Universidad Nacional de Loja

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

Maestría en Telecomunicaciones

Estudio comparativo de seguridad y cobertura entre las tecnologías de IoT: LoRaWAN y SIGFOX.

Trabajo de Investigación previa a la obtención del título de Magíster en Telecomunicaciones.

AUTOR:

Ing. Pablo Andrés Rojas Mora

DIRECTOR:

Ing. Marianela Carrión González

Loja – Ecuador

2023

Certificación

Loja, 26 de abril de 2023

Ing. Marianela Del Cisne Carrión González, M.Sc.

DIRECTORA DEL TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Titulación denominado**: Estudio comparativo de seguridad y cobertura entre las tecnologías de IoT LoRaWAN y SIGFOX**, previo a la obtención del título de **Magíster en Telecomunicaciones**, de la autoría del estudiante **Pablo Andrés Rojas Mora**, con cédula de identidad Nro.**1103873889**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

Firmado electrónicamente por:
MARIANELA DEL CISNE CARRION GONZALEZ

Ing. Marianela Carrión González Mg.Sc

DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, **Pablo Andrés Rojas Mora** 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

PABLO ANDRES ROJAS MORA

Digitally signed by PABLO ANDRES ROJAS MORA
Date: 2023.05.30 13:23:53 -05'00'

Firma:

Cédula de identidad: 1103873889

Fecha: 30/05/2023

Correo electrónico: pablo.a.rojas.m@unl.edu.ec

Teléfono: 0998809103

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

Yo, **Pablo Andrés Rojas Mora**, declaro ser autor del Trabajo de Titulación denominado: **Estudio comparativo de seguridad y cobertura entre las tecnologías de IoT: LoRaWAN y SIGFOX.**, como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo 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, en la ciudad de Loja, a los treinta días del mes de mayo de dos mil veintitrés.

Firma: PABLO ANDRES ROJAS MORA
Digitally signed by PABLO ANDRES ROJAS MORA
Date: 2023.05.30 13:24:10 -05'00'

Cédula de identidad: 1103873889
Dirección: Av. Cuxibamba
Correo Electrónico: pablo.a.rojas.m@unl.edu.ec
Teléfono: 0998809103

DATOS COMPLEMENTARIOS:
DIRECTOR DE TRABAJO DE TITULACIÒN: Ing. Marianela Carrión González

Dedicatoria

Dedico el presente trabajo a mi hijo Nicolás, mi motivación para ser una mejor persona y ser un mejor profesional, su contagiosa alegría y energía casi infinita hacen que valore cada instante de nuestras vidas.

El nivel de abstracción de los conocimientos en electrónica y telecomunicaciones a los que los profesionales en estas ramas estamos acostumbrados, son totalmente inútiles frente a lo concretos y sinceros sentimientos un niño. Este contraste trae equilibrio a mi vida y felicidad a mi corazón.

Pablo Andrés Rojas Mora

Agradecimiento

Tengo un sincero sentimiento de agradecimiento hacia mi esposa y mi familia que han hecho posible que este nuevo reto profesional se vuelva una realidad. En muchos momentos el tiempo que he dedicado a este reto lo he tomado prestado de su tiempo, tiempo en el que tuvieron que cumplir con tareas que normalmente serian realizadas por mí, pero que generosamente me otorgaron para cumplir con este objetivo académico.

A mi padre por su generoso e inagotable apoyo durante mi desarrollo profesional y a los profesores y todos quienes forman parte de la Universidad Nacional de Loja por brindarme esta gran oportunidad de estudios.

Pablo Andrés Rojas Mora

Índice de contenidos

Índice de tablas:

Índice de figuras:

Índice de anexos:

1. Titulo

Estudio comparativo de seguridad y cobertura entre las tecnologías de IoT: LoRaWAN y SIGFOX

2. Resumen

La cantidad de dispositivos conectados a Internet ha aumentado exponencialmente en los últimos años, lo que ha contribuido al rápido crecimiento de Internet de las cosas (IoT). Pero no todos los dispositivos IoT establecen su conexión a través de redes convencionales como Wi-Fi y redes celulares.

Las redes de área amplia de baja potencia LPWAN están diseñadas para vincular dispositivos que requieren tasas de transferencia de datos bajas, duración prolongada de la batería y ubicaciones remotas. Esto puede incluir dispositivos IoT que requieren una conexión para sectores tan diversos como agricultura, industria, logística, manufactura, transporte, energía, salud, etc.

En el presente estudio se expone una comparativa de cobertura y seguridad entre LoRaWAN y Sigfox, dos tecnologías LPWAN IoT similares en muchos aspectos con dos modelos de negocios muy distintos.

Se efectúa una revisión de las características técnicas que rigen a estas tecnologías para comprender y comparar sus fortalezas y debilidades en el mundo tan competitivo como lo es IoT. Para realizar una comparativa valida se utiliza un software de simulación de cobertura y se procede a analizar los resultados obtenidos

Además, se analizan los distintos enfoques de seguridad tanto en Sigfox y LoRaWAN frente a las amenazas de seguridad de las cuales pueden ser víctimas.

Palabras clave: IoT, LPWAN, Sigfox, LoRaWAN, seguridad, cobertura.

2.1 Abstract

In recent years, the number of devices connected to the Internet has exponentially increased, contributing to the fast growth of the Internet of Things (IoT). However, not all IoT devices establish their connection through conventional networks such as Wi-Fi and mobile networks.

Low-Power Wide-Area Networks (LPWAN) are designed to link devices that require low data transfer rates, long battery life, and remote locations. This may include IoT devices that require a connection for sectors as diverse as agriculture, industry, logistics, manufacturing, transportation, energy, health, etc.

This study presents a comparative analysis of coverage and security between LoRaWAN and Sigfox, two similar LPWAN IoT technologies with very different business models. A review of the technical characteristics that regulate these technologies is performed to understand and compare their strengths and weaknesses in the highly competitive world of IoT.

To accomplish a valid comparison, coverage simulation software is used, and the obtained results are analyzed. Furthermore, the different security approaches in Sigfox and LoRaWAN are analyzed in the face of the security threats they may face.

Keywords: IoT, LPWAN, Sigfox, LoRaWAN, security, coverage.

3. Introducción

La cantidad de dispositivos electrónicos que una persona usa en el día a día ha ido aumentando en los últimos años considerablemente. En los años ochenta probablemente el único dispositivo electrónico que tenían las personas comunes todo el tiempo con ellos podía ser un reloj digital Casio® con algunas funciones básicas como cronometro o fijar alarmas, si durante los ochenta usabas a diario una computadora probablemente eras visto como una persona que estaba muy interesada en la tecnología o que su trabajo lo requería.

En la actualidad la cantidad de artículos electrónicos que usamos en el día a día aumento exponencialmente, teléfonos celulares inteligentes, tabletas, computadoras portátiles, auriculares bluetooth, relojes inteligentes, electrodomésticos del hogar que se conectan a internet como cafeteras, ollas inteligentes, lavadoras, aspiradoras robóticas, etc. Asistentes de voz como Alexa, Google Home o Siri que están constantemente en nuestro hogar a la espera de un comando, los vehículos que usamos a diario tienen un gran componente electrónico para entretenimiento o navegación y la lista no para de crecer. Es ahora cuando el concepto creado por el británico Kevin Ashton, a quien se le atribuye el termino IoT (Internet de las Cosas por sus siglas en ingles) toma una verdadera importancia.

Gran parte de los sectores industriales están usando cada día más IoT; agricultura, ganadería, acuacultura, transporte, logística, manufactura, hotelería, salud, etc. Como sus usos son muy variados también tenemos varias opciones de tecnologías para implementar redes para aplicaciones de IoT, nos centraremos en redes de área amplia y baja potencia (LPWAN), dentro de esta categoría podemos mencionar tecnologías como 4G LTE para IoT, 5G para IoT, LoRaWAN, NB-IoT y Sigfox.

Determinar que tecnología usar depende de muchos factores, como el área de cobertura, el nivel de seguridad necesario, el costo de la implementación, el costo del mantenimiento, escalabilidad, consumo de batería, regulaciones locales, soporte técnico y demás.

En el presente proyecto analizare las fortalezas y vulnerabilidades en cuanto a seguridad de dos de los principales actores en redes LPWAN como son LoRaWAN y Sigfox, además realizare una comparación de cobertura de las dos tecnologías usando software de simulación especializado.

Tanto la seguridad como la cobertura son dos de las principales características para determinar la tecnología a utilizar en una red LPWAN, y tanto LoRaWAN y Sigfox tienen diferentes formas de atacar estas áreas. Si bien las dos tecnologías sirven a un nicho de mercado muy parecido la forma en que lo hacen es muy diferente y esto radica en que usan modelos de negocios muy distintos.

Por otro lado, tenemos a LoRaWAN con una estrategia totalmente diferente, en teoría es una red mucho más abierta, puedes descargar todas sus especificaciones de red desde la pagina oficial y cualquier fabricante de hardware puede desarrollar gateways o endpoints que cumplan con las especificaciones LoRaWAN pero hay un detalle, el detalle es que la única compañía que fabrica chips de radio LoRaWAN es Semtech. LoRaWAN tiene la gran ventaja que al ser un estándar abierto no está dirigido por una compañía en específico.

4. Marco Teórico

En el presente se realizará la revisión bibliográfica con respecto a las tecnologías IoT y en especial a LoRaWAN y Sigfox.

4.1 IoT

Internet de las cosas (IoT) se ha convertido en un término cada vez más popular en los últimos años, pero sus orígenes se remontan hace varias décadas. El concepto de conectar dispositivos y máquinas a una red y permitirles comunicarse entre sí se introdujo por primera vez en la década de 1980. Desde entonces, la tecnología ha evolucionado y el IoT se ha convertido en una realidad que ha transformado diversas industrias.

Los orígenes de IoT se remontan a los primeros días de Internet cuando las computadoras se conectaron por primera vez a una red. En la década de 1980, la Universidad Carnegie Mellon desarrolló el primer dispositivo IoT, una máquina de Coca-Cola que podía comunicarse con los usuarios a través de Internet. La máquina estaba conectada a una red que le permitía informar cuando tenía pocos suministros, y los usuarios podían verificar el estado de la máquina y ver si su bebida favorita estaba disponible antes de hacer el viaje a la máquina.

En las décadas siguientes, el concepto de IoT creció y se desarrollaron más dispositivos que podían conectarse a una red. Sin embargo, no fue hasta principios de la década del 2000 que se acuñó el término "Internet de las cosas". El término fue utilizado por primera vez por Kevin Ashton, cofundador del Auto-ID Center del MIT, en una presentación que hizo a Procter & Gamble. Ashton explicó que IoT permitiría identificar y rastrear objetos mediante etiquetas de identificación por radiofrecuencia (RFID), y estos objetos podrían luego comunicarse entre sí a través de Internet.

IoT ha crecido hasta convertirse en una vasta red de dispositivos que pueden comunicarse entre sí y compartir datos. La tecnología ha transformado varias industrias, incluidas la atención médica, la agricultura, la fabricación y el transporte. Los dispositivos IoT se han convertido en parte de la vida cotidiana, con hogares inteligentes, dispositivos portátiles y asistentes personales cada vez más frecuentes.

Una de las áreas más significativas en las que IoT ha impactado es la atención médica. Los dispositivos IoT, como los sensores portátiles, permiten a los médicos y proveedores de atención médica monitorear a los pacientes de forma remota. Estos dispositivos pueden controlar los signos vitales, realizar un seguimiento de la adherencia a los medicamentos y detectar señales de advertencia tempranas de posibles problemas de salud. La tecnología IoT también ha permitido el desarrollo de la telemedicina, que permite a los pacientes recibir atención médica desde la comodidad de sus hogares.

IoT también ha tenido un impacto significativo en la industria agrícola. Los dispositivos IoT se pueden usar para monitorear los niveles de humedad del suelo, la temperatura y otros factores ambientales que afectan el crecimiento de los cultivos. Esta información se puede utilizar para optimizar los programas de riego, reducir el uso de agua y aumentar el rendimiento de los cultivos. La tecnología IoT también ha permitido la agricultura de precisión, que utiliza datos para crear mapas detallados de los campos, lo que permite a los agricultores identificar áreas que requieren más atención.

El internet de las cosas ha transformado la industria manufacturera. Los dispositivos IoT se pueden usar para monitorear máquinas y equipos, detectar fallas potenciales antes de que ocurran y optimizar los procesos de producción. Esta tecnología ha llevado al desarrollo de fábricas inteligentes, donde las máquinas se comunican entre sí y con operadores humanos para optimizar la producción.

IoT ha tenido un impacto significativo en la industria del transporte. Los automóviles conectados y los sistemas de transporte inteligentes pueden comunicarse entre sí y con la infraestructura, proporcionando datos en tiempo real sobre las condiciones del tráfico y optimizando las rutas. Esta tecnología tiene el potencial de reducir la congestión del tráfico, mejorar la seguridad vial y reducir las emisiones. Además de en la actualidad los vehículos autónomos hacen uso de un sin numero de sensores, todos ellos conectados a internet.

Si bien IoT ha traído muchos beneficios, también presenta desafíos. Uno de los mayores desafíos es la seguridad. Los dispositivos IoT son vulnerables a los ataques cibernéticos y los atacantes pueden usarlos para obtener acceso a redes y datos. Garantizar la seguridad de estos dispositivos es fundamental para evitar vulnerabilidades y proteger la información personal.

Otro desafío es la falta de estandarización. Los dispositivos IoT utilizan diferentes protocolos de comunicación, lo que dificulta que se comuniquen entre sí. Esta falta de estandarización

también puede dificultar el desarrollo de aplicaciones que puedan funcionar en múltiples dispositivos y plataformas.

A pesar de estos desafíos, el futuro del IoT parece prometedor. La tecnología está en constante evolución, y los avances en inteligencia artificial y aprendizaje automático están haciendo posible extraer más valor de los datos generados por los dispositivos IoT.

El IoT tiene el potencial de revolucionar diversas industrias, y su impacto solo seguirá creciendo en los próximos años. Sin embargo, para aprovechar al máximo su potencial, es crucial abordar los desafíos que presenta, como la seguridad y cobertura, estos son los puntos en los que este proyecto se enfoca.

4.2 LPWAN

LPWAN, o red de área amplia de baja potencia, es un tipo de red inalámbrica diseñada para conectar dispositivos de baja potencia y bajo ancho de banda a largas distancias. LPWAN es ideal para aplicaciones de Internet de las cosas (IoT), ya que permite una comunicación de bajo costo, bajo consumo y largo alcance entre dispositivos.

LPWAN se remontan a principios de la década de 2000, cuando los investigadores comenzaron a explorar formas de conectar dispositivos de bajo consumo a largas distancias. Una de las primeras tecnologías LPWAN fue ZigBee, un protocolo de comunicación inalámbrica de corto alcance y baja potencia desarrollado por ZigBee Alliance. ZigBee fue diseñado para la automatización del hogar y otras aplicaciones de bajo consumo y podía operar en un rango de hasta 100 metros. Otra de las primeras tecnologías LPWAN fue LoRa, que significa Long Range. LoRa fue desarrollado por Semtech y se basa en un esquema de modulación patentado que permite la comunicación de largo alcance sobre un espectro sin licencia. LoRa opera en el rango de frecuencia sub-GHz, lo que proporciona mejores características de propagación que las bandas de frecuencia más altas. LoRa puede operar a distancias de varios kilómetros, lo que lo hace ideal para aplicaciones de IoT en agricultura, ciudades inteligentes, logistica y otras industrias.

En la actualidad la tecnología LPWAN ha avanzado significativamente, con varios estándares LPWAN disponibles, incluidos LoRa, Sigfox, NB-IoT y LTE-M. Estas tecnologías se utilizan en una amplia gama de aplicaciones, desde agricultura inteligente hasta seguimiento de activos, y están impulsando el crecimiento de IoT.

LoRa es una de las tecnologías LPWAN más ampliamente adoptadas, con implementaciones en más de 100 países. LoRaWAN, un protocolo desarrollado por LoRa Alliance, permite la interoperabilidad entre diferentes dispositivos y redes LoRa, lo que facilita la implementación y la escala de aplicaciones LPWAN.

Sigfox es otra tecnología LPWAN popular, que opera en la banda ISM sin licencia y puede brindar cobertura en áreas extensas con una tasa de consumo de energía baja. Sigfox tiene una red global que cubre más de 70 países y su tecnología se utiliza en una variedad de aplicaciones, incluidas ciudades inteligentes, agricultura inteligente y edificios inteligentes.

NB-IoT y LTE-M son tecnologías LPWAN que utilizan espectro con licencia y se basan en estándares celulares. Estas tecnologías ofrecen velocidades de datos más altas que otras tecnologías LPWAN, lo que las hace ideales para aplicaciones que requieren un mayor ancho de banda.

La tecnología LPWAN continúa evolucionando, con avances en tecnología de baterías, infraestructura de red y hardware de dispositivos que impulsan la innovación. LPWAN tiene el potencial de transformar varias industrias, permitiendo nuevos casos de uso y modelos comerciales. Sin embargo, también hay desafíos que deben abordarse, como la seguridad, cobertura y la interoperabilidad de la red.

4.3 LoRaWAN

LoRaWAN es una tecnología de red de área amplia de baja potencia (LPWAN) que se utiliza en aplicaciones de Internet de las cosas (IoT). Fue desarrollado por la empresa estadounidense Semtech Corporation en 2014. LoRaWAN es una de las tecnologías más populares en el campo de la IoT debido a su capacidad para soportar aplicaciones de IoT de baja velocidad y baja potencia que requieren una gran cantidad de sensores conectados.

El inicio de LoRaWAN se remonta a la década de 2000, cuando un grupo de investigadores de la Universidad de California en Berkeley comenzó a investigar la tecnología de espectro ensanchado. En 2009, la empresa Semtech Corporation se asoció con la Universidad de California en Berkeley para desarrollar una tecnología de red de área amplia de baja potencia (LPWAN) basada en espectro ensanchado. La tecnología de espectro ensanchado permite que varias señales de comunicación se transmitan al mismo tiempo y en la misma frecuencia, lo que mejora la capacidad de la red para manejar múltiples dispositivos conectados.

En 2011, Semtech Corporation lanzó la tecnología de espectro ensanchado, que fue la base para el desarrollo de LoRaWAN. La tecnología se centró en el uso de la Modulación por Longitud de Onda (LoRa) para transmitir señales de comunicación de larga distancia. La modulación LoRa permite una comunicación de larga distancia de hasta 15 km en áreas rurales y hasta 2 km en áreas urbanas densas, lo que hace que LoRaWAN sea ideal para la comunicación de dispositivos IoT de larga distancia.

En 2014, Semtech Corporation lanzó LoRaWAN como una tecnología de red abierta para la IoT. LoRaWAN utiliza una técnica de comunicación de transmisión de espectro ensanchado que consume muy poca energía, lo que permite que los dispositivos finales funcionen con baterías pequeñas durante varios años. Además, LoRaWAN es una tecnología escalable que puede manejar una gran cantidad de dispositivos finales en una red. Puede soportar hasta 1 millón de dispositivos finales conectados a una única red.

