Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Maestría en Telecomunicaciones

Análisis de seguridad en redes de IoT- caso LoRaWAN

Trabajo de Titulación, previo a la obtención del título de Magister en Telecomunicaciones.

AUTOR:

Ing. Alvaro Fabian González Guachisaca

DIRECTOR:

Ing. John Jossimar Tucker Yépez, Mg. Sc.

Loja - Ecuador

2024

Certificación

Loja, 15 de Julio de 2024

Ing. John Jossimar Tucker Yépez, Mg. Sc
DIRECTOR DEL TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Análisis de seguridad en redes IoT caso LoRaWAN,** previo a la obtención del título de **Magister en Telecomunicaciones**, de la autoría del estudiante **Alvaro Fabian González Guachisaca**, con **cédula de identidad Nro. 1104735772**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

JOHN JOSSIMAR TUCKER YEPEZ
Firmado digitalmente por JOHN JOSSIMAR TUCKER YEPEZ
Fecha: 2024.07.15 22:38:35 -05'00'

Ing. John Jossimar Tucker Yépez, Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, **Alvaro Fabian González Guachisaca**, declaro ser autor del presente trabajo de titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

ALVARO FABIAN GONZALEZ GUACHISACA

Firmado digitalmente por ALVARO FABIAN GONZALEZ GUACHISACA
Fecha: 2024.07.15 21:28:28 -05'00'

Firma:

Cédula de Identidad: 1104735772

Fecha: 08/07/2024

Correo electrónico: alvaro.gonzalez@unl.edu.ec

Teléfono: 0992289829

Carta de autorización

Por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica de texto completo, del Trabajo de Titulación.

Yo, **Alvaro Fabian González Guachisaca**, declaro ser el autor del Trabajo de Titulación denominado: **Análisis de seguridad en redes IoT caso LoRaWAN**, como requisito para optar el título de Magister en Telecomunicaciones, autorizó al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, suscribo, en la ciudad de Loja, a los quince días del mes de julio de dos mil veinticuatro.

ALVARO FABIAN GONZALEZ GUACHISACA

Firmado digitalmente por ALVARO FABIAN GONZALEZ GUACHISACA
Fecha: 2024.07.15 21:29:04 -05'00'

Firma:

Cédula de identidad: 1104735772

Dirección: España y Bolivia

Correo electrónico: alvaro.gonzalez@unl.edu.ec

Teléfono: 0992289829

DATOS COMPLEMENTARIOS:

DIRECTOR DEL TRABAJO DE TITULACIÓN: Ing. John Jossimar Tucker Yépez, Mg. Sc.

Dedicatoria

A Dios por guiarme por el camino correcto y darme la fuerza y sabiduría necesaria para poder cumplir mis objetivos.

A mi familia, en especial a mis padres y hermanos ya que gracias a su sacrificio y apoyo incondicional me han ayudado a cumplir una de mis metas principales, que es obtener mi maestría.

A mis hijos que son mi fuente de inspiración y entrega constante.

Alvaro Fabian González Guachisaca

Agradecimiento

A la Universidad Nacional de Loja por haber permitido culminar mis estudios de manera satisfactoria.

A mi tutor, el Ing. John Tucker Yépez, Mg. Sc, quien fue un apoyo fundamental en la realización de este trabajo, con su acertada dirección se pudo plasmar los resultados generados en la presente investigación y a todas las personas que contribuyeron de manera directa e indirecta para alcanzar mi objetivo, el desarrollo y culminación del trabajo de titulación.

Alvaro Fabian González Guachisaca

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Índice de Anexos

1. Título

Análisis de seguridad en redes IoT caso LoRaWAN

2. Resumen

En la era actual de la conectividad digital, la implementación generalizada de dispositivos de Internet de las cosas (IoT) ha impulsado significativamente la eficiencia operativa y la mejora de servicios en diversos sectores. Sin embargo, este rápido aumento de la interconexión también ha introducido desafíos críticos en términos de seguridad, particularmente en redes de bajo consumo de energía y largo alcance, como LoRaWAN.

En este proyecto se plasma las interrogantes sobre las vulnerabilidades específicas en la capa de enlace de LoRaWAN, el impacto de los ataques en la disponibilidad de las redes, el estado actual de las medidas de seguridad implementadas y la eficacia de la gestión de claves y la autenticación de dispositivos. Al obtener respuestas a estas preguntas, se contribuirá al desarrollo de estrategias y prácticas de seguridad más sólidas para la implementación de redes LoRaWAN en entornos IoT.

La relevancia de este proyecto radica en su capacidad para analizar la seguridad en la actualidad sobre las infraestructuras de IoT basadas en LoRaWAN, mostrando sus fortalezas y debilidades en la integridad de los datos y guiando en poder tomar decisiones para una adecuada protección de la privacidad en un contexto de creciente dependencia de la conectividad y la automatización.

Además, los resultados de este análisis podrían informar a diseñadores, desarrolladores y responsables de políticas sobre las mejores prácticas de seguridad para implementaciones futuras de redes LoRaWAN y, por extensión, para el desarrollo seguro de aplicaciones IoT en general.

Palabras: LoRa, LoRaWAN, Seguridad, Redes Inalámbricas.

Abstract

In the current era of digital connectivity, the widespread deployment of devices of Internet of the things (IoT)it has significantly boosted operational efficiency and service improvement in various sectors. However, this rapid increase in interconnection has also introduced critical security challenges, in low-energy and long-range networks, such as LoRaWAN.

This project captures questions about specific vulnerabilities in the LoRaWAN link layer, the impact of attacks on network availability, the current state of security measures implemented and the effectiveness of key management and device authentication. By getting answers to these questions, you will contribute to the development of more robust security strategies and practices for the deployment of LoRaWAN networks in IoT environments.

The relevance of this project lies in its ability to analyze current security on LoRaWAN-based IoT infrastructures, showing its strengths and weaknesses in data integrity and guiding decision-making for adequate privacy protection in a context of increasing dependence on connectivity and automation.

In addition, the results of this analysis could inform designers, developers and policymakers about best security practices for future LoRaWAN network deployments and, by extension, for the safe development of IoT applications in general.

Words: LoRa, LoRaWAN, Security, Wireless Networks.

3. Introducción

El Internet de las Cosas (IoT) ha revolucionado la manera en que interactuamos con el mundo digital. Esta nueva tecnología facilita un ecosistema interconectado de dispositivos y máquinas, lo que permite a los usuarios controlar sus dispositivos desde cualquier lugar, permitiendo mejorar la productividad y reduciendo el impacto ambiental. Según Michell Davidson reconocida gerente de marketing de contenido en su blog GlobalSign, de acuerdo a las estimaciones realizadas por empresas que se encargan de censar a nivel mundial los dispositivos IoT conectados; se estimó que para el 13 de marzo de 2024 existen 7.440 millones de dispositivos conectados en el mundo y se prevé que esta cifra aumente a 29.000 millones para el año 2030, surgiendo la necesidad de introducir nuevas tecnologías para permitir la comunicación de una manera segura.

En este contexto, LoRaWAN se ha posicionado como un protocolo crucial para las comunicaciones en redes IoT. Sin embargo, la seguridad en estas implementaciones es fundamental para garantizar la integridad, confidencialidad y disponibilidad de los datos.

Las comunicaciones IoT tienen requisitos específicos como largo alcance, envío de pequeña cantidad de datos, bajo consumo de energía y rentabilidad. Las tecnologías de radio de corto alcance ampliamente utilizadas como ZigBee, Bluetooth, Wi-Fi; no están adaptadas para escenarios que requieren transmisiones de largo alcance. Las soluciones basadas en comunicaciones celulares como Segunda Generación (2G), Tercera Generación (3G), Cuarta Generación (4G) y Quinta Generación (5G), pueden proporcionar una mayor cobertura, pero consumen energía excesiva del dispositivo. Por lo tanto, los requisitos de las aplicaciones IoT han impulsado el surgimiento de una nueva tecnología de comunicación inalámbrica: Red de Área Amplia de Baja Potencia (Low Power Wide Area Network (LPWAN).

Este proyecto, está basado en la tecnología IoT LoRaWAN. Este protocolo de comunicación puede soportar diferentes configuraciones, entre las que figuran:

Estrella: Es la más común, donde los dispositivos finales (nodos) se comunican directamente con una estación base central (gateway).

Malla: Donde los dispositivos pueden comunicarse entre sí a través de múltiples saltos, lo cual es útil para extender la cobertura y mejorar la redundancia de la red, aunque afectan a

la duración de la batería del dispositivo debido al reenvío de mensajes.

Híbrida o mixta: Donde se combinan elementos de estrella y malla, permitiendo una flexibilidad mayor en la configuración de la red.

4. Marco Teórico

4.1 Redes IoT (Internet de las cosas)

Es la agrupación e interconexión de dispositivos y objetos a través de una red privada o Internet, dónde todos ellos podrían ser visibles e interactuar. Estos pueden ser sensores, dispositivos mecánicos, objetos cotidianos como frigorífico, calzado, ropa, dispositivos electrónicos, focos, etc.

Todo tipo de dispositivos a futuro podrá tener una conexión a internet e interactuar entre sí, sin necesidad de que una persona tenga que estar controlándolo, el objetivo es que exista una comunicación máquina a máquina, o lo que se conoce como una interacción M2M (machine to machine).

Este tipo de dispositivos pueden dividirse en dos categorías; sensores que son los que retienen la información o datos y los trasladan a otro lugar; o interruptores que son los encargados de enviar las instrucciones.

Internet de las Cosas ha evolucionado gracias a la facilidad de Internet en la mayoría de destinos del mundo permitiendo alcanzar nuevas tecnologías y mayores beneficios. Las aplicaciones dentro de este campo permiten mejorar la vida diaria de las personas en el ámbito del campo, ciudad y empresarial, este último es el ámbito que más se ha desarrollado en esta nueva tecnología para mejorar sus procesos y obtener mejores beneficios.

Hoy en día el internet de las cosas capta la atención de las personas en todo el mundo, cuyas experiencias van relacionadas a los cambios tecnológicos, el uso de tecnología wearable o vestible que son dispositivos electrónicos inteligentes incorporados a la vestimenta o usados corporalmente como implantes o accesorios usados como una extensión del cuerpo o mente de la persona, se han visto afectadas por las preocupaciones en torno a la inseguridad y la falta de privacidad que se tiene al estar conectados de forma continua. Esta perspectiva se aplica a todos los tipos de proyectos de IoT que actualmente utilizan las empresas, especialmente cuando el usuario final es una persona común.

La tecnología wereable moderna está relacionada con el desarrollo de la computadora corporal en dispositivos electrónicos que son programados por el usuario para realizar

actividades como medir los pasos, ritmo cardiaco, tele transmitir, notificaciones y alertas por medio de bluetooth e internet.

Las soluciones en este ámbito para las empresas les permiten mejorar los modelos comerciales actuales y entablar nuevas relaciones con los clientes y los socios, pero también implican ciertos desafíos. El volumen de datos que genera un sistema de dispositivos inteligentes (lo cual se conoce como big data) puede ser abrumador. El proceso de integración del big data en los sistemas actuales y la configuración del análisis de los datos para poder utilizar la información puede resultar complicado. (RedHat s.f.)

La seguridad en redes de dispositivos inteligentes es muy importante, esta debe considerarse en el momento que se desarrolla un sistema utilizando esta tecnología, para muchas empresas es imprescindible tener la seguridad previa a la implementación de una red basada en el internet de las cosas para luego no tener que incurrir en gastos extremos adicionales.

Un ejemplo, es el ciclo de vida de la maquinaria pesada la cual se utiliza en obras de construcción. Al pasar el tiempo esta comienza a presentar problemas por el uso y desgaste de los mismos, debido al esfuerzo realizado. Para poder afrontar este problema, se puede agregar varios sensores especializados en cada parte de la maquinaria que se desea monitorear o la que más daños constantemente presenta, de esta manera se puede programar mantenimientos periódicos, con la finalidad de evitar el daño eminente de algún repuesto o maquinaria completa, adicional se puede realizar mediciones en el ámbito de desempeño del personal y poder mejorar la carga laboral de cada una de los empleados que trabajen en la empresa. IoT tiene un papel muy importante en la industria, fábricas, empresas y otros sectores, permitiendo una automatización a las máquinas que se manejan en cada una de ellas.

Gracias a los dispositivos IoT, los cuales nos permiten recopilar y transmitir información, podemos obtener resultados, en analíticas avanzadas y machine learning que nos permitan tomar decisiones respecto a la salud, industria, agricultura, etc.

Entre las ventajas y desventajas de IoT tenemos:

Ventajas:

- **Conexión**: IoT permite la conexión de dispositivos que no estaban previamente conectados a Internet. Facilitando la comunicación y transferencia de información en tiempo real, lo que permite la automatización de tareas y procesos.
- **Eficiencia**: La automatización de procesos y tareas permite una mayor eficiencia en la utilización de recursos, lo que reduce costos y mejora de la productividad.
- **Comodidad**: IoT permite controlar remotamente los dispositivos, aumentando la comodidad y la accesibilidad. Como ejemplo, se pueden controlar luces, termostatos, cámaras de seguridad y otro tipo de dispositivos desde un móvil o un computador.
- **Seguridad**: IoT también puede mejorar la seguridad en hogares y empresas. Las cámaras de seguridad y sensores de movimiento pueden detectar intrusiones y alertar a dueños, lo que ayuda a prevenir atracos y otros delitos.
- **Salud**: IoT permite monitorear signos vitales y enviar alertas a los médicos en caso de emergencia.
- **Análisis de datos:** La conexión de objetos a internet permite la recopilación de cantidades de información, lo que resulta útil para un análisis de patrones y toma de decisiones informadas.

