Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología - ESIT

Máster Universitario en Industria 4.0

Domótica y Privacidad: Navegando entre la Comodidad Tecnológica y la Seguridad de los Datos

Trabajo fin de estudio presentado por:	Yurian Inés Corro López
Tipo de trabajo:	Investigación y desarrollos teóricos
Director:	Deivis Eduard Ramirez Martinez
Fecha:	28/02/2024

Resumen

El trabajo presenta aspectos críticos de seguridad y privacidad en sistemas de domótica residencial basados en IoT, poniendo especial énfasis en los protocolos inalámbricos Z-Wave, ZigBee y Wi-Fi. Mediante una revisión de la literatura científica y técnica, y siguiendo el método PRISMA, se realiza una evaluación detallada de las vulnerabilidades y los retos asociados a la seguridad de estos protocolos. Además, se identifican y discuten las tendencias actuales y las preocupaciones emergentes en este campo. El estudio concluye con una serie de recomendaciones prácticas y fundamentadas, orientadas a mejorar la protección de datos y la privacidad en los sistemas de domótica. Estas recomendaciones están dirigidas a informar, con el objetivo de fomentar un entorno de hogar inteligente más seguro y confiable.

Palabras clave: domótica, Zigbee, Z-Wave, Wi-Fi, ciberseguridad

Abstract

The work presents critical aspects of security and privacy in IoT-based home automation systems, with a particular emphasis on the Z-Wave, ZigBee, and Wi-Fi wireless protocols. Through a review of scientific and technical literature, following the PRISMA method, a detailed assessment of vulnerabilities and challenges associated with the security of these protocols is conducted. Additionally, current trends and emerging concerns in this field are identified and discussed. The study concludes with a series of practical and evidence-based recommendations aimed at improving data protection and privacy in home automation systems. These recommendations are intended to inform, with the goal of fostering a safer and more reliable smart home environment.

Keywords: Home Automation, Zigbee, Z-Wave, Wi-Fi, cybersecurity

Índice de Contenidos

Índice de figuras

Índice de tablas

1. Introducción

Un informe realizado por Mordor Intelligence (2023) revela que el mercado de hogares inteligentes está proyectado para experimentar un crecimiento significativo, estimándose su valor en 120.10 mil millones de USD para 2024, con expectativas de alcanzar los 370.95 mil millones de USD para 2029. Este crecimiento, a una tasa compuesta anual del 25.30% durante el período de pronóstico del 2024 al 2029, refleja una tendencia hacia la redefinición de los espacios residenciales en respuesta a la "nueva normalidad" impuesta por la pandemia de COVID-19. La demanda de rediseño y la inclusión de nuevas comodidades enfocadas en la eficiencia, la innovación y el bienestar subrayan un cambio de paradigma en la concepción de los espacios de vida residenciales.

Los sistemas de hogares inteligentes, en el contexto de la seguridad y la automatización, se distinguen por su capacidad para integrar soluciones de monitoreo, control y automatización a través de interfaces de usuario avanzadas, como aplicaciones móviles y portales web. Este enfoque en la conectividad y la gestión inteligente está impulsando la adopción de tecnologías inalámbricas innovadoras, como sistemas de control de acceso, entretenimiento, y reguladores energéticos, marcando un avance significativo en la evolución del mercado de la domótica.

El rápido crecimiento del mercado de hogares inteligentes ha creado una brecha entre el conocimiento de los usuarios sobre las tecnologías emergentes y su implementación práctica, especialmente, en lo que respecta a la ciberseguridad. A medida que las tecnologías evolucionan, se hace cada vez más importante proteger los sistemas domóticos de posibles amenazas cibernéticas. La integración de dispositivos inteligentes en los hogares aumenta la conveniencia y la eficiencia, pero también introduce vulnerabilidades de seguridad, tales como accesos no autorizados y la exposición de datos personales.

La adopción de tecnologías inalámbricas avanzadas y el incremento en la conectividad de dispositivos domóticos requieren una gestión cuidadosa de la seguridad. Por ende, es vital que tanto los fabricantes como los usuarios estén informados sobre las prácticas de ciberseguridad

y adopten medidas adecuadas para protegerse; informar y educar a los usuarios finales sobre ciberseguridad es clave para mitigar los riesgos asociados con el uso de hogares inteligentes.