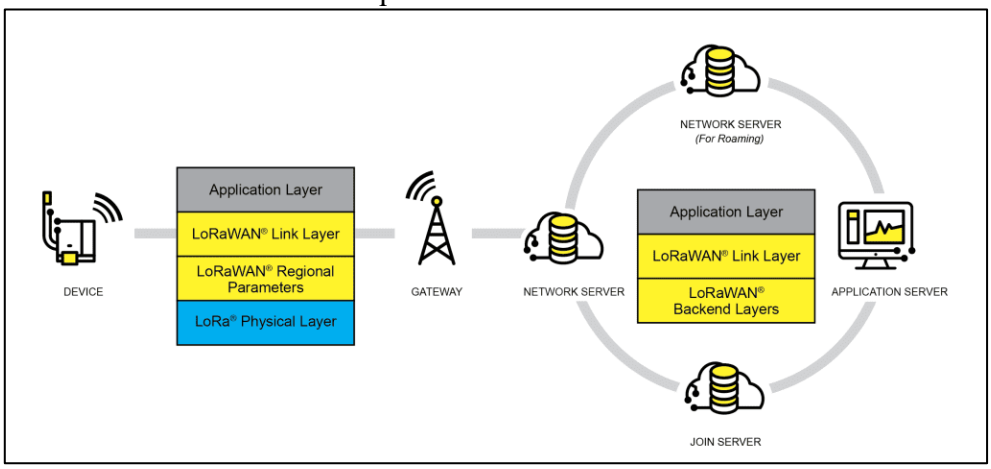
La arquitectura de red de LoRaWAN se divide en tres capas: la capa de dispositivos finales, la capa de gateways y la capa de servidor de aplicaciones. Los dispositivos finales se conectan a los gateways, que reciben las señales de los dispositivos finales y las transmiten al servidor de aplicaciones. El servidor de aplicaciones procesa los datos y envía las respuestas de vuelta a los dispositivos finales a través de los gateways.

LoRaWAN se ha convertido en una tecnología popular para aplicaciones de IoT de baja velocidad y baja potencia en una variedad de industrias, incluyendo la agricultura, la logística, la gestión de edificios, la medición inteligente y la ciudad inteligente. Los sensores conectados a LoRaWAN pueden medir la calidad del aire, la humedad del suelo, la temperatura y otros factores ambientales que afectan el crecimiento de los cultivos en la agricultura inteligente

LoRaWAN tiene un modelo de negocio abierto en los que las especificaciones y características están disponibles para todos los usuarios y miembros de la LoRa Alliance, y cualquier empresa puede fabricar dispositivos finales LoRaWAN, pero existe una restricción, y es que los módulos de radio solo los fabrica SEMTECH, por lo tanto todos los fabricantes deben adquirir los módulos de radio para sus dispositivos finales a la compañía creadora de LORA.

4.3.1 Arquitectura

Figura 1.
Arquitectura LoRaWAN



Fuente: (LoRaAlliance, 2023)

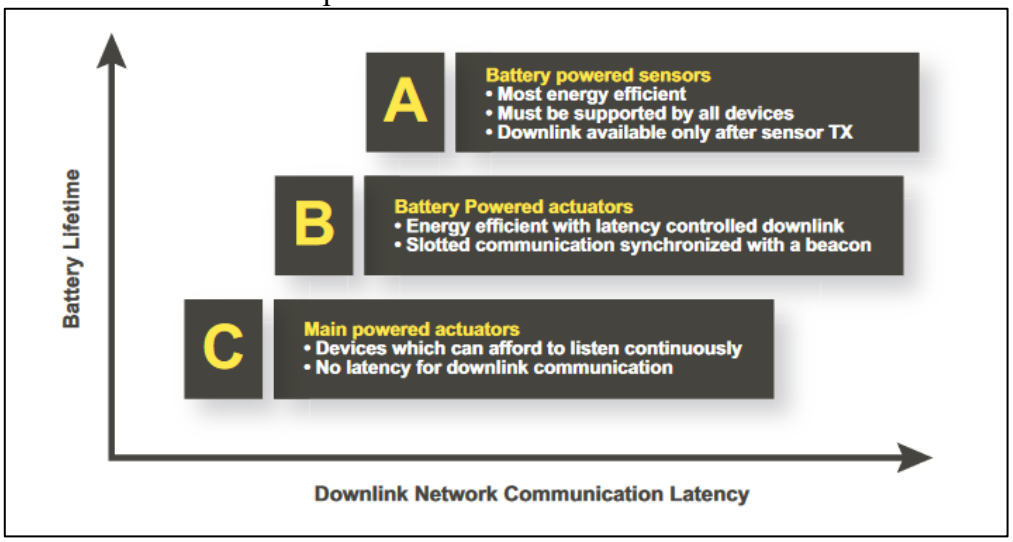
LoRaWAN utiliza una arquitectura de red estrella-de-estrellas (stars-of-stars) en la cual el Gateway es el encargado de enviar y recibir mensajes entre los dispositivos finales y el servidor central de red. Los gateways se conectan al servidor de red mediante una comunicación IP estándar y actúa como un puente (bridge) transparente que convierte paquetes RF (radio frequency) a paquetes IP (internet protocol) y viceversa.

Muchas redes usan una arquitectura de red tipo malla (mesh) en la que cada dispositivo final (end-device) reenvía información de otros dispositivos finales hacia otros, si bien esto permite aumentar la cobertura tambien agrega complejidad, reduce la capacidad de la red y aumenta el consumo de baterías ya que el nodo recibe y envia información que es irrelevante para el es por esto que LoRaWAN no usa una red tipo malla, la comunicación inalámbrica aprovecha las ventajas de LoRa (long range) para conectar cada dispositivo directamente con uno o varios gateways. Todas las clases de dispositivos finales LoRaWAN permiten comunicación bidireccional e incluso se tiene soporte para multicast haciendo un uso eficiente del espectro para tareas como actualizaciones de Firmware Over-The-Air (FOTA) y otras funciones de difusión de mensajes en masa.

4.3.2 Dispositivos Finales

No todos los dispositivos finales son iguales dentro de una red LoRaWAN distintas aplicaciones tienen distintos requerimientos, para esto se han definido tres clases diferentes de dispositivos.

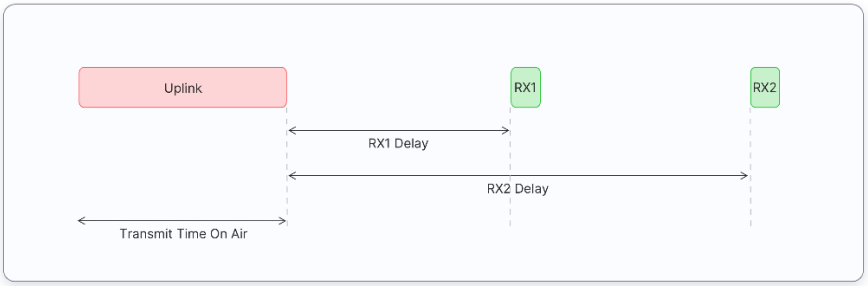
Figura 2.
Tiempo de vida de Batería vs. Latencia



Fuente: (LoRaAlliance, 2015)

- Clase A: Esta clase se caracteriza por ser el de menor consumo de energía, cuenta con una comunicación bidireccional y es la clase por defecto que todos los dispositivos LoRaWAN deben soportar. La comunicación es siempre iniciada por el dispositivo final y totalmente asincrónica además cada transmisión se puede suceder en cualquier momento y siempre es seguida por dos cortas ventanas de descarga (downlink Windows) lo cual da la oportunidad a una comunicación bidireccional en caso de que un comando sea necesario. Es importante señalar que un dispositivo final puede entrar en low-power sleep mode por tanto tiempo como sea definido por su propia aplicación, no existen requisitos de la red para que periódicamente realice un wake-up.

Figura 3.
Detalle de transmisión/recepción en dispositivos Clase A

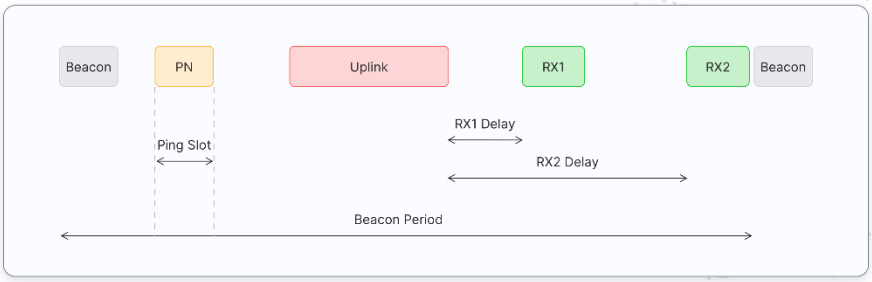


Fuente: (Suarez, 2023)

Todo lo mencionado hace que la Clase A sea la de más bajo consumo aun permitiendo comunicaciones en cualquier momento según lo defina la aplicación. Debemos tener en cuenta que todas las comunicaciones de downlink deben suceder siempre después de una de uplink, por lo tanto las comunicaciones de downlink serán almacenadas en el Gateway hasta el próximo evento de uplink del dispositivo.

- Clase B: Se caracteriza por tener una comunicación bidireccional que además de tener dos cortas ventanas de descarga para realizarlo después de cada uplink, los dispositivos clase B se sincronizan para tener enviar señales de uplink periódicas lo cual crea ventanas de descarga (downlink Windows) esto permite a la red poder enviar comunicaciones downlink cada determinado tiempo.

Figura 4.
Detalle de transmisión/recepción en dispositivos Clase B

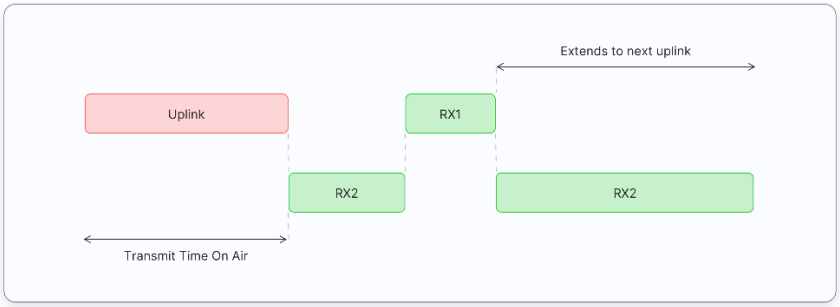


Fuente: (Suarez, 2023)

este tiempo puede ser definido hasta un máximo de 128 segundos, esta característica hace que el consumo de energía en el dispositivo final aumente, pero aun así su uso es adecuado con suministro de baterías.

- Clase C: Los dispositivos de esta clase reducen aún más la latencia en el downlink manteniendo el receptor del dispositivo final abierto en todo momento en el que el dispositivo no está transmitiendo.

Figura 5.
Detalle de transmisión/recepción en dispositivos Clase C



Fuente: (Suarez, 2023)

Esto hace que la comunicación sea halfduplex y basado en esto el servidor puede iniciar una transmisión de downlink en cualquier momento asumiendo que el receptor esta abierto permanentemente. Esto compromete el consumo de energía del receptor (hasta ~50mW) y por lo tanto los dispositivos clase C son recomendados para usos en los que un suministro de energía continuo esté disponible. (No baterías)

4.3.3 Seguridad

El Internet de las cosas (IoT) ha revolucionado la forma en que vivimos, trabajamos e interactuamos con la tecnología. El IoT nos permite conectar una amplia gama de dispositivos y sensores a Internet, lo que permite la recopilación y el análisis de datos en tiempo real. Sin embargo, con esta mayor conectividad vienen mayores vulnerabilidades y la seguridad se ha convertido en un problema crítico para las aplicaciones de IoT.

La seguridad dentro de una red LoRaWAN fue diseñada para cumplir con cuatro criterios según el fabricante

- Bajo consumo de energía
- Baja complejidad de implementación
- Bajo precio
- Alta escalabilidad

Teniendo esto en cuenta se ha seleccionado algoritmos de encriptación conocidos y probados por la comunidad criptográfica durante muchos años, LoRaWAN usa la criptografía AES combinada con CMAC[2] para la protección de la integridad de los datos y CTR[3] para la encriptación.

Cada dispositivo LoRaWAN esta personalizado con una llave AES de 128bit llamada AppKey, y un identificador global único (EUI-64-based DevEUI), tanto la llave como el identificador son usados durante el proceso de autenticación en la red.

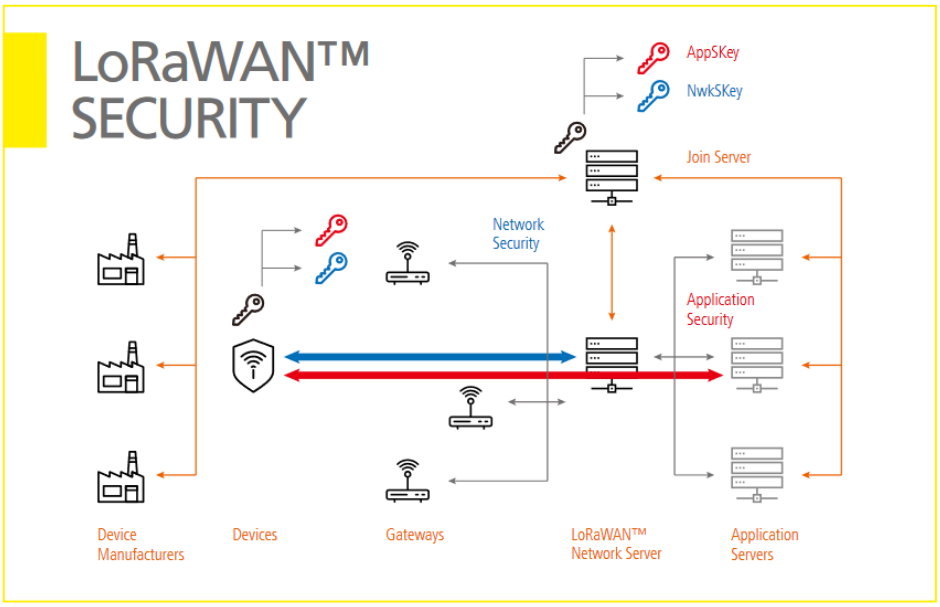
El proceso de autenticación o over-the-air activation (Join-Procedure) prueba que tanto el dispositivo final y la red tienen el conocimiento de la AppKey. Esta prueba se hace calculando un AES-CMAC[4] (usando el AppKey) en la solicitud de unión del dispositivo y por el receptor de backend.

Dos claves de sesión se generan:

- La primera para proporcionar protección a la integridad y encriptación para los comandos LoRaWAN MAC y para el payload de la aplicación (NwkSKey),

- La segunda para la encriptación de extremo a extremo (end-to-end) del payload de la aplicación (AppSKey). La NwkSKey es distribuido a la red LoRaWAN para probar/verificar la autenticación de los paquetes e integridad y la AppSKey es distribuida al servidor de aplicaciones para encriptar/desencriptar el payload de aplicación. Tanto AppKey y AppSKey se pueden ocultar del operador de la red para que no sea capaz de descifrar los payload de la aplicación.

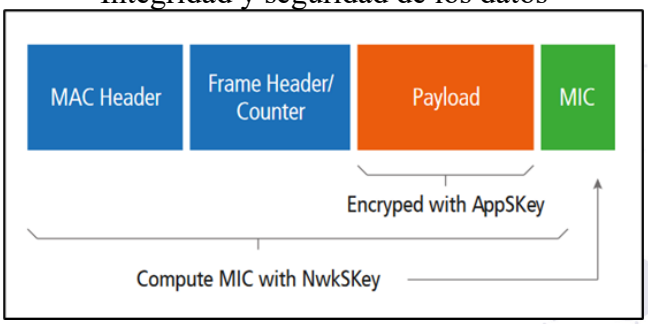
Figura 6.
Esquema de seguridad en una red LoRaWAN



Fuente: (Gemalto et al., 2017)

Todo el tráfico en una red LoRaWAN es protegido por dos claves de sesión cada payload es encriptado usando AES-CTR e incluye un contador para evitar la repetición de paquetes (paquet replay), además se usa un MIC o Message Integrity Code que ayuda a evitar la manipulación de paquetes (packet tampering)

Figura 7.
Integridad y seguridad de los datos



Fuente: (Gemalto et al., 2017)

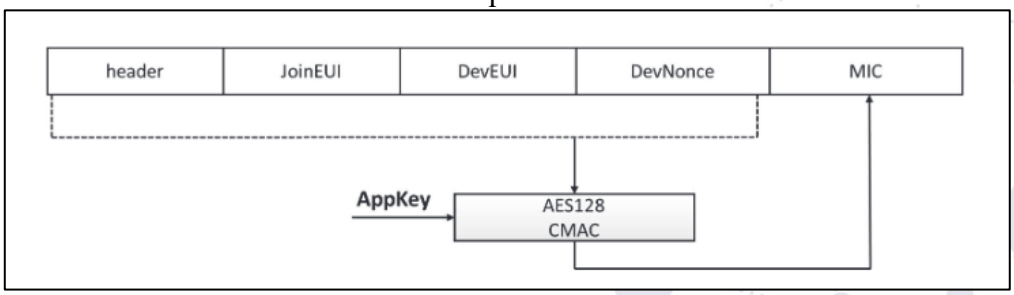
Para que un nuevo dispositivo se agregue a la red es necesario activarlo, la activación consiste en suministrar al dispositivo final de un devAddr, NwkSkey y AppSKey. Una vez que la activación es realizada la NwkSKey es almacenada en el dispositivo y en el servidor de red. DevAddr por otro lado identifica al dispositivo en el servidor de red e incluye el prefijo AddrPrefix que identifica a la red, esto permite activar el modo roaming en forma pasiva ya que los gateways visitados o servidores de red van a poder redirigir los paquetes al servidor de red correspondiente.

Existen dos tipos de activaciones:

- Activación por personalización: En este tipo de activación un dispositivo es directamente asignado a una red LoRaWAN en específico, asignándole y almacenando directamente en el dispositivo la información DevEUI, DevAddr, NwkSkey y AppSKey. Esto permite al dispositivo unirse a la red tan pronto como se lo enciende cabe señalar que la información correspondiente a DevEUI, DevAddr, NwkSkey y AppSKey también deberán ser almacenadas en el servidor de red y en el servidor de aplicaciones antes que el dispositivo sea usado por primera vez.
- Over-The-Air-Activation (OTAA): Por practicidad y escalabilidad es la opción recomendada por la LoRa Alliance, este procedimiento permite que los dispositivos cambien de red dinámicamente ya sea por roaming o por portabilidad (dejar de usar en una red para usarlo en otra permanentemente). Además, esto permite a los fabricantes de dispositivos vender dispositivos genéricos que puedan ser usados en cualquier red LoRaWAN.

  OTTA consiste en tres mensajes, el primero es una solicitud de activación (Join Request) que es enviado por el dispositivo final, el segundo es una aceptación de activación (join accept) y el tercero es una confirmación de esta aceptación criptográfica (Cryptographic handshake) que consiste en enviar un mensaje de uplink normal que es protegido por las recién creadas llaves de sesión (NwkSkey y AppSKey).

