UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Análisis de mecanismos de seguridades en redes inalámbricas mediante IoT

AUTOR:

Ing. Burbano Choez, Edison Xavier

Componente práctico del examen complexivo previo a la obtención del Grado Académico de **MAGÍSTER EN TELECOMUNICACIONES**

TUTOR:

M. Sc. Palacios Meléndez, Edwin Fernando

Guayaquil, Ecuador

24 de noviembre del 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster **Burbano Choez, Edison Xavier** como requerimiento parcial para la obtención del Grado Académico de **MAGÍSTER EN TELECOMUNICACIONES**.

TUTOR

M. Sc. Palacios Meléndez, Edwin Fernando

DIRECTOR DEL PROGRAMA

PhD. Romero Paz, Manuel de Jesús

Guayaquil, 24 de noviembre del 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Burbano Choez, Edison Xavier**

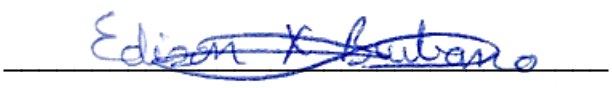
DECLARÓ QUE:

El Componente práctico del examen complexivo **"Análisis de mecanismos de seguridades en redes inalámbricas mediante IoT"**, previa a la obtención del grado Académico de **Magíster en Telecomunicaciones**, ha sido desarrollado, respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizó del contenido, veracidad y alcance científico del Componente práctico del examen complexivo del Grado Académico en mención.

Guayaquil, 24 de noviembre del 2022

EL AUTOR



Ing. Burbano Choez, Edison Xavier

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Burbano Choez, Edison Xavier**

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Componente práctico del examen complexivo de Maestría titulado: **"Análisis de mecanismos de seguridades en redes inalámbricas mediante IoT"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

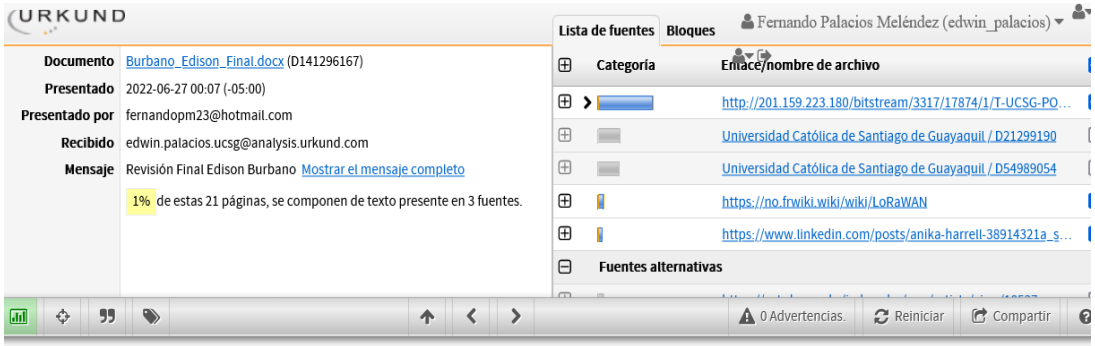
Guayaquil, 24 de noviembre del 2022

EL AUTOR

Ing. Burbano Choez, Edison Xavier

REPORTE DE URKUND

Análisis de urkund con 1% de coincidencias del trabajo de titulación desarrollado por el Ingeniero **BURBANO CHOEZ, EDISON XAVIER.**



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL SISTEMA DE POSGRADO MAESTRÍA EN TELECOMUNICACIONES

TEMA: Análisis de mecanismos de seguridades en redes inalámbricas mediante IoT

AUTOR: Ing. Burbano Choez, Edison Xavier

Trabajo de Titulación previo a la obtención del Grado Académico de Magíster en Telecomunicaciones

TUTOR: M. Sc. Palacios Meléndez, Edwin Fernando

Guayaquil, Ecuador

20 de junio del 2022

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL SISTEMA DE POSGRADO MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster Burbano Choez, Edison Xavier como

Dedicatoria

El presente trabajo va dedicado a Dios y a mis padres que siempre me han apoyado a lo largo de mi formación de grado y ahora posgrado.

EL AUTOR

Ing. Burbano Choez, Edison Xavier

Agradecimientos

A todos los docentes de la Maestría en Telecomunicaciones en la Universidad Católica de Santiago de Guayaquil, en especial a mi tutor y Director de la Maestría.

A todos mis compañeros de la promoción que me motivaron a culminar esta etapa de posgrado.

EL AUTOR

Ing. Burbano Choez, Edison Xavier

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. Palacios Meléndez, Edwin Fernando

TUTOR

f. _____

M. Sc. Córdova Rivadeneira, Luis Silvio

REVISOR

f. _____

M. Sc. Quezada Calle Edgar Raul

REVISOR

f. _____

ROMERO PAZ MANUEL DE JESÚS

DIRECTOR DEL PROGRAMA

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Capítulo 2:

Capítulo 3:

ÍNDICE DE TABLAS

Capítulo 2:

Resumen

En la actualidad, todos los dispositivos móviles, independientemente de su tipo y uso, representan una amenaza para la seguridad de los usuarios sobre el Internet de las Cosas (IoT). En efecto, más allá de las normas de seguridad que se deben aplicar en la fase de producción de los dispositivos inteligentes, los cuales alcanzan proporciones muy serias en función de sus ámbitos de uso, resulta indispensable la investigación sobre los medios de prevención de los ataques actuales, que no se detectan, después de la producción. Además, para detectar ataques desconocidos y vigentes se utilizan técnicas de inteligencia artificial como el aprendizaje automático, la lógica difusa o las redes neuronales artificiales, que resulta otro tema que se puede ampliar al presente trabajo de examen complexivo. El objetivo del presente trabajo de grado requiere la investigación de la Internet de las Cosas, y sus aplicaciones en las comunicaciones inalámbricas, como el caso de las redes de sensores inalámbricos (WSN); con el fin de garantizar la seguridad de los dispositivos inteligentes usando el IoT.

Palabras claves: INTERNET, COMUNICACIONES, DISPOSITIVOS, REDES, SENSORES, SEGURIDAD.

Abstract

Today, all mobile devices, regardless of their type and use, represent a threat to the security of users on the Internet of Things (IoT). Indeed, beyond the security standards to be applied in the production phase of smart devices, which reach very serious proportions depending on their areas of use, research into ways of preventing current attacks, which are not detected after production, is essential. In addition, artificial intelligence techniques such as machine learning, fuzzy logic or artificial neural networks are used to detect unknown and current attacks, which is another topic that can be extended to the present complex examination work. The objective of the present degree work requires the investigation of the Internet of Things, and its applications in wireless communications, such as the case of wireless sensor networks (WSN); to ensure the security of smart devices using the IoT.

Keywords: INTERNET, COMMUNICATIONS, DEVICES, NETWORKS, SENSORS, SECURITY.

Capítulo 1: Generalidades del proyecto de grado.

1.1. Introducción.

El Internet de las Cosas *(Internet of Things, IoT)* se refiere al uso de dispositivos y sistemas conectados inteligentemente para aprovechar los datos recopilados por los sensores y actuadores integrados en máquinas y otros objetos físicos. Se espera que IOT se propague rápidamente en los próximos años y esta convergencia desencadenará una nueva dimensión de servicios que mejoren la calidad de vida de los consumidores y la productividad de las empresas.

Para los consumidores, el IoT tiene el potencial de ofrecer soluciones que mejoren drásticamente la eficiencia energética, la seguridad, la salud, la educación y muchos otros aspectos de la vida cotidiana. Para las empresas, IoT puede sostener soluciones que mejoren la toma de decisiones y la productividad en la manufactura, la venta al por menor, la agricultura y otros sectores estratégicos afín al cambio de la matriz productiva.

Si bien el impacto potencial del IoT es considerable, se requiere un esfuerzo concertado para ir más allá de esta etapa inicial. Con el fin de optimizar el desarrollo del mercado, se requiere una comprensión común de la naturaleza distinta de la oportunidad. Hasta la fecha, los operadores móviles han identificado las siguientes características distintivas:

a) El Internet de las Cosas puede permitir una nueva de servicios que mejoren la vida en varios sectores fundamentales de la economía.
b) Satisfacer las necesidades de los clientes puede requerir modelos de distribución y servicios globales consistentes.
c) Internet de las cosas ofrece una oportunidad para que los nuevos modelos comerciales apoyen los despliegues globales masivos.
d) La mayor parte de los ingresos provendrá de la prestación de servicios de valor añadido y los operadores móviles están construyendo nuevas capacidades para habilitar estas nuevas áreas de servicio.

e) El comportamiento de los dispositivos y las aplicaciones ocasionará nuevas y variadas demandas a las redes móviles.

1.2. Antecedentes.

El Internet de las Cosas es una línea de investigación prometedora de las Telecomunicaciones, como es conocido su interacción con diferentes dispositivos a través de sensores que acceden al internet mediante una red de comunicación de datos. Es necesario analizar los protocolos y técnicas requeridas en redes WSN para utilizar el IoT.

Se realizó la búsqueda de información de trabajos de titulación o tesis y de artículos en revistas. De las Instituciones de Educación Superior (IES) de Ecuador, se pudo encontrar un solo trabajo del Internet de las Cosas. Por ejemplo, Cuzme Rodríguez, (2015) en su tesis realiza el estudio de las técnicas de seguridad empleadas en el uso del Internet de las Cosas. Estas seguridades fueron analizadas tanto en hardware, software, red y nube *(cloud)*.

Otro trabajo encontrado fue la tesina fin de máster realizado por Alandí P., (2016), en la cual realiza el estudio de la implantación de Internet de las Cosas, en las redes logísticas de la cadena de suministro. La perspectiva del trabajo es que tendrá una expansión significativa del IoT, es decir que cualquier dispositivo electrónico podrá acceder al internet. Mientras, que Sosa & Godoy, (2014) en su artículo analiza la evolución tecnológica considerando el Internet de las Cosas como el internet del futuro, desafíos y perspectivas.

1.3. Definición del problema

La evolución tecnológica de redes de comunicaciones de datos en Ecuador ha permitido que se puedan acceder a otras plataformas, tal como lo es el Internet de las Cosas. Por esto, es necesario realizar la evaluación práctica de seguridades en protocolos y de técnicas utilizadas en sistemas del internet de las cosas para redes WSN.

1.4. Objetivos

1.4.1. Objetivo General:

Evaluar la seguridad de protocolos y técnicas utilizadas en sistemas del internet de las cosas para redes WLAN.

1.4.2. Objetivos específicos:

- ✓ Describir la fundamentación teórica de la tecnología del internet de las cosas.
- ✓ Diseñar un modelo de simulación de una red WSN utilizando la plataforma Raspberry Pi.
- ✓ Evaluar el modelo de simulación a niveles de seguridad de protocolos y técnicas utilizadas en el IoT.

1.5. Hipótesis

Mediante la evaluación de la seguridad de protocolos y técnicas utilizadas en sistemas del internet de las cosas para redes WSN se logrará demostrar cómo interactúan dispositivos electrónicos conectados simultáneamente a una red WSN y a su vez este trabajo servirá como una herramienta para el desarrollo de futuros trabajos de investigación relacionados con redes de sensores inalámbricos.

1.6. Metodología de investigación.

Los tipos de investigación pone de relieve el hecho de que hay dos enfoques básicos de la investigación, a saber, el enfoque cuantitativo y el enfoque cualitativo. El primero implica la generación de datos en forma cuantitativa que pueden someterse a rigurosos análisis cuantitativos de manera formal y rígida. Este enfoque puede ser subclasificado en enfoques inferenciales, experimentales y de simulación para la investigación.

