UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

SEGURIDAD EN REDES DE SENSORES INALÁMBRICOS PARA INTERNET DE LAS COSAS

TRABAJO MONOGRÁFICO

PARA OBTENER EL GRADO DE

INGENIERO EN REDES

PRESENTA

ERASMO ARTURO RUIZ CAMPOS

SUPERVISORES

M.M. JOSÉ RAÚL GARCÍA SEGURA

M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA

DR. JAVIER VÁZQUEZ CASTILLO

M.T.I. MELISSA BLANQUETO ESTRADA

MS.I. LAURA YÉSICA DÁVALOS CASTILLA

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO

ÁREA DE TITULACIÓN

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

CHETUMAL QUINTANA ROO, MÉXICO, JUNIO DE 2023

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

TRABAJO MONOGRÁFICO TITULADO

"SEGURIDAD EN REDES DE SENSORES INALÁMBRICOS PARA INTERNET DE LAS COSAS"

ELABORADO POR

ERASMO ARTURO RUIZ CAMPOS

BAJO SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ SUPERVISOR

SUPERVISORA: _____

M.M. JOSÉ RAÚL GARCÍA SEGURA

SUPERVISORA: _____

M.T.I. VLADIMIR VENJAMIN CABAÑAS VICTORIA

SUPERVISOR: _____

DR. JAVIER VAZQUEZ CASTILLO

SUPERVISOR SUPLENTE: _____

M.T.I. MELISSA BLANQUETO ESTRADA

SUPERVISOR SUPLENTE: _____

MS.I. LAURA YÉSICA DÁVALOS CASTILLA

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO
ÁREA DE TITULACIÓN

CHETUMAL QUINTANA ROO, MÉXICO, JUNIO DE 2023

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO
DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

Resumen

El presente trabajo toma importancia a raíz de los denominado "internet de las Cosas" o sus siglas en ingles IoT, cada día son más populares entre distintos segmentos de adquisición, esto gracias a que en los esquemas de competencia económica y la variante de diferentes proveedores, los denominados productos inteligentes son accesibles a distintos esquemas económicos.

Uno de los temas que regularmente no se toma al momento del diseño y/o planeación de los sistemas domóticos que se incluyen en una maqueta o cuarto inteligente es el tema de la seguridad, esto es una mala práctica y algo en lo que los usuarios deberían tener cada día más conciencia , por lo que en esta monografía que hemos estado armando, se tomó como punto inicial y referible los temas que tienen que ver con la seguridad, protocolos que pueden ser utilizados para realizar las conexiones, vinculaciones y/o asociaciones hacia las cuentas en la que los usuarios tienen información sensible.
Se suele perder el foco de todos los productos que se pueden domotizar y el impacto que pudiera generar un mal funcionamiento que se vea provocado por algún ataque informático, al día de hoy se cuentan con válvulas de gas o de agua inteligentes, entre otros, los cuales si se tuviera un mal funcionamiento pudieran llegar a ocasionar accidentes, que es probable terminen en tragedia, con pérdidas materiales, monetarias o situaciones que involucran la salud de los usuarios.

Durante la investigación realizada se encontraron ciertos protocolos, de los cuales abundaremos en las secciones correspondientes, priorizando y focalizando siempre la seguridad, se recuperó información sobre temas como el alcance, tecnología, frecuencias, etc.

Agradecimientos

A mi familia que lucho día a día para poder darme los recursos necesarios que permitieron que siga estudiando esta maravillosa carrera y poder terminarla a pesar de las adversidades que pasamos, a todos los que creyeron en mi a pesar de tener muchas cosas en contra.

A todas aquellas personas que estuvieron a mi lado en la carrera, principalmente a esos amigos que logre conocer, que estuvieron apoyándome y dándome ánimos para seguir adelante.

También agradezco mucho a todos los maestros que estuvieron presentes y dieron lo mejor de sí en cada clase para que podamos aprender de sus enseñanzas, que sin ellas esto no hubiese sido posible, ya que cada día aprendíamos algo nuevo.

Finalmente, gracias a la vida por permitirme terminar esta etapa como estudiante tan significativa para mí.

Dedicatoria

¡A mi familia, que siempre estuvo apoyándome! ¡Lo logrÉ!

Tabla de contenido

Tabla de ilustraciones

Capítulo 1 Introducción

1.1 Internet de las cosas

Internet de las Cosas es una traducción de la expresión en inglés Internet of Things (IoT), que describe un escenario en el que diversas cosas están conectadas y se comunican mediante Internet. Esa innovación tecnológica tiene como objetivo conectar a Internet a los objetos que usamos diariamente, con el objetivo de aproximar cada vez más el mundo físico a la digital.

El término nació en 1999, cuando Kevin Ashton, del Massachusetts Institute of Technology (MIT), escribió el artículo “Las cosas de Internet de las Cosas”. Para él, la falta de tiempo de las personas genera la necesidad de conectarse a Internet de nuevas maneras. Estas permiten la creación de dispositivos que ejecutan tareas que no necesitamos hacer. Estos dispositivos conversan por medio de diferentes protocolos dentro de la misma red, acompañan nuestras actividades, almacenan información y, a partir de ahí, nos auxilian en el día a día.

1.2 Redes de sensores inalámbricos

Las redes de sensores son dispositivos autónomos que trabajan de manera colaborativa para recolectar información del ambiente o de un entorno específico. Cada elemento de la red es relativamente barato y normalmente se comunica de manera inalámbrica, ofreciendo un sistema flexible y fácil de instalar en grandes cantidades.

Las redes de sensores Inalámbricos (WSN, del inglés Wireless Sensor Networks) están formadas por dispositivos autónomos, distribuidos a lo largo de un área de interés y cuyo objetivo es monitorizar parámetros físicos o ambientales tales como temperatura, sonido, vibraciones, presión, movimiento o agentes contaminantes. Las WSN se consideran una de las tecnologías clave para implementar el Internet de las Cosas (IoT).

Los dispositivos trabajan de manera colaborativa para recoger los datos y enviarlos a un colector central, eligiendo la ruta de comunicaciones optima (de dispositivo a dispositivo) a través de la red hasta llegar a su destino. Las redes de sensores son a menudo bidireccionales, permitiendo configurar los dispositivos, enviar comandos, o actuar sobre el ambiente. En este último caso, se les conoce como WSAN (del inglés Wireless Sensors and Actuator Networks).

Una de las características más interesantes de las Redes de Sensores es su bajo consumo ya que dota a los dispositivos de una gran autonomía (típicamente de 5 a 10 años). Esto permite que los sensores se desplieguen en localizaciones poco accesibles o incluso integrados dentro de estructuras. Si, además, añadimos tecnologías de energy harvesting (recolección de energía del ambiente), la autonomía del dispositivo puede ser infinita.

1.3 Estándares de comunicaciones para implementar WSN en IoT.

1.3.1 WiFi

WiFi es una tecnología de red inalámbrica a través de la cual los dispositivos, como computadoras (portátiles y de escritorio), dispositivos móviles (teléfonos inteligentes y accesorios) y otros equipos (impresoras y videocámaras), pueden interactuar con

Internet. Permite que estos dispositivos, entre tantos otros, intercambien información entre sí y establezcan, de esta manera, una red.

La conectividad a Internet se logra a través de un router inalámbrico. Cuando accede a WiFi, se conecta a un router inalámbrico que permite que los dispositivos que admiten WiFi interactúen con Internet.

Imagen 1: WiFi; shutterstock
https://www.montclair.edu/student-services/2018/01/14/are-you-connected/

1.3.2 Bluetooth y Bluetooth low energy

El Bluetooth es un protocolo de comunicaciones que sirve para la transmisión inalámbrica de datos (fotos, música, contactos) y voz entre diferentes dispositivos que se hallan a corta distancia, dentro de un radio de alcance que, generalmente, es de diez metros. Por ejemplo, gracias a esta tecnología, podemos vincular nuestro smartphone con una impresora para imprimir nuestras fotos preferidas sin necesidad de cables.