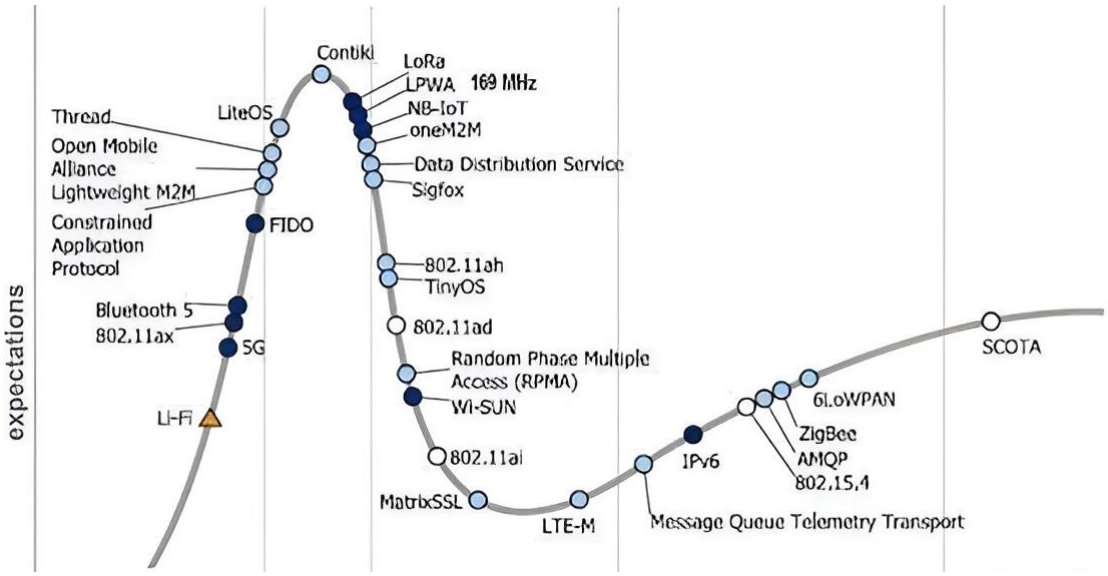
Desventajas:

- **Privacidad**: IoT pone en riesgo la privacidad de usuarios. La recopilación de información puede ser mal utilizada, como el robo de identidad y la vigilancia ilegal.
- **Vulnerabilidad**: IoT puede resultar vulnerable a ataques cibernéticos**.** La interconexión de dispositivos aumenta el riesgo de brechas de seguridad y la exposición de información personal y confidencial.
- **Costo**: IoT puede ser costoso para implementar y mantener. Al adoptar nuevas tecnologías y dispositivos se puede requerir una inversión mayor.
- **Dependencia**: La dependencia de IoT también puede ser una desventaja. Pueden producirse interrupciones de procesos y tareas importantes, si los dispositivos fallan o pierden conexión a Internet.
- **Complejidad**: La complejidad de IoT puede ser un obstáculo para la adopción generalizada. A los usuarios se les puede volver complejo el uso de este tipo de dispositivos limitando la utilidad de IoT.

- **Problemas de seguridad**: La conexión de objetos a internet puede estar expuestos a grandes riesgos de seguridad, como el hackeo y la manipulación remota.

4.2 Gráfica de Gartner

Figura 1. *Gráfica de Gartner*



Fuente: IoT, según Gartner (2022). PrensarioHub.

Gartner es una plataforma verificada de evaluación y calificación de tecnologías y servicios para empresas. En este caso nos basamos en la Figura 1 la cual nos indica cuales son las redes LPWAN y protocolos más utilizados, con una proyección de 2, 5, y 10 años. Entre estas tecnologías las más destacadas son: Sigfox, Lora y NB-IOT (Narrowband IOT), estas nos ayudan a realizar implementaciones con redes IoT a gran escala. Estas tres redes son parte de un gran ecosistema de conectividad, aunque se encuentren enfrentadas entre sí.

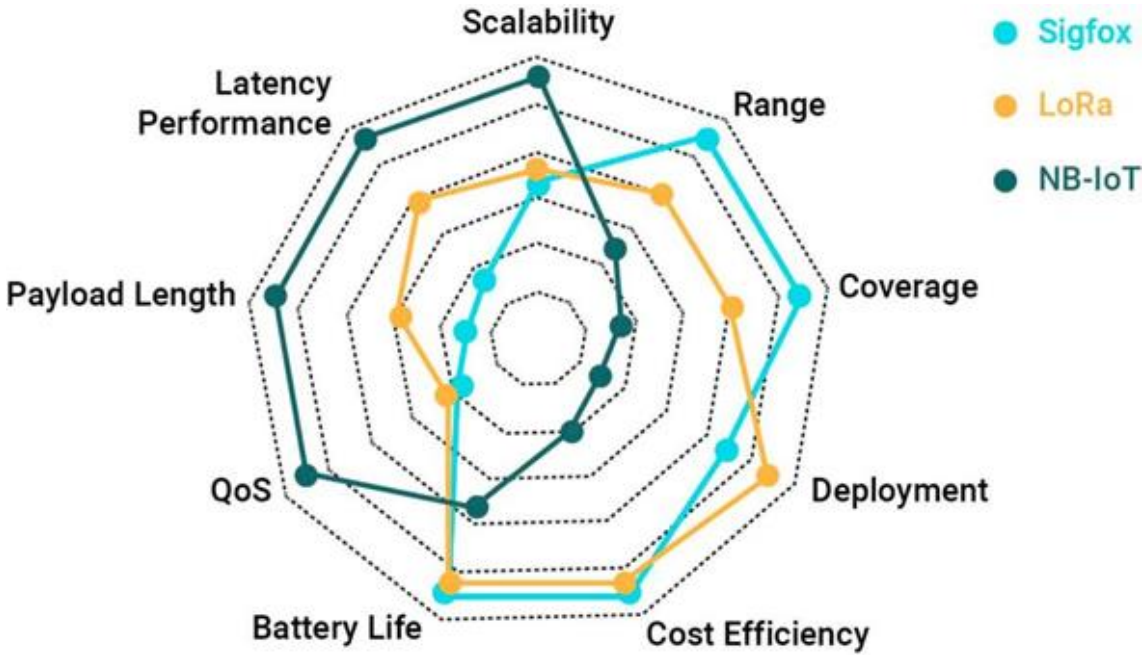
Los protocolos descritos en el párrafo anterior son los más utilizados en las redes IoT, esto es en gran parte por las características que presentan:

- Bajo consumo de batería.
- En zonas rurales tienen un alcance de 10-15 km.
- En zonas urbanas tienen un alcance de 1-5 km.
- El costo de implementación es bajo. (Pérez, A. 2021)

Como se muestra en la Figura 2, la batería de este tipo de dispositivos en algunos casos puede alcanzar varios años de duración, todo depende de la frecuencia de transmisión que tenga

cada uno; adicional es adecuado para poder transmitir pequeñas cantidades de datos a larga distancia.

Figura 2. *Redes LPWAN*



Fuente: Redes LPWAN. Fuente: Carracedo, G. 2023b, enero 17

A continuación, se detalla los protocolos más utilizados en las redes IoT:

4.2.1 Sigfox

Sigfox fue originariamente una empresa francesa fundada en 2009 por dos ingenieros apasionados por el estudio de las señales. Podemos catalogarla como la primera red IoT dedicada. (SIGFOX. s. f.).

Este tipo de red permite conexiones de máquina a máquina con un tipo de conectividad totalmente pensado y dedicado a comunicaciones de baja velocidad, adicional reduce el consumo de energía y el costo de dispositivos conectados.

Sigfox junto a los operadores de internet telefónicos ha creado una red de largo alcance y baja velocidad que permite la comunicación entre los distintos dispositivos para la transmisión de datos sin tener la necesidad de estar ligado a la cobertura y disponibilidad de la

red móvil.

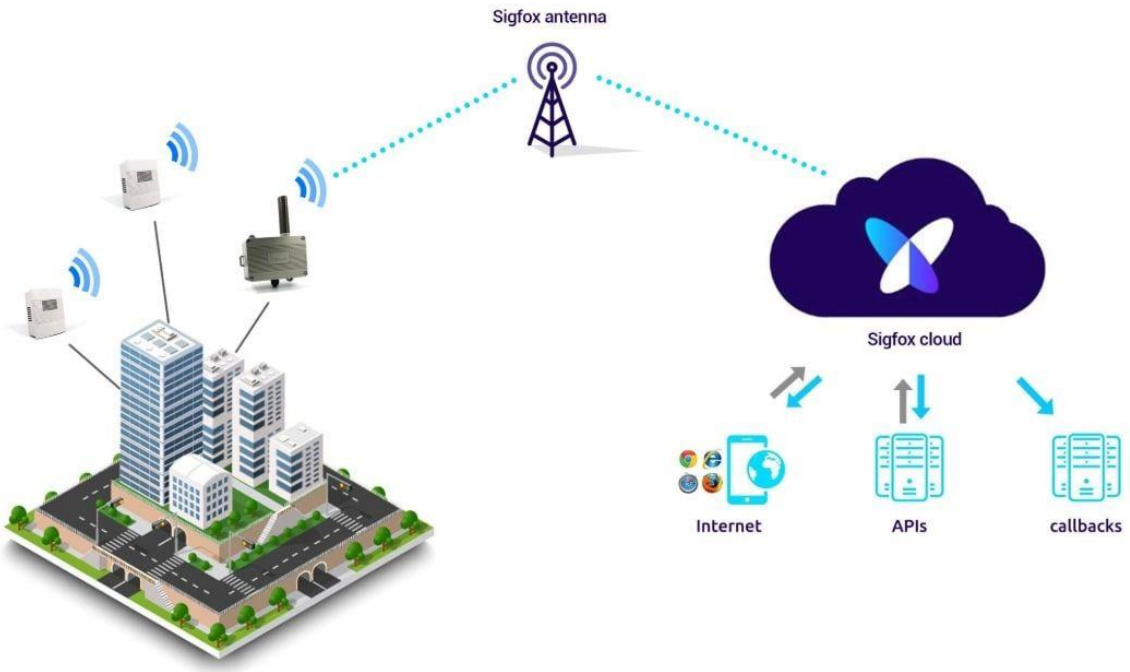
Gracias a la tecnología de radio de banda ultra estrecha se puede conectar varios dispositivos de manera eficiente energéticamente, se utiliza bandas de frecuencia libres de licencia, disponibles en todo el mundo, como lo son las bandas ISM (de radio industriales, científicas y médicas).

Una de las desventajas al utilizar las bandas de frecuencia libre es que solo permite el envío de 400 mensajes diarios por dispositivo.

Desde un punto de vista técnico, Sigfox depende de otra red distinta, basada en 868Mhz.

Cada nodo de Sigfox como se muestra en la Figura 3, puede cubrir un área bastante grande de cobertura, pero dependen de otra red basados en los 868Mhz, necesitando mejorar la cobertura en el área por medio de la instalación de un equipo repetidor.

Figura 3. *Sigfox*



Fuente: SIGFOX. (s. f.-b)

UNB (Ultra – Narrow Band)

Sigfox utiliza una tecnología llamada UNB (Banda Ultra Estrecha), es un tipo de modulación conocida como BPSK (Modulación por desplazamiento de fase binario), está

diseñada para funcionar con bajas velocidades de transferencias de 10 a 1.000 bits por segundo. (UNB Arduino, 2022)

SIGFOX requiere poca potencia para transmitir datos a grandes distancias utilizando un canal de 200Hz de ancho de banda. Los sistemas UNB se utilizan regularmente hacia un solo sentido, desde un sensor inicial hasta la estación base, pero si se puede dar los casos que se necesite servicios bidireccionales de vez en cuando. Un ejemplo, es el uso de un sensor en un parqueadero de vehículos el cual indica si existe un espacio disponible solo debe transmitirse cuando un vehículo ingresa al espacio libre en el parqueadero, y una vez más cuando un vehículo se va, abriendo su receptor unas veces cada hora para escuchar peticiones de parte del sistema.

Acceso aleatorio:

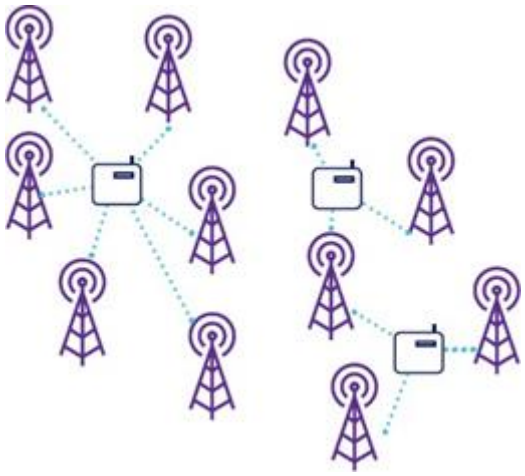
El acceso aleatorio su característica principal es obtener una alta calidad de servicio, en el cual el dispositivo se encarga de emitir un mensaje en una frecuencia de forma aleatoria y después envía dos mensajes adicionales aleatorias tanto en frecuencia como en tiempo.