Dentro de esta perspectiva, los protocolos de comunicación juegan un papel crucial en la ciberseguridad. La selección y configuración adecuadas de protocolos de comunicación seguros son indispensables para reducir las vulnerabilidades. Protocolos como Zigbee, Z-Wave y Wi-Fi, cada uno con características de seguridad distintivas, deben ser evaluados y elegidos con cautela para cada aplicación en un hogar inteligente específico. No se puede afirmar la existencia de una solución perfecta para un hogar inteligente, sin embargo, sí se pueden tomar las medidas necesarias para garantizar la privacidad y seguridad de los datos del usuario.

1.1. Motivación

La domótica, también conocida como hogar inteligente, hogar del futuro, entre otros integra técnicas de electrónica, informática y automatización industrial. Definida como la ciencia y tecnología que respalda la automatización y gestión inteligente de hogares y edificios, ha experimentado un crecimiento exponencial en las últimas décadas. Este avance ha sido impulsado por la búsqueda constante de mejorar la calidad de vida, aumentar la seguridad en el hogar y optimizar el consumo energético. (Flórez de la Colina, 2004)

Facilitando la integración de una amplia gama de sistemas y dispositivos, que van desde la iluminación y la climatización hasta los sistemas de seguridad y entretenimiento, estas soluciones se ven favorecidas por la conectividad a Internet. Esto permite a los usuarios controlar de manera remota y monitorear en tiempo real los dispositivos conectados.

En el contexto panameño, esta evolución señala claramente cómo la tecnología inteligente está transformando no solo los hogares individuales, sino también el paisaje arquitectónico y urbano del país. Desde mi perspectiva como testigo de esta transformación, se puede afirmar que la domótica desempeña un papel crucial en la configuración de un futuro más conectado y automatizado en Panamá. Este avance no es solo una tendencia pasajera, sino una transformación profunda en el mercado inmobiliario y en las expectativas de una nueva generación de compradores. La integración de soluciones domóticas en las nuevas

construcciones se está convirtiendo rápidamente en un estándar, más que en un lujo, reflejando un cambio en el estilo de vida y en la forma en que los residentes interactúan con sus hogares.

No obstante, con la creciente adopción de la domótica en hogares y edificaciones, también surgen nuevos desafíos en términos de ciberseguridad. La rápida entrada de estos sistemas al mercado a menudo descuida la evaluación de los riesgos potenciales asociados con la automatización de procesos. Este descuido ha dado lugar a vulnerabilidades de seguridad que podrían ser explotadas por ciberdelincuentes, comprometiendo así la privacidad y la seguridad de los usuarios.

Por lo tanto, uno de los principales desafíos en el campo de la domótica es abordar adecuadamente la seguridad desde el diseño y la implementación de los sistemas. La protección de datos, la autenticación segura y la actualización de software son aspectos críticos que deben ser considerados para garantizar que la automatización inteligente mejore verdaderamente la calidad de vida de las personas sin comprometer su seguridad.

Según un análisis del Digital Market Outlook de Statista (2022) revela que, en 2020, el gasto global en productos de domótica alcanzó los 78.800 millones de dólares. Esta cifra se espera que experimente un crecimiento sustancial, alcanzando los 207.800 millones de dólares para el año 2026, reflejando así una tendencia ascendente en la inversión en tecnología para el hogar inteligente. Sin embargo, a medida que la adopción de productos domóticos continúa expandiéndose, también lo hacen las preocupaciones por estos dispositivos.

Este estudio se centra en uno de los aspectos más importantes que se han descuidado en un mundo altamente digitalizado: ¿cuál es el grado de seguridad de los datos y cuál es el nivel efectivo de privacidad que se puede mantener en un entorno digitalmente interconectado? Este trabajo busca evaluar el panorama actual de seguridad y privacidad en el ámbito de la domótica, examinando las vulnerabilidades que presentan los protocolos de comunicación inalámbricos: Zigbee, Z-Wave y Wi-Fi. Así, los hallazgos servirán para orientar el desarrollo de mejores prácticas y regulaciones para garantizar que la privacidad y la seguridad sean una prioridad en este campo en rápida evolución.