Capítulo 2: Fundamentos Teóricos.

2.1. Visión general del internet de las cosas (IoT).

Observar y determinar la tendencia de IoT justo antes de examinar el concepto de IoT contribuirá a una comprensión más clara de este concepto y su importancia. La popularidad de dos paradigmas diferentes, el Internet de las cosas y el IoT, ha cambiado de vez en cuando. La popularidad de búsqueda web medida en todo el mundo por Google Trends durante los últimos 5 años para los dos términos mencionados anteriormente se presenta en la figura 2.1. Se puede observar que entre el 6 y 12 de marzo del 2022 hubo 13 y 88 millones de búsqueda del Internet de las Cosas e IoT, respectivamente.

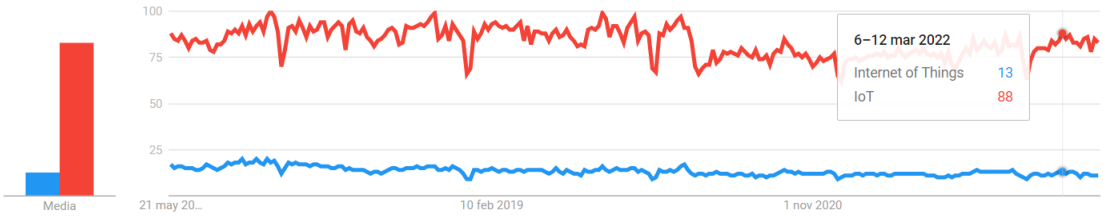


Figura 2. 1: Comparativa de búsqueda mundial entre Internet de las cosas e IoT.
Elaborado por: Autor.

Las comunicaciones, según la tradición, estaban limitadas a la voz o a la correspondencia a través de las líneas telefónicas. Desde entonces, el Internet apareció y proporcionó a la humanidad una novedosa plataforma de comunicación global. De esta manera, apareció el concepto de Voz sobre el Protocolo de Internet (VoIP) para las comunicaciones de voz que entraron en nuestras vidas. No obstante, en un lapso tan corto para el mundo, ha quedado atrás incluso el concepto de Internet y el concepto de IoT se ha instalado en nuestras vidas.

La introducción del concepto IoT en nuestras vidas se propuso en los laboratorios de Auto-ID del Instituto Tecnológico de Massachusetts (MIT) a principios de la década de 1990. Sin embargo, la primera aplicación de IoT, la “cafetera Trojan Room”, se desarrolló en 1999. En el mismo año, se desarrolló el primer dispositivo del mundo controlado por Internet, una tostadora que se

puede encender de forma remota. Sin embargo, la tecnología tampoco ha llegado a su posición actual tan repentinamente, sino que cada día aparecen nuevos términos relacionados con los avances, y la humanidad presenta siempre el siguiente paso al servicio de la humanidad. Por ello, lo más acertado es dividir los avances tecnológicos en etapas y evaluarlos de esa manera. En la figura 2.2 se presentan todas las etapas y la evolución de estas.

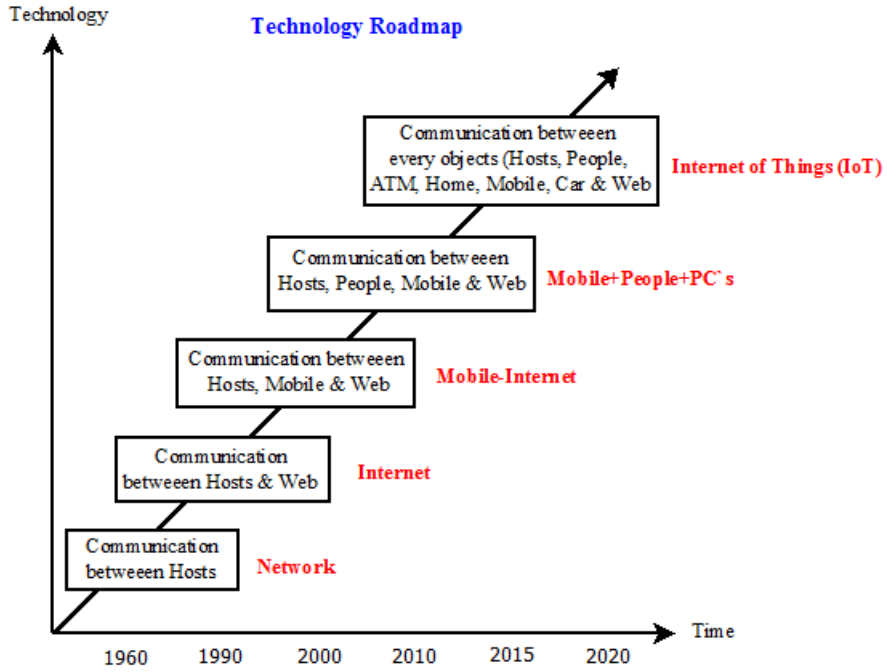


Figura 2. 2: Etapas de la evolución del IoT.
Fuente: (Khanna & Kaur, 2019)

Como primera etapa se puede mencionar el periodo pre-internet, donde la comunicación fue realizada a través de líneas telefónicas fijas y mensajes cortos. Con este escenario, el mundo conoció los dispositivos móviles y el medio de transmisión se desplazó a los dispositivos electrónicos. En la segunda etapa aparece el periodo de los contenidos de Internet. Durante esta etapa, se han incorporado conceptos como mensajes de mayor tamaño y archivos adjuntos al correo, a diferencia de la etapa anterior.

La tercera etapa corresponde a la etapa de Internet de los servicios, en este punto se han introducido aplicaciones tales como el comercio y la producción electrónicos en nuestras vidas. La cuarta etapa se define como la internet de las personas, y en esta etapa se incluyen aplicaciones como las

redes sociales, Instagram, Skype y YouTube. Ahora bien, el periodo actual en el que vivimos se llama IoT. En este periodo, los dispositivos tienen la capacidad de conectarse a Internet, comunicarse entre sí y transferir datos.

2.2. Evolución del IoT

La evolución que ha experimentado la tecnología también ha modificado los requerimientos y las perspectivas del ser humano con respecto a ella, y en la actualidad Internet de las cosas ya se define como una herramienta indispensable en términos de telecomunicación. En la actualidad, esta se ha convertido en una plataforma que permite controlar miles de millones de dispositivos a través del Internet clásico. Además, todos estos dispositivos son capaces de generar enormes cantidades de datos provenientes de los sensores a los que se conectan a Internet. (Khanna & Kaur, 2019)

Hasta ahora se han instalado más de 5.000 millones de dispositivos inteligentes conectados a Internet. Se estima que a finales de la década el valor de la IoT superará los 300.000 millones de dólares. Sin embargo, si se desconoce la evolución de IoT a lo largo del tiempo, sería erróneo apreciar su función y las capacidades que nos ha aportado. Por este motivo, la evolución de IoT desde el pasado hasta el presente se organiza en la tabla 2.1.

Tabla 2. 1: Evolución histórica del IoT.

Año	Desarrollo
1999	El término IoT apareció por primera vez en MIT Labs. Trojan Room Coffee Pot fue la primera aplicación IoT desarrollada
2000	LG anuncia los planes de Internet del primer refrigerador
2003	Se realiza el primer despliegue comercial de RFID
2005	Un grupo de empresas lanzó la Alianza IPSO para promover el uso de IP en redes de "Objetos Inteligentes" para habilitar IoT. Primera edición del informe sobre Internet de las Cosas de la Unión Internacional de Telecomunicaciones (UIT)
2008	IoT reconocido por la Unión Europea (UE)

2010	El primer ministro chino, Wen Jiabao, afirmó que IoT es una industria clave para China
2011	Se establece la Iniciativa de estándares globales de IoT (IoT-GSI)
2012	IBM, Ericsson y Cisco comienzan a desarrollar iniciativas de capacitación y marketing a gran escala sobre IoT
2013	Raspberry pi, Arduino y otras plataformas de hardware se desarrollaron y comenzaron a hacer que IoT sea accesible
2014	El uso de dispositivos de otros fabricantes, como los drones o la RFID, se combina fuertemente con el IoT

Fuente: (Khanna & Kaur, 2019)

En el ámbito académico e industrial, el concepto de IoT ha sido un área de interés desde que llegó a nuestro entorno, y todavía se están llevando a cabo varios estudios relativos a la asociación y el desarrollo de diversos dispositivos con Internet. Para los estudios de IoT son muy preferibles temáticas como la movilidad inteligente, los edificios inteligentes, las ciudades inteligentes, la seguridad pública, la salud, la medicina y la agricultura. En la figura 2.2 puede observarse el número de dispositivos conectados a Internet al año y el número estimado de dispositivos que se conectarán en los próximos años con relación a otras tecnologías que no usan IoT.

La escasez de chips sigue frenando la recuperación del mercado del Internet de las cosas (IoT), según nuestro último informe State of IoT-Spring 2022, publicado por (Hasan, 2022). El número de conexiones mundiales de IoT creció un 8% en 2021 hasta alcanzar los 12.200 millones de puntos finales activos, lo que representa un crecimiento significativamente menor que en años anteriores.

Aunque la demanda de soluciones de IoT está creciendo y la comunidad de IoT, al igual que la mayoría de los sectores de la industria, se muestra favorable, las previsiones de IoT apuntan a que la escasez de chips afectará al número de dispositivos IoT conectados mucho más allá de 2023. La

pandemia de COVID-19 y las interrupciones generales de la cadena de suministro son otros factores que afectan a los mercados de IoT. Se prevé que en 2022 el mercado de IoT crezca un 18% hasta alcanzar los 14.400 millones de conexiones activas. Además, para 2025, con la reducción de las restricciones en la oferta y una mayor aceleración del crecimiento, se espera que haya aproximadamente 27.000 millones de dispositivos IoT conectados.

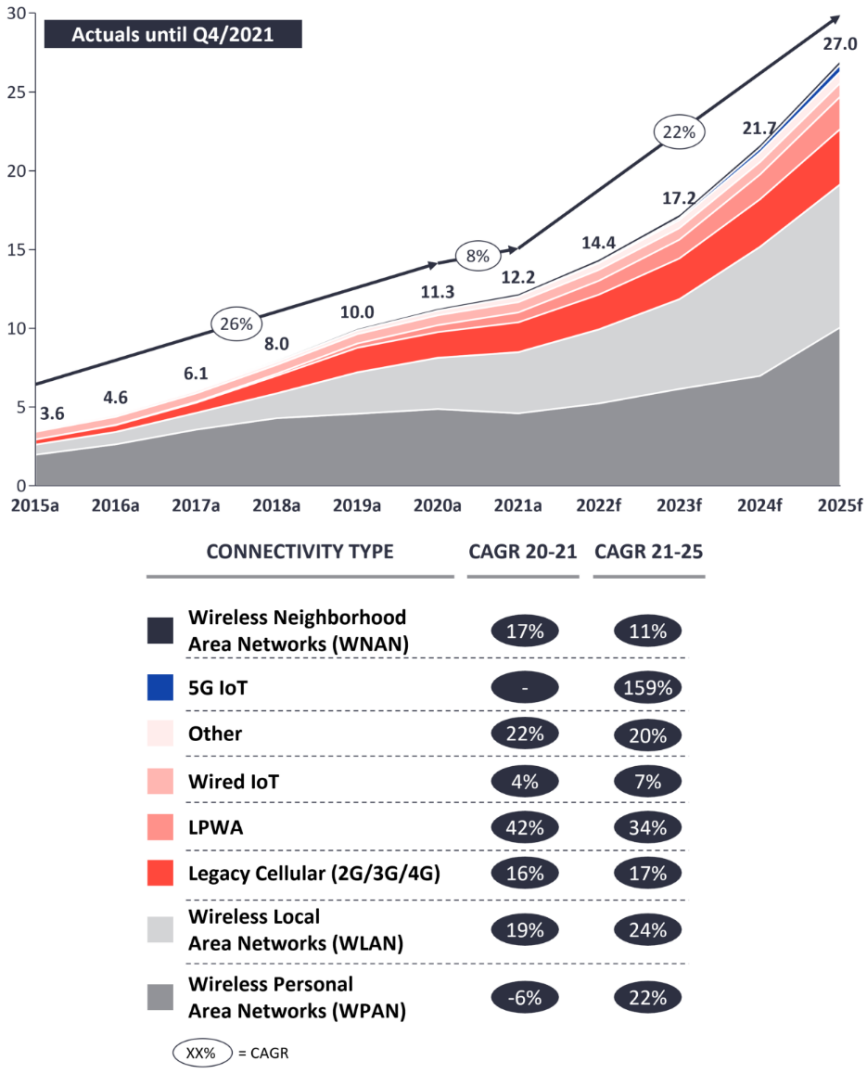


Figura 2. 3: Estado de IoT - dispositivos IoT conectados en todo el mundo.
Fuente: (Hasan, 2022)