Recepción cooperativa:

En este principio la recepción cooperativa no permite que un objeto adjunte a una estación base específica a diferencia de los protocolos ya definidos en la conexión con la telefonía celular.

En la Figura 4, las estaciones que estén dentro del área de alcance reciben los mensajes que son emitidos. Por lo general se suelen encontrar 3 estaciones base.

Figura 4. *Ultra - Narrow Band*



Fuente: Ultra - Narrow Band. Fuente: SIGFOX. (s. f.-b)

En los mensajes pequeños su tamaño es de 1 a 12 bytes, permitiendo a los sensores, gps (sistema de posicionamiento global) o algún otro dispositivo de datos realizar una carga útil por medio de este tipo de transferencias.

En la siguiente Tabla 1 se muestra el tamaño de carga por tipo de sensor:

Tabla 1. *Transferencias*

Sensor	Tamaño
GPS coordenadas	6 bytes
Temperatura	2 bytes
Reporte de velocidad	1 byte
Estado de Objeto	1 byte
Carga útil	0 byte

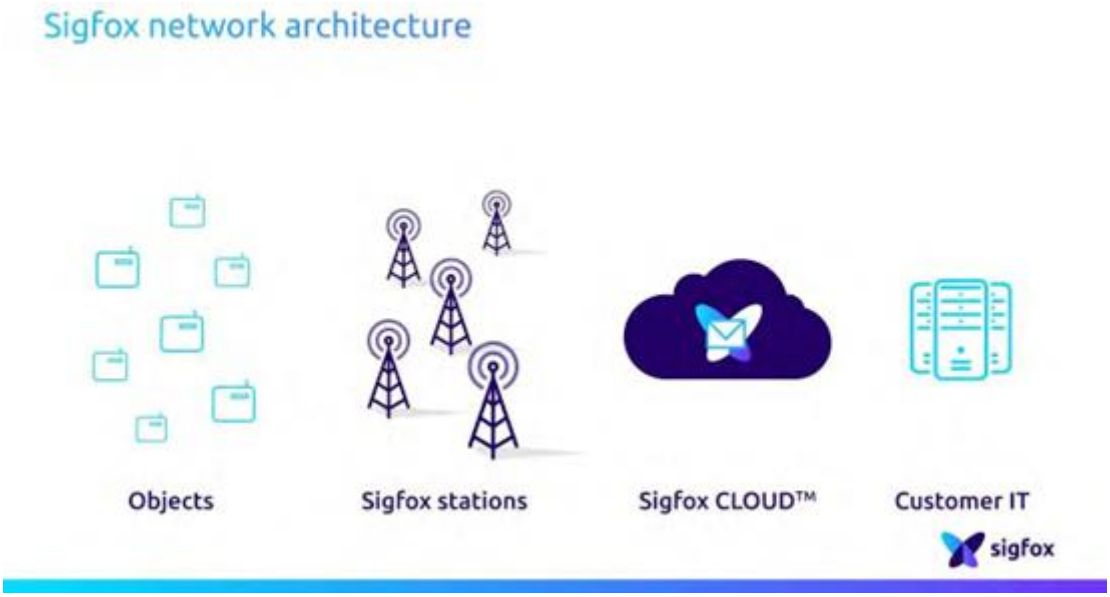
Fuente: El autor

Arquitectura de la red:

Sigfox tiene una arquitectura de red simple y fácil de entender, como se muestra en la Figura 5, esto se debe a que se encuentra dividida en 2 capas principales: La capa de equipo de red y la capa de sistema de soporte Sigfox. Las dos capas tienen características y partes que permiten estructurar red optima. La primera capa (equipo de red) está conformada por varias estaciones las cuales hacen referencia a varias antenas que permiten la recepción de mensajes que emiten los diferentes dispositivos que se encuentran dentro de la red y a su vez estos se envían a la siguiente capa que se encarga de la mayoría de la arquitectura de Sigfox.

Sigfox, cuenta con una central que es la encargada de procesar los mensajes que fueron recibidos en la capa de equipo de red y después los envía para las devoluciones de llamada al sistema del cliente. La capa tiene una variedad de características, las cuales son esenciales para poder operar y monitorear la red, siendo beneficioso para el administrador el cual tendrá toda la información recopilada en una sola parte para su análisis correspondiente. Adicional cuenta con características de soporte comercial, soporte de planificación de radio y la información que contiene el repositorio, pudiendo obtener reportes generados por medio de la red con toda la data que se obtiene con el paso del tiempo.

Figura 5. *Arquitectura Sigfox*



Fuente: SIGFOX. (s. f.-b)

Seguridad Sigfox:

La seguridad de Sigfox permite analizar y encontrar amenazas comunes que los usuarios adquieren con este tipo de servicios los cuales los categoriza dependiendo la utilización.

Sigfox maneja de forma predeterminada la seguridad conforme a lo siguiente:

- Cifrado para garantizar a los usuarios una confidencialidad en los datos de la red.

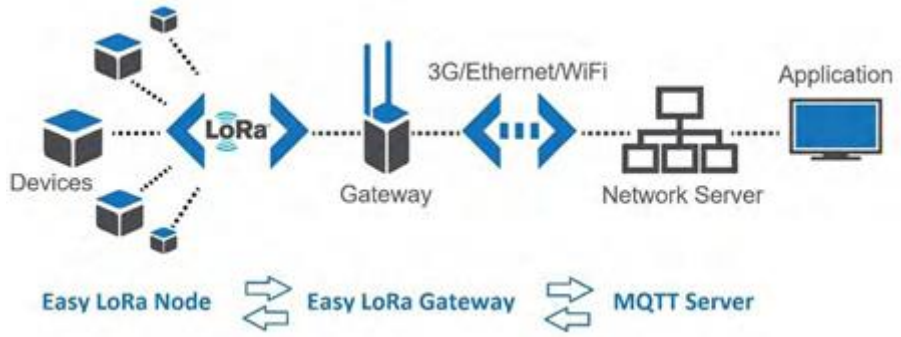
- La criptografía basada en AES (Advanced Encryption Standard) sin la llave por transmisión por el aire.
- La característica de aislar un segmento del entorno ante posibles ataques para su revisión. (Universidad de Quintana Roo, 2021)

En un segundo apartado en la seguridad del entorno Sigfox, se opera un apartado donde cada dispositivo es el principal punto de entorno para su interacción con el usuario. La seguridad está basada en 3 niveles que van desde el nivel medio hasta el nivel muy alto:

Nivel medio: En este nivel, las credenciales correspondientes a la seguridad son almacenadas en el dispositivo.
Nivel alto: En este nivel, las credenciales correspondientes a la seguridad son almacenadas en un área protegida basada en el software.
Nivel muy alto: En este nivel, las credenciales correspondientes a la seguridad son almacenadas en un elemento que sea seguro. (Universidad de Quintana Roo, 2021)

4.3 LoRa

Figura 6. *LoRa*



Fuente: He, N. (2024, 2 febrero)

LoRa (Long Range) de la Figura 6, es una tecnología inalámbrica similar a WiFi, Bluetooth, LTE, SigFox o Zigbee; el cual emplea un tipo de modulación en radiofrecuencia patentado por Semtech, una importante empresa fabricante de chips de radio. La tecnología de modulación se denomina Chirp Spread Spectrum (o CSS) y se emplea en comunicaciones militares y espaciales desde hace décadas.

LoRa utiliza una modulación de amplio espectro. El uso de este tipo de modulación permite una mejor tolerancia al ruido y de esta forma alcanzar largas distancias con un consumo muy bajo de energía, LoRa es el protocolo a Nivel de capa física (Capa OSI Nivel 1).
En la actualidad, la tecnología LoRa está administrada por la "LoRa Alliance", quien certifica a todo fabricante de hardware que desee trabajar con esta tecnología. (CatSensors. s. f.)

Ventajas:

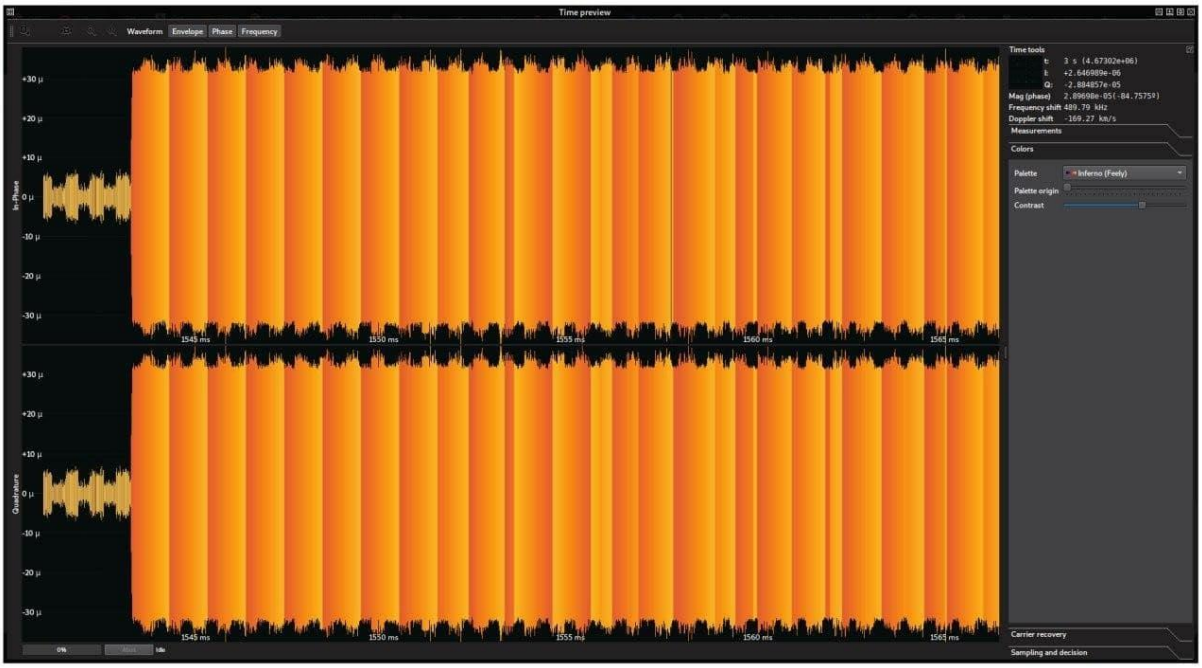
- Alta tolerancia a las interferencias
- Alta sensibilidad para recibir datos (-168dB)
- Basado en modulación "chirp"
- Bajo Consumo (hasta 10 años con una batería)
- Largo alcance 10 a 20 km
- Baja transferencia de datos (hasta 255 bytes)
- Conexión punto a punto
- Frecuencias de trabajo: 868 Mhz(Megahercio) en Europa, 915 Mhz en América, y 433 Mhz en Asia

LoRa permite conexiones a grandes distancias, es muy utilizada en redes IoT las cuales utilizan sensores que no dispongan de corriente eléctrica de red, teniendo grandes aplicaciones como, por ejemplo:

- Smart Cities (ciudades inteligentes)
- Lugares con poca cobertura (en el campo agrícola o ganadera)
- Construir redes privadas de sensores y/o actuadores.

A continuación, se describe el ejemplo de una ráfaga LoRa, como se muestra en la Figura 7, capturada cerca de los 868 MHz. Los colores indican la frecuencia instantánea, desde la más baja (naranja) hasta la más alta. Las rampas ascendientes del principio se las conoce como upchirps, las cuales forman parte del preámbulo y son utilizadas para sincronizar el reloj del receptor con el transmisor. Las únicas dos rampas descendientes de las tramas se las conoce como downchirps, y separan el preámbulo de los contenidos de la trama.

Figura 7. *Ráfaga LoRa*



Fuente: Carracedo, G. (2023c, enero 17)

LoRa es una tecnología patentada de comunicación inalámbrica en el que intervienen un consumo super bajo de energía juntamente a un largo alcance de manera efectiva.

LoRa utiliza una modulación de espectro ampliado con características muy similares a las de modulación por desplazamiento de frecuencia. En la actualidad la tecnología LoRa se ha destacado por su aumento notable en el rango de comunicaciones.

La principal ventaja que define a tecnología es poder lograr comunicaciones de largas distancias (km). También cuenta con una gran solidez frente a las interferencias. Estas frecuencias han sido utilizadas por años en comunicaciones espaciales y militares. LoRa ha intentado mantenerse con un costo inferior en el sector comercial a comparación con otras tecnologías.

Es ideal para redes loT ya que sus sensores no necesitan de corriente eléctrica de red para poder operar. Por esta razón es perfecta para poder construir redes privadas de sensores en sectores con muy baja cobertura.

4.4 LoRaWAN

Comparándola con una red Ethernet se puede ejemplificar que LoRa son los cables que conectan los dispositivos en una red Ethernet y LoraWAN es la comunicación que tienen los dispositivos a nivel de la dirección MAC (Media Access Control) y de la dirección IP (Internet protocol) de red de los dispositivos en una red de Ethernet.

El protocolo LoRaWAN es un protocolo de red que utiliza la tecnología LoRa, para redes de baja potencia y área amplia. Este protocolo se compone de gateways y nodos, siendo los primeros los que se encargan de enviar y recibir información a los nodos y estos los dispositivos finales que reciben y envían información al Gateway. (Telefónica. 2023, 18 julio).

