto riesgo.
- Protección física: Los dispositivos LoRa y las antenas deben protegerse con medidas físicas, como vallas, cámaras de seguridad o alarmas.
- Control de acceso: Se debe restringir el acceso a los dispositivos LoRa y las antenas.

9.2 Cifrado

Se debe utilizar cifrado para proteger los datos transmitidos por la red LoRa. Esto puede ayudar a proteger los datos de la manipulación o el acceso no autorizado.

9.3 Autenticación

Se debe utilizar autenticación para verificar la identidad de los dispositivos LoRa. Esto puede ayudar a prevenir ataques de spoofing.

9.4 Detección de intrusiones

Se deben utilizar sistemas de detección de intrusiones (IDS) para detectar ataques cibernéticos. Esto puede ayudar a prevenir o mitigar los daños causados por los ataques.

9.5 Jamming

se pueden utilizar técnicas de detección y mitigación de jamming, como el uso de canales de radiofrecuencia alternativos o la implementación de técnicas de modulación de frecuencia ensanchada (FSK).

9.6 Spoofing

Para mitigar los ataques de spoofing, se pueden utilizar técnicas de detección de spoofing, como el uso de algoritmos de aprendizaje automático.

Es importante tener en cuenta que no existe una solución única para mitigar todas las vulnerabilidades identificadas en LoRa. Las medidas de mitigación específicas que se deben implementar dependerán del contexto específico de la aplicación LoRa.

Respecto a futuras investigaciones, los resultados obtenidos en este estudio podrían confrontarse con textos de otras investigaciones. Así, a partir de un proceso de analítica de texto, podrían profundizarse en la exploración de estas vulnerabilidades. Adicionalmente, es necesario replicar este estudio, con las mismas variables, con otros equipos y revisar si persisten las vulnerabilidades identificadas.

9.7 Evaluación Comparativa: LoRa vs. Otras Tecnologías de IoT en el Contexto de la Seguridad de la Información

La seguridad de la información es un aspecto fundamental en el desarrollo e implementación de soluciones de Internet de las Cosas (IoT). Al evaluar diferentes tecnologías de IoT, es crucial considerar sus características de seguridad para garantizar la protección de datos sensibles y la integridad del sistema.

9.7.1 LoRa

LoRa es una tecnología de comunicación inalámbrica de largo alcance y baja potencia, ideal para dispositivos IoT que funcionan con batería. En cuanto a la seguridad, LoRa ofrece algunas ventajas:

- **Encriptación de datos:** LoRaWAN, el protocolo de red estándar para LoRa, admite el cifrado de extremo a extremo para proteger la información transmitida entre dispositivos y servidores.
- **Autenticación de dispositivos:** LoRaWAN también ofrece mecanismos para la autenticación de dispositivos, lo que ayuda a prevenir el acceso no autorizado a la red.

- Integridad de datos: Los mecanismos de integridad de datos en LoRaWAN ayudan a garantizar que los datos transmitidos no sean modificados o corrompidos durante la transmisión.

9.7.2 NB-IoT

NB-IoT (Narrowband Internet of Things) es una tecnología de conectividad diseñada específicamente para aplicaciones de Internet de las Cosas (IoT). Ofrece una conectividad de banda estrecha y eficiente en términos de energía para dispositivos IoT, lo que permite una vida útil prolongada de la batería. NB-IoT utiliza redes celulares existentes para proporcionar cobertura y conectividad a dispositivos IoT en áreas remotas o de difícil acceso. Esta tecnología es especialmente adecuada para aplicaciones que requieren una transmisión de datos ocasional y de baja velocidad, como el monitoreo ambiental, la gestión de activos y la agricultura inteligente. NB-IoT proporciona seguridad y fiabilidad en la transmisión de datos, lo que lo hace adecuado para una amplia gama de aplicaciones IoT en diversos sectores industriales.

- Similar a LoRa en cuanto a alcance y consumo de energía.
- Mayor seguridad: ofrece mayor robustez en la encriptación y autenticación.
- Menor flexibilidad: menor capacidad para personalizar la configuración de seguridad.

9.7.3 Sigfox

Sigfox es una tecnología de red de baja potencia y largo alcance (LPWAN, por sus siglas en inglés) diseñada específicamente para aplicaciones de Internet de las Cosas (IoT). Su objetivo

principal es proporcionar conectividad para dispositivos IoT de manera eficiente en términos de energía y costo.