Figura 8.
Join Reques Frame



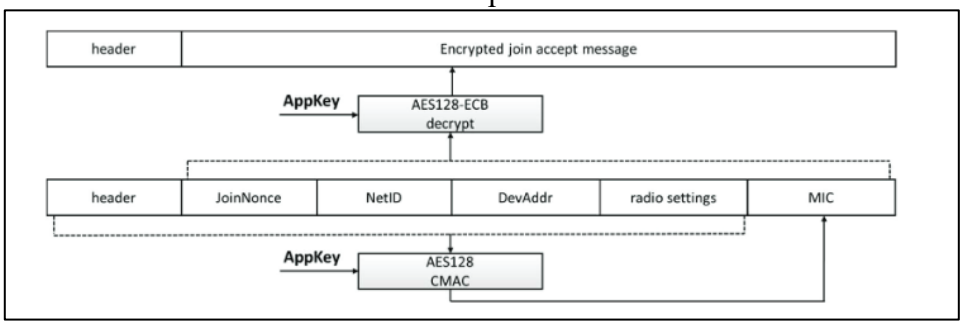
Fuente: (Seller, 2021)

En la figura previa podemos ver el mensaje de solicitud de activación o Join Request, el header determina que el mensaje es una solicitud de activación y además nos dice la versión del protocolo a utilizar.

JoinEUI es de 64 bits y contiene un identificador único del dispositivo final que serán almacenados en el servidor Join Server junto con el AppKey, cabe mencionar que el Join server puede autenticar esta Join Request usando su MIC (Message Integrity Code).

DevNonce es un contador de 16 bit no repetitivo, no se repite nunca incluso cuando el dispositivo final es apagado y encendido nuevamente, su valor se incrementa con cada join request. Este parámetro es usado para evitar ataques repetitivos (replay attacks) ya que todo el mensaje Join Request no está encriptado.

Figura 9.
Join Accept Frame



Fuente: (Seller, 2021)

La figura previa muestra la respuesta de la red LoRaWAN, el DevAddr es un identificador de 32 bits que se asigna a este dispositivo en la red, el NetID es el identificador de red y contiene 24 bits, además se envía los parámetros de radio definidos en la red que varían de acuerdo a cada región y un JoinNonce de 24 bits que es un contador no repetitivo que provee el Join Server.

4.4 Sigfox

Sigfox es una empresa con sede en Francia que proporciona una red global para dispositivos de Internet de las cosas (IoT). La empresa fue fundada en 2010 por Ludovic Le Moan y Christophe Fourtet, expertos en tecnología de comunicación por radio. La tecnología Sigfox proporciona aplicaciones M2M (Machine To Machine) e IoT de bajo costo y tiene una conexión bidireccional de extremo a extremo.

Desde sus inicios, Sigfox recibió financiamiento de gigantes de la industria como Intel y Samsung, quienes reconocieron el potencial de la tecnología. En 2012, Sigfox lanzó su primera red comercial en Francia, seguida de redes en otros países europeos. Sigfox utiliza una

tecnología patentada de banda ultra estrecha (UNB), que permite la comunicación de bajo consumo y largo alcance entre dispositivos.

Esta tecnología es administrada por la plataforma basada en la nube de Sigfox, que brinda administración de dispositivos, almacenamiento de datos y análisis. La plataforma también permite una fácil integración con otros dispositivos y aplicaciones de IoT.

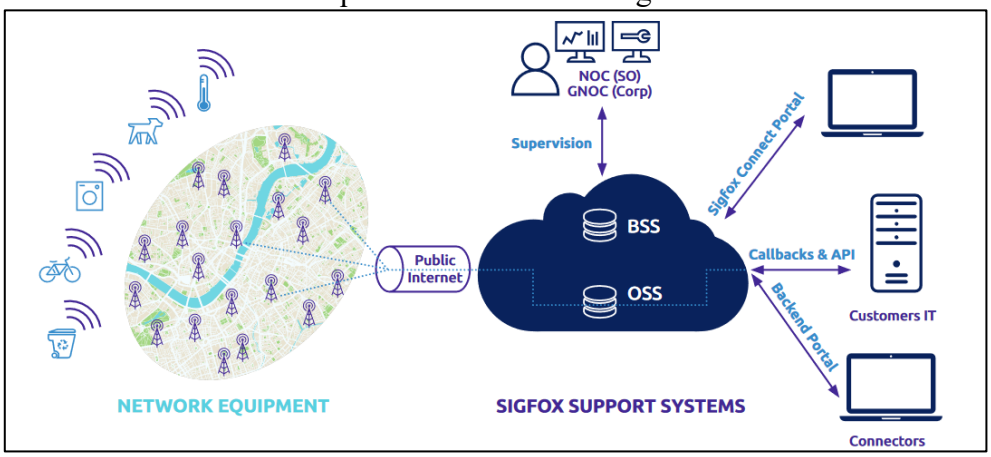
Sigfox ha establecido asociaciones con varias empresas como Bosch, Foxconn y Air Liquide para proporcionar soluciones de IoT para una variedad de industrias, incluidas la agricultura, la atención médica y la logística. La tecnología Sigfox se ha utilizado en una variedad de aplicaciones, como el seguimiento del ganado, el control de los niveles de agua y la gestión de la eliminación de desechos.

Sigfox es en sí un operador de red global que también se asocia con operadores locales en varios países para expandir su cobertura de red. Estos operadores locales son responsables de implementar y mantener las estaciones base Sigfox en sus respectivos países. Sigfox actualmente tiene asociaciones con más de 70 operadores en todo el mundo, incluidas las principales empresas de telecomunicaciones como Telefónica, Altice y NTT Docomo. Estas asociaciones permiten a Sigfox brindar cobertura global para su red de área amplia y baja potencia (LPWAN), que está optimizada para dispositivos de Internet de las cosas (IoT) con bajos requisitos de datos. La red de la empresa es reconocida por su confiabilidad, seguridad y rentabilidad, lo que la convierte en una opción popular para las aplicaciones de IoT.

Sigfox cuenta con un modelo top-down en donde la compañía es dueña de toda su tecnología; backend data, cloud servers y software de los endpoints, el diferenciador de Sigfox es que en esencia es un mercado abierto para el mercado de los endpoints, el fabricante entrega toda la tecnología de los endpoints a cualquier fabricante de chips que lo solicite siempre y cuando acepte los términos de la compañía. Y es así que grandes fabricantes de chips como STMelectronics, Atmel o Texas Instruments fabrican chips de radio Sigfox lo cual ha logrado que el precio de los chips de radio para end points Sigfox sea relativamente bajo.

4.4.1 Arquitectura

Figura 10.
Arquitectura de una red Sigfox



Fuente: (Sigfox, 2018)

Sigfox ha definido dos capas capas principales dentro de su arquitectura horizontal:

- La capa de equipos de red (Network Equipment) que está formada por estaciones base y otros elementos como antenas encargadas de recibir mensajes desde los dispositivos y transferirlos hacia el sistema de soporte Sigfox (Sigfox Support System).
- La segunda capa es el Sistema de soporte Sigfox encargada de procesar y enviar los mensajes hacia el sistema de clientes. Esta capa provee también es el punto de entrada para diferentes componentes y actores de una red Sigfox (Operadores Sigfox, Canales, Clientes finales) para interactuar con el sistema a través de APIs.

  Esta capa también incluye módulos y características que son esenciales para el despliegue, operación y monitoreo de una red Sigfox como por ejemplo Business Support System (BSS) encargado de órdenes, facturación, la planificación de radio, el despliegue de la red y el monitoreo para garantizar su correcto funcionamiento además esta capa incluye repositorios y herramientas para analizar los datos recolectados o generados por la red.

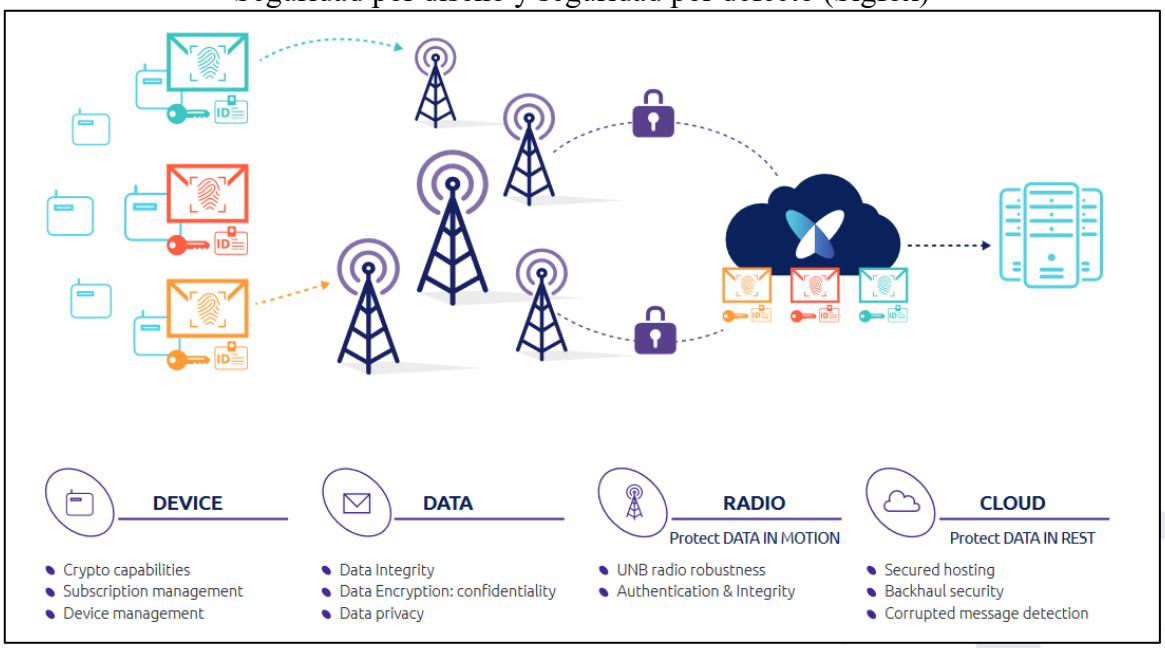
4.4.2 Dispositivos finales

Los dispositivos finales de Sigfox vienen en varios tipos, incluidos sensores, rastreadores, medidores y alarmas. Estos dispositivos están diseñados para ser de bajo consumo, económicos

y fáciles de instalar. Los dispositivos sensores se utilizan para recopilar datos sobre temperatura, humedad, presión y otros factores ambientales. Los dispositivos de seguimiento se utilizan para rastrear la ubicación de activos o personas, mientras que los dispositivos de medición se utilizan para monitorear el consumo de energía o el uso de agua. Los dispositivos de alarma se pueden utilizar para detectar y alertar a los usuarios sobre posibles peligros o infracciones de seguridad. Los dispositivos finales de Sigfox están disponibles en diferentes formatos, incluidos dispositivos independientes, módulos y circuitos integrados lo que los hace adecuados para una amplia gama de aplicaciones de IoT.

4.4.3 Seguridad

Figura 11.
Seguridad por diseño y seguridad por defecto (Sigfox)



Fuente: (Sigfox, 2018)

Sigfox ha implementado seguridad desde sus diseños y lo hace por defecto en todos sus dispositivos.

El fabricante dice tener un firewall incorporado ya que si bien los dispositivos finales son dispositivos IoT(Internet Of Things) estos no se encuentran directamente conectados al internet y no se comunican usando IP (internet protocol) y en realidad son dispositivos que no están conectados a ninguna red o estación base.

Y es que por sus características cada dispositivo final cuando tiene la necesidad de enviar o recibir información de o hacia internet, lo que hace es emitir un mensaje de radio tipo broadcast

este mensaje será tomado por una o varias estaciones bases y será conducido hacia el sistema de soporte Sigfox quien a su vez será el encargado de enviarlo hacia una aplicación IoT.

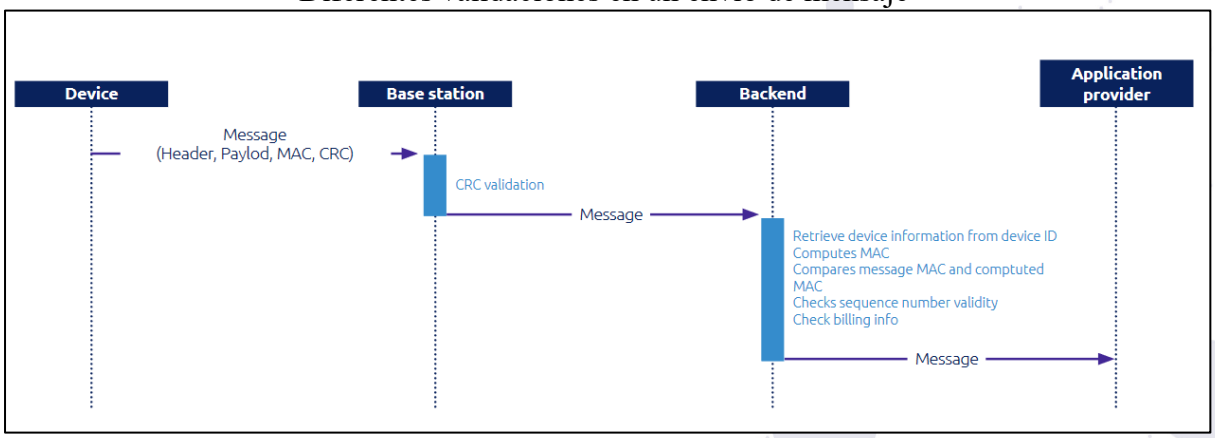
Si el dispositivo requiere una respuesta a un mensaje, la aplicación IoT tiene una corta ventana de tiempo para hacerlo a través nuevamente del sistema de soporte Sigfox y las estaciones base.

El fabricante asegura que gracias a su diseño sus dispositivos no tienen la habilidad de enviar información a entidades ajenas a través de internet y por lo tanto están protegidas por un firewall muy estricto.

Sigfox define como seguridad de datos en movimiento a una serie de características que autentican los mensajes, y evitan ataques repetitivos estas opciones vienen integradas por defecto en todos los dispositivos y existe una característica opcional para evitar escuchas no autorizadas o medidas anti-eavesdropping. Sigfox también define como seguridad de datos estacionarios, a la forma en que toda la información crítica es almacenada desde las claves de autenticación que están en los dispositivos finales hasta la información del usuario e información de red almacenadas en el sistema de soporte Sigfox. Sigfox asegura que su ecosistema usa las mejores prácticas y los mejores mecanismos de seguridad para asegurar la integridad disponibilidad y confidencialidad de los datos.

A continuación, veremos el grafico de procesamiento de un mensaje desde el dispositivo final hasta el proveedor de aplicaciones.

Figura 12.
Diferentes validaciones en un envío de mensaje



Fuente: (Sigfox, 2018)

Para entender el grafico vemos que el mensaje que envía el dispositivo final consta de :

- Header: Encabezado

- Payload: contenido del mensaje
- MAC: Código de autenticación de mensaje (Message authentication code)
- CRC: Verificacion de redundancia cíclica (Cyclic Redundancy check)

Durante el envío de un mensaje se usa el sequence number asociado al MAC como mecanismo anti-replay que consta de un contador simple que es verificado por sistema de soporte Sigfox. Existe una ventana de validación para este contador para recibir los mensajes.

El rango de esta ventana de verificación se define de esta manera (El último número del contador validado + 1) y (El último número del contador valido +1 + 3 x Nivel de suscripción) El nivel de suscripción que corresponde al número máximo de mensajes que puede enviar un dispositivo con un valor mínimo de 20.

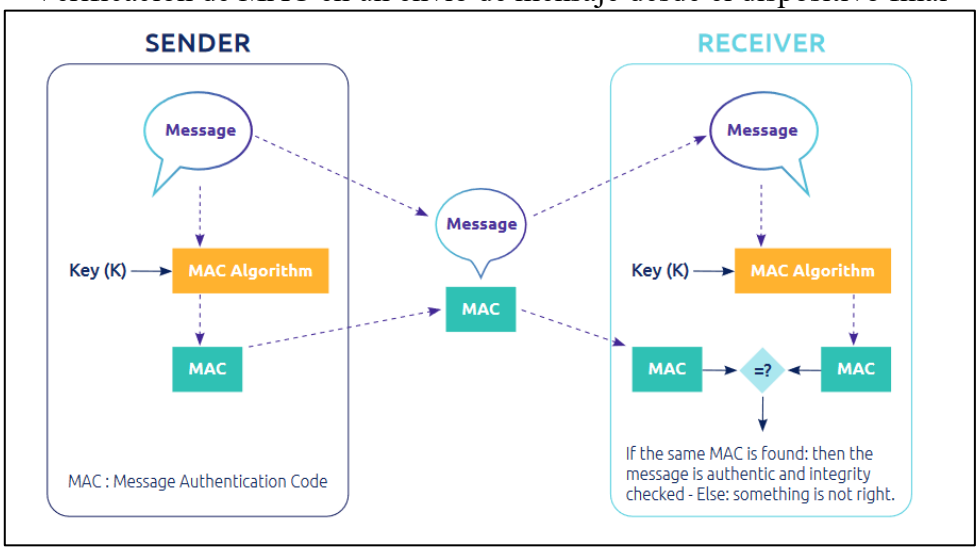
Actualmente Sigfox ofrece los siguientes niveles de mensajes por dia:

- 2 mensajes de uplink diarios y 5 mensajes de downlink mensuales.
- 70 mensajes de uplink diarios y 2 mensajes de downlink diarios
- 140 mensajes de uplink diarios y 4 mensajes de downlink diarios.

Suponiendo un numero de secuencia igual a 10, y una suscripción de 140 mensajes diarios nuestra ventana seria entre 11 y 431 que viene dado por (11 + 3 x 140) = 431

Por otro lado, además de la verificación del contador o sequence number, Sigfox también realiza una verificación de MAC (Message authentication code), cada dispositivo final cuenta con una llave de autenticación simétrica única que es provista durante el proceso de fabricación del dispositivo, cada mensaje que se va a enviar o recibir contiene un token criptográfico que es computado basado en la llave de autenticación. La verificación del token garantiza la autenticación del dispositivo final que envía el mensaje y la integridad del mensaje. Lo antes mencionado se puede apreciar en la siguiente grafica.

Figura 13.
Verificación de MAC en un envío de mensaje desde el dispositivo final



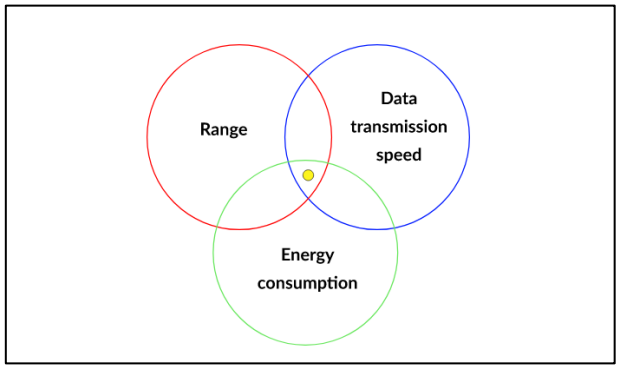
Fuente: (Sigfox, 2018)

Por defecto los datos enviados por radio en una comunicación Sigfox son transportados sin ninguna encriptación, Sigfox da la opción a sus clientes de implementar su propia solución de encriptación end-to-end o confiar en la solución que ofrece la compañía. Esta solución que ofrece Sigfox usa la llave del dispositivo, el sequence number y el rollover number para generar una llave de encriptación.