El uso del Bluetooth se ha asociado a los teléfonos móviles, ya que éstos fueron de los primeros dispositivos en incorporar el protocolo. Sin embargo, esta tecnología inalámbrica se encuentra presente, hoy en día, en smartphones, tablets, portátiles, ratones, teclados, impresoras, auriculares, televisores, cámaras digitales, reproductores MP3 o videoconsolas.

Curioso es, por otro lado, el origen del nombre Bluetooth. Para explicarlo, hemos de remontarnos a la historia del dominio de los vikingos en el norte de Europa, ya que esta denominación proviene del rey de Dinamarca y Noruega Harald Blåtand (en inglés, “Harald Bluetooth”), quien unificó las tribus danesas y noruegas y contribuyó, de esa forma, a que los miembros de unas y otras pudieran comunicarse entre ellos. De ahí el sentido de llamar Bluetooth a esta tecnología inalámbrica, encargada de facilitar la comunicación (sin tener que recurrir a cables) entre distintos dispositivos.

El Bluetooth de baja energía (Bluetooth Low Energy o BLE), es un subconjunto del estándar Bluetooth v4.0. Dispone de una pila de protocolos completamente nueva y orientada a conexiones sencillas en aplicaciones de muy baja potencia (dispositivos dependientes de batería o pila).

Dentro de las oportunidades que ofrece esta tecnología, una de sus mayores ventajas reside en el hecho de la aceptación obtenida por parte de las grandes plataformas de hoy en día como IOS, Android, Microsoft o Linux entre otras y su compatibilidad con éstas.

Cabe destacar las características fundamentales del BLE, como son su interoperabilidad en el mundo de los fabricantes de chipsets, su tamaño reducido, sus requerimientos de potencia muy bajos y un aceptable rango de alcance en las comunicaciones.

Imagen 2: Bluetooth

global-tag.com

1.3.3 NB-IoT

Narrow Band IoT (NB-IoT) es la apuesta de 3GPP para dar respuesta a las necesidades de comunicación IoT, en lo que denominan extended Machine Type Communications (eMTC). NB-IoT aparece como respuesta al auge de las Low Power Wide Area Networks (LPWAN) como lo son tecnologías LoRaWAN, Telensa o Sigfox entre otras. Las LPWAN se caracterizan por ser tecnologías de largo alcance, dando cobertura hasta 15 km en entornos abiertos y hasta 2 km en entornos urbanos.

Estas tecnologías, se han propuesto para dar acceso a un número potencialmente alto de dispositivos que tienen que transmitir pocas cantidades de datos (pocos bytes) de forma esporádica (p. ejemp. cada varios minutos), mayoritariamente en uplink. Las LPWAN se usan en aplicaciones como la tele-lectura de contadores, el control del alumbrado público, las alarmas de robo o los sistemas de control en infraestructuras entre muchas otras.

El 3GPP ha tardado bastante en unirse a la tendencia después que LoRaWAN tomara gran parte del mercado.

NB-IoT es una tecnología basada en comunicaciones celulares; es decir, usa las bandas celulares de comunicación y fue diseñada para operar de distintas formas, incluyendo el uso de la banda de GSM substituyendo el despliegue actual (standalone), usando la banda de LTE y por lo tanto compartiéndola (in-band) o incluso utilizando el espaciado que hay entre los canales LTE para aprovechar al máximo el espectro de comunicaciones (guard-band).

A diferencia de las LPWAN, NB-IoT nace condicionado por la arquitectura LTE y debe coexistir con esta tecnología sin introducir modificaciones a la estructura y

arquitectura de la red celular. Esto implica una complejidad mucho más elevada que sus competidoras LPWAN.

NB-IoT es una tecnología half-duplex que habilita de forma eficiente la comunicación uplink; es decir, permite un establecimiento de conexión a la red celular, la asignación de recursos de red al nodo (conocido como User Equipment o UE) y la transmisión de los datos.

Imagen 3: Logotipo de NB-IoT.
https://www.leixue.com/ask/what-is-nb-iot

1.3.4 LoRa

LoRa es una tecnología inalámbrica desarrollada para permitir las comunicaciones de datos a baja velocidad en grandes distancias entre los sensores y los actuadores de las aplicaciones entre máquinas M2M e IoT. Emplea un espectro de radio sin licencia en las bandas industriales, científicas y médicas (ISM) para hacer posible las comunicaciones de bajo consumo y largo alcance entre sensores remotos y puertas de enlace (gateways por sus siglas en inglés) conectadas a la red. Utiliza tecnología de espectro ensanchado con una banda más ancha. Su chip modulado por frecuencia emplea ganancias de codificación para una mayor sensibilidad del receptor.

LoRaWAN es una especificación de protocolo de infraestructura LPWAN de código abierto construida con base a la tecnología LoRa y desarrollada por LoRa Alliance,

que permite a otras empresas crear sus propias redes del IoT basadas en sus especificaciones tecnológicas. Este enfoque basado en estándares para construir una LPWAN permite que se configuren rápidamente las redes del IoT públicas o privadas en cualquier lugar utilizando hardware y software bidireccionalmente seguro, interoperativo y móvil que ofrece una localización precisa y funciona de la forma esperada.

Una red LoRa se puede configurar para ofrecer una cobertura similar a la de una red celular. muchos de los operadores LoRa son operadores de redes celulares que pueden utilizar los postes ya existentes para montar las antenas LoRa. En ciertas instancias, las antenas LoRa se pueden combinar con las antenas celulares, ya que las frecuencias pueden ser cercanas y combinar las antenas puede ofrecer ventajas de costes significativas.

Las características principales de LoRa son su largo alcance de 15 a 20 kilómetros, que se puede conectar a millones de nodos y que sus baterías duran más de 10 años. Las aplicaciones para la tecnología inalámbrica LoRa incluyen medidores inteligentes, seguimiento de inventario, máquinas expendedoras, datos y monitorización, automoción y aplicaciones que necesitan control e informes de datos.

Imagen 4: Logotipo LoRa

https://www.gorilladistribution.com.au/2015/06/05/lora-technology/

1.3.5 SigFox

SigFox es una red de conectividad celular a nivel mundial enfocada para el IoT. Esta red está diseñada para comunicaciones de baja velocidad permitiendo reducir los costos y el consumo de energía de los dispositivos conectados.

Además, la comunicación, aparte de ser de baja velocidad, también se basa en una banda muy estrecha, lo que permite a los dispositivos tener un alto poder de penetración a obstáculos, facilitando la comunicación a grandes distancias, incluso en suelo urbano.

Suscripción a SigFox

SigFox, sus precios varían según la cantidad de dispositivos que sus clientes desean conectar a su red y la cantidad de datos que pasan a través de ella. En promedio, suscribirse a esta red IoT costaría setenta pesos mexicanos por año (3 euros) y por objeto, según SigFox. Pero los precios pueden variar entre uno y nueve euros por año y por sensor, según foros especializados. (Garcia-Montero, 2020)

Infraestructura

La red SigFox se basa en una estructura formada por antenas y estaciones base repartidas por todo el territorio que se comunican con lo sensores finales y con el servidor SigFox donde se almacenan los datos. Esta red de antenas y estaciones base, en España, ha sido instalada por la empresa Cellnex y se encuentra operada por SigFox.