2.3. Enfoque básico del IoT.

IoT puede definirse como una red de objetos y personas interconectadas que comparten datos para realizar diversas tareas. El propósito principal que persigue esta red es mejorar la calidad de nuestra vida cotidiana mediante la realización de diversas tareas. Además, el IoT, tiene aplicaciones en muchos

ámbitos, como los productos domésticos, el transporte, los servicios logísticos, la salud, las ciudades inteligentes o las aplicaciones industriales, y puede alcanzar a casi todos los objetos producidos.

Todo lo que se necesita para garantizar que los objetos estén incluidos en el concepto del Internet de las Cosas mediante la unión con Internet es sólo imaginación. Así, por ejemplo, los sistemas de transporte son un ejemplo sencillo al servicio del IoT, puesto que se pueden emplear múltiples vehículos inteligentes y mecanismos de gestión inteligentes en el transporte con el fin de garantizar un sistema de transporte más seguro.

Al tratarse de la integración universal de objetos, IoT está diseñada de forma que se garantice la interoperabilidad de éstos a través de una arquitectura orientada a servicios (SOA). Así, por ejemplo, el IoT se propone lograr los siguientes objetivos:

- ✓ Con la transición de la tecnología IPv4 a la IPv6, pretenden apoyar el futuro del IoT y resolver los problemas de fragmentación existentes,
- ✓ Desarrollar una SOA basada en IPv6, facilitando así aspectos como la autonomía de las ubicaciones, interoperabilidad, integración en la nube y distribución de datos entre aplicaciones, componentes y servicios no homogéneos,
- ✓ Poder explorar las siguientes formas innovadoras de interacción:
  - ❖ integración multiprotocolo
  - ❖ interoperabilidad automática con equipos heterogéneos,
  - ❖ soluciones informáticas en la nube, incluyendo IaaS, PaaS y SaaS,
  - ❖ etiquetado mediante RFID y otros servicios relacionados, y
  - ❖ sistemas de distribución inteligentes.

2.4. Las tecnologías de comunicación del Internet de las cosas (IoT)

Con la evolución de la tecnología, en la actualidad están disponibles múltiples opciones de conexión. Estos se basan en productos y sistemas

relacionados con el IoT. Las tecnologías de comunicación básicas utilizadas en la infraestructura del IoT se presentan en la tabla 2.2.

Tabla 2. 2: Diferentes tecnologías de comunicaciones usadas en infraestructuras del Internet de las Cosas (IoT).

Tecnología	Descripción
IEEE 802.15.4	Técnica y estándar de comunicación para especificar la capa física y el control de acceso a los medios para redes inalámbricas personales de baja velocidad (LR-WPAN).
Z-Wave	La tecnología Z-Wave se basa en un protocolo de comunicación inalámbrica de bajo consumo para las aplicaciones de domótica. Se emplea mucho en aplicaciones de control remoto para residencias inteligentes y zonas comerciales pequeñas. Estas frecuencias son las más utilizadas en los diseños de casas inteligentes, siendo una de las áreas en las que más se utiliza el IoT.
LTE	La tecnología LTE, es un protocolo de comunicación inalámbrica estandarizado para la transmisión de datos de alta velocidad entre teléfonos móviles. Es compatible hasta un máximo de 100 MHz. Generalmente, la descarga y la subida de datos se enfrentan a una latencia cada vez mayor en todo el proceso
LoRa	La tecnología LoRa es utilizada en la conectividad de largo alcance para varios dispositivos IoT y que se utilizan fundamentalmente en zonas rurales, remotas y también urbanas. Además, el sistema de gestión se utiliza en diversas aplicaciones, tales como la gestión de la cadena de suministro, la logística intercontinental, la minería y la gestión de los recursos naturales.
6LoWPAN	La tecnología 6LowPAN se basa en el protocolo de red con mecanismos de encapsulación y compresión. Además, el protocolo no está sujeto a la banda de frecuencia ni a la capa física y puede utilizarse en múltiples plataformas de comunicación, como Wi-Fi e IEEE 802.15.4.

Fuente: (Capella et al., 2016; Kar & Sanyal, 2018; Zanella, 2021)

2.5. Arquitectura IoT

Aunque no es una arquitectura estándar para IoT; Hay varias arquitecturas imprecisas que constan de tres, cuatro o cinco capas.

Inicialmente, la arquitectura de IoT más popular constaba de tres capas: capa de sensor, middleware y capa de aplicación. En la figura 2.4 se muestra la arquitectura de IoT de tres, cuatro y cinco capas. Por ejemplo, la figura 2.5 muestra las diferentes aplicaciones de la arquitectura IoT de tres capas.

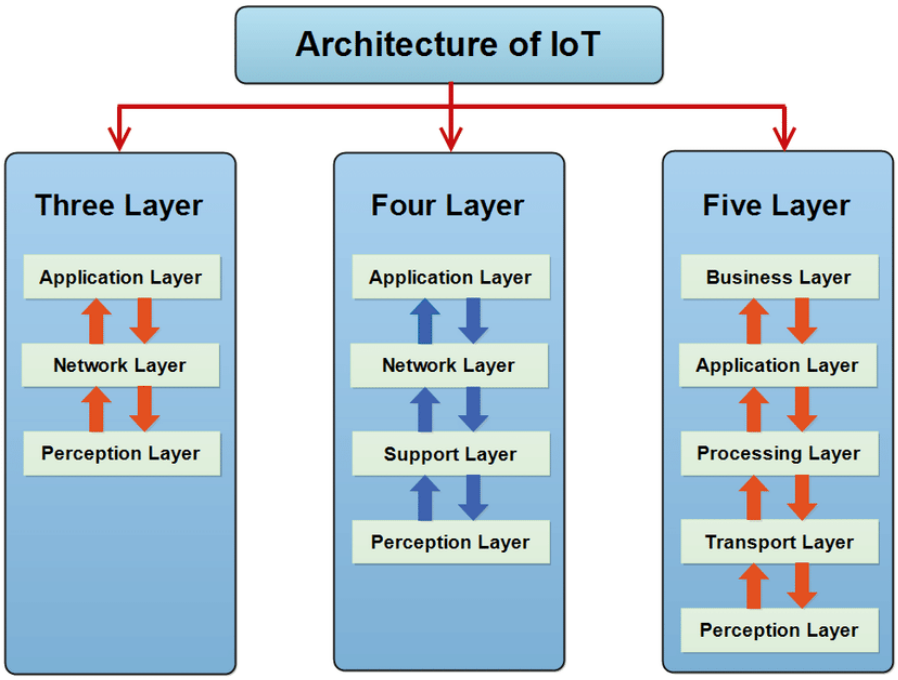


Figura 2. 4: Arquitectura del Internet de las Cosas de 3, 4 y 5 capas.
Fuente: (Burhan et al., 2018; Ebrary, 2022)

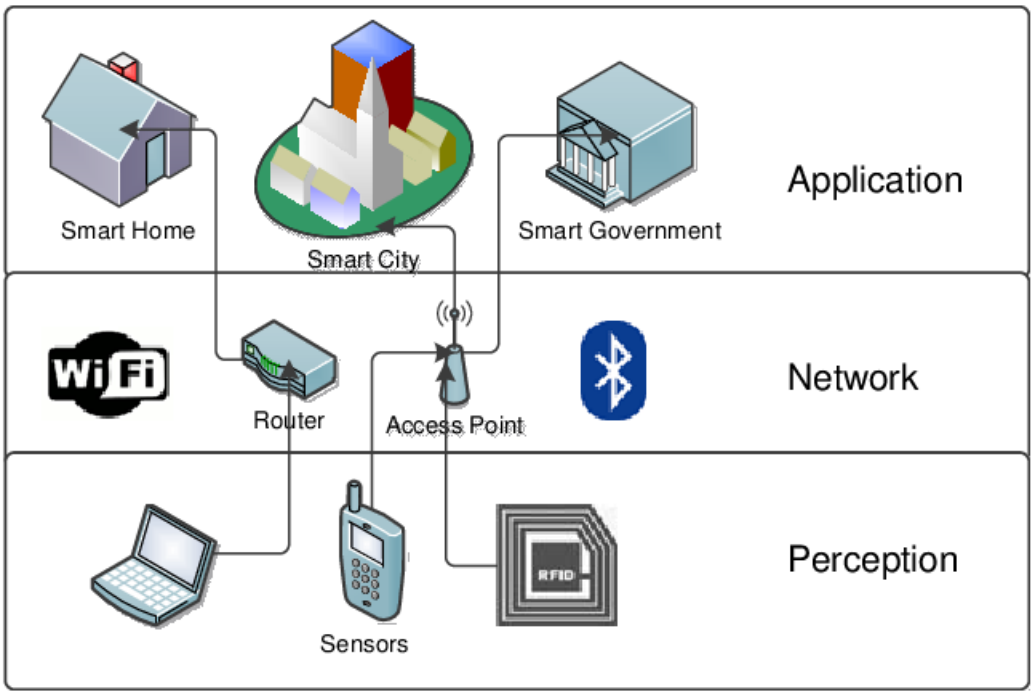


Figura 2. 5: Arquitectura del Internet de las Cosas de tres capas.
Fuente: (Mahmoud et al., 2015)

Por ejemplo, la capa de percepción o detección está compuesta por sensores o etiquetas RFID. La finalidad de la capa es identificar exclusivamente la información de los equipos de los que se van a extraer datos. Así mismo, realizan la transmisión y recepción desde el entorno de otros datos y los transmiten a las capas superiores para su procesamiento.

La capa de red o capa intermedia está destinada a proporcionar soporte de red y stack de protocolos para IoT. Por otro lado, la arquitectura puede dividirse en dos partes: por un lado, la capa de procesamiento que se encarga el tratamiento de los datos recogidos en la capa de sensores y, por otro, la capa de transporte encargada de la distribución de los datos a través de tecnologías como Bluetooth y Wi-Fi. La capa de percepción envía y recibe datos. Además, el sistema utiliza el direccionamiento IPv6 para asignar direcciones a los equipos de la red.

En la capa de aplicación se describen las aplicaciones que utilizan la tecnología de IoT o en las que se ha desplegado la tecnología de IoT. Su función radica en proporcionar servicios a las aplicaciones. Estos servicios varían de una aplicación a otra, porque dependen de la información obtenida a través de los sensores. La capa de aplicación en sí presenta varios problemas, entre los que destaca la seguridad. Si se quiere implementar un nivel de seguridad robusto en una casa inteligente basada en IoT, uno de los principales problemas radica en que los dispositivos que se utilizan en las casas inteligentes disponen de poca potencia de cálculo y poco almacenamiento, como ZigBee.