4.5. Cobertura

Hablar de cobertura en radio comunicaciones es complicado ya que existen demasiadas variables a tomar a consideración como si es una zona densamente poblada con edificaciones de gran altura, o si es una zona urbana residencial o si es una zona rural boscosa o una zona rural de topografía irregular, el tipo de transmisor, el tipo de antena, la sensibilidad del receptor, etc. Por otra parte, no todas las comunicaciones de radio son iguales algunas buscan una tasa de transferencia muy alta, otras buscan el mayor alcance posible y otras buscan el menor consumo de energía. Estas tres características son muy importantes en las radio comunicaciones y es por eso que se deben balancear correctamente.

Figura 14.
Características de una comunicación inalámbrica



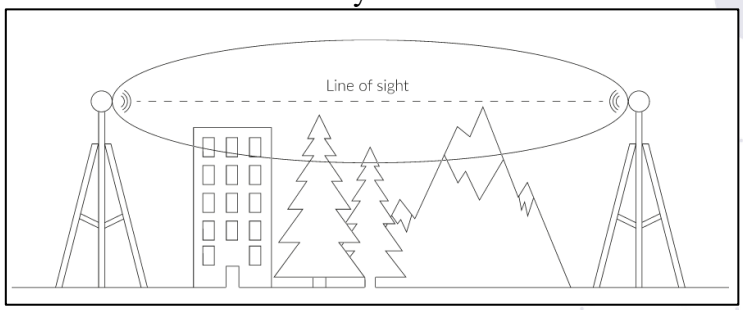
Fuente: (Daniłowski, 2021)

Dependiendo la tecnología y sus usos se balanceará el diagrama anterior según las necesidades, por ejemplo, Wifi busca altas velocidades de transmisión en un rango corto (unos pocos metros) y con un consumo de energía alto. Mientras que LoRaWAN o Sigfox buscan consumo de energía muy bajo con el mayor rango posible a costa de velocidades de transmisión muy bajas.

4.5.1 Línea de vista

Centrándonos nuevamente en IoT, sabemos que frecuentemente es necesario comunicar pequeñas cantidades de datos desde lugares remotos, y para lograr distancias considerables debemos tener en cuenta ciertos factores como la línea de vista.

Figura 15.
Línea de vista y zona de Fresnel



Fuente: (Daniłowski, 2021)

Con el objetivo de lograr la mejor área de cobertura posible se intenta lograr una línea de vista sin obstáculos, esto lo podemos lograr elevando el transmisor a una altura suficiente como para que supere posibles obstáculos, en las comunicaciones inalámbricas el área de radiación es descrita usando Zonas de Fresnel, una zona de Fresnel es un elipsoide que se forma entre el transmisor y receptor, al área que ocupa esta elipsoide está determinada por la frecuencia de transmisión y la distancia que separa la comunicación. Todos los objetos que interfieran en el área de la zona de Fresnel van a afectar negativamente la comunicación, aquí es cuando toman

ventaja tecnologías como LoRaWAN o Sigfox, que usan la banda ISM 915MHz – 923Mhz (En Ecuador), frecuencias mucho más bajas que las populares 2,4Ghz y 5Ghz que están presentes en todos nuestros hogares. El uso de frecuencias más bajas logra menores perdidas de transmisión y una penetración a los obstáculos mucho mayor.

4.5.2 Antenas

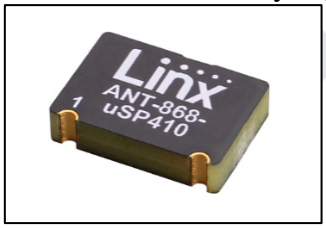
La eficiencia de la antena, diagramas de radiación y orientación son todas características que afectaran nuestra área de cobertura. La selección de una antena adecuada podrá marcar el éxito o fracaso de nuestra comunicación.

Tanto LoRaWAN como Sigfox en Ecuador usan la banda ISM de los 900MHz, y sus gateways (LoRaWAN) o Access Station (Sigfox) tienen características similares en cuanto a potencia de transmisión y antenas compatibles, siendo las más comunes las antenas omnidireccionales entre 2.5dBi y 8 dBi, la potencia del transmisor comúnmente la encontramos entre los 14dBm a 17dBm, claro está que esto solo son las configuraciones más comunes del mercado, existe un mercado especializado en el que estos valores pueden variar significativamente.

Pero las posibilidades van mucho más allá que estos valores comunes de ganancias en antenas y es así que tenemos varios tipos que podríamos usar:

- Antenas tipo chip: Antenas muy pequeñas que son directamente soldables a una placa PCB, muy populares para usos en los que la miniaturización es muy importante, en este caso tanto Sigfox como LoRaWAN usan este tipo de antenas y es mas su tecnología es tan similar que una antena como la de la siguiente imagen puede servir para crear dispositivos para cualquiera de las dos tecnologías.

Figura 16.
Antena tipo chip compatible con LoRaWAN y Sigfox del fabricante Linx

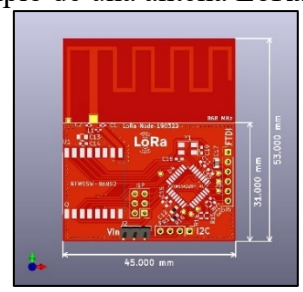


Fuente: (LinxTechnologies, 2020)

- Antenas PCB: Probablemente la forma más económica de incluir una antena en un dispositivo. Se forma usando las propias pistas de la placa PCB para diseñar una antenas, muchas veces no se logra la miniaturización deseada usando esta técnica ya

que el tamaño de la antena diseñado en las pistas depende de la frecuencia para la que está diseñada, por ejemplo en la imagen a continuación se observa que la antena PCB diseñada para frecuencias LoRa ocupa gran parte de la placa PCB (ocupa aproximadamente 4.5cm x 2.5cm).

Figura 17.
Ejemplo de una antena LoRa PCB



Fuente: (TheThingsNetwork, 2019)

- Antena omnidireccional: Antenas usadas principalmente en Gateways o Acccess Station por su gran tamaño, estas antenas emiten en un plano horizontal a grandes distancias, normalmente estan diseñadas para uso en exteriores.

Figura 18.
Antena Omnidireccional 900MHz~930MHz (LoRa o Sigfox)

Fuente: (RAKwireless, 2022)

- Antenas direccionales: Se caracterizan como su nombre lo indica por tener un diagrama de radiación muy direccional, si bien son las menos usadas en IoT, en algunos casos resultan muy útiles especialmente cuando tenemos objetos muy distantes inmóviles alineados en una dirección. Existen varios tipos como Yagi-Uda, de sector o de panel.

Figura 19.
Antena tipo panel 14dBi 790MHz~880MHz (LoRa o Sigfox)

Fuente: (Interline, 2022)

4.5.3 Sensibilidad del receptor:

La sensibilidad del receptor es un factor crucial en los sistemas de comunicación inalámbrica que afecta la calidad y el alcance de la señal. Dado que un receptor más sensible puede captar señales más débiles, puede funcionar a distancias mayores o en condiciones de mayor interferencia.

El factor de ruido, el ancho de banda y el esquema de modulación del receptor son solo algunas de las variables que afectan su sensibilidad. Por lo general, se logra una mejor sensibilidad del receptor estrechando el ancho de banda y reduciendo el factor de ruido. Además, los métodos de modulación menos complejos pueden operar a niveles de sensibilidad del receptor más bajos, ya que la demodulación exitosa generalmente requiere menos intensidad de señal.

Tanto Sigfox como LoRaWAN hacen uso de la técnica de estrechar el ancho de banda para aumentar la sensibilidad en los receptores.

Según las especificaciones de los módulos de radio Sigfox tiene una sensibilidad de -126dBm, mientras que LoRa alcanza hasta 134dBm, estos valores son referenciales porque como se mencionó previamente Semtech fabrica los módulos LoRa y existen varios modelos con diferentes características, y en cuanto a Sigfox los módulos son fabricados por varios gigantes de la industria de los semiconductores que ofrecen distintas especificaciones.

4.5.4 Potencia del transmisor en la banda ISM

El término "potencia del transmisor" en la banda Industrial, Científica y Médica (ISM) describe cuánta potencia puede producir un transmisor en un cierto rango de frecuencia designado para uso sin licencia.

Las normas internacionales han asignado una región del espectro de radio conocida como banda ISM para que la utilicen dispositivos que generan energía de radiofrecuencia (en esta banda trabaja LoRa y Sigfox).

La potencia máxima del transmisor permitida en la banda ISM varía según el rango de frecuencia particular y el país o región en el que se utilice. Por ejemplo, la potencia máxima del transmisor de la banda ISM de 2,4 GHz en los EE. UU. es de 1W, mientras que en Europa es de 100mW.

Debido a que afecta la cobertura y el alcance del transmisor, la potencia del transmisor en la banda ISM es un factor crucial. Puede ser posible un mayor alcance y una mejor cobertura con un transmisor más fuerte, pero también puede resultar en más interferencia de otros dispositivos que usan la misma banda de frecuencia. Los dispositivos que utilizan la banda ISM deben limitar la potencia de su transmisor al máximo permitido por las normas locales para cumplir con las leyes y evitar interferencias.

5. Metodología

Para una comparación de seguridad entre LoRaWAN y Sigfox se realizó un análisis de los protocolos y técnicas que utilizan cada una de las tecnologías y se tabularon para un posterior análisis de resultados además se listaran los ataques documentados exitosos a las dos tecnologías como muestra de las posibles vulnerabilidades.

Mientras que para la comparación de cobertura entre LoRaWAN y Sigfox se utilizó un software de simulación (Xirio Online) utilizando como área geográfica la ciudad de Loja – Ecuador.

5.1 Comparación de cobertura entre LoRaWAN y Sigfox.

Para realizar un análisis de cobertura valido entre las dos tecnologías se usó el software de simulación de cobertura de radio XIRIO ONLINE. El software permite realizar simulaciones profesionales de cobertura de señales de radio en ambientes urbanos y rurales.

Un estudio de cobertura tiene en cuenta el transmisor, el receptor y las características del modelo de propagación elegidos para describir los valores de la señal generada por un transmisor en términos de campo eléctrico o potencia en todos los puntos dentro del área seleccionada por el usuario.

Empezaremos definiendo algunos parámetros que las dos tecnologías compartirán durante la simulación.

Tabla 1.
Parámetros comunes usados en las simulaciones

PARAMETRO	VALOR
Localidad	Loja – Ecuador
Cantidad de transmisores	1
Ubicación del transmisor	Latitud 03º59'56.37"S Longitud: 079º12'14.45"W
Polarización de la antena transmisora	Vertical
Tipo de antena transmisora	Omnidireccional
Altura de la antena	10 metros

Altura del edificio	40 metros (nivel de azotea)
Área de simulación:	Esquina NO – Latitud 03º50'51.17"S Esquina NO – Longitud 079º17'01.59"W Esquina SE – Latitud 04º06'50.43"S Esquina SE – Longitud 079º08'10.13"W
Capas de cartografía utilizadas	Capa de Ecuador resolución 30m, año 2016
Método de calculo	UIT-R P.526-15

Fuente: El autor

Además, definiremos algunos sitios de interés de la ciudad que nos permitirán tener una idea mucho más clara de la cobertura obtenida con cada una de las tecnologías.

Tabla 2.
Sitios de interés para la simulación de cobertura

Puntos de interés	Latitud	Longitud
Barrio Ciudad Victoria	04º00'07.49"S	079º13'49.73"W
Barrio El Capulí	04º02'55.09"S	079º11'48.15"W
Barrio Sauces Norte	03º56'20.96"S	079º13'28.79"W
Barrio Tierras Coloradas	04º00'44.01"S	079º14'26.98"W
Entrada al Parque Nacional Podocarpus	04º05'00.51"S	079º12'19.54"W
Parque central	03º59'48.12"S	079º12'06.11"W
Puerta de la ciudad	03º59'22.89"S	079º12'15.02"W
Redondel de Carigan	03º57'41.90"S	079º14'17.77"W
Redondel Vía a Zamora	03º59'36.01"S	079º10'56.36"W
San Sebastián	04º00'05.54"S	079º12'04.32"W
Teatro Benjamín Carrión (Jipiro)	03º58'20.36"S	079º12'05.90"W
Universidad Nacional de Loja	04º02'00.87"S	079º12'09.86"W
Universidad Técnica Particular de Loja	03º59'13.40"S	079º11'54.99"W

Fuente: El autor

Para hacer esta simulación válida se han tomado dos transmisores muy populares en las dos tecnologías, recordemos que LoRaWAN llama a sus transmisores gateways mientras que Sigfox los llama Access Stations.

Los equipos que se detallan en la tabla a continuación son de características muy similares, y esto se debe a que las dos tecnologías ocupan la misma banda de frecuencia (En Ecuador) y que usan características similares en cuanto a potencia, ancho de banda, incluso en su forma de definir los frames de uplink y downlink tienen muchas semejanzas.

Tabla 3.
Equipos y características para la simulación

GATEWAY LORAWAN		
	Marca	RAK
	Modelo	RAK7289V2
	Tranceiver	SX1303 (SEMTECH)
	Potencia Tx	17dBm
	Sensibilidad RX	-139dBm
	Antena LoRa	1 o 2 conectores tipo N
	Backhaul (Red de retorno)	Wi-Fi, Ethernet, LTE
	Protección	IP67/NEMA-6 grado industrial
	Fuente de energía	PoE (IEEE 802.3af) - 37~57 VDC
	Frecuencia de operación	US915/AS923/AU915/IN865/KR920

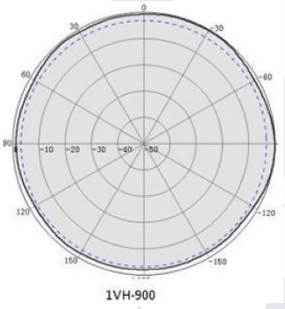
ACCESS STATION SIGFOX		
	Marca	Sigfox
	Modelo	V3
	Tranceiver	CC1120 (Texas Instrument)
	Potencia Tx	17dBm
	Sensibilidad RX	-127
	Antena LoRa	1 conector tipo N
	Backhaul (Red de retorno)	Ethernet, LTE
	Protección	IP67/NEMA-6 grado industrial
	Fuente de energía	CA 100-120V
	Frecuencia de operación	273.3-320, 410-480, 820-960

Fuente: El autor

Procederemos a definir las antenas en las que hemos basado nuestra simulación. En los dos casos se utiliza antenas omnidireccionales.

Tabla 4.
Parámetros de antena usada en la simulación propia

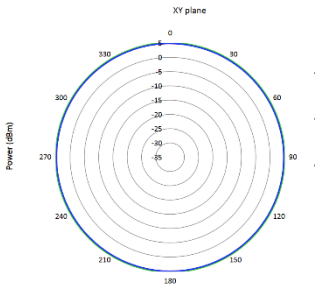
ANTENA PARA SIMULACIÓN LORAWAN	
Fabricante	RAK
Rango de frecuencias	900~930 MHz
Ganancia (max)	8.0dBi
Tipo	dipolo
Polarización	Vertical
Conector	Tipo N
Dimensiones	Φ25.0 mm x 900.0 mm
VSWR	≤ 1.5



Fuente: El autor

Tabla 5.
Parámetros de antena usada en la simulación Sigfox

ANTENA PARA SIMULACIÓN SIGFOX	
Fabricante	Pulse Larsen
Rango de frecuencias	860-960MHz
Ganancia (max)	5.0 dBi
Tipo	dipolo
Polarización	Vertical
Conector	Tipo N
Dimensiones	Φ25.7 mm x 812.4 mm
VSWR	2:01



Fuente: El autor

Se han definido umbrales de nivel de señal para la simulación. Los resultados estarán graficados con estos umbrales para realizar los análisis y comparaciones.

Figura 20.
Rango de colores para niveles de señal

Fuente: El autor

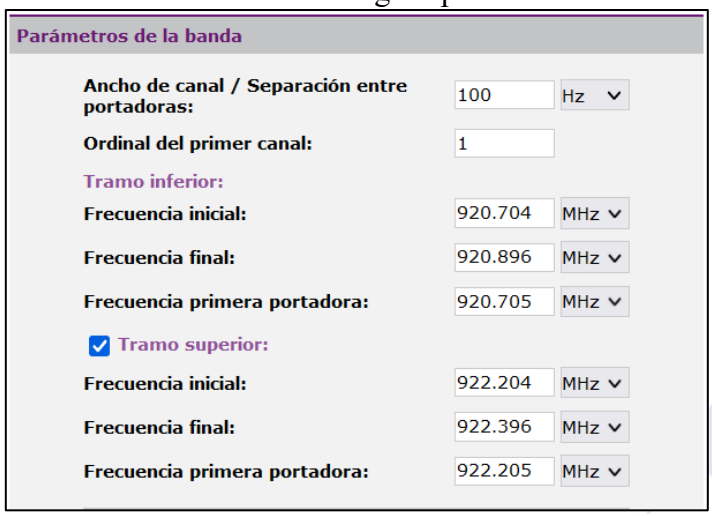
Parte de los datos necesarios para realizar una correcta simulación consiste en establecer correctamente las bandas de frecuencias en las que trabaja tanto LoRaWAN como Sigfox, cabe señalar que las bandas de frecuencias usadas en esta simulación son válidas para Ecuador, en otras regiones o países las bandas de frecuencias pueden diferir significativamente.

Empezaremos definiendo la banda de frecuencia de Sigfox, Ecuador pertenece a una lista de países que Sigfox a definido como RC4 (Radio configuración 4) a los que pertenecen los siguientes países:

- Latino América: Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, Paraguay, Perú, Trinidad & Tobago, Uruguay.
- Asia Pacific: Australia, Hong Kong, Indonesia, Malaysia, New Zealand, Singapore, Taiwan, Thailand.

Basándome en el documento oficial de especificaciones de radio Sigfox(Sigfox, 2022) publicado en marzo del 2022 he definido la banda como se muestra en la ilustración a continuación.

Figura 21.
Banda de frecuencias Sigfox para simulación



Fuente: El autor

En Ecuador LoRaWAN puede trabajar en la banda conocida como US902-928, que precisamente va desde los 902MHz hasta los 928MHz y vemos como se detalla a continuación usa un ancho de frecuencias mayor al de Sigfox.

Figura 22.
Banda de frecuencia LoRaWAN para simulación

Fuente: El autor

5.2 Comparación de Seguridad entre LoRaWAN y Sigfox

En el marco teórico se han definido las técnicas y mecanismos que utilizan las dos tecnologías para garantizar una comunicación segura, para lograr comparar de una manera adecuada las dos tecnologías se detallara los ataques que pueden ser victimas las dos tecnologías.