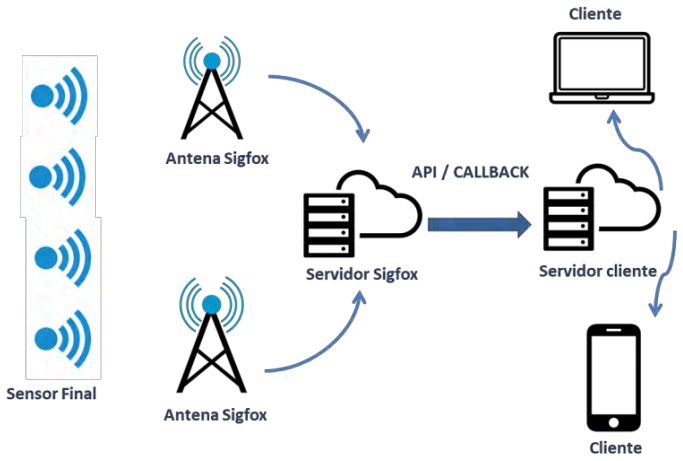

Imagen 5: Infraestructura

productos-iot.com

Cómo funciona SigFox

Desde un punto de vista técnico, como hemos visto SigFox depende de otra red distinta, basada en 868Mhz.

Cada nodo puede cubrir un área de cobertura bastante grande. Además, empresas que necesiten mejorar la cobertura en su área pueden instalar un equipo repetidor. (Ferrer, s.f.)

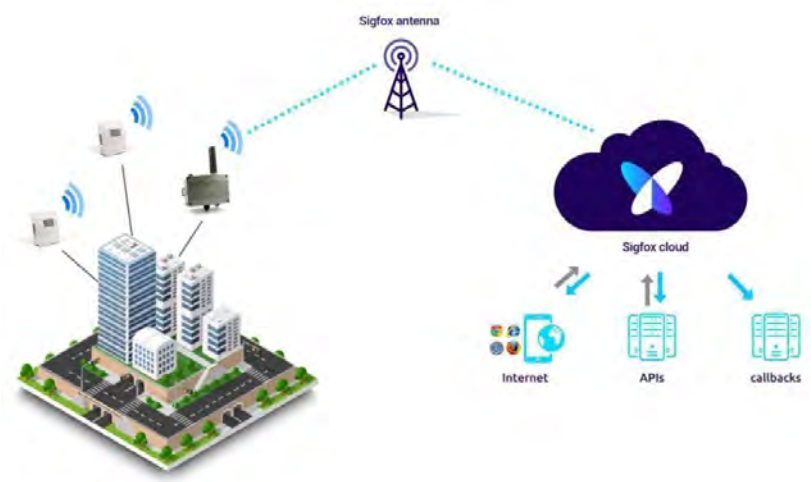

Imagen 6: Función de SixFox

vicentferrer.com

1.4 Justificación

La facilidad de tener diversos dispositivos conectados a Internet por parte de los usuarios ha ocasionado que se incremente el riesgo de que su información se vea comprometida. Lo anterior puede aplicar para dispositivos de usuario común o dispositivos nodos sensores de red bajo el paradigma IoT. En este sentido, los estándares actuales y propuestos para desarrollar IoT son: WiFi, BLE, NB-IoT, LoRa y SigFox, los cuales han incorporado una serie de técnicas/estrategias a sus arquitecturas de red buscando incrementar la seguridad de los nodos sensores, así como también, la confianza de los usuarios finales.

Este trabajo busca realizar una revisión y documentar las técnicas empleadas para incrementar la seguridad en los estándares en redes WSN-IoT.

1.5 Objetivo general

Proporcionar una revisión bibliográfica sobre esquemas de seguridad en redes de sensores inalámbricos implementados con diferentes estándares de comunicaciones.

1.6 Objetivos específicos

1. Revisión del estado del arte de las tecnologías de radio con las cuales es posible implementar redes de sensores inalámbricos (Wireless Sensor Networks, WSN).
2. Revisión de los distintos estándares de comunicación para implementar WSN.

3. Revisión de los esquemas de seguridad proporcionados en los estándares de comunicación de datos.
4. Redacción del trabajo monográfico.

Capítulo 2 Marco conceptual

2.1 Esquemas de seguridad en los estándares de comunicaciones

2.1.1 WiFi

En informática, se conoce como WiFi a una tecnología de telecomunicaciones que permite la interconexión inalámbrica entre sistemas informáticos y electrónicos**,** tales como computadoras, consolas de videojuego, televisores, teléfonos celulares, reproductores, etc.

Esta tecnología les permite a dichos dispositivos conectarse entre sí para intercambiar datos, o bien conectarse a un punto de acceso de red inalámbrica, pudiendo tener así conexión a Internet.

El WiFi surgió como respuesta a la necesidad de estandarización y compatibilidad en los modelos de conexión inalámbrica de los diversos dispositivos digitales, superando además otras formas no compatibles de conexión como son el Bluetooth, GPRS, UMTS, etc. A diferencia de estos, el WiFi emplea las ondas de radio como vehículo de transmisión de la información.

Esta tecnología está diseñada para conectar dispositivos a distancias relativamente cortas (100 metros como máximo), en especial en entornos que ofrezcan mucha interferencia o ruido a la señal, como la producida por la saturación del espectro radioeléctrico debido a multiplicidad de emisiones. Además, es una conexión más lenta que la cableada, pero significativamente más cómoda y versátil.

La seguridad del WiFi es variable, principalmente en función del cifrado que se aplique a las comunicaciones entre el router y los adaptadores inalámbricos. Existen varias opciones, y se pueden dividir entre seguras y no seguras por sus características técnicas.

Una WiFi abierta, sin contraseña, no aplica cifrado en las comunicaciones y no tiene contraseña de acceso. Esta es la opción más insegura, en tanto que cualquiera puede conectarse con el router e interceptar sus comunicaciones con los dispositivos conectados al mismo. Por lo tanto, es relativamente sencillo espiar a cualquier usuario. Pero también es inseguro el cifrado WPS (WiFi Protected Setup), que es el más básico. Es un cifrado débil y con vulnerabilidades demostradas que permiten conseguir la clave de cifrado en apenas unos minutos.

El cifrado WPA, que es posterior, sí se considera seguro, aunque no lo es al cien por cien. También se considera seguro el cifrado WPA2, que es una evolución de este anterior, y no solo mejora la seguridad, sino que también introduce mejoras relativas al rendimiento en los intercambios de información. Estas dos opciones, como comentábamos anteriormente, son las que se consideran seguras en la actualidad.

Los diferentes tipos de WiFi se clasifican según los estándares 802.11 y, en función del utilizado, varia la velocidad de la señal:

- IEEE 802.11. Creado en 1997, en el presente ya no se usa. Éste permitía una velocidad máxima de conexión de dos megabits por segundo, unos valores muy lentos para la mayor parte de las aplicaciones.

- IEEE 802.11a. Surgió en 1999 con una velocidad máxima de 54 megabits por segundo. Esta versión fue la primera en funcionar a 5 GHz, una

frecuencia bloqueada fácilmente por los objetos, hace que este estándar tenga un alcance limitado.

- IEEE 802.11b, IEEE 802.11g, IEEE 802.11n. Cuentan con velocidades máximas de 11, 54 y 300 megabits por segundo y disponen de una frecuencia de 2,4 GHz, una banda casi universal que los convierte en los más empleados internacionalmente.

- IEEE 802.11ac. Nacido en 2014 y conocido como WiFi 5, funciona a una velocidad máxima de 1.300 megabits por segundo y opera en la banda de 5GHz.

Se conocen diversos tipos de WiFi, de acuerdo con los estándares que emplean pueden distinguirse en dos categorías:

- Banda de 2,4 GHz. Aquí se encuentran los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n, cuyo manejo es internacional y permite velocidades de 11 Mbit/s, 54 Mbit/s y 300 Mbit/s respectivamente. Sin embargo, es el tipo que mayor interferencia cuenta, dado que la banda de 2,4 GHz es también empleada por Bluetooth y otros sistemas inalámbricos.

- Banda de 5GHz. Conocido como WiFi 5, aplica el estándar IEEE 802.11ac y se maneja en un canal libre de interferencias, por lo que, a pesar de ser una tecnología y de tener la desventaja de un 10% menos de distancia de alcance, se le considera sumamente conveniente dada su estabilidad y velocidad.