4.4.1 Elementos en una red LoraWan:

La tecnología LoRaWAN se encuentra compuesta de los siguientes elementos:

Nodos (End points): Son los dispositivos finales que envían o reciben datos a través de la conectividad LoRaWAN, por medio de sensores, actuadores o trackers.

Gateway: Es el dispositivo al cual se conecta cada nodo por medio de LoRaWAN y permite una comunicación de cada uno de estos con el Servidor de Red.

Servidor de Red: Es donde se encuentra alojado el software que permite el control de la red y la lógica de comunicaciones entre los nodos y el Gateway, de esta manera se evita un duplicado de paquetes de información y el acceso de cada uno de los dispositivos. El servidor de red en algunos casos se encuentra alojado en el mismo Gateway, trayendo como ventaja el bajo costo en la solución total y su principal desventaja es que limita la escalabilidad.

Aplicación de servidor: Es el software que opera con la información que permite la comunicación a través de LoRaWAN, este software es completamente independiente de la red LoRaWAN y dependiendo del servidor de aplicación se podrá tener una comunicación por ejemplo con MQTT, Modbus TCP, API REST, entre otros.

Según su consumo los dispositivos LoRaWAN se clasifican en las siguientes clases:

Clase A: Son dispositivos que tienen un máximo ahorro de energía, se encargan de enviar datos solo cuando es estrictamente necesario, luego de enviar espera unos segundos para poder recibir información del Gateway, luego de esto si no existe más peticiones, pasa a modo reposo, permitiendo que los dispositivos se puedan comunicar durante varios años sin necesidad de tener que cambiar de batería.

Clase B: En este nivel se puede configurar en cada dispositivo el tiempo de mensaje de recepción, si ya tuvo respuesta pasa a modo reposo.

Clase C: Son los dispositivos que necesitan estar conectados siempre a una fuente de alimentación ya que se encuentran activos de manera constante.

4.4.2 Cálculo del tiempo de la carga útil de la batería

En los nodos LoRaWAN el tiempo de la carga útil de una batería puede depender de varios factores como: la temperatura, el número de muestras, el entorno, la frecuencia, el factor de expansión, etc; por eso no es fácil determinar el tiempo de carga.

En la Tabla 2 se puede determinar un ejemplo de la estimación en años de la vida útil de la batería utilizando un factor de expansión de 7 y una muestra de X minutos. El factor de expansión 7 nos permite tener una mayor vida útil de la batería ya que consume menos energía en modo de espera en comparación con la energía utilizada durante la transmisión.

En el caso que necesitemos transmitir datos con mayor frecuencia debemos elegir un factor de expansión más alto como 12, esto permite transmisiones más frecuentes pero una vida útil de la batería más corta.

Tabla 2. *Carga de Batería*

Ciclo en minutos	Factor de expansión	Años
10	7	3
60	7	7
1440	7	11

Fuente: El autor

4.4.3 Spreading factor (Factor de expansión)

En LoraWAN se puede configurar como deseamos que los datos sean transmitidos, si deseamos tener un mayor alcance o si lo que necesitamos es permitir una mayor tolerancia en ambientes con mucho ruido, ejemplificando con el lenguaje del habla, es como si estuviéramos deletreando, el spreading factor puede ir desde SF7 a SF12 de menor a mayor esparcimiento.

La fundación LoRa Alliance es la empresa que certifica que los dispositivos LoRaWAN puedan ser compatibles entre sí, pero debemos considerar que no todos los dispositivos son compatibles ya que depende también de la ubicación geográfica las bandas de frecuencia que se deben utilizar. Como se indica en la Tabla 3 en América la banda que se utiliza es la misma banda similar a la asignada a Australia 915-928 Mhz, por eso es importante antes de adquirir los dispositivos saber en qué banda pueden operar para luego no tener complicaciones.

Tabla 3. *NB-IoT*

Región	Banda MHz
Asia	433
Europa, India, Rusia, África	863-870
Estados Unidos	902-928
Australia	915-928
Canadá	779-787
China	470-510

Fuente: El Autor

4.4.4 Gateway LoRaWAN

Un Gateway puede trabajar con varios canales de manera simultánea, es por esta razón que puede conectarse con varios nodos a la vez.

Existen Gateways Full Duplex o half dúplex, este último no puede recibir datos mientras transmiten, esto se debe a que por lo general el Gateway no envía datos a los nodos, sino al caso contrario. Cabe recalcar que el RSSI es el indicador de intensidad de la señal recibida y el SNR es la relación señal ruido.

Carga de los recursos de la Gateway

Al utilizar el Network Server, una de las mayores limitaciones que se tendrá es la cantidad de datos que se comunica desde los Nodos LoraWAN al Application Server.

En LoRaWAN no se puede determinar la cantidad de nodos que pueden conectarse a un Gateway, ya que mucho depende de los factores de variabilidad como la distancia, obstáculos, interferencia y topografía, además de la capacidad de procesamiento y almacenamiento del gateway.

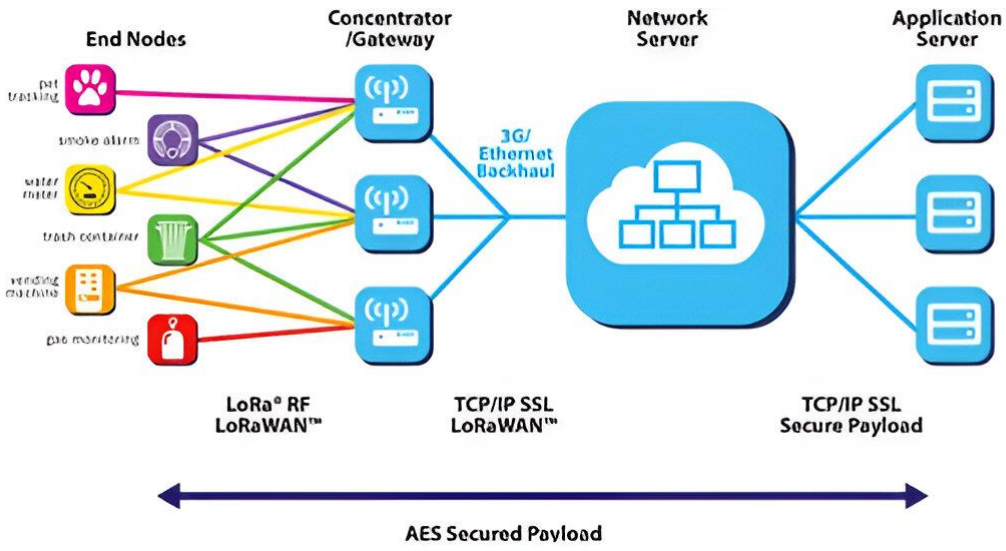
4.4.5 Network Server

El network server que se muestra en la Figura 10, permite la administración de la red LoRaWAN de una manera centralizada o descentralizada, además permite definir la escalabilidad que se puede tener en un futuro.

El network server se encuentra alojado en un servidor diferente a donde se encuentra los gateways, esto ayuda a mantener una configuración de manera sencilla y una alta escalabilidad, para proyectos grandes el costo de la implementación siempre será alto, pero se facilitará en la manera como se lo administre.

El network server permite trabajar directamente con los datos desde la Gateway, siendo una gran ventaja a futuro y permitiendo abaratar costos en la administración y mantenimiento del mismo.

Figura 8. *Network Server*



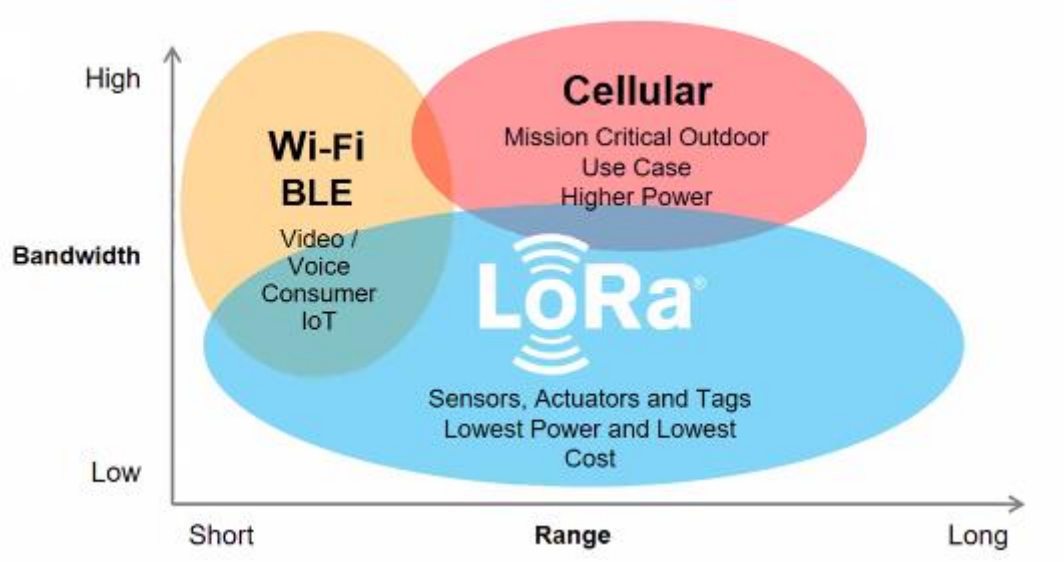
Fuente: Yujiannet. (s. f.)

Una de las desventajas de LoRaWAN es las limitaciones con la tecnología,

dependiendo de varios factores como la distancia, ancho de banda y el consumo de energía, debemos utilizar la tecnología acorde para poder resolver los problemas que se nos puedan presentar.

En la Figura 10, se puede apreciar la tecnología que debemos utilizar acorde a la distancia que tengamos.

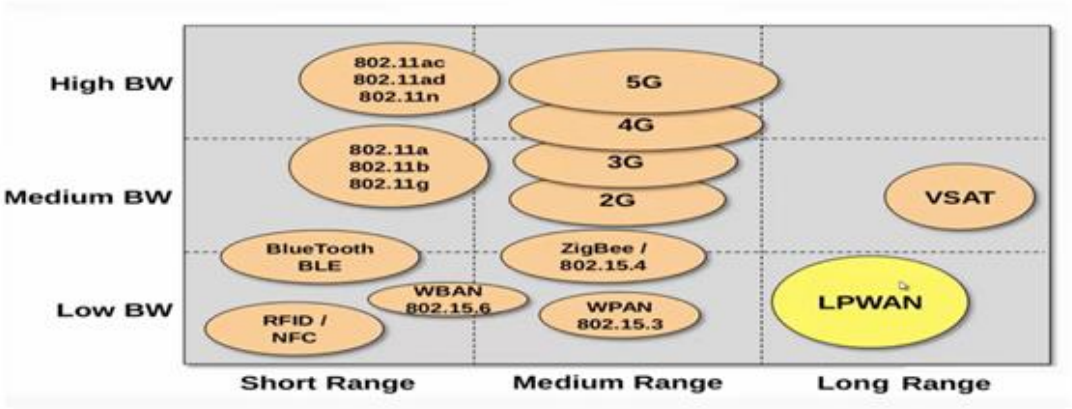
Figura 9. *Tecnologías LoRaWAN*



Fuente: Aprendiendoarduino, P. (2022, 7 marzo)

En la Figura 12, se puede apreciar la tecnología que debemos utilizar de acuerdo al ancho de banda con el que contemos.

Figura 10. *Tecnología según ancho de banda*



Fuente: Wang, A. (2023, 14 junio)

De la Figura 11 y Figura 12, podemos llegar a la conclusión que LoRaWAN es una

tecnología pensada para comunicar dispositivos que no necesitan un gran ancho de banda y que su distancia entre sí es corta.

Las redes LoRaWAN se encuentran conectadas por medio de una topología tipo estrella en la que uno o varios nodos finales se comunican con uno o más mediante LoRa PHY. La información que se recibe de parte de las pasarelas LoRa se envía a los servidores de aplicación a través de la red de retorno, estas responden por medio de las tramas recibidas. LoRaWAN adicional ofrece servicios de integridad, confidencialidad y autenticación, mediante AES128.

Quien se encarga de gestionar el acceso a la red es un servidor de red el cual se ubica entre las pasarelas y los servidores de aplicación, permitiendo eliminar paquetes duplicados, ajustar tasas de transmisión y determinar la mejor pasarela para enviar una respuesta de los servidores de aplicación.

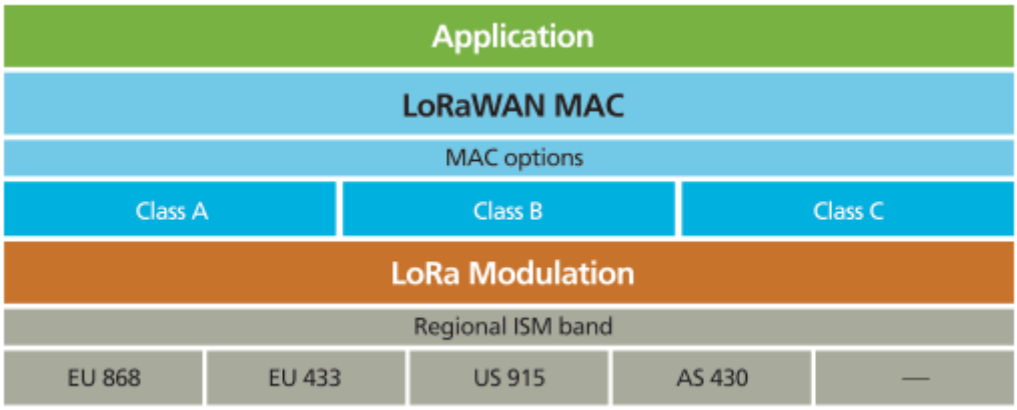
Por medio de esta arquitectura, el servidor de red a veces se desacopla en el servidor de unión (Join Server), el cual es el encargado de definir quién tiene acceso a la red y de gestionar el resto de servicios MAC como se muestra en la Figura 13.