Para garantizar la seguridad de las aplicaciones de IoT, hay que abordar aspectos de seguridad y privacidad en cada capa de la arquitectura IoT. Todos estos problemas deben tenerse en cuenta y ser corregidos en la fase inicial del diseño del sistema. La arquitectura de IoT existente requiere controles adecuados de seguridad para una red de IoT desde el inicio y a intervalos regulares. Las tecnologías más utilizadas en la capa de percepción son las técnicas de detección e identificación, como las redes sociales inalámbricas

(WSN) y la identificación por radiofrecuencia (RFID). A continuación, se describen el tipo de amenazas más comunes a las que se enfrenta esta capa:

- ✓ Cobertura del nodo: En los dispositivos que están presentes en la red hay probabilidades reales de que se vean comprometidos, lo que puede comprometer la seguridad de toda la red y provocar la fuga de información importante.

ii. Nodo falso y datos maliciosos: En este caso, se trata de un dispositivo malicioso capaz de infiltrarse en todo el sistema, haciéndolo circular a través de la red.

iii. Los ataques basados en la interrupción del servicio (DoS-DDoS): Tanto los ataques DoS como los DDoS son los más comunes y los más perjudiciales en la red. Los ataques consisten en el uso de los recursos de la red provoca el agotamiento y la indisponibilidad de los servicios

2.6. Aplicaciones IoT

El IoT es el ámbito en el que el concepto de Internet ha evolucionado con las tecnologías actuales y ha entrado en nuestras vidas. Tanto es así que ya se ha hecho un hueco en ámbitos que afectarán a nuestras vidas. En un estudio, se evaluaron 1600 proyectos reales de IoT y se determinaron las 10 áreas en las que se utiliza más intensamente.

En las ciudades inteligentes recae la mayor participación en las aplicaciones de IoT. Este crecimiento se debe a que los estados y gobiernos del mundo entero han decidido invertir en ciudades inteligentes. En la actualidad, las ciudades inteligentes abarcan proyectos como la supervisión y el control del tráfico, la compartición de vehículos de transporte, por ejemplo, bicicletas, carriles inteligentes para el transporte urbano y los servicios de taxi, así como sistemas inteligentes de estacionamiento. En este ámbito, Europa y América lideran los principales centros de atención, y el concepto de ciudades inteligentes muestra una tendencia creciente.

Tras las ciudades inteligentes, el concepto de industria conectada ocupa el segundo lugar, con un 17%. Dentro de esta idea existen diversos elementos dentro y fuera de la fábrica. La aplicación principal que se le da a este concepto es la supervisión de equipos e inventarios en el entorno externo. En este campo, Estados Unidos es uno de los países líderes. Sin embargo, los edificios inteligentes, la seguridad de los edificios y los sistemas de climatización están incluidos en el concepto de edificio controlado, que ocupa el tercer lugar de la lista, y se ha observado que el objetivo de reducir los costes energéticos ha sido el punto central en el último periodo.

Además, el concepto de automóvil conectado, que ocupa el cuarto lugar de la lista con una cuota del 11%, se presenta también como el concepto que ha experimentado un mayor incremento. En este concepto están incluidos el monitoreo en tiempo real de los vehículos, el control de las lecturas obtenidas por los sensores y de la gestión de los vehículos a distancia. Como se puede ver, el concepto de IoT y sus aplicaciones se están volviendo cada vez más a integrar y facilitarnos el trabajo.

2.6.1. En la domótica.

Esta categoría incluye dispositivos de control remoto: encender y apagar aparatos a distancia para evitar accidentes y ahorrar energía, uso de energía y agua: controlar el consumo de energía y agua para obtener consejos sobre cómo ahorrar costes y recursos, arte y conservación de la propiedad : vigilancia del estado de conservación en el interior de los museos y almacenes de arte, y sistemas de detección de intrusos: detección de aperturas de puertas y ventanas y de brechas para prevenir las intrusiones.

La iluminación inteligente atrae cada vez más la atención de la comunidad investigadora. HomeKit es un entorno diseñado por Apple que permite a los usuarios configurar, comunicar y controlar dispositivos domésticos inteligentes. Los usuarios pueden realizar acciones automáticas en el hogar mediante un simple dictado de voz. Por ejemplo, Google Home es un asistente personal inteligente con un altavoz y dos micrófonos. dos

micrófonos permiten que el dispositivo responda a las órdenes de voz de las personas cercanas.

Nest es un termostato que recuerda los hábitos y las temperaturas preferidas de los usuarios. Baja la calefacción en su ausencia y calcula el tiempo necesario para calentar la casa y utilizar la mínima cantidad de energía. El termostato puede controlarse a distancia mediante una aplicación móvil específica.

2.6.2. Ambientes inteligentes.

Esta categoría incluye la alerta temprana de terremotos: monitorización distribuida en lugares específicos de terremotos, prevención de desprendimientos y avalanchas: monitorización de la humedad del suelo, vibración y densidad de la tierra para detectar tendencias peligrosas en las condiciones del terreno, monitorización del nivel de nieve: medición de la cota de nieve para conocer en tiempo real la calidad de las pistas de esquí y permitir la seguridad en caso de avalanchas, detección de incendios forestales: seguimiento de los gases de combustión y de las condiciones del incendio para definir las zonas de alerta, y contaminación atmosférica: seguimiento de las emisiones de CO2 de las fábricas, de la contaminación emitida por los automóviles la contaminación de los coches y los gases tóxicos.

2.6.3. Transporte y logística.

Esta categoría incluye la detección de incidencias en el almacenamiento: las emisiones de los contenedores que almacenan productos inflamables cerrados a otros que contienen materiales explosivos, el seguimiento de la flota: la supervisión del seguimiento de las rutas de mercancías sensibles como joyas, medicamentos o mercancías peligrosas, la localización de artículos: la búsqueda de artículos individuales en grandes áreas como almacenes o puertos, y la calidad de las condiciones de envío: la supervisión, a efectos de seguros, de las vibraciones, los golpes, las aperturas de los contenedores o su mantenimiento.

2.6.4. Agricultura inteligente

Esta categoría incluye el abono: control de los niveles de humedad y temperatura del heno, la paja, etc. para evitar los hongos y otros contaminantes microbianos, estaciones meteorológicas: estudio de las condiciones meteorológicas en los campos para predecir la formación de hielo, la lluvia, la sequía, la nieve o los cambios de viento, mejora de la calidad del vino: seguimiento de la humedad del suelo y del diámetro del tronco en las vides para controlar la cantidad de azúcar en la vid y su salud, campos de golf: riego selectivo en zonas secas para reducir las necesidades de agua, invernaderos: control de las condiciones microclimáticas para maximizar la producción y la calidad de las frutas y hortalizas y el cultivo hidropónico: controlar el estado de las plantas cultivadas en el agua para conseguir las cosechas más eficientes

Capítulo 3: Simulación y Resultados Obtenidos.

3.1. Introducción de IoT en tecnologías de comunicaciones inalámbricas.

El Internet de las Cosas (IoT) no es más que un sistema descentralizado y débilmente vinculado a objetos (dispositivos físicos, vehículos, electrodomésticos, ...) con capacidad suficiente para la detección o captación, así como para el almacenamiento y la interpretación de la información generada por sí mismos y por el entorno externo en el que se encuentran.

Puesto que en la actualidad las tecnologías de comunicación inalámbricas son una tendencia, el propósito principal del capítulo es explicar el estado actual de las diferentes tecnologías de comunicación y los ámbitos utilizados por la IoT, incluyendo sus arquitecturas y modos de funcionamiento. Sobre todo, se estudiarán y se analizarán en detalle los mecanismos de seguridad, en particular la confidencialidad.

3.2. Los sistemas de seguridad basados en IoT.

La seguridad de IoT puede definirse como la garantía de que un sistema funciona correctamente y ofrece los resultados esperados de su diseño. En otras palabras, la seguridad es el conjunto de políticas y prácticas adoptadas para prevenir y controlar el acceso no autorizado, el uso indebido, la modificación o la negación de una operación informática. De esta definición podemos extraer los fundamentos de la seguridad que son (Autenticación, Confidencialidad, Integridad, ...). Según lo mencionado anteriormente, el interés del presente trabajo es únicamente sobre la gestión de la privacidad en un entorno de IoT.

Este mecanismo se utiliza para proteger la información, e inclusive la existencia de esta. Así, se impide que cualquier persona o entidades no autorizada(s) puedan disponer del acceso a estos datos. Generalmente, esta prestación se hace mediante la codificación de los datos. Éste es un método de cifrado de datos y está basado principalmente en algoritmos matemáticos

(AES, DES, RSA) lo que permite la distorsión de un texto plano y el restablecimiento a su forma original a través del empleo de una o varias claves criptográficas. El presente estudio describe la confidencialidad de las comunicaciones del IoT en algunas tecnologías.

3.3. Análisis descriptivo de las tecnologías de comunicaciones sobre IoT.

Los sistemas tecnológicos del IoT se clasifican a través de una serie de características comunes, como son el rendimiento, la cobertura y el rango de frecuencias en que funcionan. En las siguientes secciones se analizan cada una de estas tecnologías en la que describen sus arquitecturas, seguridad y confidencialidad.

3.4. Aplicaciones para redes inalámbricas extensas (WWAN)

Las redes de este tipo han sido consideradas en su mayor parte como redes extensas. En general representan redes inalámbricas de baja potencia (LoRaWAN y Sigfox), y también redes móviles tales como GSM, UMTS y LTE. Las redes WWAN se caracterizan asimismo por redes satelitales tal como los sistemas GPS.

3.4.1. Tecnología inalámbrica LoRaWAN.

LoRaWAN pertenece a las tecnologías basadas en redes de área amplia de baja potencia *(Low Power WAN, LPWAN)* y que han recibido considerable importancia entre los investigadores que trabajan en este campo en los últimos años. Además, este sistema proporciona una transmisión de datos y energía de bajo consumo dentro de un amplio espectro radioeléctrico. Su arquitectura se adapta al IoT, permitiéndole detectar con facilidad los objetos móviles. Está desplegada sobre redes públicas a través de grandes operadores de telecomunicaciones (por ejemplo, Orange).

En general, el modelo de las redes LoRaWAN adopta una topología en estrella que permite establecer una conexión entre los terminales (por ejemplo, sensores, ordenadores, etc.) de la red y sus servidores centralizados,

que se conectan respectivamente con los servidores de aplicaciones. servidor de aplicaciones.

3.4.1.1. Arquitectura de la tecnología inalámbrica LoRaWAN.

A continuación, en la figura 2.1, se muestra un esquema de la arquitectura LoRaWAN formada por nodos finales, puertas de enlace, un servidor de red y un servidor de aplicaciones.