2.1.2 WiFi 6E

En abril de 2020, la Comisión Federal de Comunicaciones (FCC) anunció la apertura de la banda de 6 GHz para WiFi y otros usos sin licencia. Podría decirse que es una de las mejores cosas que han sucedido en WiFi desde que surgieron WiFi 6 y el acceso múltiple por división de frecuencia ortogonal (OFDMA).

La lista de ventajas es larga para WiFi 6E:

- **Solo requiere WiFi 6 y OFDMA (Orthogonal Frequency Division Multiple Access)**: no hay dispositivos heredados lentos (802.11a/b/g/n/ac)
- **Programado**: puede segmentar e implementar políticas de seguridad y calidad de la experiencia (QoE)
- **Retraso optimizado**: menos de dos ms a escala, incluso en entornos de alta densidad
- **Ancho de banda increíble**: los canales amplios se admiten y fomentan fácilmente.
- **RF limpia**: bajo nivel de ruido, menos congestión

Lo relevante son los 1200 MHz de espectro entre 5,925 GHz y 7,125 GHz, que se conoce colectivamente como la banda de 6 GHz. Sin embargo, una distinción importante aquí es que este es un espectro "contiguo". Eso significa que no hay interrupciones ni espacios en el rango de frecuencia de principio a fin. Los rangos definidos históricamente para las operaciones de WiFi se han agregado con el tiempo a medida que el espectro estuvo disponible y se pudo demostrar la necesidad. Los rangos de espectro deseables que no se utilizan son difíciles de conseguir, pero las tecnologías cambian o se vuelven obsoletas con el tiempo. A medida que esto sucede, los rangos de espectro ven cada vez menos usuarios

principales, y algunos rangos finalmente se resignan a otros usos. El espectro es un recurso valioso y, a medida que el WiFi ha madurado, también lo ha hecho la tecnología.

WiFi fue diseñado desde su inicio para ser un buen vecino y nunca interferir con otros servicios que operan en la misma banda. Las restricciones de nivel de potencia para limitar la interferencia de los vecinos siempre han sido parte de las reglas regulatorias.
WiFi 6E cambia un poco las cosas y define cuatro clases de acceso separadas para WiFi, cada una con sus propias reglas:

- **Alimentación estándar (interior/exterior)**: Standard Power es la única clase de acceso que admite operaciones WiFi 6E AP (Access Point) en exteriores. La energía estándar también se puede usar en interiores siempre que se cumplan todos los requisitos. La potencia está limitada a un máximo de 36 dB de Potencia Radiada Isotrópica Efectiva (EIRP por sus siglas en inglés) y los puntos de acceso deben coordinarse a través de un servicio de Coordinación de Frecuencia Automática (AFC). Standard Power también es la única clase de acceso limitada a operaciones en U-NII-5 y 7 (Unlicensed National Information Infrastructur) en los EE. UU. y, como resultado, obtiene un acceso total de 850 MHz.

- **Bajo consumo (interior):** Las operaciones de bajo consumo (interiores), o LPI (Logistic Performance Index) para abreviar, es donde es más probable que operen la mayoría de los puntos de acceso WiFi 6. Las operaciones solo en interiores hacen que los dispositivos de esta clase de activos tengan menos probabilidades de interferir con los servicios establecidos. Además, debido a que está operando en interiores, los niveles de potencia requeridos para una buena operación serían más bajos que los que necesitaría un

enlace punto a punto al aire libre, por ejemplo. Como resultado, las reglas de acceso para LPI no requieren un AFC Los límites de potencia para un AP LPI, expresados como Densidad espectral de potencia (PSD), son 5 dBm/MHz como máximo. Si bien ver la potencia máxima expresada como un PSD puede ser desconocido para algunos, en realidad es una de las claves para comprender el potencial de WiFi 6E. En WiFi basado en 5 GHz, el uso de canales más amplios (40, 80 y 160 MHz) en 5 GHz se ha mantenido limitado

- Muy bajo consumo/portátil (interior/exterior): Esta es la clase de muy baja potencia/portátil (interior/exterior), o VLP con un límite de PSD extremadamente bajo de -8 dBm/MHz. Este límite se traduce en un EIRP máximo de 5 dBm para un dispositivo de canal de 20 MHz. VLP también obtiene una ganancia de 3 dB por cada duplicación del ancho del canal, al igual que en las operaciones LPI. Los dispositivos de muy baja potencia tienen la libertad de operar en interiores y exteriores sin un impacto de interferencia significativo.

- Clientes (interiores/exteriores): Los clientes también obtienen nuevas reglas y su propia clase de acceso. Los clientes pueden acceder a la totalidad de los 1200 MHz. La potencia está restringida y debe permanecer siempre 6 dB por debajo de la EIRP máxima del AP al que está asociado el cliente. Entonces, si el AP está operando como un dispositivo LPI, la potencia máxima del cliente comenzaría en 12 dBm para un cliente en un AP de 20 MHz y se permitiría hasta 21 dBm para una celda de 160 MHz. La regla es la misma para los clientes independientemente de la clase de acceso del AP (estándar o bajo consumo).

Imagen 7: WiFi

xataka.com

2.2 Cifrados de Seguridad IoT

El IoT ha creado nuevos valores al conectar varios dispositivos a la red, pero también ha llevado a que las amenazas a la seguridad se conviertan en problemas importantes, como se ve en los informes recientes de manipulación ilegal de cámaras de vigilancia y piratería de automóviles, etc. La Agencia de Promoción de Tecnología de la Información de Japón (IPA) ha clasificado la "Exteriorización de la vulnerabilidad de los dispositivos IoT" en el octavo lugar en su informe titulado "Las 10 principales amenazas de seguridad de 2017".

El cifrado es una contramedida eficaz, y ahora se requiere que IoT aplique el cifrado a los dispositivos sensores en entornos con diversas restricciones que no han estado sujetos previamente al cifrado. La criptografía ligera es una tecnología investigada y desarrollada para responder a este problema.

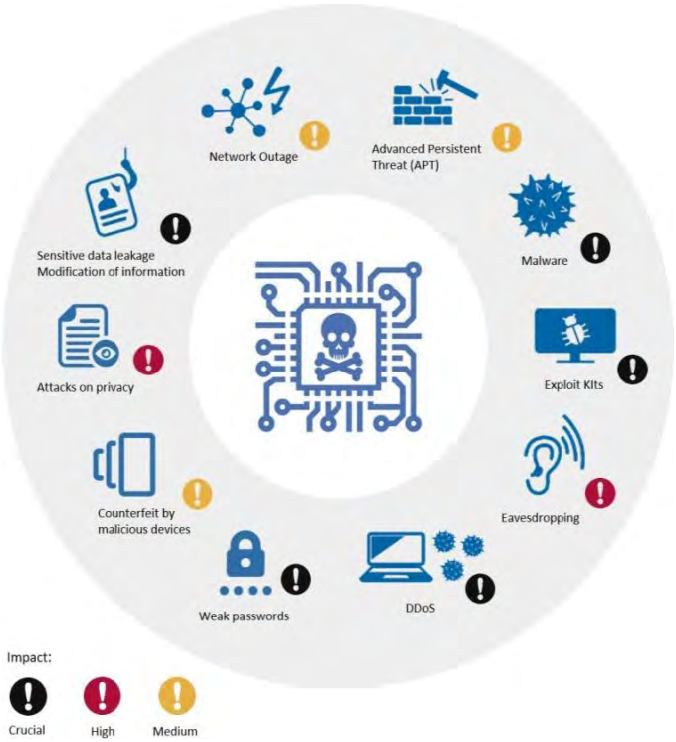

Imagen 8: Cifrados IoT y RGPD

https://www.almendron.com/tribuna/cifrado-iot-y-rgpd-tres-desafios-de-ciberseguridad-en-2018/

2.2.1 Criptografías de clave simétrica y clave pública

Se puede dividir aproximadamente en criptografías de clave simétrica y de clave pública (clave asimétrica). La criptografía de clave simétrica utiliza la misma clave secreta para el cifrado y descifrado. Con un procesamiento que es relativamente ligero, se utiliza en el cifrado y la autenticación de datos. Por otro lado, la criptografía de clave pública utiliza una clave secreta en el descifrado y una clave pública diferente de la clave secreta en el cifrado, y es bastante difícil adivinar la clave secreta de la clave pública. La complejidad computacional de la criptografía de clave pública suele ser más de 1000 veces mayor que la de la criptografía de clave

simétrica, pero esta tecnología se utiliza para compartir la clave secreta utilizada en la criptografía de clave simétrica y la firma digital, gracias a la propiedad asimétrica.