5.2.1 Ataques a LoRaWAN

- Reutilización de contadores de mensajes (DevNonce) Recordemos que se utiliza un contador no repetitivo de 16 bits que puede ser víctima de ataques ya sea poniéndolo a 0 o desbordándolo para que su contador vuelva a empezar.
- Los nonces se pueden usar de nuevo. Es posible que los valores se repitan porque la red no los registra correctamente.
- Existe la posibilidad de ataques de repetición. Debido a la reutilización de nonces, un dispositivo OTAA podría recibir múltiples mensajes Join-Accept al hacer coincidir sus valores de DevNonce y/o AppNonce con otro dispositivo en la red. Recordemos que el modo de activación por aire está definido por las siglas en ingles OTAA.
- Los mensajes ACK no están asociados con ningún mensaje específico, lo que permite ataques de repetición para que un nodo pueda retransmitir un mensaje cuando no recibe el ACK correspondiente o recibir ACK de mensajes que en realidad no han llegado al servidor de red.

- Los mensajes de Join-Accept no se asocian únicamente con un mensaje de Join-Accept. La vulnerabilidad permite la suplantación de identidad.
- Un ataque de interferencia (jamming) es una denegación de servicio en la que un canal de comunicación está completamente ocupado por otro dispositivo. En el caso de LoRaWAN, dado que los mensajes Join-Request y Join-Accept no están encriptados, es posible saber qué canal está utilizando un dispositivo.
- Si se rastrea el tráfico entre un Gateway y un dispositivo y se capturan dos mensajes con el mismo contador, los datos se pueden recuperar. Este tipo de ataques se denominan Eavesdropping o escuchas maliciosas.
- Ataques de descifrado de contraseñas (Password cracking): si tiene acceso a la red y captura los mensajes de Join-Request y Join-Accept intercambiados durante la unión de un dispositivo, es posible descifrar la AppKey del dispositivo. Una vez que se obtiene esta clave, las claves de sesión (NwkSKey y AppSKey) se pueden recuperar utilizando los mismos mensajes de Join-Request y Join-Accept capturados.
- Conocer la AppKey de un dispositivo puede servir para realizar ataques de spoofing a través de las comunicaciones por radio, así como a través del plano tcp/ip, donde es posible realizar ataques de spoofing con la misma AppKey obtenida. Esto puede ser utilizado para volver invisible a un dispositivo legitimo de la red.
- Ataques a dispositivos clase B en una red LoRaWAN: En una red LoRa clase B, además de tener ventas de recepción después de la transmisión, hay ventanas de recepción adicionales en tiempos programados para los dispositivos finales. Estas ventanas se abren periódicamente y se activan mediante beacons (balizas) enviadas por el gateway. Para abrir ventanas de recepción a horas fijas, los gateways deben transmitir un beacon sincrónicamente para dar una referencia de tiempo a los dispositivos finales. La vulnerabilidad de las redes LoRa clase B es que los beacons (balizas) no están encriptadas. Como no hay cifrado, toda la información que contienen los beacons está en texto plano. Si se transmite algún dato crucial, el atacante puede leerlo.

5.2.2 Ataques a Sigfox

- Ataques físicos de seguridad: Si el atacante tiene acceso a un dispositivo final, a un Gateway o a un servidor y estos dispositivos no están asegurados todo el dispositivo e incluso la red pueden verse comprometidos, recordemos que los dispositivos finales en

sigfox suelen ser muy económicos y que las medidas de seguridad que pueden establecer bajo ese costo suelen no ser muy efectivas y en algunos casos inexistentes.

- Jammin: Probablemente la tecnología más sencilla para corromper e inutilizar un sistema Sigfox sea utilizar este tipo de ataques que consisten en emitir señales de gran potencia en las frecuencias en las que trabaja Sigfox, en este caso es en especial sencillo ya que el ancho de banda usado por Sigfox para realizar una comunicación es de solo 100Hz, esto sumado a que se usan transmisores de baja potencia hacen que el ataque tipo jamming sea muy efectivo en su objetivo de disminuir la relación señal a ruido.
- Ataques de replay: Para protegerse contra ataques de replay, Sigfox usa un numero de secuencia de 12 bits que es transmitido con cada mensaje de uplink y que es protegido por un código de autenticación de mensaje (MAC). Si un mensaje llega con un numero de secuencia menor al del ultimo mensaje recibido, será descartado por el servidor. Si el número de secuencia es de 12 bits esto permite solo $2^{12} = 4096$ entes de volver a cero, esto combinado con que la key usada para calcular la MAC no cambia durante toda la vida del dispositivo hacen que un ataque de replay sea altamente probable.
- Un ataque de denegación de servicio (DoS) es una de las amenazas de seguridad que Sigfox puede encontrar con más frecuencia. Un ataque DoS incluye inundar un servidor con tráfico o solicitudes, lo que puede inhibirlo e impedir que responda a solicitudes válidas. Toda la red puede verse afectada por este tipo de ataque, haciéndola inalcanzable para los usuarios.
- Ataque por un hombre en el medio (MitM). Este tipo de ataque incluye escuchar en dos dispositivos que hablan entre sí y cambiar los datos que se envían. Esto le da al atacante la oportunidad de robar datos privados o potencialmente apoderarse de los dispositivos.
- Falta de cifrado: la ausencia de cifrado obligatorio es uno de los problemas de seguridad más comunes en las redes IoT. Los datos se transfieren entre los dispositivos IoT y la plataforma en la nube de Sigfox mediante tecnología de comunicación propietario. Sin embargo, los datos pueden ser interceptados y leídos por cualquier persona con acceso a la red porque esta tecnología no ofrece cifrado de extremo a extremo obligatorio.

6. Resultados

A lo largo de la realización de este estudio ha sido cada vez más claro que son más cosas las que estas dos tecnologías tienen en común que las que las separan, si bien son dos tecnologías que tienen un modelo de negocio muy diferente, las dos coinciden en muchos aspectos técnicos y por la misma razón son vulnerables en muchas ocasiones a las mismas amenazas

En cuanto a cobertura nuevamente nos encontramos con tecnologías muy similares, que si bien usan métodos de codificación y de modulación diferentes, comparten características en común que hacen que los resultados no sean tan diferentes como sus propulsores quisieran parecer.

6.1 Resultados de comparación de cobertura

Tabla 6.
Tabla de cobertura en los puntos de interés de la ciudad de Loja

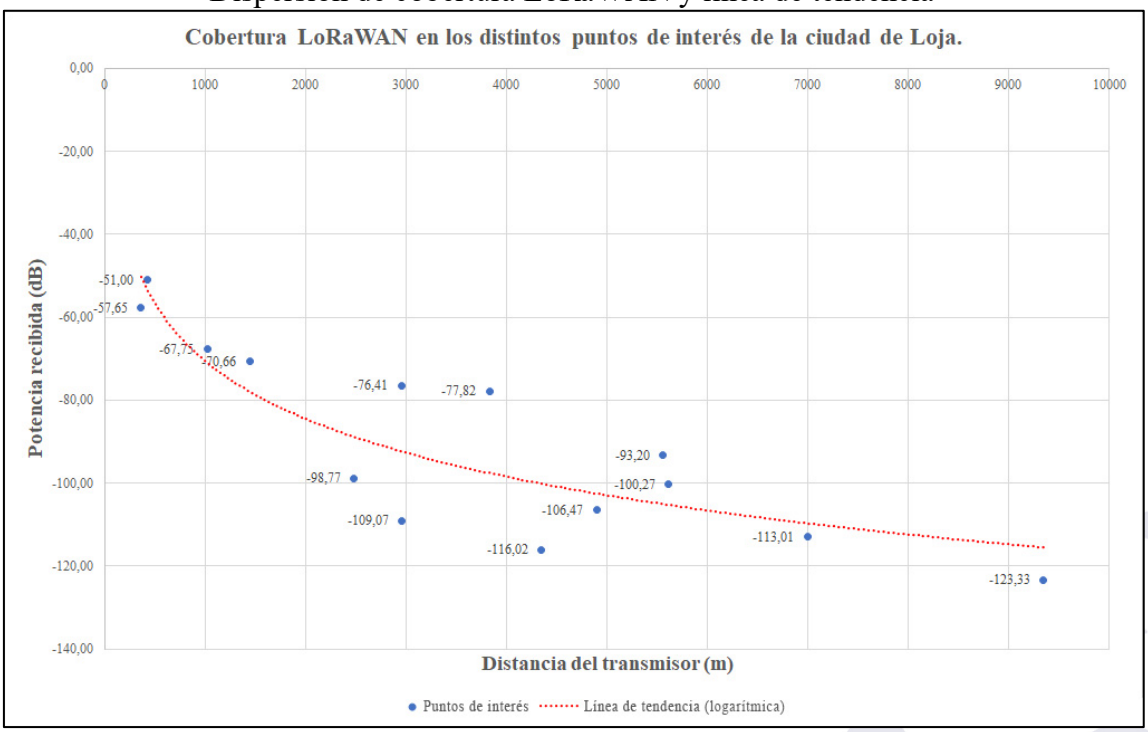
PUNTOS DE INTERES	LORAWAN (dBm)	SIGFOX (dBm)	DISTANCIA AL TRANSMISOR (m)
Barrio Ciudad Victoria	-108,82	-99,94	2961
Barrio El Capulí	-93,03	-94,67	5555
Barrio Sauces Norte	-112,76	-115,30	6998
Barrio Tierras Coloradas	-115,77	-119,03	4346
Entrada al Parque Nacional Podocarpus	-123,08	-125,25	9349
Parque central	-57,48	-59,51	365
Puerta de la ciudad	-67,58	-69,72	1023
Redondel de Carigán	-100,06	-101,98	5612
Redondel Vía a Zamora	-98,52	-101,91	2486
San Sebastián	-50,83	-53,07	423
Teatro Benjamín Carrión (Jipiro)	-76,24	-78,40	2955
Universidad Nacional de Loja	-77,65	-79,84	3833
Universidad Técnica Particular de Loja	-70,49	-72,67	1444
Urbanización Parquenor	-106,22	-108,52	4899

Fuente: El autor

En la tabla 6 se detalla los resultados obtenidos por el software de simulación Xirio Online en los puntos de interés definidos previamente para el ambiente urbano de la ciudad de Loja – Ecuador. Se han seleccionado puntos de interés intentando cubrir zonas céntricas y las zonas más alejadas de la ciudad. La zona con menor cobertura es la Entrada al Parque nacional Podocarpus, que cabe señalar que es un punto que está casi 3 kilómetros por fuera del perímetro urbano.

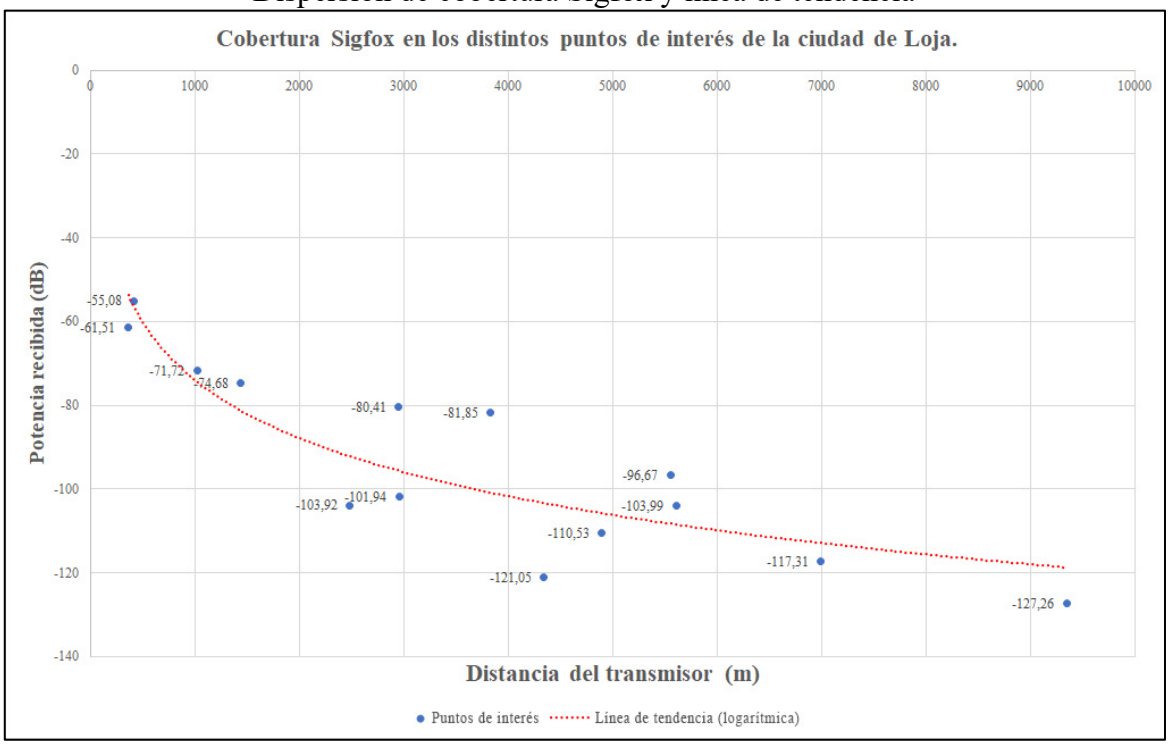
Los resultados visualizados en una gráfica de dispersión resultan interesantes, en la misma se detalla una línea de tendencia en escala logarítmica, tanto los resultados de LoRaWAN como de Sigfox resultan muy similares y sus líneas de tendencia son casi idénticas.

Figura 23.
Dispersión de cobertura LoRaWAN y línea de tendencia



Fuente: El autor

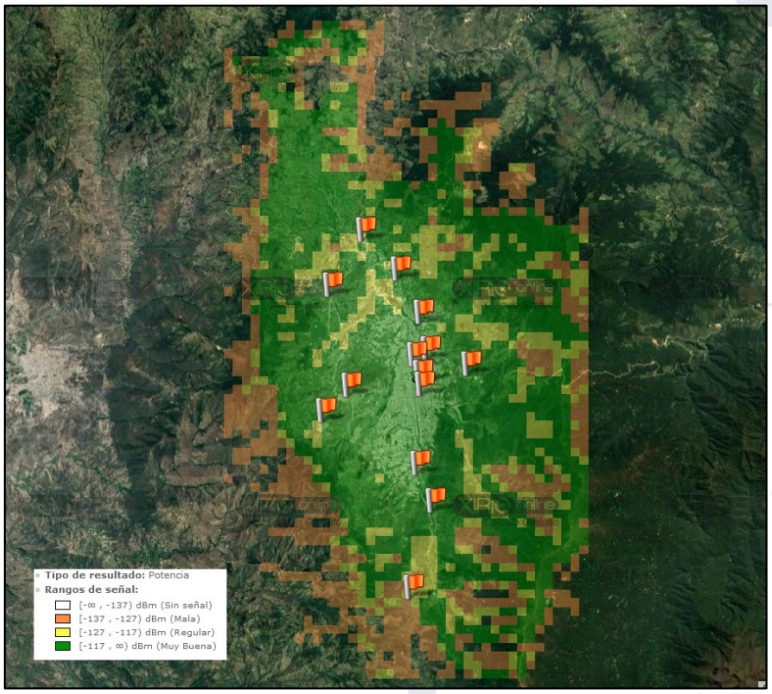
Figura 24.
Dispersión de cobertura Sigfox y línea de tendencia



Fuente: El autor

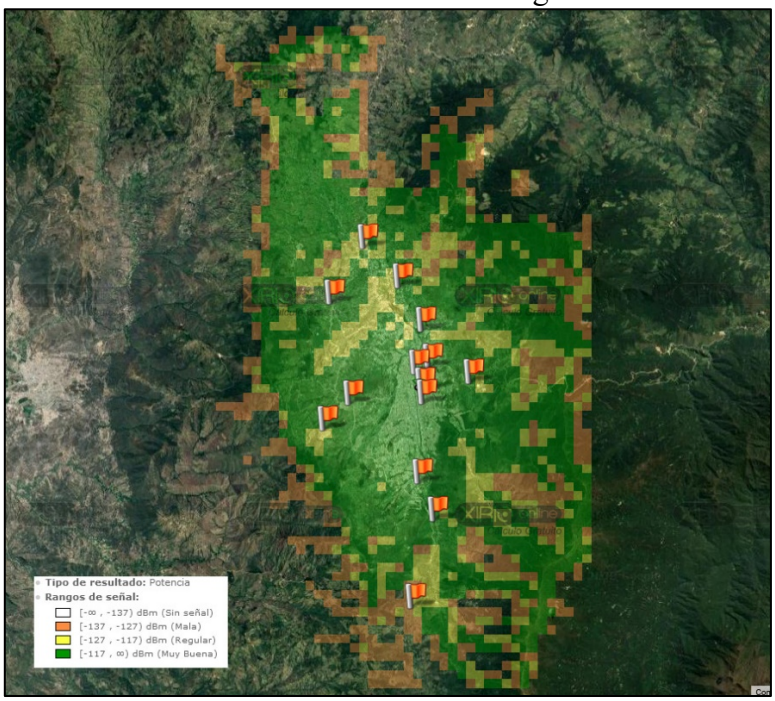
Quizá los resultados gráficos más asimilables son los mapas de la ciudad con los niveles de intensidad de señal de acuerdo a los colores de rangos establecidos.

Figura 25.
Simulación de cobertura LoRaWAN



Fuente: El autor

Figura 26.
Simulación de cobertura Sigfox

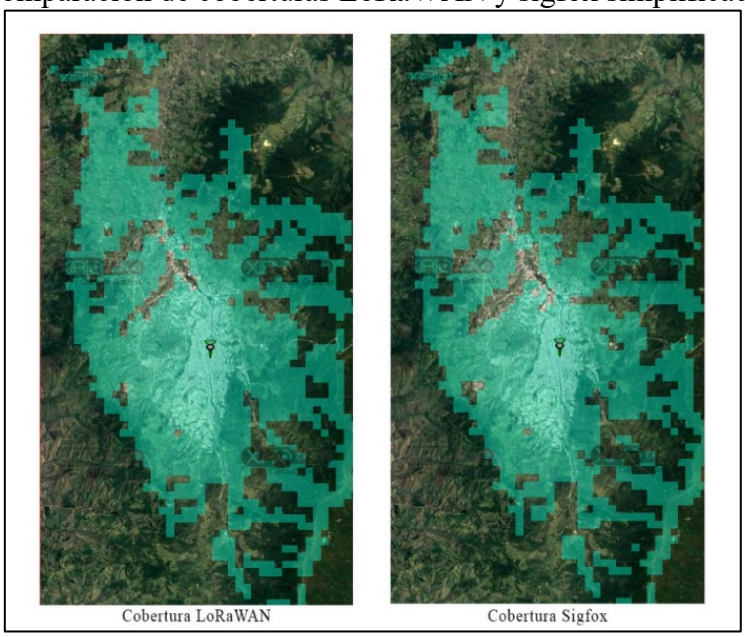


Fuente: El autor

Las dos imágenes previas parecen ser a simple vista idénticas, hace falta ver a detalle las gráficas para apreciar las diferencias. Las cuales son sutiles dado que los dos sistemas tienen características muy similares.

En la imagen a continuación vemos la cobertura simplificada en un solo color, en donde se aprecia la similitud de las mismas.

Figura 27.
Comparación de coberturas LoRaWAN y sigfox simplificada



Fuente: El autor

Podemos ver en la tabla a continuación la verdadera diferencia en dBm (Valor absoluto) en los puntos de interés determinados.