1.2. Planteamiento del Trabajo

La domótica se ha vuelto más accesible y económica, con dispositivos como asistentes de voz, bombillas inteligentes y electrodomésticos conectados que se han popularizado, lo que ha impulsado su adopción en los hogares. Esta tendencia ha dado lugar a la creación de nuevos protocolos de comunicación inalámbricos optimizados para el Internet de las cosas (IoT), así como a la evolución de los protocolos inalámbricos existentes. Estos avances permiten una mayor interconexión y automatización, y abren nuevas posibilidades para la gestión y el monitoreo eficiente de los entornos domésticos.

Sin embargo, la rápida velocidad de estas mejoras tecnológicas, combinada con la creciente demanda de interoperabilidad entre dispositivos, ha llevado a menudo a que la ciberseguridad no sea priorizada adecuadamente. Este descuido en la seguridad deja vulnerabilidades sin resolver, exponiendo los sistemas domóticos a riesgos significativos de ataques cibernéticos y comprometiendo la privacidad y seguridad de los datos. Los sistemas domóticos recopilan y procesan una amplia gama de datos personales, desde preferencias de iluminación y consumo energético hasta patrones de actividad y presencia en el hogar.

La seguridad de la información transmitida a través de estos protocolos es fundamental para proteger la privacidad de los usuarios y prevenir el acceso no autorizado o la manipulación de los dispositivos domóticos. Los riesgos asociados incluyen vulnerabilidades cibernéticas que podrían permitir a los hackers interceptar o alterar datos, así como la posibilidad de que terceros realicen un seguimiento o recopilación indebida de información personal sin consentimiento.

Este estudio se centra en el análisis de la seguridad y privacidad de datos en los protocolos de comunicación inalámbricos Z-Wave, ZigBee y Wi-Fi en el contexto residencial de la domótica. Se propone identificar y documentar las vulnerabilidades específicas de estos protocolos, evaluar las estrategias actuales de protección de datos y privacidad implementadas, y proponer recomendaciones para mejorar la seguridad y protección de la privacidad en los hogares automatizados. A través de este análisis, se busca contribuir al desarrollo de sistemas

domóticos más seguros y confiables que garanticen la protección de la información personal de los usuarios.

1.3. Estructura del Trabajo

Este trabajo se estructura en varias secciones clave, destinadas a abordar de manera exhaustiva los aspectos de seguridad y privacidad en los sistemas de domótica basados en IoT, centrándose en los protocolos inalámbricos Z-Wave, ZigBee y Wi-Fi.

En la introducción, se establecerá el contexto y la relevancia del estudio, presentando la domótica y su evolución, con un enfoque particular en la importancia de los protocolos inalámbricos y los desafíos de seguridad asociados.

Luego, en el estado del arte, se proporcionará una base sobre los conceptos clave de la domótica y los protocolos de comunicación inalámbricos específicos. Se explorarán las tendencias actuales, la importancia de la interoperabilidad y cómo estas influyen en la ciberseguridad.

En la metodología, se describirá el enfoque metodológico del estudio, siguiendo las pautas de PRISMA para la revisión sistemática. Se explicarán los criterios de selección de estudios, las estrategias de búsqueda de literatura y los métodos de análisis de datos. Tras la revisión de los artículos, se presentarán los hallazgos obtenidos, incluyendo una evaluación de las vulnerabilidades y estrategias de protección en los protocolos estudiados.

Posteriormente, en la discusión, se analizarán los resultados en el contexto del panorama actual de la domótica, discutiendo las implicaciones prácticas y teóricas de los hallazgos. En las conclusiones y recomendaciones, se ofrecerá una síntesis de las principales conclusiones, se señalarán las limitaciones del estudio y se propondrán recomendaciones para futuras investigaciones, así como para el desarrollo y diseño de sistemas domóticos más seguros y respetuosos de la privacidad.

Finalmente, en las referencias se incluirá una lista de todas las fuentes bibliográficas utilizadas en el estudio. Esta estructura está diseñada para proporcionar un análisis completo y sistemático de los aspectos críticos de seguridad y privacidad en la domótica, asegurando un enfoque integral y bien fundamentado en la investigación.