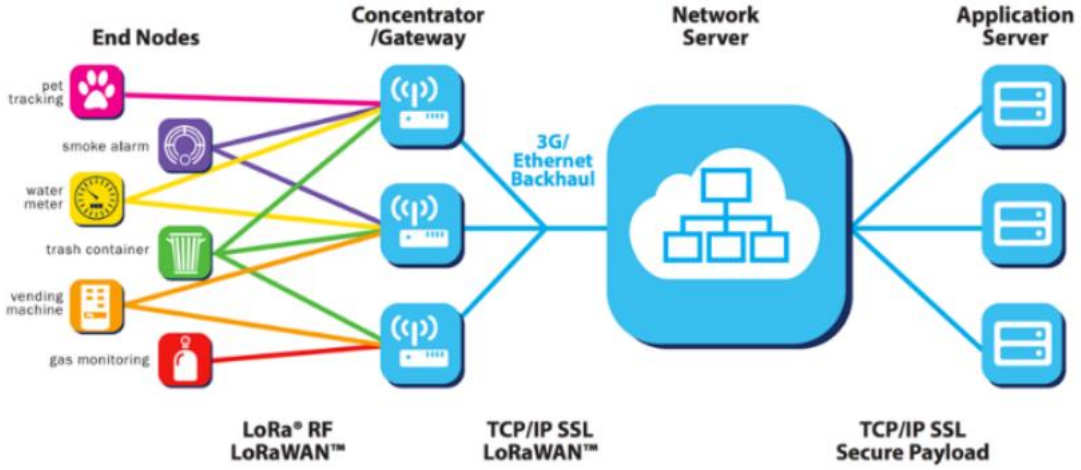


Figura 3. 1: Diagrama esquemático de la arquitectura de LoRaWAN.
Fuente: (Naoui et al., 2016)

Inicialmente, el nodo final transfiere de forma automática los datos obtenidos a diferentes puertas de enlace que utilizan la capa física del sistema LoRa. Después, cada puerta de enlace transmitirá los datos obtenidos del nodo de extramuros hasta el servidor de la red a través de un enlace (Wi-Fi, ethernet celular o satélite). Los servidores de red son entidades inteligentes que se encargan de gestionar la red, hacer comprobaciones de seguridad, establecer tasas de datos adaptativas, y filtrar paquetes redundantes recibidos, etc.

3.4.1.2. Seguridad y confidencialidad de la tecnología inalámbrica LoRaWAN.

Los mecanismos fundamentales de autentificación y confidencialidad de los datos están garantizados a través de la política de seguridad del sistema

LoRaWAN. Asimismo, dicha política especifica los métodos para el intercambio de claves.

Cuando se asocia en la red LoRaWAN, se codifican los mensajes transmitidos para asegurar la confidencialidad a través de claves de sesión reconocidas exclusivamente por el servidor de la red y el objeto en cuestión. La encriptación de los mensajes corresponde a la norma AES128 utilizando la modalidad de funcionamiento de contador (CTR).

3.4.2. Tecnología inalámbrica móvil.

Estos sistemas constituyen redes de gran alcance (desde unos pocos kilómetros en las ciudades hasta 30 km en las zonas rurales) y requieren un gran consumo de energía. Así como las redes GSM, 2G, 3G o 4G, éstas son capaces de transmitir una gran cantidad de datos (vídeos, imágenes, etc.) y ofrecen gran cobertura a nivel nacional e internacional.

Los sistemas móviles 2G utilizan para su funcionamiento las tecnologías de comunicación móvil global (GSM). Además, los sistemas 2G incorporan las tecnologías TDMA (Acceso Múltiple por División de Tiempo) y FDMA (Acceso Múltiple por División de Frecuencia). De esta manera, puede conectarse simultáneamente una mayor cantidad de usuarios a una determinada banda de frecuencias.

Los sistemas móviles 3G se basan en las tecnologías de acceso múltiple por división de código (CDMA) y acceso múltiple por división de código de banda ancha (WCDMA). El esquema CDMA es una técnica con la cual se atribuye una codificación única para cada usuario del sistema en ese instante. El código que se asigna depende de que el usuario se encuentre en ese momento utilizando el sistema. Una vez asignado un código único, se le asigna al usuario un ancho de banda completo se utiliza de forma eficiente en él. Como resultado, un gran número de usuarios puede utilizar el canal al mismo tiempo en comparación con TDMA y FDMA.

El sistema LTE (Long Term Evolution) o 4G es una tecnología basada principalmente sobre una red de transporte de paquetes IP. Esta tecnología no prevé un enrutamiento de voz diferente de VoIP, en contraste con el sistema 3G, que transmite información de voz en modo de circuito. En LTE se emplean bandas de radiofrecuencia que van de 1.4 MHz a 20 MHz, a fin de permitir (para una banda de 20 MHz) una velocidad de transmisión de datos teórica de hasta 300 Mbps, en tanto que en 4G la velocidad de transmisión es de 1 Gbps.

3.4.2.1. Arquitectura de la tecnología LTE.

La arquitectura general del sistema LTE se muestra en la figura 2.2 con su configuración básica del sistema y los nodos lógicos. Estos elementos son necesarios cuando la E-UTRAN está en la red de acceso. La arquitectura se subdivide en cuatro subsistemas principales:

1. UE: Dispositivos de usuarios o terminal móvil
2. E-UTRAN: Red Universal de Acceso Radioeléctrico Terrestre Evolucionado.
3. EPC: Núcleo de paquetes evolucionado.
4. Dominio de los servicios: Redes externa y/o internet

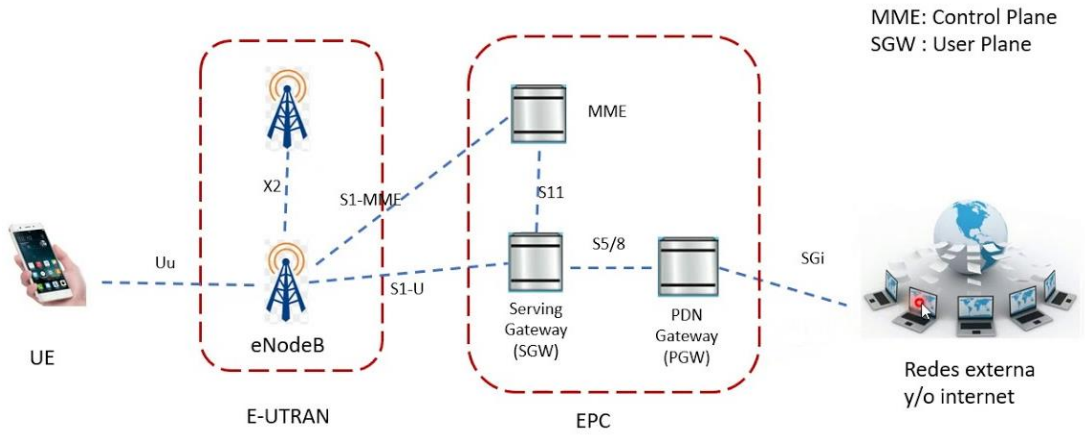


Figura 3. 2: Arquitectura de la tecnología 4G-LTE.
Elaborado por: Autor

A continuación, se presentan los diferentes elementos que operan en los sistemas 4G-LTE.

- - eNB: Estación base E-UTRAN.

- MME: Unidad de Gestión de la Movilidad.
- SGW: Service Gateway.
- PGW: Packet Data Network Gateway.
- HLR: registrador de localización de abonados.
- HSS: superconjunto de HLR que integra nuevos protocolos de red central (Diameter y SIP) específicos para las redes 4G.
- HSS: se comunica con los MME -a través de pasarelas si es necesario- que están conectados al HSS/HLR.

3.4.2.2. Seguridad y confidencialidad de tecnología inalámbrica LTE.

El enfoque es únicamente en LTE, debido a que a partir de 2012 se convirtió en la tecnología de mayor despliegue. El sistema LTE garantiza principalmente prestaciones de seguridad, es decir, autenticación y confidencialidad de los datos. El sistema LTE emplea el estándar que protege la privacidad, llamado Algoritmo de Encriptación del Sistema de Paquetes Evolucionado (128-EEA3). El algoritmo de privacidad 128-EEA3 proporciona un cifrado de flujo utilizado para cifrar/encriptar bloques de datos a través de una clave simétrica (por ejemplo, CK). El bloque de datos puede tener una longitud de entre 1 y 32 bits.

3.4.3. Tecnología inalámbrica satelital.

En un sistema de comunicaciones por satélite de tipo híbrido es posible establecer una comunicación, en especial acceder a Internet, con usuarios que utilizan computadoras. Este sistema híbrido de comunicaciones satelitales está compuesto tanto por un dispositivo satelital y un sistema terrestre de comunicaciones. Así, pues, el sistema satelital se compone de dos transmisores receptores.

Esta primera unidad transmisora receptora se encarga de recibir y transmitir todo un conjunto de señales provenientes de la red de comunicación terrestre destinadas un gran número de equipos móviles. Por el contrario, el segundo transmisor receptor del sistema satelital se encarga de recibir un segundo conjunto de señales en otra banda de frecuencias del usuario.

3.4.3.1. Arquitectura de tecnología inalámbrica satelital.

Las redes satelitales están integradas por redes terrestres y es posible combinarlas de diferentes maneras. En este sentido, es posible plantearse diversas propuestas tecnológicas, aunque el criterio fundamental para la integración estará determinado por los modelos funcionales y económicos que resulten de ello. A pesar de todo, se pueden establecer 3 tipos generales de integración:

1. Un sistema móvil (3G, LTE, WIMAX) totalmente integrado y transparente que soporta las comunicaciones satelitales como un canal de acceso alternativo.
2. El sistema de retransmisión, donde el satélite es integrado a la infraestructura de la red móvil, aunque no directamente a la interfaz aérea, sino por medio de una retransmisión ("gateway") que le permite el acceso a la infraestructura móvil principal.
3. Los sistemas móviles satelitales están dotados de una interfaz específica para acceder a una red IP terrestre utilizando dicha interfaz. En consecuencia, se requieren dispositivos multimedia y de múltiples tecnologías, con capacidad para gestionar diversas interfaces y los correspondientes protocolos específicos (por ejemplo, DVB-RCS+M).

3.4.3.2. Seguridad y confidencialidad de tecnología inalámbrica satelital.

En la actualidad se han realizado numerosos estudios que tienen como finalidad garantizar la seguridad en las redes por satélite. Este trabajo estudia la privacidad de los servicios en una red satelital bidireccional formada por dos usuarios móviles que desean intercambiar mensajes a través de un satélite con múltiples haces. Asimismo, existen estudios sobre el uso del protocolo SSL (Satellite Secure Sockets Layer), el cual permite utilizarlo en las redes satelitales para garantizar la autenticación de los usuarios, y la privacidad e integridad de los datos. En la tecnología satelital, la confidencialidad se garantiza gracias al estándar de encriptación de datos (DES)

3.5. Aplicaciones para redes inalámbricas metropolitanas (WMAN)

Las redes inalámbricas metropolitanas (WMAN) son conocidas como bucles locales de radio (RLL). Las redes WMAN están basadas en el estándar IEEE 802.16. Esta tecnología está pensada principalmente para las empresas operadoras de telecomunicaciones, por lo que su velocidad máxima oscila entre 1 y 10 Mbps para un alcance comprendido entre 4 y 10 kilómetros.

3.5.1. Tecnología inalámbrica WiMAX.

WiMAX o Interoperabilidad Mundial para Acceso por Microondas es un grupo de estándares destinados al establecimiento de conexiones inalámbricas de alta velocidad, que ha sido desarrollado por el Consorcio del Foro WiMAX y homologado en 2001 por la IEEE como IEEE-802.16. Además, WiMAX es la denominación comercial otorgada por el Foro WiMAX a los dispositivos compatibles con el estándar IEEE 802.16, para asegurar la interoperabilidad entre ellos.

3.5.1.1. Arquitectura de tecnología inalámbrica WiMAX.

En la arquitectura de la red WIMAX intervienen las estaciones base (Base Station, BS) y las estaciones móviles o clientes (Subscriber Station, SS) tal como se muestra en la figura 3.3. Las estaciones base desempeñan la función de antena principal responsable de la comunicación y del servicio ofrecido a las estaciones móviles, quienes a su vez prestan servicios a los clientes mediante WIFI o ADSL. Dicha estación base está compuesta por dos módulos:

1. Dispositivo interior con procesador, módem, interfaz Ethernet y módulo de radio.
2. Dispositivo exterior que contiene un módulo de radio y una antena de transmisión-recepción.