2.2.2 Tendencias en criptografía ligera

PRESENT es un cifrado de bloque considerado como el precursor de la criptografía ligera. Fue publicado en 2007 y ha sido registrado en ISO/IEC 29192. Tiene un tamaño de circuito pequeño que permite la implementación en la etiqueta RFID, lo que no es posible utilizando el cifrado AES estándar. La Agencia de Seguridad Nacional de EE. UU. (NSA) publicó el cifrado de bloque ligero SIMON/SPECK que presenta un tamaño de ROM muy pequeño adecuado para un microprocesador restringido (2013) y propuso su adición a ISO/IEC 29192 con el objetivo de lograr la estandarización internacional.

Un modo de operación de cifrado en bloque que puede lograr tanto el cifrado como la autenticación de mensajes se denomina "cifrado autenticado". Teniendo en cuenta la importancia de la detección de datos falsos en IoT, se espera que el cifrado signifique cifrado autenticado en el futuro. Incluso cuando se utiliza el mismo cifrado de bloque, la eficiencia y la seguridad varían considerablemente según cómo se implemente como cifrado autenticado. Existen cifrados autenticados recomendados por NIST llamados AES-CCM/GCM, pero considerando la importancia del cifrado autenticado y el progreso en la investigación, son deseables cifrados autenticados de próxima generación de peso más ligero y mayor seguridad

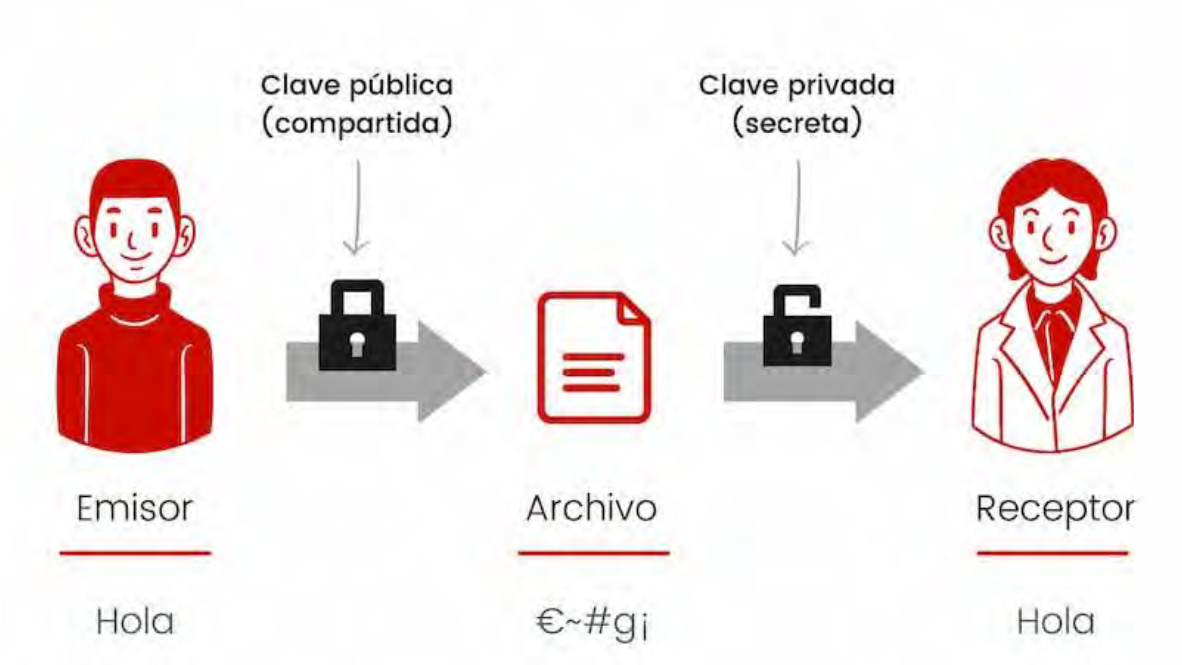

Imagen 9: Criptografía, ATICOSA

https://protecciondatos-lopd.com/empresas/criptografia-asimetrica/

2.2.3 Cifrado de bloque TWINE

El cifrado de bloque ligero de NEC llamado TWINE1 está diseñado para resolver problemas con la criptografía ligera anterior PRESENTE por su facilidad de implementación en el software. Al mismo tiempo se habilitará su implementación en circuitos de pequeño tamaño. Emplea la misma configuración que para PRESENTE, es decir, una longitud de bloque de 64 bits y dos tipos de longitudes de clave secreta de 80 y 128 bits.

TWINE fue seleccionado como uno de los sistemas de cifrado para ser evaluado por el grupo de trabajo de criptografía ligera de CYRPTREC descrito anteriormente, y manifestó rendimientos de primera clase tanto en hardware como en software.

2.3 Bluetooth

El Bluetooth es un estándar de conectividad inalámbrica presente en nuestros dispositivos electrónicos del día a día. Se trata de un estándar inalámbrico que permite la transmisión de datos entre dispositivos a corto alcance, facilitando las comunicaciones entre ambos, eliminando la presencia de cables o conectores, permitiendo una interacción sencilla y rápida entre los aparatos.

Desde sus inicios hasta hoy, hay muchas versiones de Bluetooth que han ido mejorando desde hace casi veinte años. La versión más reciente es la de Bluetooth 5.0 aunque concretamente ya está disponible el modelo Bluetooth 5.2 con todo tipo de mejoras frente a los anteriores, que incluyen mayor velocidad de conexión, menor consumo energético y un mayor alcance entre los dispositivos conectados.

Para poder realizar una conexión correcta entre dispositivos, hace falta que existan protocolos que hagan posible que se pueda enviar la información:

- ACL (Asyncrhronus Connection-Less) o Enlace sin conexión asíncrono. Se trata de un enlace de control de datos.

- SCO (Syncrhonus Connection-Oriented) o Enlace orientado a la conexión síncrono. Es un enlace de datos de voz.

- LMP (Link Management Protocol) o Protocolo de control de enlace. Se usa para establecer y controlar el enlace de radio entre dos dispositivos.

- HCI (Host Controller Interface) o Interfaz del controlador de la máquina. Permite la comunicación entre un host y un controlador a través de un interfaz.

- LE LL (Low Energy Link Layer) o Baja energía en la capa de enlace. Responsable de procesos de control tales como el cambio de parámetros de conexión o la encriptación.

- L2CAP (Logical link control and adaptation protocol) o Protocolo de control y adaptación del enlace lógico. Se utiliza para segmentar, reensamblar y multiplexar los paquetes en las capas superiores, y establecer una buena gestión para la transmisión a otros dispositivos bluetooth.

- BNEP (Bluetooth network encapsulation protocol) o Protocolo de encapsulamiento de red bluetooth. Utilizado para transportar, de manera inalámbrica, paquetes de control y de datos.

- RFCOMM (Radio frequency communication) o Comunicación por radio frecuencia. Es un conjunto de protocolos de transporte construido sobre el protocolo L2CAP visto anteriormente.

- SDP (Service discovery protocol) o Protocolo de descubrimiento de servicios. Permite a los dispositivos descubrir qué servicios soporta el otro y en qué parámetros para conectarse a él.

- TCS (Telephony control protocol) o Protocolo de control telefónico. Controla los datos de voz y llamadas entre dos dispositivos Bluetooth.