Los distintos elementos que integran la red hacen necesaria la existencia de una serie de identificadores que permitan diferenciarlos de los demás. Estos identificadores son:
DevEUI: identificador de 64 bits, único para cada dispositivo final y gestionado por el fabricante.

AppEUI: identificador de 64 bits, gestionado por el operador de los servidores de unión y que identifica los distintos servidores de aplicación en el otro extremo de la red.

DevAddr: identificador de 32 bits, gestionado por el servidor de red, que identifica unívocamente a un dispositivo final que ha completado el procedimiento de activación en la red. De forma análoga a las direcciones IP, hasta 24 de los bits más significativos del DevAddr componen el identificador de red (NetID) y es asignado por la LoRa Alliance. Este identificador permite aprovechar la cobertura de otras redes para acceder a la red deseada mediante mecanismos de roaming. (Carracedo, G. - 2023, 17 enero).

Figura 11. *Jerarquía de capas de la red*



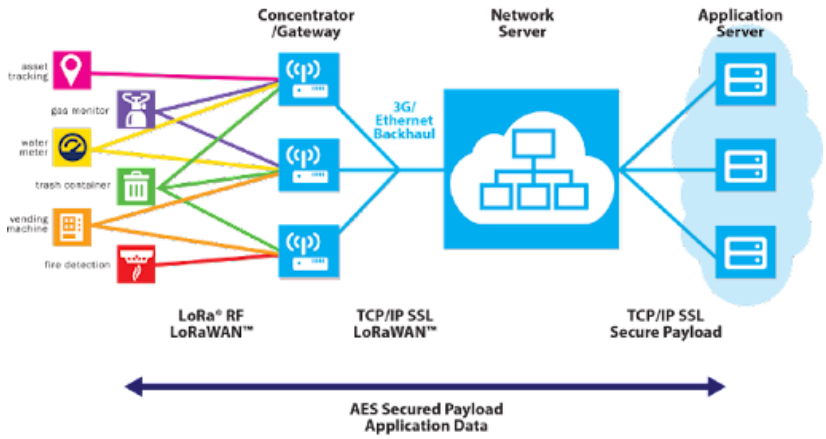
Fuente: (Aprendiendoarduino, P. 2022, 7 marzo)

4.5 Arquitectura LoRaWAN

La arquitectura que define a una red LoRaWAN consiste en que por medio de la tecnología LoRa los dispositivos finales se puedan comunicar por medio del Gateway con las puertas de enlace. Estas puertas de enlace envían las tramas LoRaWAN que no han sido procesados de los dispositivos hacia un servidor de red por medio de una interfaz de retorno que tenga un rendimiento superior, esta puede ser 3G o Ethernet.

Las puertas de enlace son solo conversores de protocolos, que permiten que el servidor de red responsable pueda decodificar los paquetes enviados por los dispositivos y generar paquetes que tienen que ser enviados de vuelta a los dispositivos. Como se muestra en la Figura 14, existen tres clases de dispositivos finales LoRa, que difieren respecto a la programación del enlace descendente.

Figura 12. *Clases de dispositivos LoRa*



Fuente: (LoRaWAN 2019, 22 octubre)

Elementos que conforman una red LoRaWAN:

Dispositivo o mota: Tiene un consumo muy bajo de potencia y permite realizar la medición de información en el lugar donde se implante.

Red: Es el camino de comunicación que permite el envío de mensajes recibidos por los nodos y enviados a la aplicación.

Gateway: Es el dispositivo capaz de enviar y recibir información a los diferentes nodos. Conocido como puerta de enlace que establece la comunicación entre nodos y dispositivos, para poder retransmitir a Internet y tener una visualización de información desde cualquier lugar.

Aplicación: Es el dispositivo capaz de gestionar un software que permita interpretar datos y hacer lectura de la información recibida por parte del Gateway.

Mensaje de enlace ascendente: Es el envío de información que se realiza desde un determinado dispositivo a la aplicación.

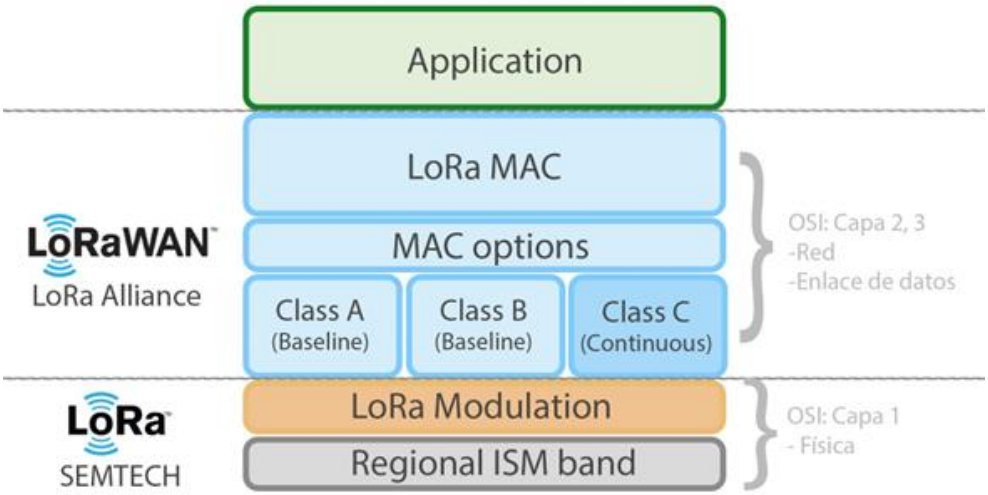
Mensaje de enlace descendente: Es el envío de información que se realiza desde una determinada aplicación a un dispositivo.
Ventajas:

- Conexiones bidireccionales seguras mediante encriptación de extremo a extremo
- Bajo consumo de energía (duración de las pilas hasta 10 años)
- Largo alcance de comunicación (10 - 20 km)
- Conexión de infinidad de sensores y equipos a redes públicas o privadas (hasta 1 millón de nodos en red)
- Bajas velocidades de datos
- Baja frecuencia de transmisión, movilidad y servicios de localización
- Interoperabilidad de las diversas redes LoRaWAN en todo el mundo
- El coste de los dispositivos LoRaWAN es asequible para cualquier proyecto
- Curva de aprendizaje rápida.

- Ofrece un nivel alto de seguridad entre los dispositivos de la red, desde los nodos hasta el servidor de aplicaciones.

LoRaWAN es un protocolo de comunicación, que va sobre la capa física LoRa a nivel de red (Capa OSI Nivel 2,3), como se puede ver en la Figura 8, el protocolo de comunicación LoRaWAN es abierto, esto permite que varios fabricantes puedan desarrollar e implementar dispositivos y de esta forma abaratar los costos en el mercado.

Figura 13. *LoRaWAN*



Fuente: (Telefónica. 2023, 18 julio)

Permite a los desarrolladores y empresas conectar varios objetos inteligentes sin tener la necesidad de instalaciones locales complejas, además otorga una amplia libertad de uso para el usuario final.

4.6 NB-IoT (Narrow Band IoT)

La red NB-IoT de la Figura 9, forma parte de las redes del tipo LPWA (Bajo Consumo Área Extensa), de baja potencia y ancho de banda estrecho, el cual permite operar en zonas amplias. El objetivo de esta tecnología móvil es tener en cuenta las diferentes necesidades de conectividad ya que su diseño permite la comunicación de dispositivos de internet de las cosas y brinda soporte a equipos que realizan bajos volúmenes de transferencia de datos durante largos periodos de tiempo, especialmente en sitios con un acceso difícil.

Esta tecnología de red fue desarrollada por 3GPP, para dar soluciones de conectividad al crecimiento de IoT, en lo que se denomina eMTC (extended Machine Type

Communications), ofrece una amplia cobertura de red de manera estable con una alta densidad de conexiones**.** La NB-IoT tiene la ventaja de conectarse sin inconvenientes en redes móviles ya establecidas**.**

Desde 2016 NB-IoT es un estándar para las comunicaciones inalámbricas que puede intercambiar pequeñas cantidades de datos de forma eficiente a múltiples dispositivos, adicional minimiza el consumo de energía y aumenta el rango de cobertura en ubicaciones alejadas que no cuenten con la implementación de tecnologías móviles convencionales. (Telefónica. 2023, 18 julio).

La red NB-IoT está basada en tecnología LTE(Long term evolution) ya existente. Este tipo de comunicación móvil ofrece conexiones con menor número de interferencia y una buena cobertura**,** ya que permite operar en frecuencias que no han sido utilizadas por redes de comunicaciones existentes.

A continuación, se describen algunas aplicaciones NB-IoT:

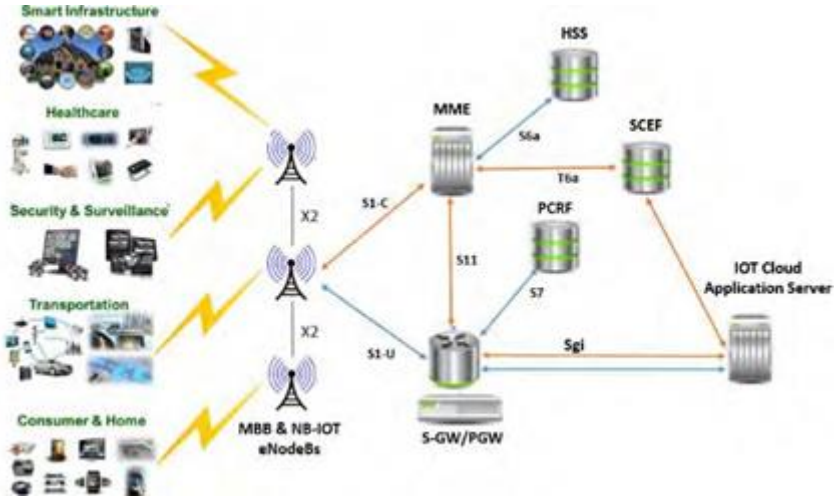
- Agricultura y Ganadería
- Cuidado de la Salud
- Seguimiento de personas y animales
- Manufactura y Logística
- Ciudades inteligentes

Este tipo de sistemas de conexión están compuestos por dispositivos y sensores fabricados con la finalidad de poder recopilar información del entorno en el que se encuentran instalados y poder transmitir a estaciones base o nodos NB-IoT. Una de sus principales ventajas es que, al estar diseñada para poder operar con una potencia de transmisión muy baja, la batería de los dispositivos IoT alcanzan una vida útil mucho más amplia porque los consumos de energía son bajos y la cobertura es mucho más amplia.

Es una tecnología de bajo costo, por lo que pequeñas empresas y organizaciones públicas las utilicen para poder acceder a una cobertura de largo alcance. En zonas rurales y de difícil acceso se puede tener un gran número de dispositivos conectados por IoT.

Las tecnologías, NB-IoT y LTE-M, son buenas alternativas de conectividad ya que están diseñadas para aplicaciones de IoT, la diferencia se encuentra en su cobertura, ancho de banda, velocidad de transmisión de datos y eficiencia energética. Dependiendo de los requisitos específicos del dispositivo y el tipo de aplicación utilizada, una tecnología puede resultar más acorde que otra red.

Figura 14. *NB-IoT*



Fuente: (Techplayon 2020, 23 julio)

De los dos estándares, NB-IoT es el estándar menos potente en cuanto a soporte para móviles, velocidad y capacidad de transmisión de datos. Está diseñada para lugares o sitios donde no se necesita tener una comunicación móvil de gran exigencia, y para aplicaciones que utilicen pequeñas cantidades de datos y que requieren transmisiones de baja velocidad, en cambio el estándar LTE-M permite manejar una amplia gama de aplicaciones de IoT**,** desde dispositivos de bajo consumo de energía y baja velocidad, hasta dispositivos de alta velocidad y gran ancho de banda. Por ello LTE-M se considera una mejor opción para lugares urbanos con una mayor población, en la cuales encontramos un mayor número de estaciones base, la diferencia está en que, aunque consume muy poca energía, no es tan eficiente como la NarrowBand-IoT.

4.7 Seguridad en redes IoT

La seguridad en IoT es el acto de proteger los dispositivos de Internet y las redes a las que están conectados frente a amenazas e intrusiones de personas que no estén autorizadas a su utilización; la seguridad permite monitorear, proteger e identificar los riesgos, además permite corregir vulnerabilidades de los dispositivos conectados a la misma red que puedan

representar algún riesgo de seguridad para la empresa. (Fortinet. s. f.).

En un inicio los dispositivos IoT no fueron creados pensando en la seguridad, lo que trajo posibles vulnerabilidades en un sistema de múltiples dispositivos. En la mayoría de los casos, no hay manera de instalar software de seguridad en el dispositivo, por lo que nació la necesidad de poder dar seguridad de otras maneras. En ocasiones el dispositivo a instalar ya viene infectado con algún malware que puede infectar la red a la que se los conectan.