2. Estado del Arte

La domótica, desde sus inicios, ha buscado la integración de tecnologías en el hogar con el propósito principal de mejorar la calidad de vida de los habitantes. La domótica moderna ha trascendido la simple automatización de tareas en el hogar y con el auge del Internet de las Cosas (IoT), la domótica ha incorporado una amplia gama de dispositivos conectados que permiten una interacción más dinámica y personalizada con el hogar. Estos dispositivos, equipados con sensores y actuadores, facilitan la recopilación de datos y la comunicación en tiempo real, permitiendo a los usuarios tener un control más preciso y adaptado a sus necesidades (Domínguez y Vacas, 2006).

En el ámbito de la domótica, la conexión de dispositivos dentro de la red del hogar se realiza tanto mediante tecnologías cableadas, basadas en el estándar IEEE 802.3 (Ethernet), como inalámbricas. Aunque las tecnologías cableadas ofrecen una conexión estable, su implementación puede resultar costosa y compleja debido a la necesidad de cables individuales para cada dispositivo. Por otro lado, las tecnologías inalámbricas ofrecen una alternativa más flexible y económica, especialmente adecuada para viviendas ya construidas, al evitar el uso de cables y permitir una instalación más sencilla. Estas tecnologías inalámbricas, que incluyen protocolos como Wi-Fi, Bluetooth, Z-Wave y ZigBee, están en constante evolución, mejorando en términos de costo, velocidad y calidad, aunque aún enfrentan desafíos en cuanto a la estabilidad de la conexión y la eficiencia en la transmisión de datos.

Para la creación de redes inalámbricas en Sistemas de Hogares Inteligentes (SHS por sus siglas en inglés), es necesario seleccionar un protocolo de comunicación que brinde las funciones necesarias y asegure el funcionamiento confiable de los componentes inteligentes, como dispositivos, sensores y actuadores. Los análisis comparativos muestran que, aunque los protocolos como Z-Wave y 6LoWPAN son más eficientes en la transmisión de datos, tienen un costo relativamente alto. Mientras opciones más económicas como Bluetooth y Wi-Fi son frecuentemente elegidas para la implementación de SHS, a pesar de no ser protocolos inicialmente diseñados para la domótica (Domínguez y Vacas, 2006).

Por otro lado, la elección de la topología de red adecuada (Punto a Punto, Estrella, Árbol, Malla) es un paso importante, ya que ciertos protocolos funcionan mejor dentro de topologías específicas, influyendo directamente en la seguridad y fiabilidad del sistema.

En el mercado actual, existen numerosas soluciones listas para usar basadas en tecnologías inalámbricas; ejemplos de estas soluciones incluyen Xiaomi Smart Home (ZigBee), Apple HomeKit (Protocolo de Accesorios HomeKit), Orvibo (ZigBee), Fibaro (Z-Wave), Broadlink (QUIC), INELS (ZigBee), Connect Home (Z-Wave), Aeotec (Z-Wave), lifesmart (RF433 GFSK), Ferguson Smart Home (ZigBee, Wi-Fi), entre otros. Los fabricantes prefieren protocolos como Z-Wave y ZigBee por su capacidad para implementar topologías de red en malla, satisfaciendo las preferencias de los usuarios finales en términos de estabilidad, fiabilidad y seguridad. Estos protocolos utilizan módulos de radiofrecuencia de bajo consumo y tamaño reducido, integrados en la electrónica de consumo y diversos dispositivos.

Sin embargo, el protocolo Wi-Fi, ampliamente utilizado en aplicaciones domésticas, destaca por su avanzada tecnología y el segmento de soluciones de bajo costo para su implementación, aunque se debe considerar el consumo significativo de energía de algunos módulos, lo cual puede contradecir los requisitos de autonomía prolongada en SHS (Tulenkov et al., 2018). Esto posiciona a Zigbee, Z-Wave y Wi-Fi entre los protocolos de comunicación inalámbrica más utilizados actualmente en la domótica residencial.