Adicionalmente a la estación móvil o cliente la cual contiene ambos módulos con las mismas funciones que la BS, hace falta una terminal similar al módem ADSL para asegurar la conexión. La trayectoria de la comunicación entre la SS y la BS tiene dos direcciones:

- ✓ Enlace ascendente (de la SS a la BS)
- ✓ Enlace descendente (de la BS a la SS)

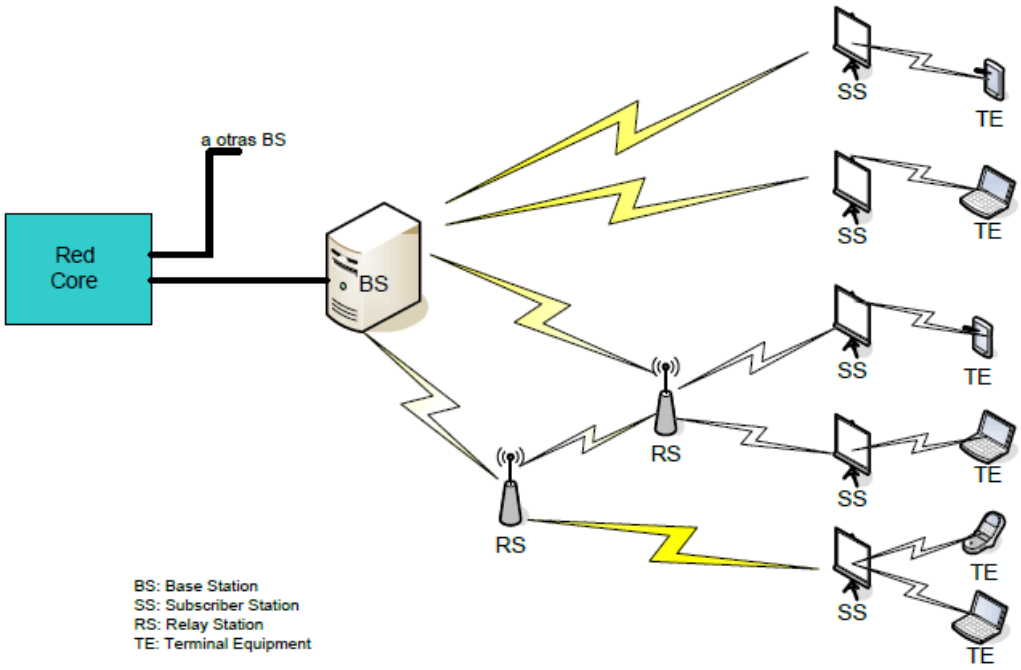


Figura 3. 3: Arquitectura de la tecnología WiMAX.
Elaborado por: El Autor

Entre las funciones de la capa física destacan los procesos de codificación/descodificación de señales, la generación/eliminación de preámbulos y la transmisión/recepción de bits. Por su parte, las funciones de la capa de enlace de datos incluyen el control de acceso al medio:

- Al transmitir, los datos son agrupados a través de tramas que incluyen direcciones y detecciones de errores.
- Al recibir, la trama se despliega y lleva a cabo el reconocimiento de la dirección y la detección de errores.
- Gobernar la accesibilidad al medio de transmisión inalámbrico

Las funciones de la capa de convergencia son: Encapsular las tramas PDU de las capas superiores en tramas MAC/PHY nativas de 802.16, mapear las direcciones de la capa superior en direcciones de 802.16, traducir los parámetros de QoS de la capa superior al formato MAC nativo de 802.16 y adaptar las dependencias temporales del tráfico de la capa superior en un servicio MAC equivalente. de la capa superior a un servicio MAC equivalente.

3.5.1.2. Seguridad y confidencialidad de tecnología inalámbrica WiMAX.

La seguridad fue reconocida como uno de los principales puntos débiles de las primeras versiones de WiMAX. El último estándar 802.16e ha permitido perfeccionar los aspectos mencionados con la introducción en las redes inalámbricas de banda ancha con relación a la integridad, autentificación y confidencialidad. Además, la subcapa de seguridad proporciona a los usuarios una gran protección contra la apropiación de los servicios. Por ejemplo, las estaciones base BS están protegidas contra los accesos no autorizados protegiendo así los flujos de servicios asociados en la red.

La subcapa de seguridad también introduce los mecanismos de autenticación en el protocolo de gestión de claves cliente/servidor, mediante el cual la BS controla la distribución de los elementos de cifrado a las estaciones móviles (Mobile Station, MS). Además, se reforzaron los mecanismos básicos de seguridad añadiendo una autentificación del dispositivo basada en un certificado digital. En este sentido, la tecnología WiMAX proporciona una mayor fiabilidad, ya que permite segmentar sus comunicaciones para conseguir una mayor confidencialidad. En este caso se trata de una versión más robusta, AES, con el protocolo CCMP.

3.6. Aplicaciones para redes inalámbricas metropolitanas (WLAN)

Los sistemas de redes inalámbricas locales (WLAN) abarcan el rango correspondiente a la red de área local de una empresa, es decir, un alcance de 100 metros aproximadamente. Este sistema permite interconectar entre sí los terminales que se encuentran dentro de la zona de cobertura. Por ejemplo, existen diferentes tecnologías que compiten entre sí: Wifi; HiperLAN.

3.6.1. Tecnología inalámbrica Wifi.

En la actualidad, la red Wi-Fi (contracción de Wireless-Fidelity) es un estándar universal de redes inalámbricas locales (WLAN). Esta tecnología permite establecer radioenlaces entre, por ejemplo, terminales y puntos de acceso que se conectan a una red local o a Internet. En la práctica, la

tecnología Wi-Fi hace posible que se conecten laptops, computadoras de oficina, asistentes digitales personales (PDA) y dispositivos móviles a un enlace de banda ancha o a dispositivos electrónicos que se comunican sobre un radio de algunas decenas de metros en interiores y varios cientos de metros en un entorno abierto.

3.6.1.1. Arquitectura de tecnología inalámbrica Wifi.

El estándar IEEE 802.11 determina las capas básicas del modelo OSI para una conexión inalámbrica a través del uso de ondas electromagnéticas, es decir

- La capa física: permite realizar tres formas de codificación de la información.
- La capa de enlace de datos: comprende de dos subcapas: Control de Enlace Lógico (LLC) y Control de Acceso al Medio (MAC).

En WiFi se establece que las dos primeras capas (inferiores) del modelo OSI corresponden a las capas físicas y enlace de datos. Además, el sistema incorpora mejoras en la capa inferior del nivel de enlace (es decir, en la MAC) y nivel físico mediante diversos mecanismos para el acceso radioeléctrico y de reglas de comunicación entre diferentes estaciones. También hay que señalar que la nueva capa MAC se aplica a todas las capas físicas. La figura 3.4 muestra la arquitectura por niveles del estándar IEEE802.11.

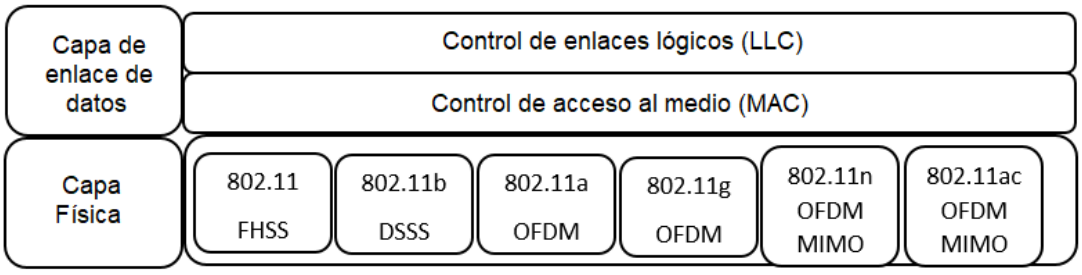


Figura 3. 4: Arquitectura del estándar IEEE 802.11 – Wifi.
Elaborado por: El Autor

3.6.1.2. Seguridad y confidencialidad de tecnología inalámbrica Wifi.

El sistema de seguridad Wifi utiliza el estándar 802.11i, que soporta hasta tres protocolos de seguridad:

- WEP, heredado del estándar 802.11 original.
- TKIP es el protocolo de integridad de clave temporal posterior a WEP. Se implementa en él el algoritmo de desencriptación RC4 y se agrega a cada MAC SDU11 una firma de 64 bits llamada código de integridad del mensaje (MIC). La codificación RC4 tiene un tamaño de 128 bits y se deduce de un contador de transmisión de secuencias de 48 bits transmitido en modo abierto y una clave temporal (TK).
- CCMP (Counter-Mode/CBC-MAC), este protocolo utiliza el algoritmo de cifrado AES en modo CCM y una firma MIC. Los parámetros de encriptación (¿bloque inicial?) se derivan de un contador de 48 bits transmitido de forma transparente y con clave temporal (TK).

3.7. Aplicaciones para redes inalámbricas metropolitanas (WPAN)

Las redes inalámbricas de cobertura limitada, es decir, del orden de unas decenas de metros. Así como la cobertura varía de una tecnología WPAN a otra, lo mismo sucede con la velocidad de transmisión de datos. En este sentido, la velocidad puede ser de 250 Kbps (ZigBee) a 1 Mbps (Bluetooth). Es decir, son tecnologías pertenecientes a la familia IEEE 802.15, de las cuales la más conocida es la subestándar IEEE 802.15.1 (Bluetooth), así como las que se utilizan en el campo de las redes de sensores inalámbricos (WSN), cuyo estándar fundamental es el subestándar IEEE802.15.4, tales como ZigBee, OCARI, 6LoWPAN, etc.

3.7.1. Tecnología inalámbrica 6LoWPAN.

La red inalámbrica inteligente 6LoWPAN tiene como objetivo el desarrollo de redes inalámbricas personales de bajo consumo. Esta red inteligente se puede implementar mediante una topología en estrella o mallada. Está basada sobre el protocolo IPv6, que permite tener diversas ventajas, como la capacidad de usar la infraestructura IP existente y tecnologías comprobadas y autorizadas. Además, la conexión física a otras redes IP es muy sencilla, ya que no hace falta recurrir a entidades intermediarias, como, por ejemplo, las plataformas.

3.7.1.1. Arquitectura de tecnología inalámbrica 6LoWPAN.

En la figura 3.5 se representa la arquitectura de red 6LoWPAN conformada por nodos sensores, enrutadores, enrutadores de borde 6LoWPAN (6LBRs), plataforma de gestión de la información y otras aplicaciones relacionadas con el Internet de las Cosas. Así, por ejemplo, en la capa de detección, la arquitectura permite clasificar a los nodos sensores mediante códigos o protocolos heterogéneos, a través de la técnica de clasificación de dominios virtuales.