- AVCTP (Audio/video control transport protocol) o Protocolo de control del transporte de audio y vídeo. Transfiere comandos de audio y vídeo de un control remoto al dispositivo sobre un canal L2CAP.

- AVDTP (Audio/video data transport protocol) o Protocolo de transporte de datos de audio y vídeo. Se usa para reproducir audio en unos auriculares desde el dispositivo.

- OBEX (Object Exchange) o Protocolo de intercambio de datos. Facilita el intercambio de objetos binarios entre dispositivos.

- ATT (Low Energy Attribute Protocol) o Protocolo de baja energía en atributos. Basado en atributos presentados por dispositivo, permite el intercambio de información.

- SMP (Low Energy Security Manager Protocol) o Protocolo de manejo de la seguridad. Se utiliza el Protocolo de administrador de seguridad (SMP) para establecer el emparejamiento, la autenticación y el cifrado entre los dispositivos Bluetooth Low Energy. Genera y almacena varias claves (como encriptación e identidad). El conjunto de pruebas de cliente Bluetooth LE SMP de Defensics se puede utilizar para evaluar las implementaciones de Bluetooth SMP en busca de fallas de seguridad y problemas de robustez.

Desde que la primera versión se lanzó en 1999 hasta hoy, hay muchas evoluciones de esta tecnología inalámbrica que nos ha permitido solucionar problemas de conexión, mejorar la velocidad de transmisión de datos o mejorar el alcance. Por ejemplo, aunque actualmente la versión publicada más reciente es Bluetooth 5.2, es Bluetooth 5.0 o Bluetooth 5.1 por la que apuestan la mayoría de los aparatos más modernos del mercado, como algunos teléfonos móviles de última generación.

2.3.1 Bluetooth 1.0

Fue la primera versión, lanzada en 1999, usada para la transmisión de datos. Se tuvo que enfrentar a muchos problemas de seguridad**,** tanto la primera versión, 1.0a como la segunda 1.0b, hasta que con el lanzamiento de Bluetooth 1.1, en febrero de 2001, apareció como producto más finalizado y listo para su comercialización, con una tasa de transmisión de 732.2 kb/s. La versión 1.2 redujo las interferencias.

2.3.2 Bluetooth 2.0

Con una tasa de transmisión de más de 2 Mb/s, la versión 2.0 se lanzó en noviembre de 2004 con una tecnología ya consolidada. Una evolución que, tres años después, en 2007, tuvo aún más mejoras con la llegada de Bluetooth 2.1, una versión que mantuvo la tasa de transmisión al mismo nivel pero que trajo consigo una mejora importante en cuanto a conexión. Se permitió desde entonces que un dispositivo pudiera detectar y conectar automáticamente, sin PIN, a otro dispositivo con Bluetooth.

2.3.3 Bluetooth 3.0

Su vida fue efímera, apenas de unos meses, pero con un salto muy importante al incorporar un canal de alta velocidad (High Speed), basado en WiFi y en la ultra banda ancha. Su tasa de transferencia es de 24 Mb/s, hace esta versión perfecta para el intercambio de volúmenes con más datos, como los correspondientes al audio y al vídeo.

2.3.4 Bluetooth 4.0

La versión 4.0 de Bluetooth se lanzó en 2010 y con un objetivo principal: reducir los efectos en el consumo de la batería de los dispositivos. Con la 4.0 llega Bluetooth Low Energy. Gracias a esta nueva versión, la tecnología empezó a utilizarse en aparatos más pequeños o menos potentes como pulseras de actividad, por ejemplo. La tasa de transferencia se mantuvo en los 24 Mb/s. También llegó el Bluetooth 4.1, una versión mejorada que nos permitía conexión entre dispositivos pequeños sin intermediarios y que incluía el protocolo IPv6, y la versión 4.2, que hasta la llegada del 5.0 fue la tecnología más avanzada y la que trabajaba a mayor velocidad.

2.3.5 Bluetooth 5.0

El Bluetooth 5.0 llegó a finales de 2016 y se lanzó enfocado principalmente al IoT. Con respecto a versiones anteriores, el Bluetooth 5.0 puede alcanzar el doble de velocidad que la versión anterior y tiene un ancho de banda ocho veces mayor. Es decir, podemos enviar archivos más grandes el doble de rápido que con las versiones anteriores. Eso sí, el consumo se mantiene y sigue siendo bajo el gasto de energía que supone su uso.

Respecto a la localización, podemos obtener posicionamiento en lugares cerrados en los que no llega la cobertura GPS así que nos posicionará correctamente si estamos en un museo, por ejemplo, si estamos en un centro comercial o en cualquier gran superficie interior similar. Otra de las mejoras es el alcance. Que mejora el rango de señal cuatro veces con respecto a los modelos anteriores, lo que quiere decir que podremos alejarnos mucho más del aparato que queremos conectar y podría llegar hasta 200 metros en exterior.

Los dispositivos con Bluetooth 5.0 ya son la mayoría de los teléfonos móviles o tablets lanzadas en el año 2019 y esta versión cuenta con la particularidad de que puede transmitir audio a dos dispositivos diferentes. Por ejemplo, a dos altavoces diferentes o un altavoz inalámbrico y unos auriculares, etc.

2.3.6 Bluetooth 5.1 y Bluetooth 5.2

Las últimas novedades en el mundo Bluetooth han sido dos actualizaciones de la versión 5.0. La 5.1, presentada en enero de 2019, y la 5.2 recientemente publicada a principios de este 2020. La versión 5.1 trajo mejoras en la velocidad de conexión y en la reducción del consumo, además de novedades como la detección y ubicación de otros dispositivos conectados, parecida a la ubicación GPS. La 5.2, de la cual ya se han anunciado los primeros chips compatibles, trae consigo tres novedades importantes. El Enhanced Attribute Protocol (EATT), una mejora del ATT; el LE Power Control, para optimizar de forma dinámica la potencia de transmisión que se usa entre los dispositivos conectados; y los LE Isochronous Channels, unos canales diseñados para LE Audio, otra de las novedades de este estándar y que permite a un dispositivo, por ejemplo, un smartphone, mandar audio a varios dispositivos a la vez.

2.4 NB-IoT

“Narrowband Internet of Things” (NB–IoT) también conocida como LTE Cat NB1, es una tecnología de área amplia de baja potencia (LPWA) que se ha desarrollado para conectar varios dispositivos utilizando redes móviles existentes. Narrowband Internet of Things” (NB–IoT) ha sido desarrollada para soportar la implementación de las aplicaciones de Internet de las Cosas (IoT). Es una tecnología de banda

estrecha y de baja potencia que maneja pequeñas cantidades de transmisión de datos bidireccional de manera eficiente, segura y confiable

La tecnología NB–IoT funciona utilizando redes LTE existentes o bloques de recursos del espectro en la banda de protección del operador de LTE. También puede utilizar el espectro de ancho de banda de 200 khz utilizado anteriormente por GSM, pero no utilizado actualmente.

La especificación NB–IoT se congeló en junio de 2016 en la 13ª edición de la Especificación de protocolo 3GPP (LTE-Advanced Pro) (ambas 3GPP, versión 13). De acuerdo con la definición de la Versión 13, las especificaciones técnicas de NB–IoT son las siguientes:

- Tasa máxima de enlace descendente: 250 kbps
- Velocidad máxima de enlace ascendente: 250 kbps (multitono) y 20 kbps (mono)
- Tiempo de retardo: 1,6 a 10 segundos
- Tecnología Dúplex: Half Duplex
- Ancho de banda de recepción del dispositivo: 180 kHz
- Potencia de transmisión del equipo: 20/23 dBm.

NB–IoT es una de las tecnologías LPWA más populares que se pueden usar en aplicaciones IoT. Proporciona la combinación correcta de características. La señal bajo demanda de banda estrecha de baja frecuencia tiene características de propagación a larga distancia que pueden penetrar paredes y conductos metálicos. Los requisitos de alimentación son lo suficientemente bajos como para que la vida útil de un solo dispositivo con batería pueda superar los 10 años. Su velocidad de datos es la adecuada para aplicaciones de IoT como lecturas de medidores, farolas,

monitoreo de espacios de estacionamiento, monitoreo de datos industriales y algunas otras aplicaciones de baja velocidad de datos.