En la actualidad aún existen redes IoT que no cuentan con un nivel de seguridad o detección de todos los dispositivos que se encuentran conectados o se comunican dentro de la misma red.

Una estructura de seguridad holística permite tener una seguridad que pueda cumplir con visibilidad, segmentación y protección en toda la infraestructura de red.

Para esto se debe cumplir con las siguientes capacidades:

Conocer: Las soluciones de seguridad deben autenticar y clasificar los dispositivos de IoT para poder crear un perfil de riesgo y asignar a los grupos de dispositivos de IoT.
Segmentar: Se pueden segmentar en grupos IoT impulsados por políticas con base en los perfiles de riesgos.
Proteger: Los grupos de IoT deben permitir el monitoreo, inspección y ejecución de políticas impulsados por políticas y segmentación de la red interna.

4.8 IoT en la Nube

Los dispositivos IoT y las redes de computadoras en la nube se complementan entre sí, permitiendo trabajar juntos para brindar un mejor servicio de IoT de manera general. Sin embargo, difieren en lo que hace que cada uno de ellos por lo que se debe considerar una solución técnica y eficaz por separado y en conjunto al mismo tiempo.

Cloud Computing permite almacenar datos de IoT en la nube, este es un servidor centralizado que dispone de recursos informáticos a los que se puede acceder de una manera fácil cada vez que sea necesario a través de Internet.

IoT y Cloud Computing conjuntamente permiten que los sistemas se automaticen de una manera rápida, eficiente y rentable permitiendo el control y el monitoreo de datos en tiempo real.

Big Data y Cloud Data son dos herramientas que se pueden usar en conjunto para almacenar grandes cantidades de datos y proporcionar un análisis de datos en tiempo real. En las empresas una de las falencias es el alto costo que se necesita para que este tipo de infraestructura física puedan funcionar juntos, pero la gran ventaja que ofrece es sobre la capacidad analítica a la larga permite reducir costos ya que no se necesita estar preocupándose por el mantenimiento y soporte del mismo.

Las principales ventajas que ofrece son:

- Mayor eficiencia en las tareas diarias
- IoT y Big Data generan una gran cantidad de información y la nube proporciona el camino para que viaje esta información.
- Uso y distribución más rápidos de las aplicaciones por todo el mundo
- Se puede acceder a la información en la Big Data de forma remota y sencilla desde cualquier parte del mundo para seguir utilizando y realizando acciones en los dispositivos cuando utilizan la nube, lo que permite una mejor colaboración.
- Avance en el análisis y revisión del estado de los dispositivos IoT conectados.

Ya no se necesita el uso de servidores físicos centrales, sino solo una conexión a internet y apuntar los diferentes dispositivos hacia allá creando una necesidad de contar con dispositivos inteligentes para enviar datos a los servidores para su procesamiento. La gran ventaja es que se puede acceder desde cualquier lugar con conexión a internet y dentro de nuestra red, permitiendo una respuesta más rápida al tiempo de inactividad y predecir cuándo pueden ocurrir errores. El uso de la nube con IoT ayuda a mejorar la seguridad, ya que se puede mantener actualizado de manera periódica cualquier brecha en la infraestructura que se pueda tener.

Beneficios de las economías de escala

Nos ayuda a preservar el valor comercial con un almacenamiento y una administración efectiva de nuestra Big Data e IoT en la nube, nos brinda el uso de herramientas de administración integradas, mejor capacidad de procesamiento y múltiples aplicaciones que nos permitirá administrar de una mejor manera los recursos.

El uso conjunto de Big Data, IoT y la nube significa que se puede tener una conexión, comunicación, y transferencia de datos exitosos entre varios dispositivos, de la manera más eficaz y efectiva.

5. Metodología

La seguridad es una necesidad fundamental en todas las aplicaciones, pero vamos hacer énfasis en la seguridad que debe existir en los tipos de red utilizando el protocolo LoRaWAN, esto debido al crecimiento de la conexión que existe a nivel mundial y que estamos experimentando en dispositivos IoT, los cuales cada día aumentan de forma constante. De la misma forma aumenta la problemática en la seguridad que debe existir en este tipo de dispositivos y la forma de comunicarse, ya que por medio de estos dispositivos y conexión se intercambia información confidencial a través de internet. El tema de seguridad abarca múltiples propiedades como son, los mecanismos criptográficos, firmware, actualizaciones de seguridad, etc. El presente trabajo tiene como objetivo mostrar la seguridad con la que en la actualidad se maneja LoRaWAN. Primero, indicaremos las propiedades de seguridad que vienen incluidas con la especificación LoRaWAN, luego los detalles que mantiene en su implementación y finalmente algunas definiciones sobre el diseño de seguridad en LoRaWAN. La seguridad de LoRaWAN está diseñada para acoplarse a los criterios generales de diseño como son: bajo consumo de energía, baja complejidad de implementación, alta escalabilidad y bajo costo.

5.1 Seguridad en redes LoRaWAN

La seguridad en LoRaWAN está establecida por la implementación de medidas que permitan proteger la información transmitida a través de la red. Para esto es importante utilizar medidas como el cifrado y firmas en paquetes de datos. Para llevar a cabo un cifrado exitoso, se debe emplear claves simétricas que sean compartidas entre los nodos finales y los servidores de red y de aplicaciones. Este tipo de claves se pueden distribuir de dos maneras diferentes según el método de activación utilizado: activación por aire (OTAA) y activación por personalización (ABP).

Estos métodos de activación nos permiten asegurar un alto nivel de seguridad al utilizar un cifrado simétrico durante el intercambio de mensajes entre los nodos finales y los servidores. Estos mecanismos utilizados permiten eliminar la posibilidad de que un atacante pueda introducir nodos finales maliciosos o aprovechar el mal uso de la red durante el proceso de activación sin conocer las claves utilizadas en los nodos finales. LoRaWAN incluye diferentes capas de cifrado, haciendo uso del algoritmo AES-128 para proteger las comunicaciones de

datos:

Clave de Sesión de Red (Network Session Key): Es una clave compuesta de 128 bits la cual garantiza la seguridad a nivel de red.
Clave de Sesión de Aplicación (Application Session Key): Es una clave compuesta de 128 bits que garantiza la seguridad de extremo a extremo.
Clave de Aplicación (Application Key): Es una clave compuesta de 128 bits utilizada en despliegues con activación por aire (OTAA).

En periodos largos de tiempo en los dispositivos que se encuentran desplegados en el campo, la seguridad debe estar a prueba de cambios futuros. El diseño de seguridad de LoRaWAN debe ajustarse a principios diseñados dentro del estado del arte el cual describe el uso de algoritmos estándar bien examinados y una seguridad de punto a punto.

Los dispositivos auténticos y autorizados se unirán a redes auténticas y genuinas cuando exista una autenticación mutua entre un dispositivo final LoRaWAN y la red LoRaWAN como parte del procedimiento de conexión a la red.

La MAC LoRaWAN y los mensajes de la aplicación son autenticados y protegidos desde su origen, integridad y respuesta mediante el método de encriptación. Esta protección, permite que intrusos no puedan capturar la información y reproducirla fraudulentamente gracias a la autenticación mutua, la cual garantiza que el tráfico de la red no sea alterado, y que provenga de un dispositivo legítimo.

El encriptado de punto a punto es una fortaleza de la seguridad de LoRaWAN para la comunicación con aplicaciones en servidores o entre dispositivos.

LoRaWAN permite un encriptado de extremo a extremo siendo una de las pocas redes de IoT que brindan este beneficio. En unas cuantas redes celulares tradicionales, el tráfico se encripta a través de una interfaz vía aérea, pero al momento de transportarla se envía como texto simple en la red central del operador. Por esta razón, a los usuarios finales se les complica en el momento de poder seleccionar, implementar o administrar una capa de seguridad adicional generalmente por medio de una VPN o seguridad de encriptación.

Este enfoque en redes LPWAN genera un consumo considerable de energía adicional, complejidad y costo.

5.1.1 Implementación de la seguridad

Los mecanismos anteriormente mencionados de seguridad son basados en algoritmos criptográficos AES los cuales son probados y estandarizados.

La comunidad criptográfica analiza durante muchos años este tipo de algoritmos, los cuales son aprobados por el NIST (Instituto nacional de estándares y tecnología), siendo consideradas entre las mejores prácticas de seguridad para redes y nodos restringidos. La seguridad LoRaWAN utiliza una primitiva criptografía AES, la cual se combina con varios nodos de operación: CMAC para protección de integridad y CTR para encriptación.

En los dispositivos LoRaWAN las claves se personalizan por medio de AES de 128 bits (llamada AppKey) y un identificador global único (DevEUI basado en EUI-64), estos componentes se utilizan durante el proceso de autenticación del dispositivo. Se puede asignar identificadores EUI-64 los cuales requieren que el asignador tenga un Identificador Único de la Organización (OUI) y de la Autoridad de Registro IEEE. En cambio, las redes LoRaWAN se pueden identificar mediante un identificador único global generado de 24 bits, el cual es asignado por LoRa Alliance.

El dispositivo final y el servidor de aplicaciones permite tener cifrada la información gracias a los datos de la aplicación LoRaWAN. La protección de integridad se realiza de salto por salto, es decir un salto por el aire a través de la protección de integridad la cual es proporcionada por medio del protocolo LoRaWAN y el otro salto se realiza entre la red y el servidor de aplicaciones, haciendo uso de soluciones de transporte seguro como HTTPS y VPN.

5.1.2 Autenticación mutua

El procedimiento de conexión de la activación por aire permite demostrar que tanto el dispositivo final como la red tienen el conocimiento de la AppKey. Esta prueba se la ha podido realizar mediante el cálculo de un AES-MAC4 (usando la AppKey) en la solicitud de conexión del dispositivo y por el último receptor.

Como se muestra en la Figura 15, luego en la autenticación mutua se derivan dos claves

de sesión, una para proporcionar protección de integridad y encriptación entre comandos MAC de LoRaWAN y la carga de la aplicación, y otra para la encriptación de punto a punto de la carga de la aplicación. La NwkSKey se distribuye a la red LoRaWAN permitiendo verificar la autenticidad de los paquetes enviados y la integridad de los mismos. En cambio, la AppSKey se distribuye al servidor de aplicaciones para cifrar y descifrar la carga útil de la aplicación. De esta manera la AppKey y AppSKey se pueden ocultar del operador de red para que no pueda descifrar las cargas útiles de la aplicación.

La autenticación mutua garantiza la seguridad del nodo en la red, esta se puede activar por aire (OTTA) y por activación por personalización (ABP), el nodo y el servidor d red deben conocer la AppKey cuya clave es de 128 bits (AES 128) y el DevEUI que es un identificador.

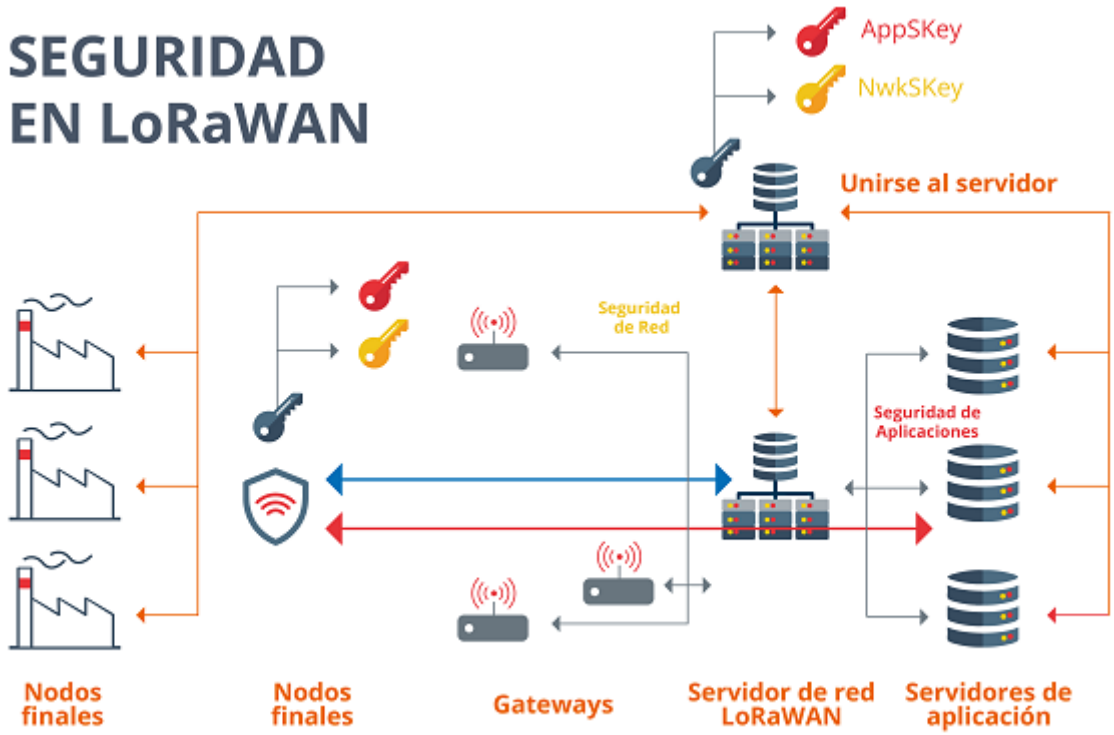
En la aplicación la capa de seguridad protege los datos del usuario final, lo que evita que el operador de red no tenga acceso a la información, esto se logra gracias al protocolo HTTPS o conexiones VPN (redes virtuales privadas).