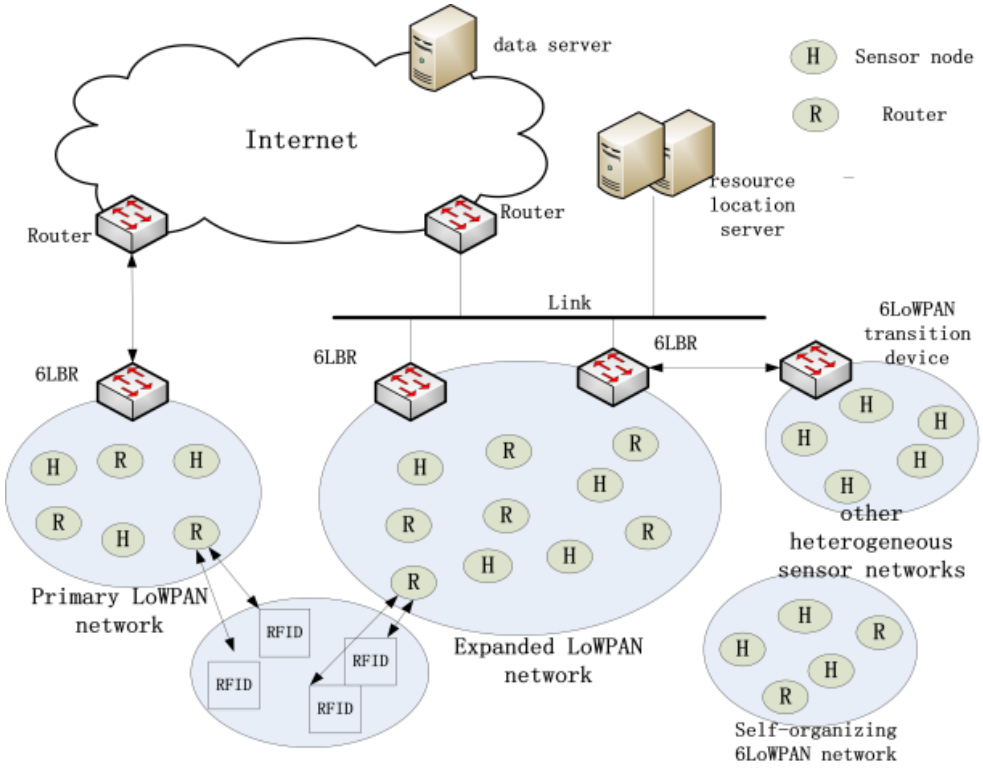


Figura 3. 5: Arquitectura del estándar inalámbricos 6LoWPAN.
Fuente: (Luo et al., 2015)

La información que ingresa en la red 6LoWPAN tiene como destino final a uno de los dispositivos que la componen. Una red 6LoWPAN puede conectarse a otras redes IP a través de uno o varios routers de borde que transfieren datagramas IP entre diferentes medios de transmisión. Pero a diferencia de lo que significa un gateway de Internet, 6LBRs se sitúa en la capa de red, es decir, tiene que reenviar paquetes en la capa de red y adaptarse a diferentes redes de detección realizando la configuración y conversión de direcciones. Además, la plataforma de gestión de recursos del Internet de las Cosas se encarga de localizar y adquirir eficazmente los

recursos a través del direccionamiento de dispositivos terminales, debido a la diversidad, heterogeneidad y gran cantidad de dispositivos existentes en el entorno del Internet de las Cosas.

3.7.1.2. Seguridad y confidencialidad de tecnología inalámbrica 6LoWPAN.

Las tecnologías 6LoWPAN, a diferencia de la mayoría de las tecnologías IEEE 802.15.4, proporcionan un alto grado de privacidad. No obstante, esto no define un método específico para la autenticación, ni tampoco para la gestión del enlace. En este sentido, un trabajo interesante fue la definición de un método de autenticación que utiliza el Protocolo de Autenticación Extensible de clave precompartida generalizada (EAP-GPSK), que se basa en la criptografía simétrica. Para proteger los datos intercambiados, se recomienda el uso del estándar AESCCM, que es un algoritmo que garantiza tanto los servicios de integridad como de confidencialidad.

3.7.2. Tecnología inalámbrica Zigbee.

Con el rápido desarrollo de la tecnología de redes y la tecnología de comunicación inalámbrica, ZigBee tiene ahora una aplicación cada vez más amplia, que es un tipo de tecnología emergente en el campo de la red de sensores inalámbricos. Por ello, la seguridad de ZigBee es cada vez más importante. La tecnología Zigbee funciona a baja velocidad y con pocos recursos (energía, computación y almacenamiento) y puede ser implementada con una topología de estrella o mallada. Los datos de la banda de 2.4 GHz alcanzan los 250 Kbps, mientras que en la banda de 868 MHz sólo llegan a los 20 Kbps.

3.7.2.1. Arquitectura de tecnología inalámbrica Zigbee.

ZigBee se basa en el estándar de redes inalámbrica personales (WPAN) IEEE 802.15.4 para implementar protocolos de red que soportan los procesos de nivel superior y, en última instancia, permiten la aplicación de destino. La figura 3.6 se muestra la arquitectura de red Zigbee. Los sistemas Zigbee están compuestos por tres clases de dispositivos: el coordinador Zigbee, el router y

el dispositivo final. En toda red Zigbee es necesario disponer al menos de un coordinador que funcione como base y enlace de la red. En la actualidad, el coordinador es responsable de procesar y almacenar la información recibida y transmitida. Por su parte, los routers Zigbee actúan como dispositivos intermediarios encargados de la transmisión de datos a otros dispositivos.

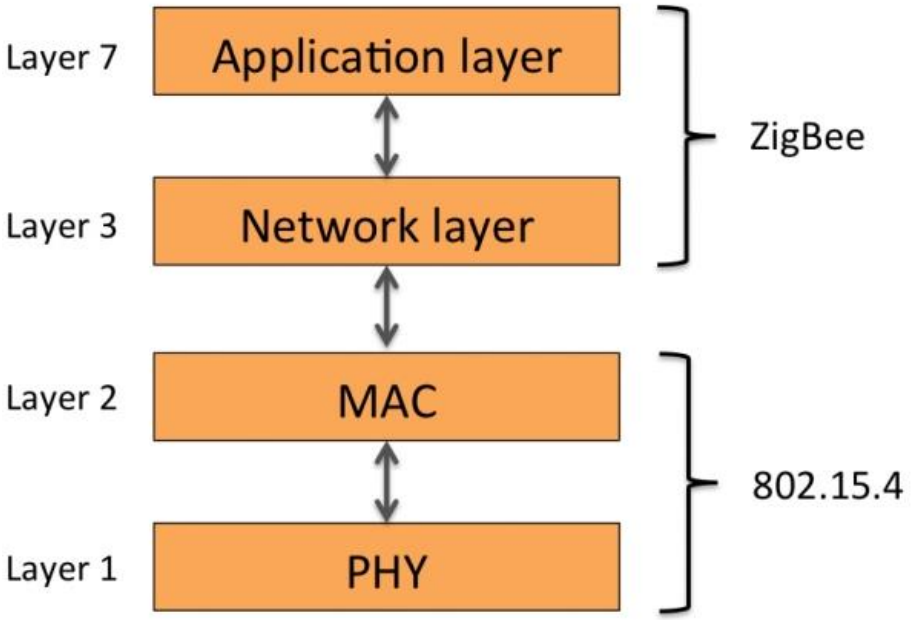


Figura 3. 6: Arquitectura del estándar inalámbrico Zigbee.
Fuente: (Chin et al., 2015)

3.7.2.2. Seguridad y confidencialidad de tecnología inalámbrica Zigbee.

Los niveles de seguridad abarcan las capas de aplicación y de red. Así, en cada capa se garantiza que los intercambios de datos sean seguros. El cifrado de los servicios de confidencialidad e integridad garantiza la autenticidad en las capas de aplicación y de red. De hecho, las comunicaciones están protegidas doblemente en ambas capas por separado, utilizando el estándar AES-CCM.

3.8. Sistemas de detección de amenazas en IoT.

En esta sección, se presenta de forma experimental un análisis de seguridad del sistema PHYSEC. Así pues, se analizan los nodos secundarios de la estructura del ataque. Es decir, las condiciones que deben cumplirse para que el nodo principal sea verdadero. Recientemente, algunos análisis de

seguridad de sistemas procedentes de observaciones correlacionadas están basados en abstracciones de canales de comunicación amplios o en afirmaciones fundamentadas en pruebas experimentales aisladas y, por lo tanto, no están totalmente fundamentadas, no obstante, más adelante se verá.

3.8.1. Implementación de la plataforma de pruebas.

Por medio del protocolo se garantiza que las tres mediciones realizadas conjuntamente se realicen en un tiempo aproximado de 5 ms. De este modo, la tasa de muestreo es 100 Hz. En la figura 3.7 se muestra la forma de realizar las mediciones sincronizadas entre los nodos A y B, y un posible atacante pasivo (C). La medición del canal compartido se ha implementado en la plataforma Raspberry Pi. Se trata de una computadora pequeña y universal, que tiene un sistema operativo basado en Linux y opciones de expansión flexibles.

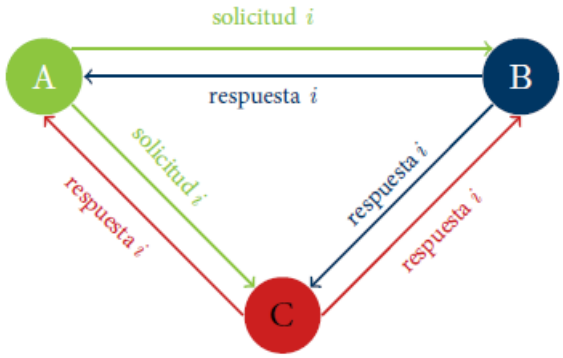


Figura 3. 7: Configuración de las pruebas en los nodos A, B y posible ataque C.
Elaborador por: Autor.

Para ello, se ha equipado el equipo con un adaptador USB inalámbrico TP Link TL-WN722N, además de una batería que permite la movilidad. El nodo A queda instalado en una plataforma rotativa de medición con movimiento circular. La movilidad es necesaria porque, si no, no se produce la reciprocidad de los canales debido a la baja relación reciprocidad/ruido. Por otra parte, la ausencia de movimiento aleatorio, en escenarios realistas, no genera ningún cambio de tendencia.

Tanto el nodo B como el posible atacante “C” tienen una configuración de posicionamiento de antena autónoma. A través de esta configuración, se

evalúan las posibilidades de correlación de un posible ataque a la medición para distancias diferentes entre el nodo B y C. En este caso, la distancia mínima entre el nodo B y C es de 1mm≤d≤300mm.

3.8.2. Diseño estadístico de lecturas aleatorias

La estadística difusa y aleatoria de la fuente representa el único ataque vectorial utilizado. El análisis realizado revela que las mediciones obtenidas en un intervalo de 300 ms presentan aún correlaciones temporales. Además, se pueden emplear otros enfoques que permitan el análisis del error estadístico. Así, por ejemplo, el análisis de las correlaciones temporales I (X; Y) entre la observación X de un nodo autorizado y la observación Y de un intruso representa otros potenciales errores estadísticos.

Por simplificación, en este caso se analizó el error estadístico de las lecturas obtenidas por los sensores mediante análisis espectral. El espectro de magnitudes de las dos configuraciones (escenario estático y escenario con movilidad) se muestran en las figuras 3.8 y 3.9.

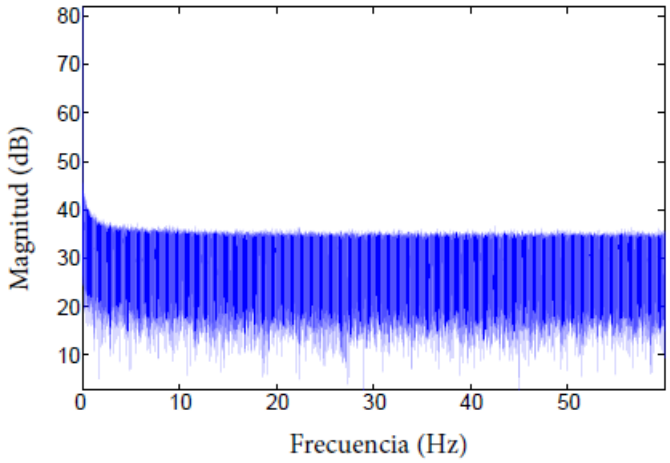


Figura 3. 8: Representación de la magnitud espectral del escenario estático.
Elaborador por: Autor.