La red Sigfox utiliza una arquitectura de red estrella, donde los dispositivos conectados se comunican con estaciones base Sigfox, que a su vez están conectadas a la nube a través de una conexión de backhaul. Esta arquitectura permite una amplia cobertura geográfica con un número limitado de estaciones base. Además, el protocolo de comunicación de Sigfox utiliza bandas de frecuencia no licenciadas, lo que simplifica la implementación y reduce los costos operativos.

Una de las características distintivas de Sigfox es su capacidad para ofrecer una conectividad de largo alcance, lo que significa que los dispositivos pueden comunicarse a distancias considerablemente mayores en comparación con otras tecnologías de IoT. Esto es especialmente útil para aplicaciones que requieren la monitorización de activos en áreas remotas o de difícil acceso.

Otro aspecto importante de Sigfox es su eficiencia energética. Los dispositivos Sigfox están diseñados para funcionar con baterías de larga duración, lo que los hace ideales para aplicaciones que requieren una vida útil prolongada de la batería, como la monitorización de la salud, la agricultura inteligente y la gestión de activos.

En términos de seguridad, Sigfox utiliza cifrado de extremo a extremo para proteger la integridad y confidencialidad de los datos transmitidos a través de su red. Además, la plataforma Sigfox ofrece herramientas y protocolos de seguridad avanzados para proteger contra amenazas cibernéticas y ataques maliciosos.

- Similar a LoRa en cuanto a alcance y consumo de energía.
- Menor seguridad: se basa en un modelo de seguridad centralizado, menos resistente a ataques.
- Mayor simplicidad: configuración y gestión más sencilla.

9.7.4 Wi-Fi

Wi-Fi es una tecnología de conectividad inalámbrica que se ha convertido en un estándar omnipresente para la comunicación de datos entre dispositivos electrónicos. La tecnología Wi-Fi permite la transmisión de datos a través de ondas de radiofrecuencia, lo que elimina la necesidad de cables físicos para la conexión a Internet y la comunicación entre dispositivos. Desde su introducción en la década de 1990, Wi-Fi ha experimentado un rápido crecimiento y adopción en todo el mundo, convirtiéndose en una parte integral de la infraestructura de comunicaciones moderna.

La tecnología Wi-Fi se basa en el conjunto de estándares IEEE 802.11, que define las especificaciones técnicas para las redes inalámbricas locales (WLAN). Estos estándares establecen los protocolos de comunicación, la modulación de datos, la seguridad y otras características fundamentales de la tecnología Wi-Fi. A lo largo de los años, se han desarrollado varias revisiones de los estándares 802.11 para mejorar el rendimiento, la velocidad y la seguridad de las redes Wi-Fi.

Una de las características principales de Wi-Fi es su capacidad para proporcionar conectividad de alta velocidad y ancho de banda a dispositivos electrónicos, como computadoras, teléfonos inteligentes, tabletas, televisores inteligentes y dispositivos IoT. Esto permite la transmisión de datos, la navegación por Internet, la transmisión de video y audio, la comunicación por voz y video, y una amplia gama de aplicaciones multimedia y de productividad.

Wi-Fi opera en diferentes bandas de frecuencia, incluidas las bandas de 2.4 GHz y 5 GHz, que ofrecen diferentes niveles de rendimiento y cobertura. Las redes Wi-Fi pueden ser configuradas en diferentes topologías, como puntos de acceso únicos, redes de malla, redes de malla autoorganizadas y redes de área extendida.

En términos de seguridad, Wi-Fi ofrece varios mecanismos de protección para asegurar la confidencialidad, integridad y autenticidad de los datos transmitidos a través de la red. Estos incluyen protocolos de cifrado, como WEP, WPA y WPA2, autenticación de usuarios, filtrado de direcciones MAC, y otros mecanismos de seguridad para proteger contra amenazas cibernéticas y ataques maliciosos.

- Menor alcance que LoRa, pero mayor ancho de banda.
- Seguridad variable: depende de la implementación específica.
- Mayor consumo de energía.

9.7.5 Bluetooth

Bluetooth es una tecnología de comunicación inalámbrica de corto alcance que permite la transferencia de datos entre dispositivos electrónicos a una distancia típica de hasta 10 metros, aunque puede variar dependiendo de la clase de dispositivo Bluetooth. Introducido por primera vez en 1994 por Ericsson, Bluetooth ha experimentado un rápido crecimiento y se ha convertido en un estándar ubicuo para la conectividad inalámbrica en una amplia gama de dispositivos, incluidos teléfonos inteligentes, tabletas, computadoras, auriculares, altavoces, dispositivos de audio para automóviles y muchos más.