Tabla 7.
Diferencia de potencia en la cobertura en puntos de interés seleccionados

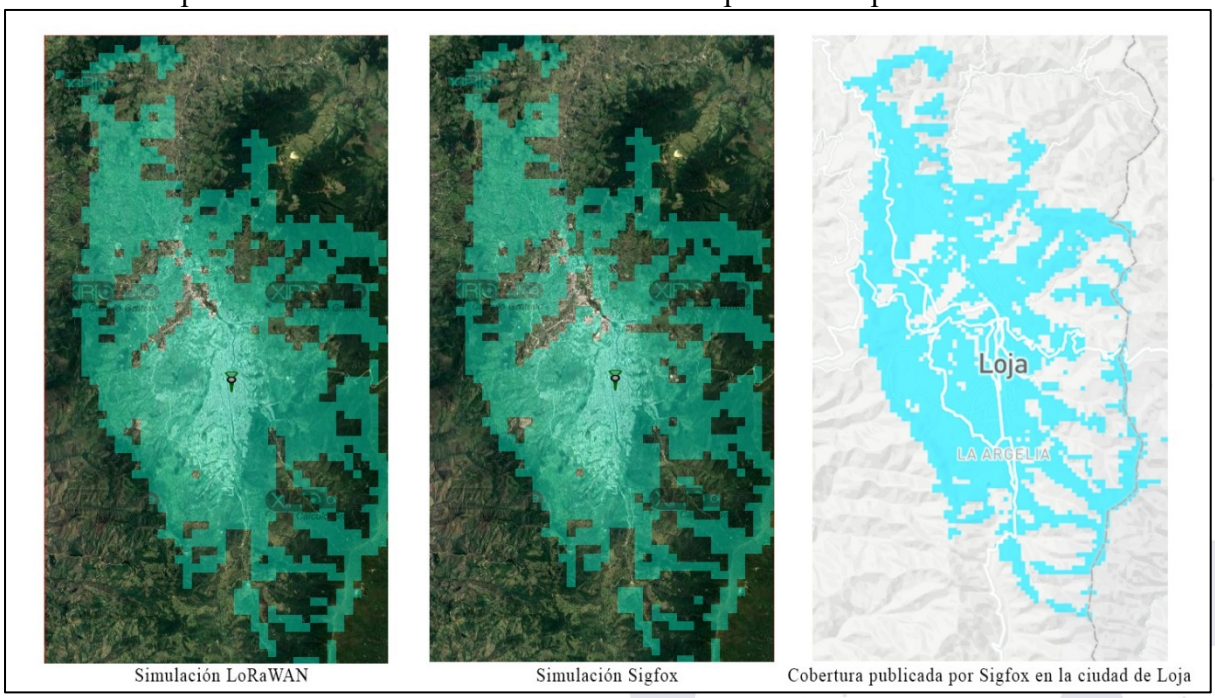
PUNTOS DE INTERES (CIUDAD DE LOJA)	LORAWAN (dBm)	SIGFOX (dBm)	DISTANCIA AL TRANSMISOR (m)	DIFERENCIA DE POTENCIA (dBm)
Barrio Ciudad Victoria	-108,82	-99,94	2961	8,88
Barrio El capulí	-93,03	-94,67	5555	1,64
Barrio Sauces Norte	-112,76	-115,30	6998	2,54
Barrio Tierras Coloradas	-115,77	-119,03	4346	3,26

Entrada al Parque Nacional Podocarpus	-123,08	-125,25	9349	2,17
Parque central	-57,48	-59,51	365	2,03
Puerta de la ciudad	-67,58	-69,72	1023	2,14
Redondel de Carigan	-100,06	-101,98	5612	1,92
Redondel Via a Zamora	-98,52	-101,91	2486	3,39
San Sebastián	-50,83	-53,07	423	2,24
Teatro Benjamín Carrión (Jipiro)	-76,24	-78,40	2955	2,16
Universidad Nacional de Loja	-77,65	-79,84	3833	2,19
Universidad Técnica Particular de Loja	-70,49	-72,67	1444	2,18
Urbanización Parquenor	-106,22	-108,52	4899	2,30

Fuente: El autor

Otra comparación útil resulta al comparar las áreas de cobertura simuladas con el área de cobertura publicada por la página oficial de Sigfox en el área de la ciudad de Loja.

Figura 28.
Comparativa de las simulaciones con los datos publicados por el fabricante.



Fuente: El autor

Como se puede apreciar los resultados de las simulaciones son consistentes con los del fabricante.

6.2 Resultados de comparación de seguridad

Los resultados de seguridad muestran que las dos tecnologías tienen falencias de seguridad que han sido explotadas por la comunidad, en algunos casos las actualizaciones por parte de Sigfox o LoRaWAN han subsanado ciertas vulnerabilidades. Existen ciertas amenazas que son propias de las características de estos dos sistemas como por ejemplo un ataque tipo jamming es fácilmente realizable ya que las dos tecnologías usan un ancho de banda estrecho que para el atacante es mucho más sencillo de contaminar con ruido haciendo que las comunicaciones reales se vuelvan ilegibles.

El modelo de negocio de las dos tecnologías también se ve reflejado en la seguridad, las especificaciones y detalles de LoRaWAN están disponibles al público mientras que las especificaciones de seguridad de Sigfox no son publicadas en su totalidad, aunque según la compañía planean hacerlo.

7. Discusión

La comparación de dos tecnologías puede parecer una tarea sencilla en un primer momento, pero existen un sin número de variables que hacen que esta tarea sea mucho más compleja como lo son diferentes implementaciones o versiones de las dos tecnologías, bandas de frecuencias permitidas según cada región o país, equipos con diferentes características para su implementación, información no divulgada por los fabricantes, etc.

Todas estas variables hacen que para lograr una comparación válida se tenga que delimitar el estudio lo más claramente posible como lo he intentado hacer en el presente estudio.

En el ámbito de las redes LPWAN todo está cambiando rápidamente, y tanto LoRaWAN como Sigfox están intentando cambiar sobre la marcha.

Las dos tecnologías tienen modelos de negocios muy diferentes y estos modelos afectan cada una de las características, por ejemplo, en este estudio hemos detallado los aspectos de seguridad de cada una de las tecnologías, pero existen factores no técnicos que también afectan la seguridad. Como por ejemplo la prevalencia en el tiempo de estas tecnologías, Sigfox ha tenido grandes problemas económicos(lunden, 2022) y en abril del 2022 se confirmó su compra por parte de UnaBiz (Wooden, 2022) un proveedor de servicios IoT con sede en Singapur. Cambios como estos o una banca rota son problemas externos que pueden afectar a la seguridad de una implementación de IoT. Qué pasaría si realizamos una implementación y el fabricante desaparece, junto con actualizaciones y mejoras de seguridad.

Y esto no solo le sucede a Sigfox, recordemos que LoRaWAN depende de la fabricación de módulos de radio LoRa cuyo único fabricante es SEMTECH, una empresa privada que no está ajena a problemas como los mencionados para Sigfox.

Las posibilidades son infinitas y la carrera tecnológica por ser la tecnología estándar para IoT es grande y tiene cada vez más participantes.

En cuanto a la cobertura las dos tecnologías son muy similares, vemos una competencia que por un lado tiene de protagonista a SEMTECH produciendo módulos de radio cada vez con sensibilidades menores (-149dBm) e intentando transmitir cada vez a mayor potencia de la forma más eficiente posible (30dBm) y por otro lado tenemos a gigantes de la industria como Texas Instruments o STMicroelectronics fabricando módulos de radio Sigfox intentando lo mismo. Nuevamente las diferencias la pueden marcar los modelos de negocios ya que con

LoRaWAN podemos implementar redes privadas adquiriendo gateways a precios muy razonables, mientras que con Sigfox dependemos de proveedores de servicios celulares y empresas proveedoras de servicios IoT para el despliegue de Access Stations.

La discusión sobre que tecnología usar prevalecerá en el tiempo, porque no existe un claro ganador en la rama de los servicios IoT, el propio mercado esta cambiando, Sigfox tiene una tasa de transferencia de datos muy baja (100bps) y si bien LoRaWAN supera esa tasa de transferencia significativamente (300bps ~ 50kbps) también se queda corto para aplicaciones actuales que necesitan gran cantidad de transferencia de datos con la menor latencia posibles.

8. Conclusiones

Luego de analizar los resultados puedo concluir que las áreas de cobertura simuladas entre LoRaWAN y Sigfox son muy similares, los niveles de potencia obtenidos en todos los puntos de interés determinados tienen una diferencia de potencia mínima entre las dos tecnologías, y los mapas de cobertura coinciden con el presentado por el fabricante, lo cual nos da una certeza de una correcta simulación.

Basándonos exclusivamente en las especificaciones, Sigfox tiene una mejor cobertura que LoRaWAN, pero vemos que llevado a la practica con una simulación de equipos reales en una ciudad de topografía irregular, esta ligera ventaja se vuelve imperceptible. La topografía resulta ser la variable determinante en cuanto a cobertura.

La selección adecuada de transmisor, antenas y sobre todo la ubicación de los mismos son las variables determinantes en el área de cobertura, si queremos mayor cobertura tenemos que invertir recursos en estas variables.

En cuanto a seguridad podemos concluir que no existe una tecnología con un nivel de seguridad perfecto, ya que los requerimientos de seguridad de las diferentes aplicaciones van desde sistemas en los que la seguridad es prácticamente innecesaria a aplicaciones en las que la seguridad puede ser de vital importancia como en control de sistemas de inundaciones, desastres naturales o vehículos autónomos. Pero si es importante que la tecnología seleccionada sea lo suficientemente flexible como para ajustarse a nuestras necesidades de seguridad. Sigfox en la actualidad brinda la opción de establecer tu propia encriptación end-to-end, lo cual es una gran ventaja para desarrollos profesionales que quieren tener el control de su seguridad implementándola por sí mismos, aunque esto implique costos adicionales.

LoRaWAN tiene un diseño muy seguro (autenticación y encriptación por defecto), pero las redes y los dispositivos pueden ser atacados si las claves de seguridad no se almacenan de forma segura, no se distribuyen al azar entre los dispositivos o se utilizan repetidamente en operaciones criptográficas.

Un sistema de comunicaciones es tan seguro, como el más débil de sus componentes, y en este caso esa debilidad corresponde a los dispositivos finales. Con el afán de producir dispositivos finales cada vez más económicos los fabricantes obvian medidas de seguridad que pueden afectar a los sistemas IoT, Usar dispositivos certificados por Sigfox y LoRaWAN nos permite

tener un mayor nivel de confianza sobre como fueron almacenadas y distribuidas las claves de seguridad y así evitar brechas de seguridad en nuestro sistema IoT.

9. Recomendaciones

La elección de equipos adecuados es un paso crucial en el futuro desempeño de nuestro sistema IoT, elegir fabricantes que brinden soluciones profesionales con soporte y actualizaciones es crucial para obtener buenos resultados a largo plazo.

Cada una de las especificaciones técnicas como ganancias de antenas, potencia de transmisor o sensibilidades de receptor son sumamente importantes, pero en sistema de radio comunicaciones es también crucial el emplazamiento físico, muchas veces invertir en una mejor ubicación resulta mas conveniente que invertir en un mejor equipo.

Cada aplicación requiere diferentes características en un sistema IoT, no podemos esperar una misma implementación para sistemas tan diferentes como el control de ganado en haciendas ganaderas muy extensas, que brindar servicios de telemetría a proveedores de agua potable en un ambiente urbano. Es absolutamente necesario un estudio previo y simulaciones con las especificaciones exactas de los fabricantes para obtener resultados de implementación adecuados.

El nivel de seguridad tiene que ser establecido por el desarrollo o implementación IoT en la que estemos involucrados, para luego elegir la mejor opción de tecnología a utilizar que mas se acerque a nuestras necesidades.

10. Bibliografía

Daniłowski, P. (2021, diciembre 22). *Yosensi | What is the real range of LoRa?* https://yosensi.io/posts/what_is_the_real_range_of_lora/

Gemalto, Actility, & SEMTECH. (2017, febrero). *LoRaWAN Security Whitepaper—LoRa Alliance®*. https://lora-alliance.org/resource_hub/lorawan-security-whitepaper/

Interline. (2022, diciembre 9). *Antennas and accessories | for wireless networks*. https://interline.pl/antennas/PANEL-14-HELIUM

LinxTechnologies. (2020). *microSplatch® uSP410 868 MHz Antenna—Linx Technologies*. https://linxtechnologies.com/wp/product/868-usp410-lpwa-antenna/

LoRaAlliance. (2015, noviembre). *What is LoRaWAN®—LoRa Alliance®*. https://lora-alliance.org/resource_hub/what-is-lorawan/

LoRaAlliance. (2023). *What is LoRaWAN® Specification—LoRa Alliance®*. https://lora-alliance.org/about-lorawan/

lunden, I. (2022). *Sigfox, the French IoT startup that had raised more than $300M, files for bankruptcy protection as it seeks a buyer | TechCrunch*. https://techcrunch.com/2022/01/27/sigfox-the-french-iot-startup-that-had-raised-more-than-300m-files-for-bankruptcy-protection-as-it-seeks-a-buyer/

RAKwireless. (2022, enero 10). *900-930MHz 8dBi Fiberglass Antenna Datasheet | RAKwireless Documentation Center*. https://docs.rakwireless.com/Product-Categories/Accessories/RAKARG15/Datasheet/

Seller, O. (2021). LoRaWAN Security. *Journal of ICT Standardization*. https://doi.org/10.13052/jicts2245-800X.915

Sigfox. (2018, enero). *LoRa and LoRaWAN: Technical overview | DEVELOPER PORTAL*. https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

Sigfox, S. (2022, marzo 1). *Sigfox Device Radio Specifications | Sigfox build*. Sigfox Connected Objects Radio Specifications. https://build.sigfox.com/sigfox-device-radio-specifications

Suarez, J. (2023, febrero 23). *Estudio del comportamiento de la tecnología LoRa en entornos urbanos*. https://repositorio.unican.es/xmlui/handle/10902/24050

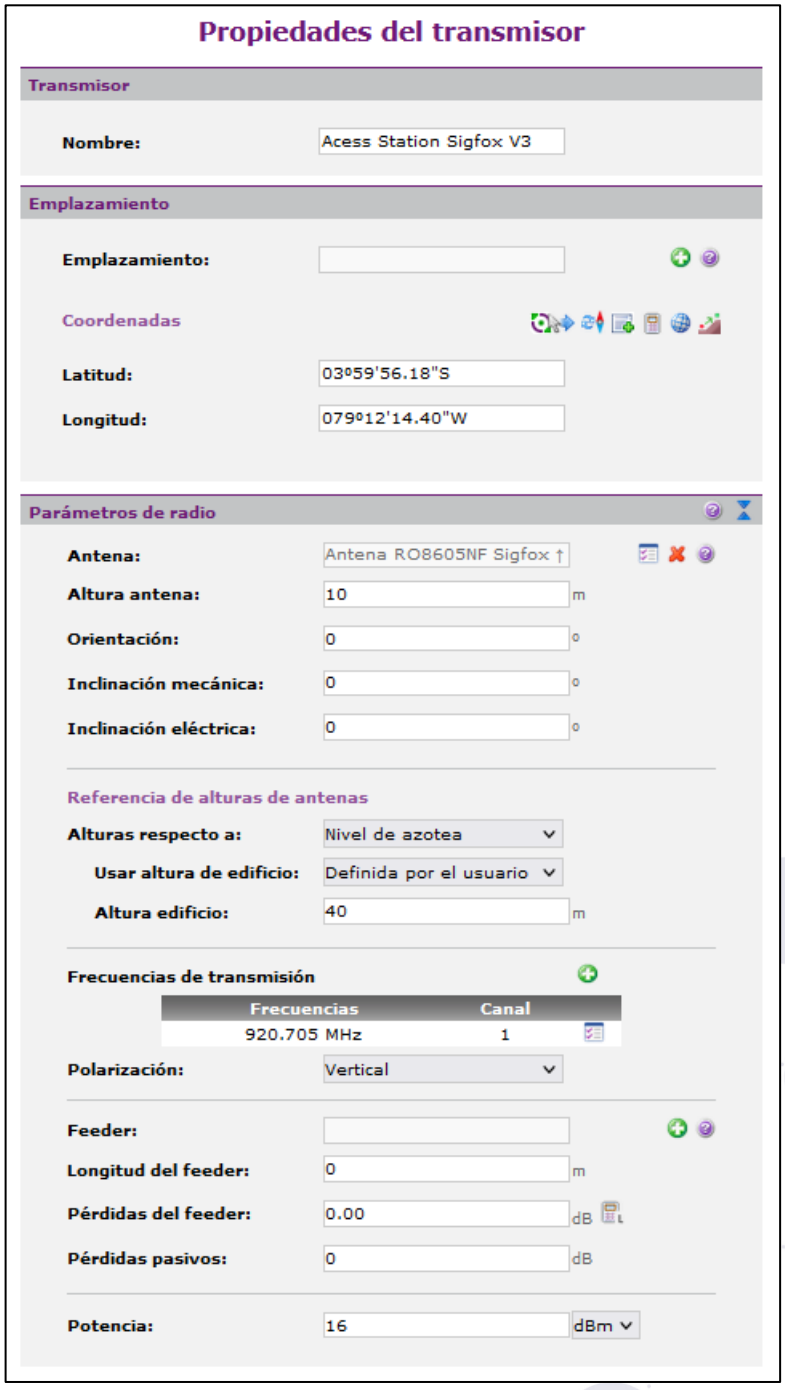
TheThingsNetwork. (2019, enero). *Super cheap LoRa node with PCB antenna—Hardware—The Things Network*. https://www.thethingsnetwork.org/forum/t/super-cheap-lora-node-with-pcb-antenna/24203

Wooden, A. (2022). *IoT firm Sigfox acquired by UnaBiz—Telecoms.com* [News]. telecoms.com. https://telecoms.com/514867/iot-firm-sigfox-acquired-by-unabiz/