Los mecanismos de seguridad más fundamentales provistos por una red de comunicaciones son:

- Identificación y autenticación de las entidades involucradas en un servicio de IoT (es decir, puertas de enlace, dispositivos periféricos, red doméstica, redes en itinerancia, plataformas de servicio).
- Control de acceso a las diferentes entidades que necesitan conectarse para crear un servicio de IoT.
- Protección de datos para garantizar la seguridad (confidencialidad, integridad, disponibilidad, autenticidad) y la privacidad de la información transmitida por la red para un servicio de IoT.
- Procesos y mecanismos para garantizar la disponibilidad de los recursos de la red y protegerlos contra los ataques (por ejemplo, implementando un cortafuegos adecuado, prevención de intrusiones y tecnologías de filtrado de datos).

2.5 LoRa

LoRaWAN es una especificación de redes LPWAN (Low Power Wide Area Network). Correlacionando a los niveles OSI, sería el nivel 2 (enlace de datos). Es lo que se conoce como la subcapa MAC (Media Access Control). LoRaWAN se encarga de unir diferentes dispositivos LoRa gestionando sus canales y parámetros de conexión: canal, ancho de banda, cifrado de datos, etc.

En el nivel 1 de OSI, nivel físico, encontramos la tecnología LoRa de comunicación. Esta tecnología permite el envío y recepción de información punto-a-punto. Lo que caracteriza a un dispositivo LoRa es su largo alcance con un mínimo dispositivo. Para ello emplea la técnica de espectro ensanchado, donde la señal a mandar utiliza más ancho de banda que el necesario teóricamente pero que permite una recepción de múltiples señales a la vez que tengan distinta velocidad.

Las frecuencias de comunicaciones que LoRa usan son principalmente las de la banda ISM, aunque la tecnología puede operar en cualquier frecuencia por debajo del 1 GHz.

El uso de estas frecuencias se debe a que mientras se respete los valores de emisión, cualquier persona o empresa puede hacer uso de ella sin necesidad de licencia.

LoRa suele operar en las bandas 433 MHz, 868 MHz y 915 MHz. Según el pais, estas bandas pueden estar restringidas. Por ejemplo, en Europa no se puede usar la 915 Mhz.
Los parámetros de comunicación LoRa son:

- Canal dentro de la banda:
  frecuencia central que representa el canal. El canal 10 dentro de la banda 868 MHz tiene un valor de 865.200.000 Hz.

- Spreading factor (SF):
  define el número de bits usados para codificar un símbolo. A mayor SF, menor velocidad de transferencia tendremos, pero mayor inmunidad a interferencias.

- Coding rate (CR):
  indica la forma de codificar para corrección de errores. Es decir, según la técnica especificada, añade símbolos de control para saber si los datos son correctos o no e incluso poder determinar los valores correctos.

- Bandwidth (BW): indica el ancho de frecuencia que vamos a usar.

Los mecanismos de seguridad se basan en los algoritmos criptográficos AES los cuales son bien probados y estandarizados. Estos algoritmos han sido analizados por la comunidad criptográfica durante muchos años, están aprobados por el NIST y son tomados como la mejor práctica de seguridad para redes y nodos restringidos. La seguridad LoRaWAN utiliza la primitiva criptografía AES combinada con varios modos de operación: CMAC para protección de integridad y CTR para encriptación.

Cada dispositivo LoRaWAN se personaliza con una clave AES de 128 bits (llamada AppKey) y un identificador único global (DevEUI basado en EUI-64), ambos se utilizan durante el proceso de autenticación del dispositivo. La asignación de identificadores EUI-64 requiere que el asignador tenga un Identificador Único de la Organización (OUI) de la Autoridad de Registro IEEE. De manera similar, las redes LoRaWAN se identifican mediante un identificador único global de 24 bits asignado por LoRa Alliance

2.6 SIGFOX

SigFox es una compañía francesa fundada en 2009 que proporciona el servicio de red de cobertura amplia de bajo consumo –Low-Power Wide-Area Network

(LPWAN)-, esta red es inalámbrica y fue creada para que funcione e interactúe con dispositivos de bajo consumo energético tales como sensores que funcionan con pilas convencionales con tasas de transferencias de datos de hasta 12 bytes.

La red funciona con la tecnología de transmisión UNB ultra narro band y consiste en emplear canales estrechos del espectro para alcanzar grandes distancias con un requerimiento mínimo de energía.

El funcionamiento de esta red es muy similar a las redes de telefonía celular debido a que esta red funciona a partir de la colocación de varias estaciones receptoras y transmisoras; la diferencia entre las estaciones SigFox y las de telefonía celular es en que los dispositivos y sensores que estén conectados a la red SigFox no están sujetas a una sola estación base específica, esto es, que cualquier estación puede recibir la información y transmitirla hacia la nube.

La banda pública empleada para el intercambio de mensajes en SigFox es en 200 kHz y en la que cada mensaje tiene un ancho de 100 Hz y puede ser transmitido a una de tasa desde 100 bits hasta 600 bits –esas tasas varían de acuerdo con el país en donde se encuentre. Además, la red SigFox emplea las bandas bidireccionales de radio sin licencia ISM –industrial, scientific and medical radio bands, las cuales son bandas usadas para usos múltiples excepto para telecomunicaciones- en Estados Unidos de 902 MHz y en Europa de 868 MHz.

La seguridad es muy importante en esta red por lo que cada dispositivo debe tener asignado un código de identificación, cuenta con protocolos de encriptación VPN y emplea al final el protocolo https.

Para que un dispositivo funcione en esta red se requiere que contenga un módulo de comunicación compatible con SigFox –chips, tarjetas como la MKRFox1200 o kits específicos.

Se han implementado diversos mecanismos de verificación de los dispositivos y mensajes que son enviados a través de la red. Cada dispositivo cuenta con una identificación. A su vez cada mensaje lleva un número de secuencia único y una marca de tiempo que permite protección ante ataques de tipo replay.

Las estaciones base cuentan todas con un mecanismo Trusted Platform Module (TPM) de protección de las claves implicadas en la seguridad de las mismas. Se utiliza el algoritmo AES-ECB para la encriptación mediante clave pública y Redes Privadas Virtuales (VPNs) para el acceso desde el sistema de soporte de SigFox.

Imagen 10: Logotipo de identificación de SigFox.
https://www.emitech.fr/fr/emitech-sigfox-partner

Capítulo 3 análisis de los estándares de comunicación

La siguiente Tabla, ilustra las características principales de los estándares de comunicaciones. La tabla proporciona información relacionada a diversos aspectos como: cobertura de los sistemas, tecnología, espectro, esquema de seguridad, entre otros.

	Wi Fi	Bluetooth	NB-IoT	sigfox	LoRa
Cobertura	200m	10 m	< 15 km	< 12km	< 10 km
Tecnología	Propietaria	Propietaria	Abierto LTE	Propietaria	Propietaria
Espectro	No licenciada	No licenciada	Licenciada	No licenciada	No licenciada
Ancho de banda	2.4 - 5 GHz	2.4 GHz	200 kHz	100 Hz	250-500 kHz
Tasa de bits	< 100 Mbps	< 2 Mbps	< 67 kbps	< 100 bps	< 10 kbps
Caso de uso	• Red inteligente • Industria	• Red inteligente • industria	• Red inteligente • Ciudad • Monitoreo	• Red inteligente • Ciudad • Monitoreo	• Red inteligente • Ciudad • Monitoreo
Umbral de confort (MCL)	25 dBm	10 dBi	164 dB	160 dB	157 dB
Tipo de encriptado	• WPA2-PSK (AES)	• AES-CCM	• AES	• HMAC	• AES

Como podemos observar en la tabla que antecede, se logra identificar que a nivel de cobertura se tiene variaciones en cuanto a una tecnología y otra en las cuales podemos observar que el protocolo que tiene menos rango es el bluetooth el cual mayormente se utiliza para transferencia de archivos en redes PAN (Personal Area Network) que se encuentren dentro del rango de cobertura, a comparación del protocolo NB-IOT el cual tiene un rango de -15 Km, este a comparación del bluetooth puede ser utilizado para distancias mas lejanas permitiendo la comunicación entre dispositivos ya que esta diseñada para permitir la comunicación en telefonía móvil, las cuales sabemos que necesitan mayor alcance.