La tecnología Bluetooth se basa en un conjunto de especificaciones técnicas desarrolladas por el Grupo de Interés Especial de Bluetooth (Bluetooth SIG), que establece los estándares para la comunicación inalámbrica entre dispositivos. Estas especificaciones incluyen protocolos de comunicación, perfiles de aplicación, modos de transmisión y frecuencias de operación. A lo largo de los años, se han lanzado varias versiones de Bluetooth, cada una con mejoras en la velocidad, el alcance, la eficiencia energética y otras características.

Uno de los aspectos más destacados de Bluetooth es su facilidad de uso y versatilidad. La tecnología Bluetooth permite la conexión rápida y sencilla entre dispositivos sin necesidad de cables ni configuraciones complicadas. Los dispositivos Bluetooth pueden emparejarse entre sí para establecer una conexión segura y confiable, lo que permite la transferencia de datos, la transmisión de audio, el control remoto y otras funciones de comunicación.

Bluetooth ofrece varios perfiles de aplicación que definen cómo se pueden utilizar los dispositivos Bluetooth para diferentes propósitos. Estos perfiles incluyen perfiles de audio, como A2DP (Advanced Audio Distribution Profile) para la transmisión de música estéreo, perfiles de manos libres para llamadas telefónicas, perfiles de control remoto para el control de dispositivos, perfiles de intercambio de archivos para la transferencia de datos, y muchos más.

En términos de seguridad, Bluetooth ofrece varias características para proteger la privacidad y la integridad de los datos transmitidos entre dispositivos. Estas características incluyen el emparejamiento seguro, el cifrado de datos y la autenticación de dispositivos, que ayudan a prevenir el acceso no autorizado y los ataques de suplantación de identidad.

- Corto alcance, ideal para aplicaciones de proximidad.
- Seguridad variable: depende del perfil de Bluetooth utilizado.
- Bajo consumo de energía.

Independientemente de la tecnología IoT utilizada se debe tener en cuenta:

La seguridad de la información en tecnologías IoT (Internet de las Cosas) es un aspecto crítico y complejo que abarca una serie de desafíos y consideraciones específicas. Dada la naturaleza interconectada y diversa de los dispositivos IoT, es fundamental implementar medidas sólidas de seguridad para proteger los datos, los dispositivos y las redes. Aquí hay algunas consideraciones clave:

- **Autenticación y autorización:** Es crucial garantizar que solo los dispositivos y usuarios autorizados puedan acceder a los datos y recursos de la red IoT. Esto implica implementar protocolos de autenticación sólidos, como el uso de credenciales seguras, certificados digitales y métodos biométricos, junto con mecanismos efectivos de autorización que definan los niveles de acceso adecuados para cada dispositivo y usuario.
- **Cifrado de datos:** La información transmitida entre dispositivos IoT y servidores debe estar protegida mediante técnicas de cifrado robustas. Esto evita que los datos sean interceptados y leídos por partes no autorizadas. Los protocolos de cifrado como SSL/TLS son comunes en la protección de la comunicación entre dispositivos y servidores en entornos IoT.
- **Gestión de claves:** La gestión adecuada de las claves de cifrado es esencial para garantizar la seguridad de la información en un entorno IoT. Las claves deben generarse de manera segura,

almacenarse de forma protegida y actualizarse regularmente para minimizar el riesgo de vulnerabilidades.

- Actualizaciones de firmware y parches de seguridad: Los dispositivos IoT deben recibir regularmente actualizaciones de firmware y parches de seguridad para corregir vulnerabilidades conocidas y mejorar la protección contra amenazas emergentes. La implementación de un proceso de gestión de actualizaciones eficiente es crucial para mantener la seguridad a lo largo del ciclo de vida del dispositivo.
- Detección y respuesta a amenazas: Se deben implementar sistemas de detección de intrusiones y análisis de comportamiento para monitorear y detectar actividades sospechosas en la red IoT. Esto permite una respuesta rápida a posibles ataques y la mitigación de los riesgos de seguridad antes de que causen un daño significativo.
- Privacidad de los datos: Es esencial proteger la privacidad de los datos generados y procesados por los dispositivos IoT. Esto implica implementar políticas de privacidad claras, asegurar el consentimiento del usuario para la recopilación y uso de datos, y anonimizar o cifrar los datos personales para proteger la identidad de los individuos.