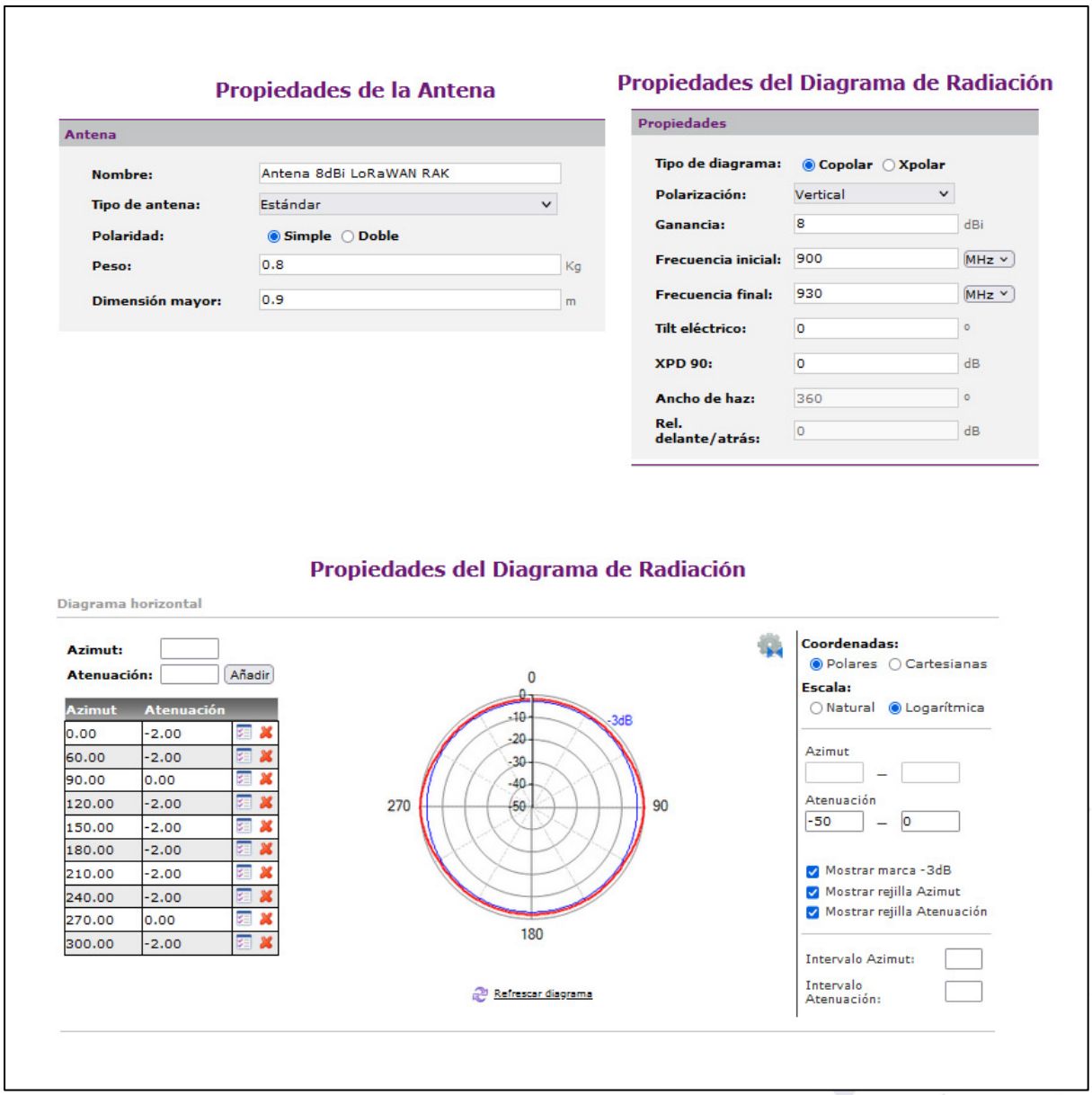
11. Anexos

Anexo 1. Configuración de transmisores LoRaWAN en Xirio Online

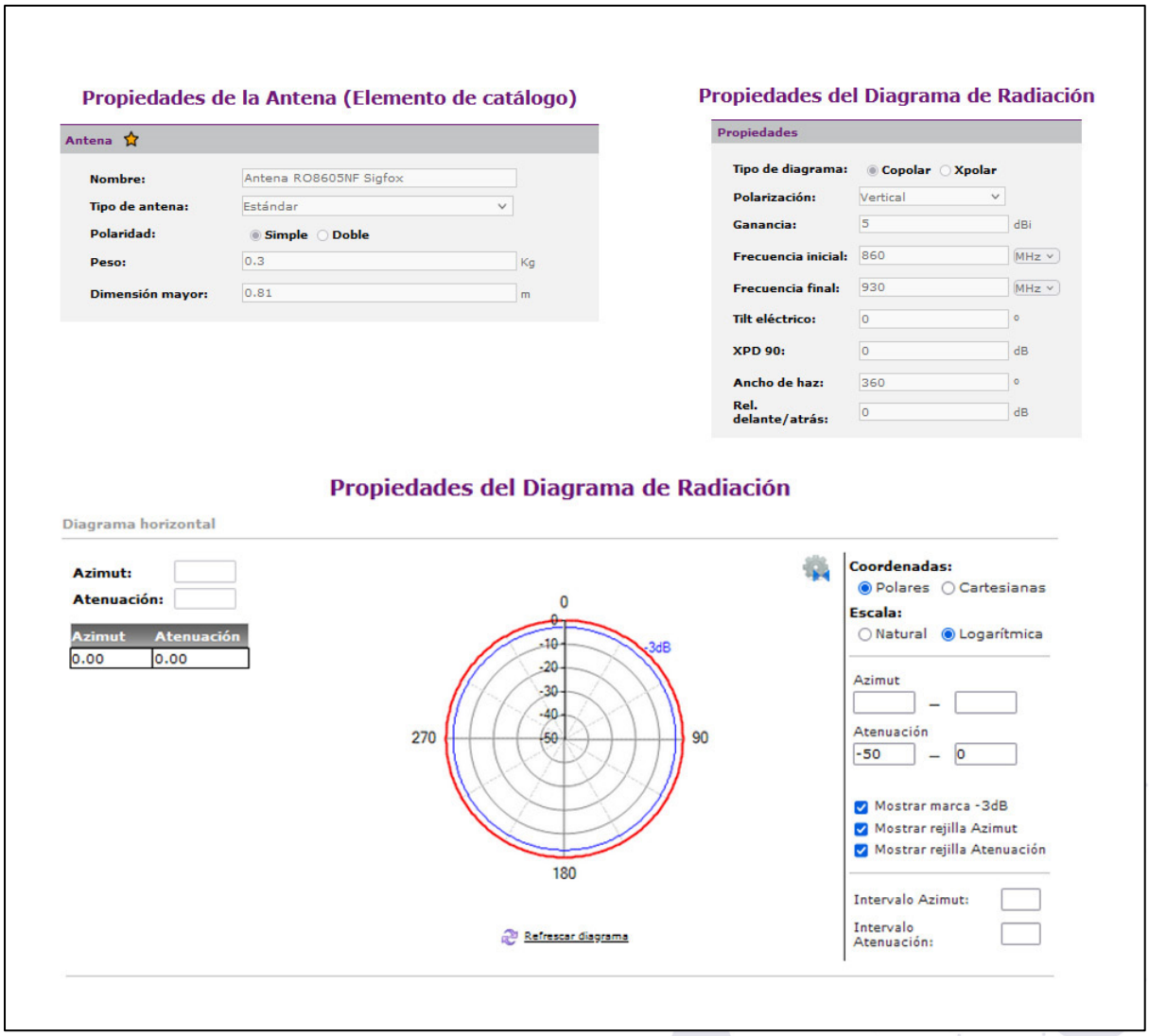
Anexo 2. Configuración de transmisores Sigfox en Xirio Online



Anexo 3. Configuración de la antena LoraWAN



Anexo 4. Configuración de antena Sigfox



Anexo 5. Puntos de interés

	Fav.	Nombre	Grupo	Latitud	Longitud	Altura (m)
			-- Sin grupo -			
	☆	Barrio Ciudad Victoria	-- Sin grupo --	04°00'07.49"S	079°13'49.73"	0
	☆	Barrio El capulí	-- Sin grupo --	04°02'55.09"S	079°11'48.15"	0
	☆	Barrio Sauces Norte	-- Sin grupo --	03°56'20.96"S	079°13'28.79"	0
	☆	Barrio Tierras Coloradas	-- Sin grupo --	04°00'44.01"S	079°14'26.98"	0
	☆	Entrada al Parque Nacional Podc	-- Sin grupo --	04°05'00.51"S	079°12'19.54"	0
	☆	Parque central	-- Sin grupo --	03°59'48.12"S	079°12'06.11"	0
	☆	Puerta de la ciudad	-- Sin grupo --	03°59'22.89"S	079°12'15.02"	0
	☆	Redondel Via a Zamora	-- Sin grupo --	03°59'36.01"S	079°10'56.36"	0
	☆	Redondel de Carigan	-- Sin grupo --	03°57'41.90"S	079°14'17.77"	0
	☆	San Sebastian	-- Sin grupo --	04°00'05.54"S	079°12'04.32"	0
	☆	Teatro Benjamin Carrio (Jipiro)	-- Sin grupo --	03°58'20.36"S	079°12'05.90"	0
	☆	Universidad Nacional de Loja	-- Sin grupo --	04°02'00.87"S	079°12'09.86"	0
	☆	Universidad Tecnica Particular de	-- Sin grupo --	03°59'13.40"S	079°11'54.99"	0
	☆	Urbanizacion Parquenor	-- Sin grupo --	03°57'18.62"S	079°12'39.05"	0

Anexo 6. Capas de cartografía utilizadas

Selección de capas

Capas disponibles en el sistema

Filtro geográfico:

Esquina	Latitud	Longitud
NorOeste:	03°50'51.17"S	079°17'01.59"W
SurEste:	04°06'50.43"S	079°08'10.13"W

Seleccione en esta lista las capas que desee utilizar. Si no encuentra una capa apropiada, contacte con nosotros: support@xirio-online.com

	Tipo	País	Nombre	Año	Res. (m)	Inc. coste (%)	CD (€)	CS (€)
	Terreno	Mundo	Altimetría mundial	2006	100	0	0	0
	Morfografía	Mundo	Clutter Mundial	2019	100	0	0	0
	Terreno	Colombia	Colombia	2016	30	30	160	400
	Terreno	Colombia	Colombia	2016	30	20	160	400
	Morfografía	Colombia	Colombia	2016	30	30	160	400

9 elementos (0 seleccionados)

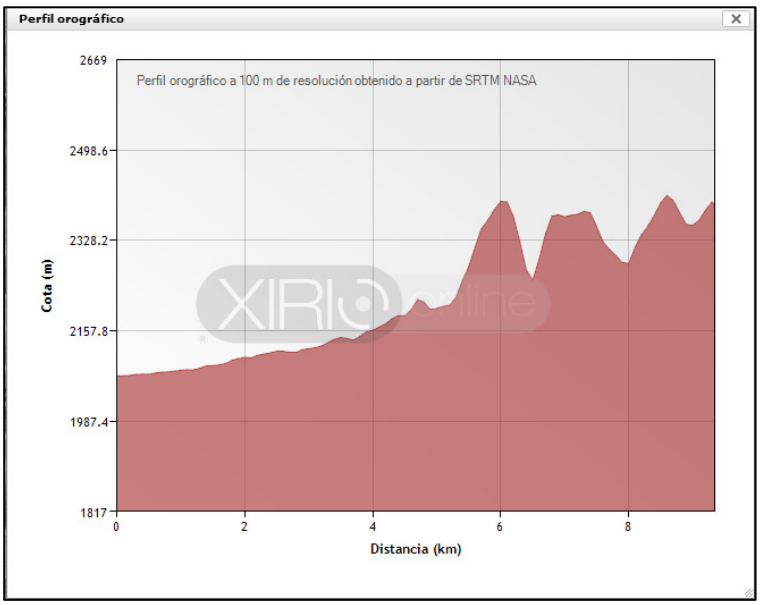
Añadir

Capas utilizadas

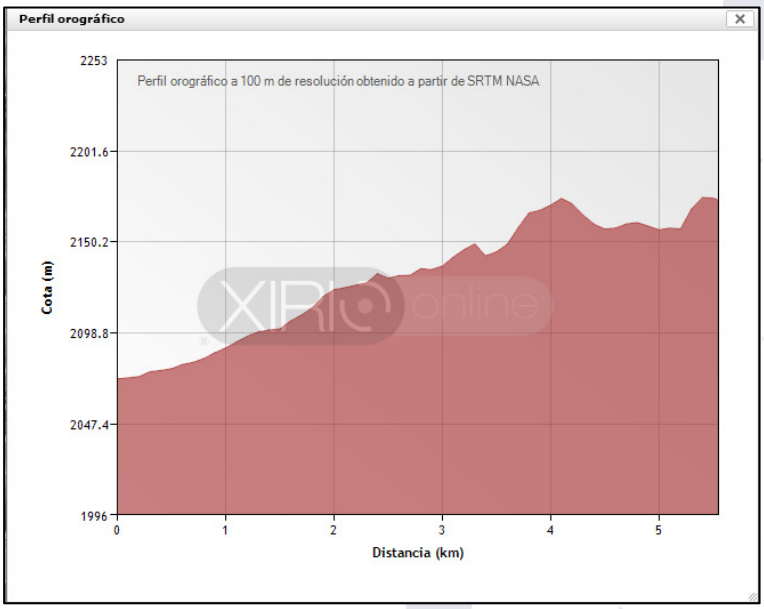
	Tipo	País	Nombre	Año	Res. (m)	Inc. coste (%)	CD (€)	CS (€)
	Terreno	Mundo	Altimetría mundial	2006	100	0	0	0
	Terreno	Ecuador	Ecuador	2016	30	20	160	400