También podemos observar que la mayoría de protocolos cuentan con diferentes estándares de seguridad, uno de los mas seguros hasta el momento es el WPA2 el

cual esta siendo utilizado en la mayoría de los dispositivos para evitar que sean vulnerados.

Estos protocolos los podemos utilizar en diferentes casos de uso, dependiendo de la situación que se presente, varían desde la transferencia de un archivo, hasta armar una red de dispositivos inteligentes

Capítulo 4 Conclusiones

El Internet de las cosas es un concepto que llegó para quedarse. Conforme pasan los días, la tecnología avanza más rápido, desde teléfonos inteligentes, casas, oficinas y hasta réplicas de humanos robotizados.

En el presente documento se muestra en general nuestra dependencia hacia la tecnología; actualmente estamos sujetos a utilizar la tecnología para automatizar la seguridad, salud, necesidades del hogar, conexiones de punto a punto, recolección y análisis de datos, etc.

El objetivo del Internet de las cosas es automatizar las necesidades del ser humano mediante la tecnología y reducir el tiempo, dinero y esfuerzo de diferentes trabajos que puedan ser realizados por máquinas.

El WiFi, es una tecnología móvil que ha permitido el avance del Internet de las cosas, pues es el medio por el cual los dispositivos se conectan a Internet e interactúan uno con otro, sin la necesidad de utilizar cables, que pueden ser molestos o que aumente los costos. Ahora, tan solo con un equipo (router inalámbrico) que se encarga de dispersar la señal inalámbrica, pueden conectarse varios dispositivos (que tengan el software de WiFi) cercanos puedan conectarse al mismo, y así poder interactuar tanto al Internet, como uno con otro.

A pesar de que el router y que el WiFi, funcionan de maravilla, siempre existen fallas en el sistema, y esta tecnología no es la excepción. Pues las redes inalámbricas se ven afectadas por la intensidad de la señal, o dispositivos conectados al mismo router, e incluso por ondas electromagnéticas en el mismo canal.

SigFox, una empresa que proporciona el servicio de red de cobertura amplia de bajo consumo Low-Power Wide-Area Network (LPWAN), creada para que funcione e interactúe con dispositivos de bajo consumo energético tales como sensores que funcionan con pilas convencionales.

La red funciona con la tecnología de transmisión UNB ultra narro band y consiste en emplear canales estrechos del espectro para alcanzar grandes distancias con un requerimiento mínimo de energía. Pue esta funciona mediante antenas receptoras, similar a las redes de telefonía como lo hace WiFi, por lo tanto, podemos decir que la tecnología siempre tendrá forma de comunicarse de manera remota, desde redes locales, hasta redes de área amplia.

Finalmente, la seguridad en las redes inalámbricas más que un simple lujo, se ha vuelto una necesidad, dado que a través de ella podemos proteger nuestra información, y hasta nosotros mismos.

Bibliografía

330ohms. (11 de 05 de 2017). *Blog 330 ohms*. Obtenido de https://blog.330ohms.com/2017/05/11/que-es-sigfox-y-como-funciona/

Cisco. (18 de 11 de 2021). *Cisco*. Obtenido de https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ax-solution/nb-06- WIFI -6e-wp-cte-en.html

Cisco. (24 de 05 de 2022). *Cisco*. Obtenido de https://www.cisco.com/c/es_mex/products/wireless/what-is-wifi.html

Energy, D. (22 de 05 de 2022). *Dset Energy*. Obtenido de https://www.dset-energy.com/2019/06/05/tecnologia-sigfox

Etecé, E. (5 de 08 de 2021). *Concepto*. Obtenido de https://concepto.de/wifi/

GR, R. (7 de 12 de 2022). *adslzone*. Obtenido de https://adslzone.net/reportajes/tecnologia/bluetooth

GSMA. (27 de 08 de 2017). *gsma*. Obtenido de https://www.gsma.com/iot/wp-content/uploads/2018/05/CLP.14-v1.0_Spanish.pdf

Martres, P. (29 de 08 de 2019). *UDE*. Obtenido de https://ude.edu.uy/particularidades-de-la-red-sigfox/

Mcielectronics, C. (27 de 06 de 2019). *Cursos Mcielectronics*. Obtenido de https://cursos.mcielectronics.cl/2019/06/27/que-es-nb-iot/

Moes, T. (24 de 05 de 2022). *Softwarelab*. Obtenido de https://softwarelab.org/es/que-es-wifi-que-significa-y-para.que-sirve/

PROFESORUOC. (22 de 11 de 2018). *Informatica Blogs*. Obtenido de http://informatica.blogs.uoc.edu/2018/11/22/que-es-nb-iot/

Reimondo, G. (15 de 01 de 2019). *Humanizationoftechnology*. Obtenido de https://humanizationoftechnology.com/seguridad-en-redes-lorawan/revista/iot/01/2019/

softwarelab. (24 de 05 de 2022). *softwarelab*. Obtenido de https://softwarelab.org/es/bluetooh/

Sousa, M. (2 de 05 de 2019). *SmartLighting*. Obtenido de https://smart-lighting.es/bluetooth-low-energy-introduccion-la-tecnologia/

Synopsys. (24 de 05 de 2022). *Synopsys*. Obtenido de https://www.synopsys.com/software-integrity/security-testing/fuzz-testing/defensics/protocols/btle-smpc.html

Toshihiko, O. (24 de 05 de 2022). *Nec*. Obtenido de https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html

Valero, C. (2 de 03 de 2023). *adslzone*. Obtenido de https://www.adslzone.net/reportajes/tecnologia/que-es-wifi-como-funciona/

Valois, M. A. (24 de 05 de 2022). *hostgator*. Obtenido de https://www.hostgator.mx/blog/internet-de-las-cosas/

Acrónimos

ACL: Asyncrhronus Connection-Less
AES: Advanced Encryption Stand
AES: Advanced Encryption Standard
AES-CCM: Advanced Encryption Standard Counter Mode
ATT: Low Energy Attribute Protocol
AVCTP: Audio/video control transport protocol
BLE: Bluetooth Low Energy.
BNEP: Bluetooth network encapsulation protocol
GPRS: General Packet Radio Service
GSM: Global System for Mobile communications
HCI: Host Controller Interface
HMAC: Hash-based Message Authentication Code
IEEE: Institute of Electrical and Electronics Engineers
IoT: Internet of Things.
L2CAP: Logical link control and adaptation protocol
LE LL: Low Energy Link Layer
LMP: Link Management Protocol
LPWAN: Low Power Wide Area Network
LTE: Long Term Evolution
M2M: Machine to machine
NIST: National Institute of Standards and Technology
OBEX: Object Exchange
OFDMA: Orthogonal Frequency Division Multiple Access
QoE: Quality of experience
RFCOMM: Radio frequency communication
SCO: Syncrhonus Connection-Oriented
SDP: Service discovery protocol
SMP: Low Energy Security Manager Protocol
TCS: Telephony control protocol
UMTS: Universal Mobile Telecommunications System
WiFi: Wireless Fidelity
WPA: Wi-Fi Protected Access
WPA2: Wi-Fi Protected Access 2
WPS: WiFi Protected Setup
WSAN: Wireless Sensors and Actuator Networks
WSN: Wireless Sensor Networks