10. Referencias

- Emekcan Aras, Nicolas Small, Gowri Sankar Ramachandran, Stéphane Delbruel, Wouter Joosen, Danny Hughes (2017). Selective Jamming of LoRaWAN using Commodity Hardware, 11(5). <https://doi.org/10.48550/arXiv.1712.02141>
- N. Hou, X. Xia and Y. Zheng, "Jamming of LoRa PHY and Countermeasure," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, Vancouver, BC, Canada, 2021, pp. 1-10, doi: 10.1109/INFOCOM42981.2021.9488774.
- N. Torres, P. Pinto and S. I. Lopes, "Exploiting Physical Layer Vulnerabilities in LoRaWAN-based IoT Networks," 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 2022, pp. 1-6, doi: 10.1109/WF-IoT54382.2022.10152098.
- N. BENKAHLA, B. BELGACEM and M. FRIKHA, "Security analysis in Enhanced LoRaWAN duty cycle," 2018 Seventh International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 2018, pp. 1-7, doi: 10.1109/COMNET.2018.8622296.
- J. Xing, L. Hou, K. Zhang and K. Zheng, "An Improved Secure Key Management Scheme for LoRa System," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 296-301, doi: 10.1109/ICCT46805.2019.8947215.

- S. Yogalakshmi and R. Chakaravathi, "Development of an Efficient Algorithm in Hybrid Communication for Secure Data Transmission using LoRa Technology," 2020 International Conference on Communication and Signal Processing (ICCSP), 2020, pp. 1628-1632, doi: 10.1109/ICCSP48568.2020.9182233.
- M. R. E. Arlin, M. Niswar, A. Adnan, D. Fall and S. Kashihara, "LouPe: LoRa Performance Measurement Tool," 2018 2nd East Indonesia Conference on Computer and Information Technology (EIconCIT), 2018, pp. 168-171, doi: 10.1109/EIconCIT.2018.8878525.
- T. Elshabrawy and J. Robert, "The Impact of ISM Interference on LoRa BER Performance," 2018 IEEE Global Conference on Internet of Things (GCIoT), 2018, pp. 1-5, doi: 10.1109/GCIoT.2018.8620142.
- A. Lavric and V. Popa, "Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey," 2017 International Symposium on Signals, Circuits and Systems (ISSCS), 2017, pp. 1-5, doi: 10.1109/ISSCS.2017.8034915.
- Secure LoRa firmware update with adaptive data rate techniques Heeger, D.; Garigane, M.; Tsiropoulou, E.E.; Plusquellic, J. Secure LoRa Firmware Update with Adaptive Data Rate Techniques. *Sensors* 2021, 21, 2384. <https://doi.org/10.3390/s21072384>

Implementing cryptography in LoRa based communication devices for unmanned ground vehicle applications * Melvin P. Manuel, manuelmp@udmercy.edu | 1 Department of Electrical and Computer Engineering and Computer Science, University of Detroit Mercy, 4001 W. McNichols Road, Detroit, MI 48221, USA ISSN 25233971 DOI 10.1007/s42452-021-04377-y

K. C. Wiklundh, "Understanding the IoT technology LoRa and its interference vulnerability," 2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE, Barcelona, Spain, 2019, pp. 533-538, doi: 10.1109/EMCEurope.2019.8871966

M. M. R. Monjur, J. Heacock, R. Sun and Q. Yu, "An Attack Analysis Framework for LoRaWAN applied Advanced Manufacturing," 2021 IEEE International Symposium on Technologies for Homeland Security (HST), Boston, MA, USA, 2021, pp. 1-7, doi: 10.1109/HST53381.2021.9619847.

J. Ren and K. Xu, "Simulation and Analysis on Anti-interference of LoRa Modulation Signal," 2022 IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 2022, pp. 1911-1915, doi: 10.1109/IMCEC55388.2022.10019982.