AES128 es un estándar avanzado de encriptación por bloques, que se encuentra basado en el protocolo LoRaWan, aquí se establece dos tipos de clave detalladas:

Network Session Key: Esta clave es enviada al servidor de red, el cual protege el contenido de los mensajes MAC que se encuentran en el interior del paquete.

Application Session Key: Esta clave asegura una conexión de extremo a extremo, es decir una vez que llega al servidor, se protege en los aplicativos.

Figura 15. *Autenticación Mutua*



Fuente: INCIBE. (s. f.)

5.1.3 Integridad de datos y protección

El tráfico de LoRaWAN se encuentra protegido por medio del uso de dos claves de sesión.

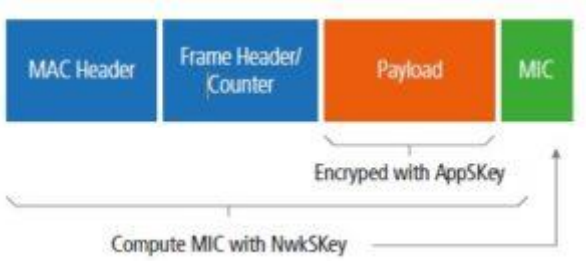
Como se muestra en la Figura 16, cada carga útil (payload) está encriptada por medio de AES-CTR, el cual lleva un contador de cuadros para de esta manera evitar la reproducción del paquete y adicional un código de integridad del mensaje (MIC), el cual es calculado por medio de AES-CMAC para evitar la manipulación indebida de paquetes.

La integridad se logra al agregar un código MIC, este se calcula utilizando un algoritmo AES-CMAC con la clave NwkSKey en todos los campos del mensaje. Por esta razón el dispositivo y el servidor de red utiliza el campo MIC para verificar la integridad de los datos. Mediante el cifrado se consigue la confidencialidad hasta el servidor de aplicación usando una clave de sesión.

Para proteger la integridad de los datos se utiliza un cifrado de extremo a extremo, de esta manera se protege las comunicaciones entre los nodos y el servidor, lo que evita la

interceptación y manipulación de datos; LoRaWAN utiliza técnicas de autenticación y autorización para garantizar que solo nodos autorizados puedan acceder a la red.

Figura 16. *Integridad de Datos*



Fuente: Reimondo, G. (2019, 12 agosto)

5.1.4 Seguridad física de un dispositivo LoRaWAN

Considerando que el AppKey y las claves de sesión generadas se almacenan de forma persistente en un dispositivo LoRa Alliance, su protección depende exclusivamente de la seguridad física del dispositivo. Si el dispositivo se encuentra sujeto a amenazas físicas, las claves se pueden proteger en un dispositivo de almacenamiento a prueba de manipulaciones (a.k.a. Secure Element), donde será muy difícil de poder extraer.

La comunicación inalámbrica aprovecha las características de largo alcance dentro de la capa física de LoRa, permitiendo un enlace de un solo salto entre el dispositivo final y uno o varios gateways. En todos los modos se es capaz de ofrecer comunicación bidireccional, existiendo soporte para grupos de direccionamiento de multidifusión para hacer un uso eficiente del espectro durante tareas como actualizaciones de firmware por el aire (FOTA) u otros mensajes de distribución masiva.

Se define los parámetros de la capa física LoRa de dispositivo a infraestructura y hacia el protocolo LoRaWAN, esto permite, proporcionar una interoperabilidad perfecta entre todos los fabricantes.

Si bien la especificación define la implementación técnica, no se define ningún modelo comercial o tipo de implementación (pública, compartida, privada, empresarial) y, por esta razón, se ofrece a la industria la libertad de innovar y diferenciar cómo se la utilice. Se

desarrolla la especificación LoRaWAN mantenida por LoRa Alliance, una asociación abierta de miembros colaboradores.

5.1.5 Criptografía

LoRaWAN se basa en una criptografía simétrica, esto permite transmisiones de radio seguras, debido a las limitaciones del uso de banda ISM (industriales, científicas y médicas), que especifican que las tramas sean muy pequeñas en tamaño y número. Esto requiere una clave de raíz simétrica que sea propia para el dispositivo y se encuentre disponible en la red antes que el dispositivo intente activarse. Al definir e implementar una interfaz estándar entre NS (Network Server- Servidor de red) y JS (Join Server- Servidor de unión), hace posible que el dispositivo se puede activar en cualquier red o NS de cualquier lugar del mundo, debido a la especificación de la interfaz del backend de LoRaWAN.

La seguridad de la red es primordial en despliegues IoT y LoRaWAN en esta se define dos capas de criptografía:

- Una única clave de sesión de red de 128 bit compartida por el end-point y servidor de red
- Una única clave (AppSKey) de aplicación de 128 bit compartida end-to-end y la capa de aplicación

5.1.6 Distribución de la llave (key) de sesión

A partir de la misma AppKey se genera el AppSKey y NwkSKey, por tal motivo se argumenta que, si el operador LoRaWAN tiene la AppKey, puede derivar la AppSKey y, por lo tanto, descifrar el tráfico. Para poder controlar esta situación, se puede ejecutar por una entidad fuera del control del operador para que el servidor gestione la manera de almacenar el AppKey, la autenticación mutua y la obtención de claves.

Para que se pueda dar a los operadores flexibilidad adicional, en una versión futura de la especificación LoRaWAN se podrá definir dos claves maestras independientes: una para la red (NwkKey) y otra para las aplicaciones (AppKey).

Para iniciar el proceso de acceso a la red, el nodo envía un join request a la red con datos de configuración y abre una ventana de recepción que permite recibir la respuesta de

parte del GW. En el momento que el GW recibe la respuesta, se envía al servidor, en el cual se verifica que el nodo que requiere acceder a la red y la llave de encriptación sean correctos. Si la información se encuentra correcta, se otorga una sesión temporal y por medio del GW se notifica al nodo que ya se puede empezar a enviar datos a la red.

Un dispositivo debe tener credenciales que le permitan unirse a una red. Si se conoce la red LoRaWAN especifica durante la fabricación, se puede programar en el dispositivo la información de autenticación que necesita para unirse a esa red.

Sin embargo, en la mayoría de los casos de uso, el dispositivo se lo debe agregar de manera segura a una red. Por esta razón, se utiliza la autenticación inalámbrica (OTTA). Por medio de esta forma de autenticación, se puede generar solo cuando es necesario las claves de sesión de red y aplicación. Brindando a los usuarios flexibilidad de poder llevar un dispositivo a una red LoRAWAN sin saber de antemano a que red se va a conectar.

En la capa de aplicación, para una mayor seguridad se usa una clave de sesión de aplicación para cifrar y descifrar datos mientras viaja por medio del canal. Garantizando que los datos no cifrados se encuentren disponibles solo para el nodo del sensor que generó los datos y la aplicación destinada a recibirlos.

Por esta razón, LoRaWAN utiliza el cifrado AES de 128 bits, que es el estándar de la industria para comunicaciones seguras. Para poder descifrarlos se requiere el acceso a los datos de la clave de sesión. Por lo tanto, todos los dispositivos intermedios a lo largo del canal de comunicación solo pueden pasar datos, no verlos ni cambiarlos. LoRaWAN ya viene integrado con métodos de seguridad, de esta manera facilita a los desarrolladores a diseñar rápidamente sistemas seguros sin tener que implementar complejos algoritmos de seguridad.

5.1.7 Seguridad de interfaces del lado servidor

En las interfaces del backend implica que se realice el control y señalización de datos entre los servidores de red y de las aplicaciones. Las tecnologías HTTPS y VPN se utilizan para asegurar la comunicación entre elementos críticos de la infraestructura, tal como se realiza en otros sistemas de telecomunicaciones.

El servidor de red permite supervisar y gestionar una comunicación correcta. Suelen

ser plataformas basadas en la nube de la red LoRaWAN, las cuales por medio de un software de aplicación garantiza la seguridad validando la autenticidad de la identidad de los dispositivos y usuarios hacia el servidor, de esta manera se evita interferencias en la comunicación.

El servidor permite supervisar y garantizar el enrutamiento bidireccional adecuado de los datos, por medio del UPLINK se puede detectar la comunicación desde las aplicaciones LoRa a los nodos finales o viceversa desde los nodos finales a las aplicaciones.

En el servidor se debe tener las precauciones necesarias para la vida útil de la batería, de esta manera se mantendrá la integridad y la eficiencia de toda la red de comunicación sin contratiempos.

La función principal del servidor de aplicaciones es decodificar y procesar los datos transmitidos desde los nodos finales a las aplicaciones y codificar la información enviada desde las aplicaciones hacia los nodos finales, adicional permiten vincular fácilmente la administración de datos hacia la red.

5.2 Arquitectura LoRaServer

Como se muestra en la Figura 17, la arquitectura LoRaServer, es un conjunto de aplicaciones de código abierto que existen desde las pasarelas de enlace o gateways de una red LoRaWAN, estas a su vez reciben información de nodos, hasta un poco antes de que las aplicaciones reciban estos datos.

La plataforma LoRaServer, posee una arquitectura en la que cada bloque cumple un papel diferente como se detalla a continuación:

LoRa Gateway Bridge: Es el componente responsable de la comunicación con la pasarela. Este proporciona un servicio el cual transforma los datos del protocolo UDP del packet forwarder en mensajes sobre MQTT.

LoRa Server: Es el servidor de red LoRaWAN. Sus funciones son manejar las tramas de enlace ascendente recibidas de las pasarelas, manejar la capa MAC y programar las transmisiones de datos de enlace descendente.

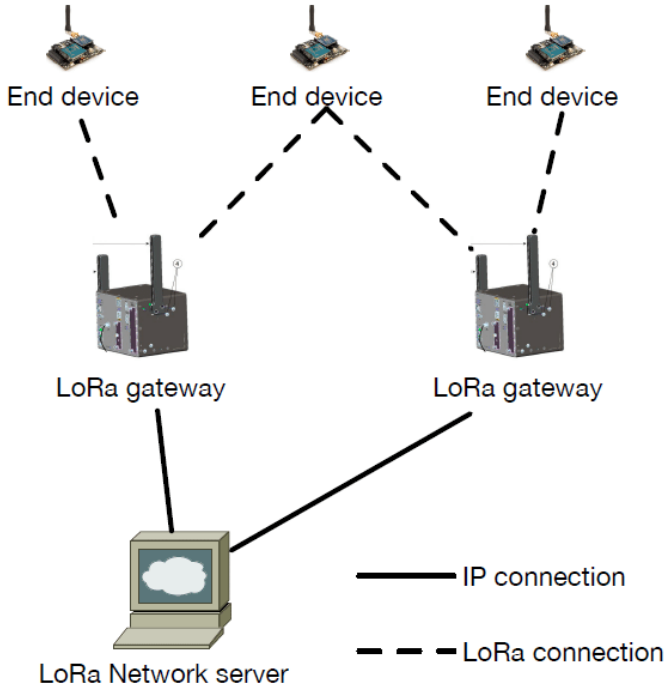
LoRa App Server: Este servidor de aplicación LoRaWAN coordina las solicitudes de unión, el cifrado de las cargas útiles de la aplicación y ofrece una API RESTful JSON, una API gRPC

o MQTT para servicios externos. Adicional, ofrece una interfaz web para que los usuarios puedan acceder y modificar sus dispositivos, puertas de enlace y aplicaciones de manera sencilla.

LoRa Geo Server: Es un elemento opcional, nos brinda servicios de geolocalización para poder ubicar cada dispositivo.

Application: Es la aplicación final que maneja las cargas útiles que envían sus dispositivos. Recibe estos datos del servidor de aplicación por medio de gRPC o JSON REST.

Figura 17. *Arquitectura LoRa Server*



Fuente: Tolocka, E. (2024, 2 enero)

El servidor de red LoRa o LoRa Server almacena todos los datos no persistentes o temporales en una base de datos Redis. Tanto el servidor de red LoRa como el servidor de aplicación LoRa utilizan otra base de datos para el almacenamiento de datos persistente.

La base base de datos que se utiliza es PostgreSQL. Una sola instancia permite almacenar varias bases de datos. Por ejemplo, una instancia de PostgreSQL nos permite almacenar la base de datos del servidor de red LoRa y también la base de datos que corresponda al servidor de aplicación LoRa.

5.3 Seguridad en 3GPP(Asociación de proyectos de tercera generación)

3GPP Es una colaboración entre organizaciones de desarrollo de estándares de telecomunicaciones, las cuales se encargan de desarrollar estándares técnicos en seguridad para redes en tecnologías móviles incluida las comunicaciones LoRaWAN.

Al integrar esta seguridad definida mediante tarjetas SIM/USIM, se aprovecha la robusta infraestructura de seguridad desarrollada para las tecnologías móviles, esto permite contribuir significativamente a mejorar la seguridad y la confiabilidad de las conexiones LoRaWAN.
La Censes International Telecom Alliance reconoce las normas 3GPP como la norma técnica mundial 5G, lo que ayuda al desarrollo de industrias y ecología relacionada con LoRaWAN, ayudando al crecimiento del comercio global de una manera estandarizada.