Anexo 7. Perfiles de terreno desde transmisor hasta puntos de interés

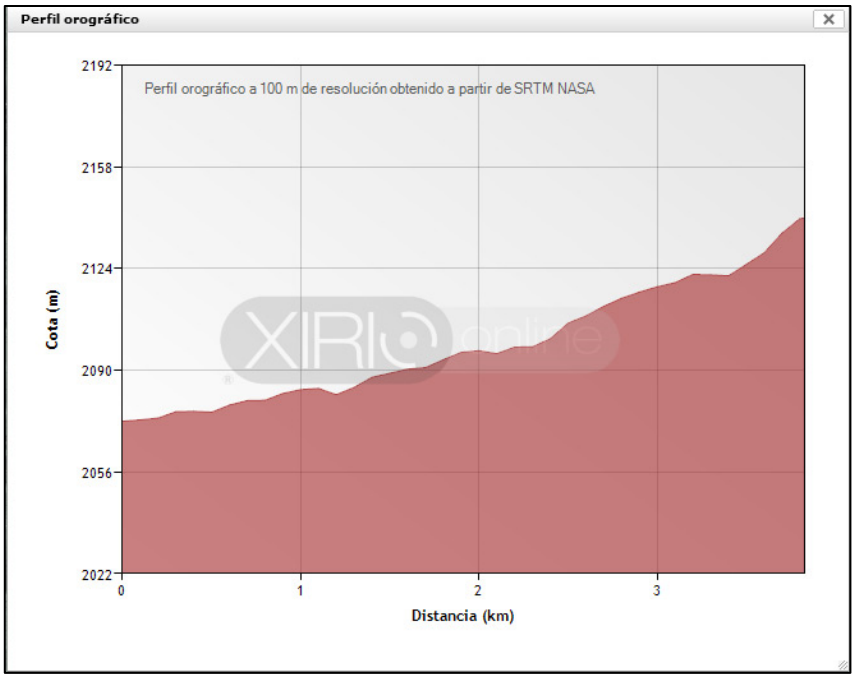
Entrada al parque nacional Podocarpus



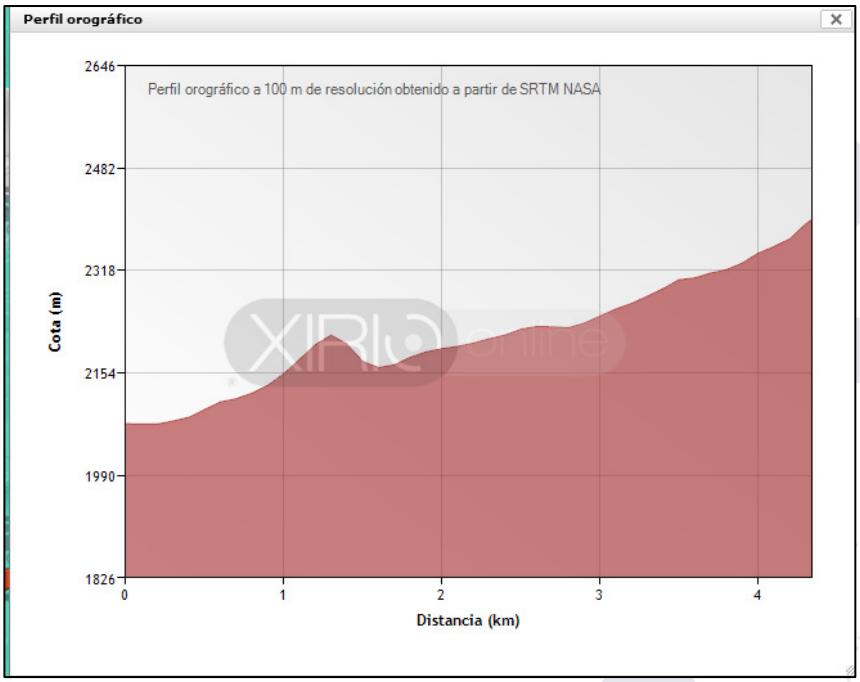
Barrio el Capulí



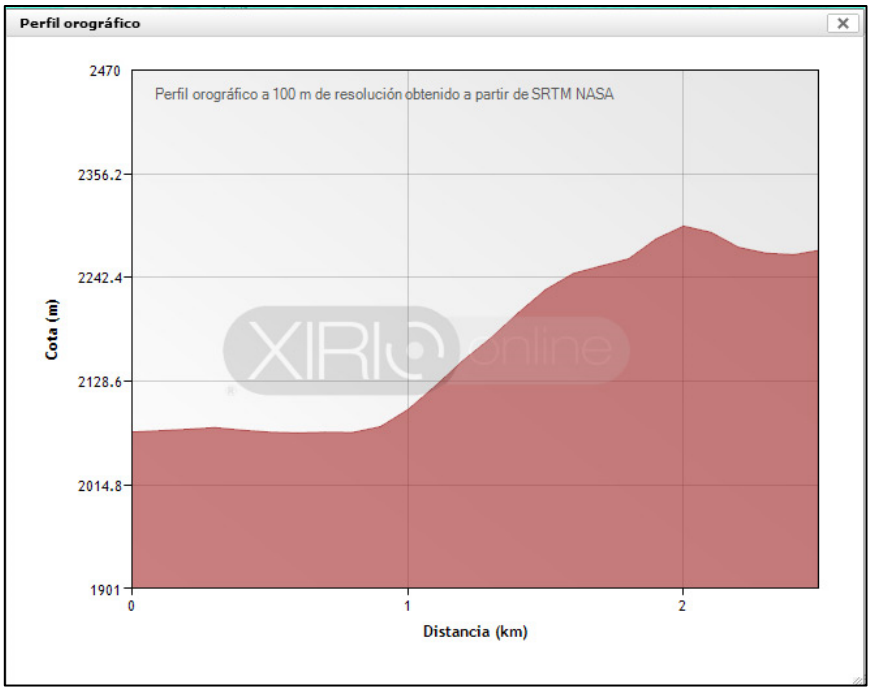
Universidad Nacional de Loja



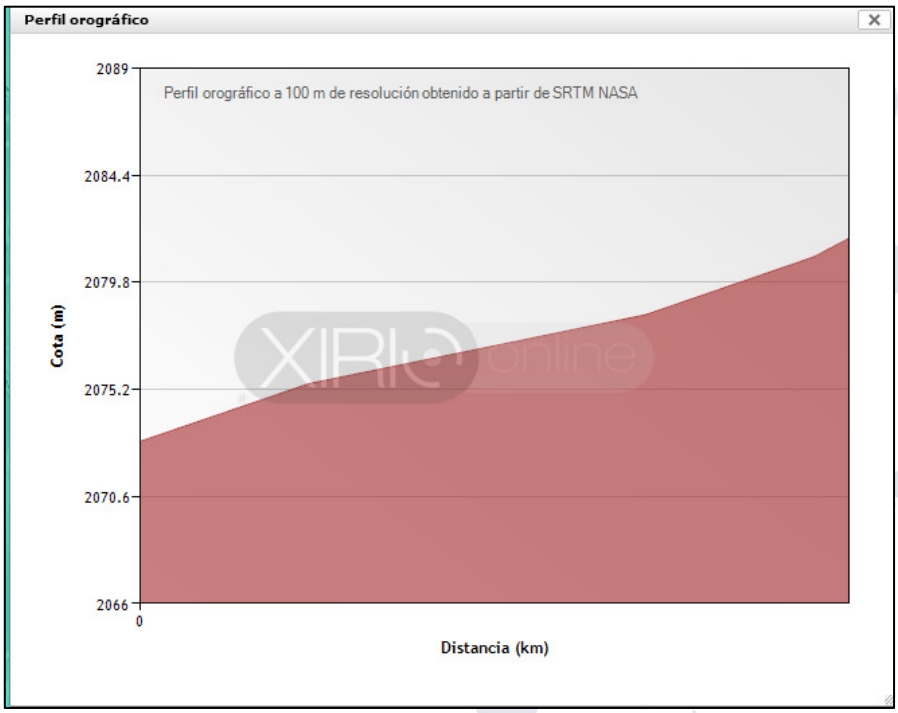
Barrio tierras coloradas



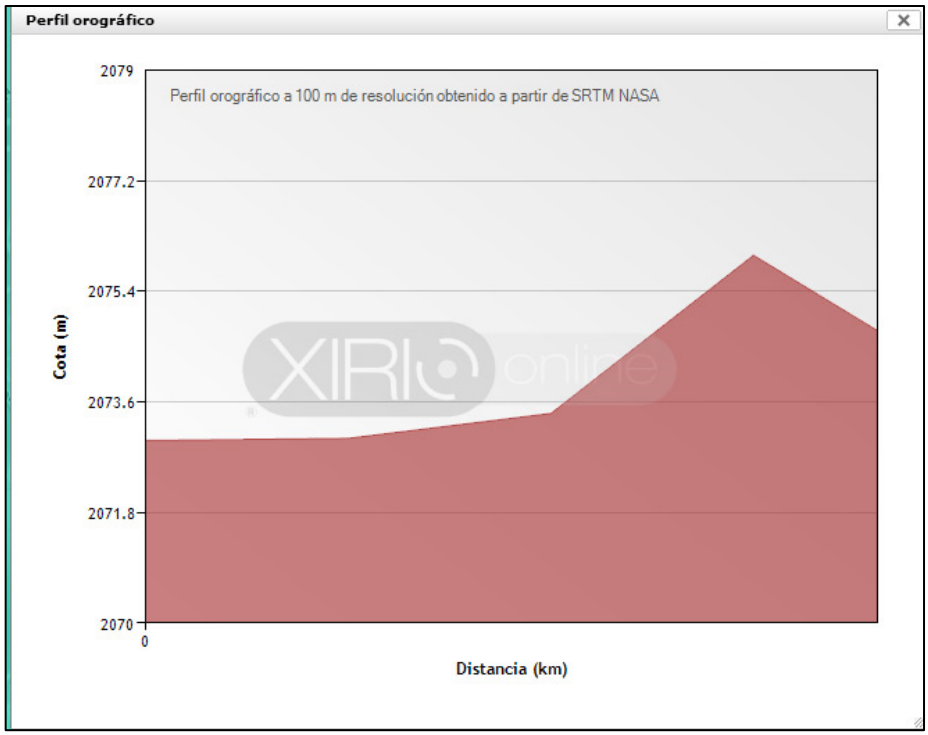
Redondel vía a Zamora



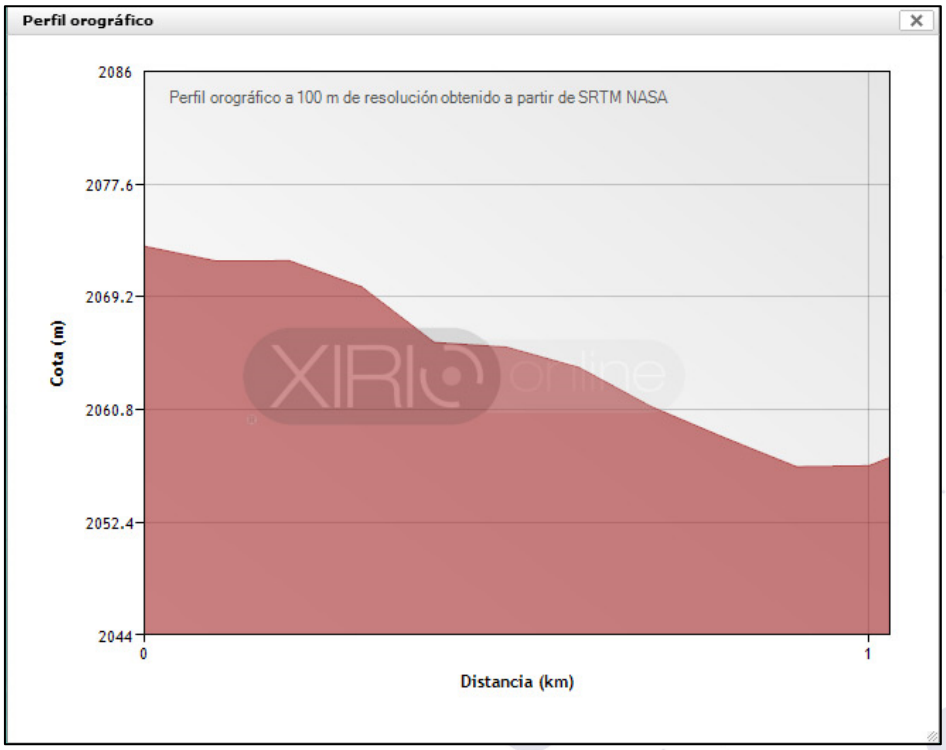
Parque San Sebastían



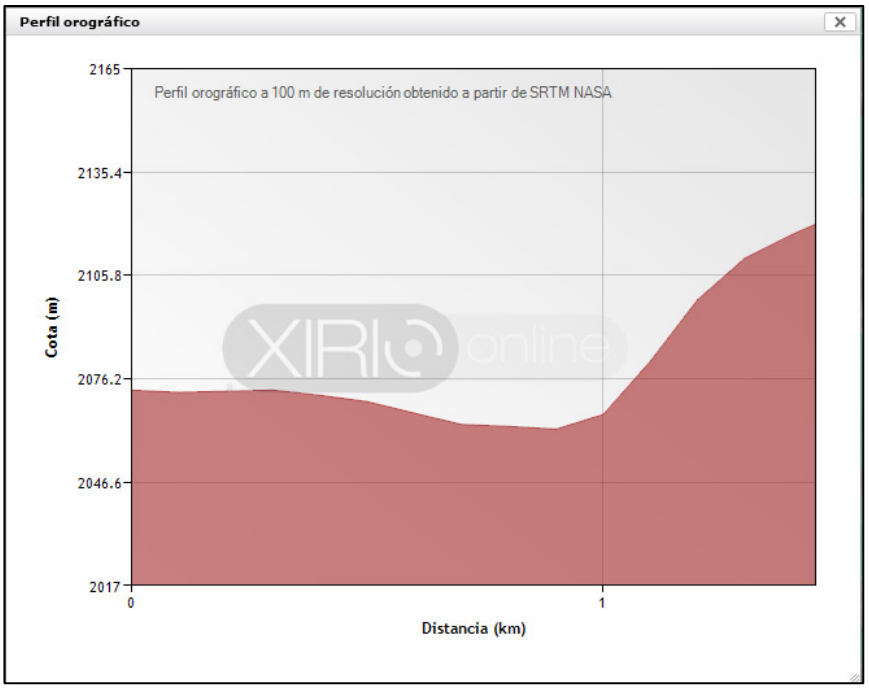
Parque Central



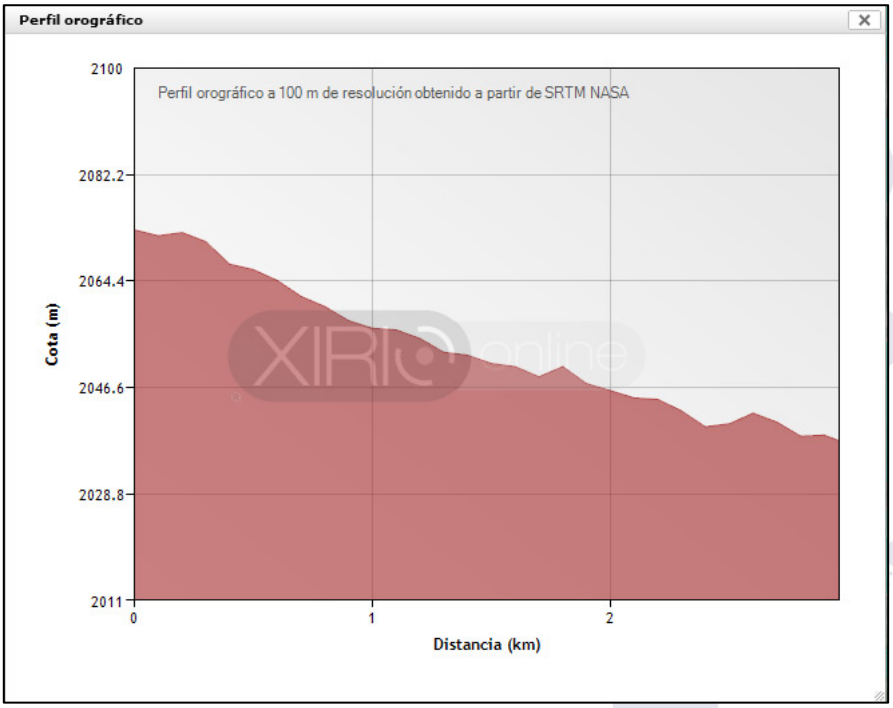
Puerta de la ciudad



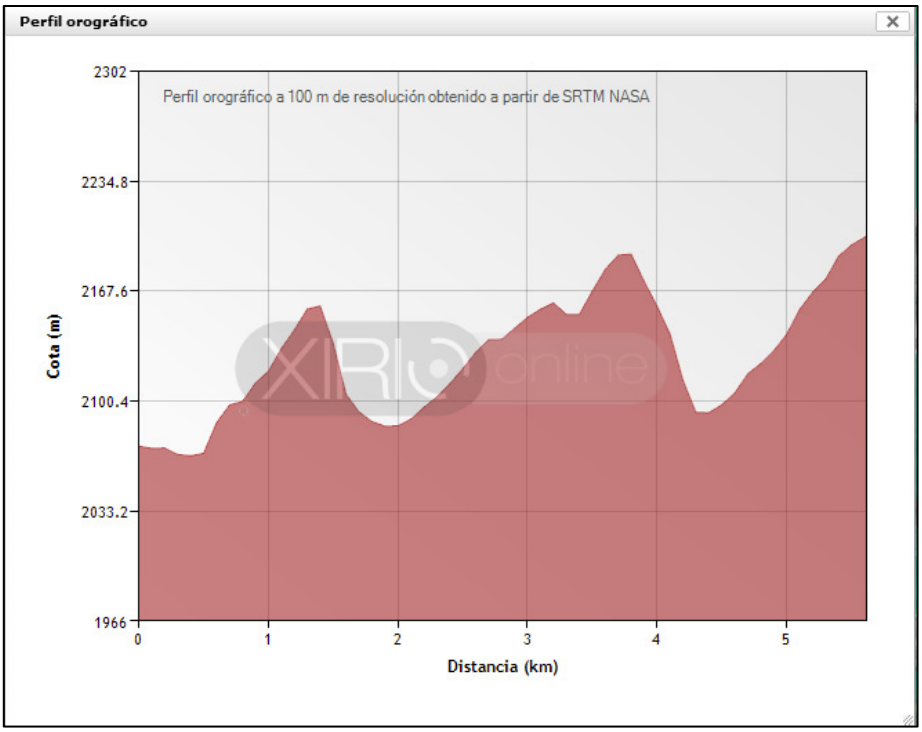
Universidad Técnica Particular de Loja



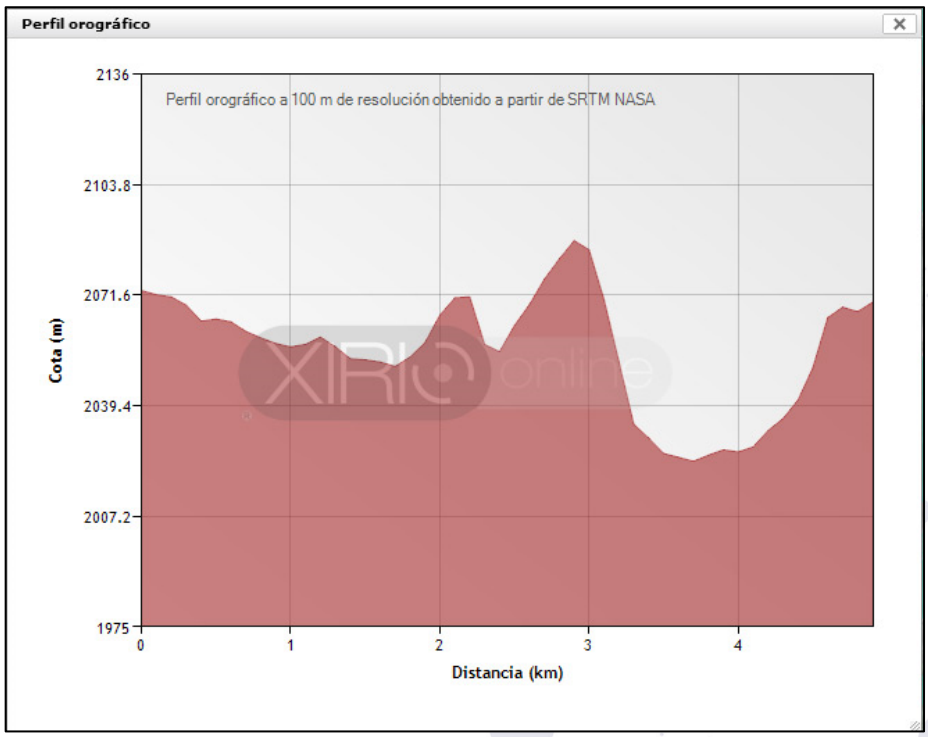
Teatro Benjamín Carrión



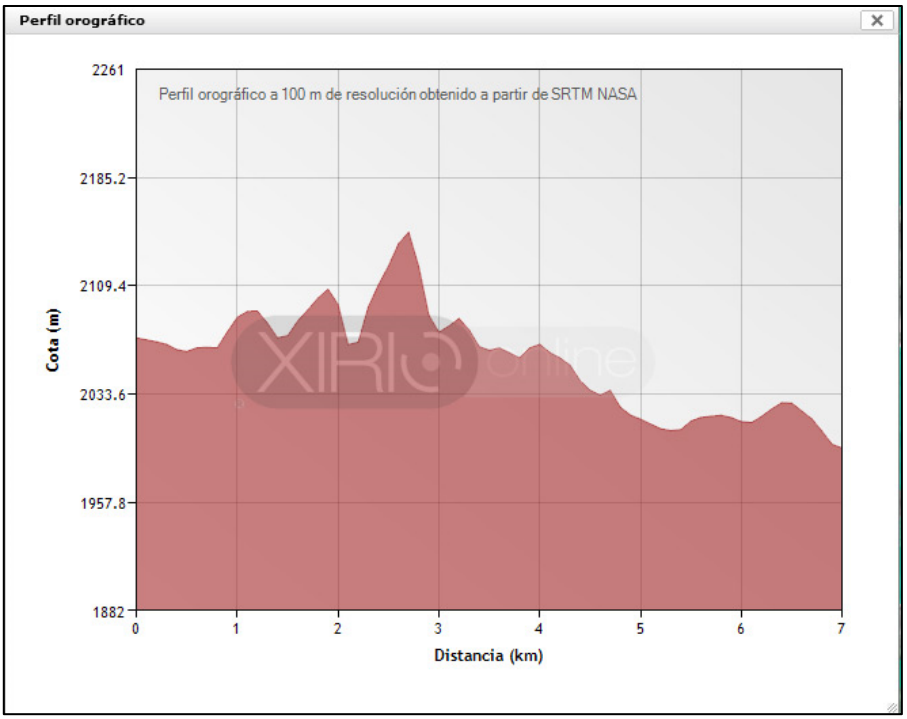
Redondel de Carigán



Urbanización Parquenor



Barrio Sauces Norte



Anexo 8. Certificado de traducción

CERTIFICADO DE TRADUCCIÓN

Andrés Baldassari
MA.App.Lng

CERTIFICO:

Haber realizado la traducción de español a inglés del resumen de la tesis titulada: "Estudio comparativo de seguridad y cobertura entre las tecnologías de IoT LoRaWAN y SIGFOX", de autoría PABLO ANDRÉS ROJAS MORA con cédula de identidad Nro. 1103873889, 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 de la Ing. Marianela Carrión González previo a la obtención del título de Magíster en Telecomunicaciones.

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

Quito, 25 de abril de 2023

Firmado electrónicamente por:
ANDRES ROBERTO
BALDASSARI CASQUETE

Andrés Baldassari MA.App.Lng
Certified Translator – Senescyt - MDT-3104-CCL-259519
Celular: (593) 098 7030 511
Email: andresbaldassari@hotmail.com

Andres Baldassari
CERTIFIED TRANSLATOR
MDT-3104-CCL-259519

CERTIFICATION OF TRANSLATION ACCURACY

An instance of a certificate of translation sample follows.

I, Andres Roberto Baldassari C. declare that I am fluent in the English and Spanish languages, and that the translation of this ABSTRACT, related to ROJAS MORA PABLO ANDRÉS, the original of which is in the Spanish language, truly reflects the content, meaning and style of the original text and constitutes in every respect a correct and true translation of the original document.

TRANSLATORS QUALIFICATIONS

Universidad Central del Ecuador - Bachelor in Arts in English Teaching.

Pontificia Universidad Católica – Master in Applied Linguistics English – Spanish

Certified Translator – Senescyt register

Universidad Central del Ecuador – Autorized translator

Andres Baldassari C. does not vouch for the authenticity of the aforementioned copy of the document or statements contained therein.

Andres Baldassari C. and his associates are not liable for any action/losses taken by the holder of this translation.

Firmado electrónicamente por:
ANDRES ROBERTO
BALDASSARI CASQUETE

Andrés Baldassari MA.App.Lng
Certified Translator – Senescyt - MDT-3104-CCL-259519
Phone: (593) 098 7030 511
Email: andresbaldassari@hotmail.com

Andres Baldassari
CERTIFIED TRANSLATOR
MDT-3104-CCL-259519