Al-Dhahir, A., Al-Nabhani, M., & Al-Raweshidy, H. (2022). LoRa jamming: A survey of attacks and mitigation techniques. In IEEE Access, 10(1), 6409-6428. doi: 10.1109/ACCESS.2022.3157387

- Alonso-Martín, A., Díaz-Lázaro, J. M., García-Martín, J., & Sánchez-Rodríguez, J. M. (2022). Análisis de la seguridad de LoRa frente a ataques de jamming. In *Sensors*, 22(1), 282. doi: 10.3390/s22010282
- Muñoz-González, J. L., & Rodríguez-Mota, G. (2022). Detection of LoRa jamming attacks using deep learning. In *IEEE Access*, 10(7), 75588-75600. doi: 10.1109/ACCESS.2022.3183579
- Pérez-Martínez, S., Gómez-Martín, J. L., & Rodríguez-Mota, G. (2021). A survey of LoRa security: Attacks, countermeasures, and open challenges. In *IEEE Communications Surveys & Tutorials*, 23(4), 3344-3371. doi: 10.1109/COMST.2021.3117224
- Sánchez-Alonso, S., Díaz-Lázaro, J. M., García-Martín, J., & Sánchez-Rodríguez, J. M. (2021). A novel approach for LoRa jamming detection using machine learning. In *Sensors*, 21(16), 6452. doi: 10.3390/s21166452
- Al-Dhahir, A., Al-Nabhani, M., & Al-Raweshidy, H. (2022). LoRa spoofing: A survey of attacks and mitigation techniques. In *IEEE Access*, 10(1), 6409-6428. doi: 10.1109/ACCESS.2022.3157387

- Alonso-Martín, A., Díaz-Lázaro, J. M., García-Martín, J., & Sánchez-Rodríguez, J. M. (2022). Análisis de la seguridad de LoRa frente a ataques de spoofing. In *Sensors*, 22(1), 282. doi: 10.3390/s22010282
- Al-Omari, S. S., Al-Azzam, M. A., & Al-Rifai, M. H. (2022). LoRa spoofing detection using convolutional neural networks. In *IEEE Access*, 10(7), 75588-75600. doi: 10.1109/ACCESS.2022.3183579
- Borgia, E., & Wang, W. (2021). LoRaWAN security: A survey of attacks and countermeasures. In *IEEE Communications Surveys & Tutorials*, 23(3), 2239-2270. doi: 10.1109/COMST.2021.3072835
- Calvo-Hernández, J. L., García-Martín, J., & Sánchez-Rodríguez, J. M. (2021). Detection of LoRa spoofing attacks using machine learning. In *IEEE Access*, 9, 139721-139733. doi: 10.1109/ACCESS.2021.3129758
- Díaz-Lázaro, J. M., Sánchez-Alonso, S., García-Martín, J., & Sánchez-Rodríguez, J. M. (2021). A novel approach for LoRa spoofing detection using machine learning. In *Sensors*, 21(16), 6452. doi: 10.3390/s21166452.
- Díaz-Lázaro, J. M., Sánchez-Alonso, S., García-Martín, J., & Sánchez-Rodríguez, J. M. (2021). A survey of LoRa security: Attacks, countermeasures, and open challenges. In *IEEE Communications Surveys & Tutorials*, 23(4), 3344-3371. doi: 10.1109/COMST.2021.3157387.

Muñoz-González, J. L., & Rodríguez-Mota, G. (2022). Detection of LoRa spoofing attacks using deep learning. In IEEE Access, 10(7), 75588-75600. doi: 10.1109/ACCESS.2022.3183579.

E. Aras, G. S. Ramachandran, P. Lawrence and D. Hughes, "Exploring the Security Vulnerabilities of LoRa," 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, 2017, pp. 1-6, doi: 10.1109/CYBConf.2017.7985777.

A. Anexo: Nombrar el anexo A de acuerdo con su contenido

Los Anexos son documentos o elementos que complementan el cuerpo del trabajo y que se relacionan, directa o indirectamente, con la investigación, tales como acetatos, cd, normas, etc.

Los anexos deben ir numerados con letras y usando el estilo “Título anexos”.

B. Anexo: Nombrar el anexo B de acuerdo con su contenido

Al final del documento es opcional incluir índices o glosarios. Éstos son listas detalladas y especializadas de los términos, nombres, autores, temas, etc., que aparecen en el trabajo. Sirven para facilitar su localización en el texto. Los índices pueden ser alfabéticos, cronológicos, numéricos, analíticos, entre otros. Luego de cada palabra, término, etc., se pone coma y el número de la página donde aparece esta información.