Se observa claramente cómo las frecuencias del espectro no se distribuyen uniformemente, mostrando un sesgo hacia las frecuencias bajas. Sin embargo, la cuantificación de este error conlleva la aparición de frecuencias de símbolos que reducen considerablemente la superficie disponible del material clave anterior. En consecuencia, se requiere una

comprobación estadística en línea urgente. Después, en la sección 5.3.7 se aborda cómo este error puede afectar a la seguridad de forma aún más drástica.

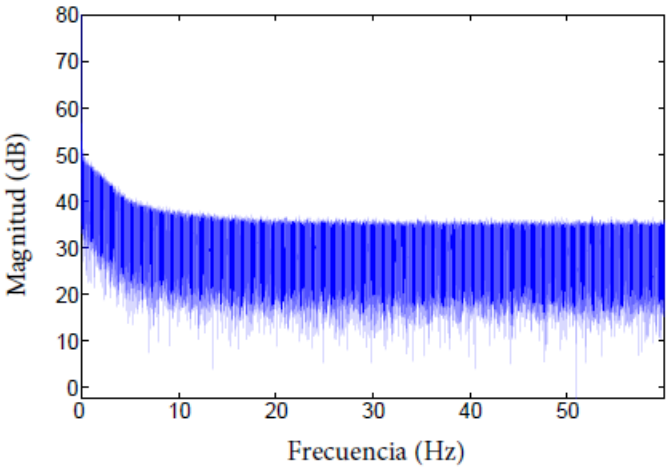


Figura 3. 9: Representación de la magnitud espectral del escenario con movilidad.
Elaborador por: Autor.

3.8.3. Análisis de resultados.

Se ha evaluado un ataque repetitivo mediante la plataforma en movimiento. Se midieron 10000 veces el recorrido a lo largo de todo el trayecto. Un recorrido está representado por aproximadamente 700 valores de indicador de fuerza de señal recibida (RSSI). Los resultados de la correlación entre una observación y las repeticiones resultantes se muestran en la figura 3.10.

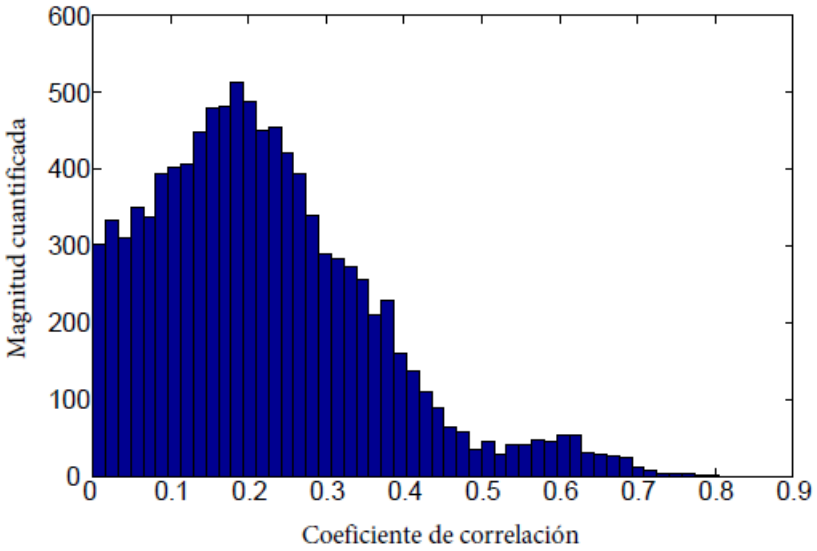


Figura 3. 10: Representación de la magnitud espectral del escenario con movilidad.
Elaborador por: Autor.

Los resultados muestran que la reproducción de las mediciones del canal correlacionadas es posible. El porcentaje de éxito del ataque depende en gran medida del esquema de cuantificación aplicado. Por ejemplo, el mal comportamiento de la BER para correlaciones bajas del esquema de un solo bit conduce a un resultado muy parecido en cuanto al potencial de las claves. Las repeticiones del ataque conducen a una reproducción del 96% del potencial de las claves después de la cuantificación y del 100% después de la recuperación de la información.

Los datos del código pueden ser revelados debido a la información de corrección de errores transmitida públicamente. En este caso, el espía pasivo Eve puede escuchar la comunicación en la red. La distancia del atacante que escucha las comunicaciones del canal es de 100 metros. Con equipamiento especial, por ejemplo, con antenas dirigidas, el ataque actúa inclusive fuera del rango de conexión de las especificaciones de la red.

Conclusiones

1. En la literatura se aprecia un interés cada vez mayor por los enfoques criptográficos incondicionalmente seguros para una gran variedad de sistemas y mecanismos de seguridad en el Internet de las Cosas.

2. El ataque a una red o a un sistema se refiere a cualquier actividad no autorizada o ilícita. Los ataques representan actividades no deseadas obtenidas de forma pasiva o activa en una red. Así, por ejemplo, los llamados "gusanos" y "virus" de Internet suelen propagarse rápidamente por el mundo. El ataque a una red o a un sistema se refiere a cualquier actividad no autorizada o ilícita. Los ataques representan actividades no deseadas obtenidas de forma pasiva o activa en una red. Toda red deberá reconocer y mitigar de forma inmediata los riesgos de los gusanos y los virus.

3. La estructura de ataque presentada aporta información sobre la forma en que los posibles atacantes debilitan los supuestos de seguridad de los dispositivos en el amplio campo del IoT. Además, la estructura de ataque no es completa, puesto que es un problema complicado de encontrar todos los vectores de ataque. Es estrictamente necesario seguir trabajando para aumentar su utilidad.

Recomendaciones

A continuación, se presentan dos recomendaciones para futuros trabajos de investigación:

1. Diseño de un sistema de gestión de una red mediante redes definidas por software basadas en infraestructuras de IoT.

2. Análisis de anomalías mediante Deep Learning para el IoT móvil con aplicaciones en la planificación de la logística inteligente

Bibliografia

Alandí P., A. (2016). *Estudio de la implantación de Internet de las Cosas, en las redes Logísticas de la Cadena de Suministro* [Universidad Politécnica de Valencia]. https://riunet.upv.es/bitstream/handle/10251/70877/TFM%20Antonio%20Alandi%20Pajares%20vFinal_1467729669912151915990933821249 9.pdf?sequence=3

Burhan, M., Rehman, R., Khan, B., & Kim, B.-S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, *18*(9), 2796. https://doi.org/10.3390/s18092796

Capella, J., Campelo, J., Bonastre, A., & Ors, R. (2016). A Reference Model for Monitoring IoT WSN-Based Applications. *Sensors*, *16*(11), 1816. https://doi.org/10.3390/s16111816

Chin, C. S., Atmodihardjo, W., Woo, L. W., & Mesbahi, E. (2015). Remote temperature monitoring device using a multiple patients-coordinator set design approach. *ROBOMECH Journal*, *2*(1), 4. https://doi.org/10.1186/s40648-015-0027-x

Cuzme Rodríguez, F. G. (2015). *El Internet de las cosas y las consideraciones de seguridad* [Tesis de Maestría, Pontificia Universidad Católica del Ecuador]. http://repositorio.puce.edu.ec:80/xmlui/handle/22000/8492

Ebrary, N. (2022). *IoT Reference Architectures*. Ebrary. https://ebrary.net/194544/computer_science/reference_architectures

Hasan, M. (2022). State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. *IoT Analytics*. https://iot-analytics.com/number-connected-iot-devices/

Kar, U. N., & Sanyal, D. K. (2018). An overview of device-to-device communication in cellular networks. *ICT Express*, *4*(4), 203–208. https://doi.org/10.1016/j.icte.2017.08.002

Khanna, A., & Kaur, S. (2019). Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. *Computers and Electronics in Agriculture*, *157*, 218–231. https://doi.org/10.1016/j.compag.2018.12.039

Luo, B., Tang, S., & Sun, Z. (2015). Research of Neighbor Discovery for IPv6 over Low-Power Wireless Personal Area Networks. *Proceedings of the 11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*. 11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Taipei, Taiwan. https://doi.org/10.4108/eai.19-8-2015.2260186

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 336–341. https://doi.org/10.1109/ICITST.2015.7412116

Naoui, S., Elhdhili, M. E., & Saidane, L. A. (2016). Enhancing the security of the IoT LoraWAN architecture. *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, 1–7. https://doi.org/10.1109/PEMWN.2016.7842904

Sosa, E. O., & Godoy, D. A. (2014). Internet del futuro: Desafíos y perspectivas. *Revista de Ciencia y Tecnología*, *21*, 40–46.

Zanella, A. (2021). Smart cities: Potential and challenges. *CIIS Ulima Congreso Internacional de Ingeniería de Sistemas*, 41–61. https://doi.org/10.26439/ciis2018.5490

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Burbano Choez, Edison Xavier** C.C: # 0919762617 autor del Componente práctico del examen complexivo: **Análisis de mecanismos de seguridades en redes inalámbricas mediante IoT**, previo a la obtención del título de **Magister en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 24 de noviembre del 2022

f. _____

Nombre: **Burbano Choez, Edison Xavier**

C.C: 0919762617

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Análisis de mecanismos de seguridades en redes inalámbricas mediante IoT		
AUTOR(ES)	Burbano Choez, Edison Xavier		
REVISOR(ES)/TUTOR(ES)	M. Sc. Córdova Rivadeneira, Luis Silvio; M. Sc. Quezada Calle Edgar / M. Sc. Palacios Meléndez, Edwin Fernando		
INSTITUCIÓN:	**Universidad Católica de Santiago de Guayaquil**		
FACULTAD:	**Sistema de Posgrado**		
PROGRAMA:	**Maestría en Telecomunicaciones**		
TITULO OBTENIDO:	**Magister en Telecomunicaciones**		
FECHA DE PUBLICACIÓN:	24 de noviembre del 2022	**No. DE PÁGINAS:**	40
ÁREAS TEMÁTICAS:	Comunicaciones Inalámbricas, Internet de las Cosas		
PALABRAS CLAVES/ KEYWORDS:	Internet, Comunicaciones, Dispositivos, Redes, Sensores, Seguridad.		

RESUMEN/ABSTRACT:

En la actualidad, todos los dispositivos móviles, independientemente de su tipo y uso, representan una amenaza para la seguridad de los usuarios sobre el Internet de las Cosas (IoT). En efecto, más allá de las normas de seguridad que se deben aplicar en la fase de producción de los dispositivos inteligentes, los cuales alcanzan proporciones muy serias en función de sus ámbitos de uso, resulta indispensable la investigación sobre los medios de prevención de los ataques actuales, que no se detectan, después de la producción. Además, para detectar ataques desconocidos y vigentes se utilizan técnicas de inteligencia artificial como el aprendizaje automático, la lógica difusa o las redes neuronales artificiales, que resulta otro tema que se puede ampliar al presente trabajo de examen complexivo. El objetivo del presente trabajo de grado requiere la investigación de la Internet de las Cosas, y sus aplicaciones en las comunicaciones inalámbricas, como el caso de las redes de sensores inalámbricos (WSN); con el fin de garantizar la seguridad de los dispositivos inteligentes usando el IoT.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593997372282	E-mail: ediburbano@hotmaiñ.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Manuel Romero Paz	
	Teléfono: 0994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	