Algunos puntos clave de los estándares de seguridad 5G desarrollados por 3GPP son:

AES (Estándar de cifrado avanzado): Utiliza el algoritmo AES para proteger la confidencialidad e integridad de los datos transmitidos en redes 5G.

SSL/TLS: Estos protocolos de cifrado aseguran una comunicación exitosa en las redes 5G. Estándares de seguridad 5G: 3GPP, ETSI, NIST, GSMA. (2023, diciembre 9).

Dentro de 3GPP, hay proyectos como CBRS (espectro de radiofrecuencias), sin embargo, todavía están en proceso y lejos de estar listos para implementaciones de IoT a gran escala. Este modelo permite una colaboración público-privada para compartir los gastos y las ventas de la red al mismo tiempo que se densifica la red donde las aplicaciones y los servicios son más frecuentes. Dado que varias puertas de enlace aceptarán mensajes LoRaWAN, y el servidor de red elimina la redundancia, este modelo es posible.

En situaciones en las que la red es operada por varios operadores y empresas, LoRa Alliance ya ha aceptado una arquitectura de roaming que permite a los operadores compartir la red. Este modelo reduce el gasto del operador y, al mismo tiempo, proporciona un modelo de negocio transformador para implementar la capacidad de IoT donde más se necesita. Wang, A. (2023a, marzo 9).

6. Discusión

El análisis de seguridad en redes IoT caso LoRaWAN que se ha desarrollado en esta investigación ha permitido determinar las principales vulnerabilidades presentes en la tecnología SigFox. Adicional al uso de la metodología se realizó una investigación sobre vulnerabilidades en las tecnologías LPWAN similares y riesgos que pueden darse al ejecutarse un ataque a estas tecnologías. Estos desafíos de seguridad respaldan al objetivo general como específicos al descubrir las principales amenazas y como mitigarlas en estas redes IoT con la finalidad de brindar seguridad a los usuarios.

En un inicio se aborda un marco teórico referente a la evolución del Internet de las cosas y sus principales características. De igual manera se hace mención de la seguridad empleada en las principales tecnologías utilizadas dentro de las redes LPWAN con la finalidad de definir la seguridad empleada en cada una de ellas.

Se realizo un análisis de las ventajas existentes al utilizar el protocolo LoRaWAN y como se encuentra estructurado, permitiendo comprender de mejor manera como se envía y se recibe la información entre los nodos y gateways, con la finalidad de brindar mejores controles de seguridad para garantizar la confidencialidad, integridad, disponibilidad de tal modo que la red pueda ofrecer a los usuarios una plataforma de comunicación segura.

De acuerdo con el análisis de la investigación, se evaluó la efectividad de las medidas de protección existentes en la red LPWAN de acuerdo a varios casos de estudio, así como la posibilidad de que se pueda llegar a dar. Estos estudios permitieron determinar las principales amenazas y vulnerabilidades que siendo bien ejecutadas pueden lograr la no disponibilidad de la red y servicios de IoT.

Como resultado, se planteó varias mejoras y medidas concretas en la seguridad de redes LoRaWAN. Estas mejoras incluyen una gestión efectiva de claves, implementación de prácticas de cifrado sólidas. El objetivo de estas mejoras y prácticas permitirán evitar cualquier pérdida o robo importante de información de estos dispositivos, manteniendo la disponibilidad, confidencialidad e integridad de los datos.

7. Conclusiones

En la actualidad la diversidad existente de dispositivos IoT, junto con su integración en áreas críticas como la salud, la energía y la industria, resalta la necesidad urgente de tener una prevención constante en la seguridad y de esta manera poder estar protegidos tanto en la integridad, confidencialidad y disponibilidad de los datos.

Las redes LoRaWAN nos ofrece ventajas significativas en términos de alcance y eficiencia energética, pero así mismo de esta manera su entorno inalámbrico y la transmisión de datos a larga distancia nos plantean desafíos únicos en términos de seguridad, en la cual debemos dar principal énfasis en la protección contra ataques de denegación de servicio (DoS) y la interceptación de datos.

En la implementación de redes LoRaWAN existen diversas vulnerabilidades que incluyen debilidades en la autenticación de dispositivos, la gestión de claves y la falta de cifrado end-to-end, lo que podría exponer la red a ataques de intrusión y comprometer la privacidad de los datos.

Se concluye que para fortalecer la seguridad en redes LoRaWAN se debe tener una gestión efectiva de claves y la implementación de prácticas de cifrado sólidas que se realicen de manera constante por parte de profesionales adecuados y de esta manera evitar cualquier pérdida o robo de información importante de los dispositivos.

8. Recomendaciones

En el presente proyecto se determinó la necesidad de establecer políticas y procedimientos por parte de las empresas, las cuales les permitirá realizar actualizaciones de firmware de manera constante con la finalidad de prevenir ataques informáticos que provengan de personas mal intencionadas, adicional se puede corregir vulnerabilidades conocidas que aparecen en cada versión publicada.

Se sugiere que las industrias que utilicen o planeen implementar redes LoRaWAN en su negocio incorporen soluciones de seguridad en tiempo real. Esto puede incluir sistemas de detección de intrusiones, monitoreo continuo del tráfico de red y alertas automáticas para identificar y responder rápidamente a posibles amenazas.

Se debe dar una relevante importancia en la educación y concienciación de los usuarios finales, administradores de red y desarrolladores de aplicaciones IoT, sobre buenas prácticas de seguridad, como el uso de contraseñas seguras, la autenticación de dos factores y la configuración adecuada de permisos de acceso, el cual permita prevenir que intrusos traten de acceder a las redes LoRaWAN.

Se recomienda a futuros investigadores a explorar, investigar y desarrollar nuevas técnicas y enfoques para abordar los desafíos continuos en el campo de seguridad de las redes LoRaWAN el cual es un entorno en constante cambio dentro de las redes IoT.

9. Bibliografía

¿Qué es el Internet de las cosas (IoT) y cómo funciona? (s. f.). https://www.redhat.com/es/topics/internet-of-things/what-is-iot

Perez, A. (2021, 29 junio). Sigfox vs. Lora vs. NB-IoT: Redes LPWAN para IoT. Bismark Colombia. https://bismark.net.co/sigfox-lora-nb-iot-redes-lpwan-para-iot/

¿Qué es sigfox? – SIGFOX. (s. f.). https://sigfox.com.py/que-es-sigfox/

UNB – Aprendiendo arduino. (2022, 7 marzo). https://www.aprendiendoarduino.com/tag/unb/

Universidad de Quintana Roo – Cristhoper Antonio Sandy Castan. (2021, México) http://risisbi.uqroo.mx/bitstream/handle/20.500.12249/2757/TK7895.E43.2021-2757.pdf?sequence=1

Tecnología LORA y LoRAWAN - CatSensors. (s. f.). https://www.catsensors.com/es/lorawan/tecnologia-lora-y-lorawan

Henandez, D. (2020, 12 febrero). El protocolo LORAWAN. ZOOstock.com. https://www.zoostock.com/redes-y-sistemas/el-protocolo-lorawan

Telefónica. (2023, 18 julio). ¿Qué es NB-IoT y cómo funciona? Telefónica. https://www.telefonica.com/es/sala-comunicacion/blog/que-es-nb-iot-y-como-funciona/

¿Qué es la seguridad IoT? Internet de las Cosas| Fortinet. (s. f.). Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/iot-security

Carracedo, G. (2023, 17 enero). Ciberseguridad en LoRa y LoRaWAN - Contexto e historia. Tarlogic Security. https://www.tarlogic.com/es/blog/ciberseguridad-lora-lorawan/

Wang, A. (2023a, marzo 9). Why LoRaWAN IoT is Thriving over Other LPWAN - mokolora. Tecnología IoT LoRaWAN para sus proyectos. https://www.mokolora.com/es/lorawan-iot-is-thriving-over-other-lpwan/

Estándares de seguridad 5G: 3GPP, ETSI, NIST, GSMA. (2023, diciembre 9). Todo sobre Apple, Android, Juegos Apks y Sitios de Peliculas. https://applexgen.com/estandares-de-seguridad-5g-3gpp-etsi-nist-gsma/

10. Anexos

Anexo 1. Certificación de traducción del resumen

Loja, 11 de julio de 2024

CERTIFICADO DE TRADUCCIÓN

Licenciada
Mónica Susana Guachizaca Armijos
LICENCIADA EN CIENCIAS DE LA EDUCACIÓN MENCIÓN IDIOMA INGLES

CERTIFICO:

Haber revizado la traducción de español a inglés del resumen de tesis titulada "**Análisis de seguridad en redes IoT caso LoRaWAN"** de autoría de **ALVARO FABIAN GONZÁLEZ GUACHISACA** con cédula de identidad 1104735772, egresado de la facultad de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, trabajo que se encuentra bajo la dirección del Ing. John Tucker Yépez, Mg. Sc, previo a la obtención del título de Magister en Telecomunicaciones.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado en hacer uso del presente en lo que se creyera conveniente.

Atentamente,

Mónica Susana Guachizaca Armijos
C.I.1103623706
LICENCIADA EN CIENCIAS DE LA EDUCACIÓN MENCIÓN IDIOMA INGLES
Registro Senescyt: 1008-06-693375

Anexo 2. Glosario de Términos

LPWAN: siglas de Low Power Wide Area Networks, Tecnologías de transmisión inalámbrica de bajo consumo y para zonas extensas. Las tres grandes LPWAN actualmente son LoRaWAN, Sigfox y NB-IoT.

LoRa: capa física de la comunicación. Define las frecuencias y modulación para transmitir con este estándar.

LoRaWAN: capa de aplicación que describe el control, arquitectura y protocolo que corre sobre una modulación LoRa.
Nodo: dispositivo que es el origen o destinatario final de un mensaje en una red LoRaWAN, típicamente los nodos son sensores, instrumentación o actuadores.

Gateway: dispositivo con la función de crear la cobertura de red y dar de alta a los nodos para que trabajen en ella. En una red pequeña también tiene la función de traducir el Payload de los mensajes LoRaWAN a un protocolo de sistemas (típicamente MQTT).

Network Server: gestor de redes LoRaWAN, en arquitecturas con varios Gateways es un elemento independiente de la red. Sus funciones son de coordinación de los Gateways, eliminar los mensajes duplicados, la movilidad y localización de los nodos, gestionar la seguridad con la red y las aplicaciones, traducir los mensajes a un formato entendible por los demás sistemas o habilitar o deshabilitar dispositivos conjuntamente, entre otras funciones.

Uplink: indica la dirección de un mensaje, concretamente un mensaje Uplink implica que es el nodo quien envía un mensaje hacia el Gateway.

Downlink: indica la dirección de un mensaje, concretamente un mensaje Uplink implica que es el Gateway quien envía un mensaje hacia el nodo.

Payload: propiamente el mensaje que se quiere transmitir sin tener en cuenta el resto de la trama que incorpora el protocolo LoRaWAN. Son los datos útiles que requiere la aplicación final del sistema (SCADA, BMS, GMAO, etc.)

Canal: dentro de la banda 868 MHz, se subdividen diferentes rangos de frecuencia por donde diferentes nodos pueden transmitir simultáneamente. Cada uno de ellos es un canal.

Data Rate: cantidad de datos que se transmiten por segundo. Depende principalmente del ancho de banda y del SF.

SF: siglas de Spreading Factor. Cantidad de bits utilizados para transmitir un único símbolo. Equivalente al boundrate en comunicaciones serie, cuanto menor sea el SF, mayor inmunidad a interferencias, pero menor Data Rate.

ToA: siglas de Time on Air. Tiempo que transcurre desde que una señal es enviada por un dispositivo hasta que llega al receptor. A mayor ToA, mayor saturación de la banda de frecuencia y mayor consumo energético.

ADR: siglas de Adaptive Data Rate. Mecanismo utilizado en LoRaWAN para cambiar dinámicamente el SF con el fin de optimizar la energía consumida a la hora de transmitir, pero garantizando una buena inmunidad al ruido.

Duty Cycle: proporción de tiempo (ratio o porcentaje) en el que un componente, dispositivo o antena está operando. En LoRaWAN se aplica comi el tiempo en el que un dispositivo está ocupando un canal concreto.

ABP: siglas de Activation by Personalization. Configuración de acceso manual a una red LoRaWAN donde se requiere introducir en el Gateway los siguientes parámetros DevAddr, NwkSKey y AppSKey

DevAddr: dirección del nodo dentro de la red

NwkSKey: siglas de Network Session Key. Clave necesaria para el cifrado de los mensajes entre el nodo y el Gateway.

AppSKey: siglas de Application Session Key. Clave necesaria para el cifrado entre el nodo y la aplicación. En resumen, es la que permite al Network Server (o al Gateway cuando asume parte de sus funciones) interpretar y traducir el Payload del mensaje.

OTAA: siglas de Over-the-Air activation. Configuración de acceso dinámica a una red LoRaWAN, donde se necesita introducir en el Gateway los parámetros DevEui, AppEui, AppKey.

DevEui: identificador único que viene de fábrica

AppEui: identificador único de aplicación. Sirve para poder separar o clasificar los nodos según la aplicación que va a interactuar con ellos.

AppKey: clave AES 128 secreta que comparten el nodo y la red.