2.1. Partes de un Hogar Inteligente (Domótica)

Aunque el enfoque principal de este trabajo se centra en los protocolos de comunicación en la domótica, es importante primeramente mencionar las partes que componen un sistema domótico en términos generales como se muestra en la figura 1; cada sistema domótico es único y difiere en su composición. Estos sistemas integran una variedad de componentes que trabajan en conjunto para automatizar y mejorar las funciones del hogar. A continuación, se presentan las partes esenciales de un sistema domótico explicados por Domínguez y Vacas (2006):

- Sensores y Actuadores: Los sensores monitorean cambios ambientales como movimiento, temperatura y luz, mientras que los actuadores realizan acciones físicas, como ajustar la temperatura o manejar cerraduras inteligentes. Ambos son fundamentales para la automatización y respuesta inteligente del sistema.
- Controladores e Interfaces de Usuario: Los controladores, actuan como el cerebro del sistema, procesan datos de los sensores para operar actuadores. Los usuarios interactúan con el sistema a través de interfaces, que pueden ser aplicaciones móviles, paneles de control, asistentes de voz o controles remotos, permitiendo un control y la fácil personalización del hogar inteligente.
- Software y Sistemas de Seguridad: El software coordina la automatización, integrando dispositivos para gestionar energía, seguridad y confort. Los sistemas de seguridad, como cámaras y alarmas, aunque no obligatorios, añaden una capa de protección al hogar inteligente. Además, se utilizan plataformas de integración cuando existen múltiples subsistemas.
- Red de Comunicación: Este componente se utiliza para conectar todos los elementos del sistema domótico, permitiendo la transmisión de datos entre sensores, controladores y actuadores. La investigación se centrará en este aspecto, analizando los protocolos Wi-Fi, Zigbee y Z-Wave.

Figura 1. *Partes de un sistema domótico*

Fuente: Freepik

2.2. Conectividad en la Domótica

La evolución de la domótica, en términos de conectividad y comunicaciones, refleja su adaptación a las necesidades cambiantes de los usuarios. Los sistemas domóticos modernos emplean una variedad de tecnologías y protocolos para garantizar una gestión eficiente y flexible de los dispositivos del hogar. La implementación de configuraciones híbridas que combinan conectividad Wi-Fi con puentes, y el uso de tecnologías como Radiofrecuencia y Bluetooth, junto con protocolos como Z-wave o Zigbee, evidencian esta evolución (Vida Domótica, 2023).

En términos sencillos, descrito por Vida Domótica (2023) un protocolo de comunicación «es un conjunto de reglas que establecen cómo los dispositivos de la domótica deben comunicarse entre sí. Los protocolos son esenciales para garantizar que los distintos componentes de la domótica se comuniquen de forma eficiente, segura y rápida».

2.2.1. Protocolos de Comunicación Inalámbrica en la Domótica

Las redes cableadas ofrecen una mayor seguridad en comparación con las redes inalámbricas, pero están limitadas por costo y distancia. Mientras que las redes cableadas envían datos directamente entre dos puntos, A y B, a través de un cable físico, las redes inalámbricas transmiten datos en todas direcciones, potencialmente accesibles para cualquier dispositivo dentro de su alcance. Aunque se pueden implementar medidas de seguridad en ambos tipos de redes, como restringir el acceso físico y utilizar cortafuegos, las redes inalámbricas siguen siendo más vulnerables a la interceptación de datos. Por lo tanto, garantizar la seguridad en las redes inalámbricas requiere un enfoque más riguroso y específico. (Salazar, 2016)

La amplia selección de protocolos de comunicación, como Z-Wave, ZigBee, ModBus, KNX, BLE, LoRaWAN y BACnet, subraya la complejidad y la especificidad técnica de los sistemas domóticos actuales. La creciente diversidad y amplitud de opciones en sistemas de hogar inteligente presenta un desafío significativo en términos de gestión de seguridad. Esta variedad, aunque ofrece flexibilidad y personalización, complica la tarea de asegurar de manera efectiva los hogares inteligentes, ya que cada sistema y dispositivo puede tener

requisitos de seguridad únicos y específicos (Ojeda-Crespo, Cabrera-Mejía, 2020; Vida Domótica, 2023).

A continuación, se describen los protocolos de comunicación inalámbricos más utilizados extraídos de la "Revisión de Tecnologías de Comunicación para Aplicaciones en Hogares/Edificios Inteligentes" por Kuzlu, Pipattanasomporn y Rahman (2015):

- ✓ Wi-Fi: Basada en estándares IEEE 802.11, ofrece velocidades de hasta 300 Mbps y opera en varias bandas de frecuencia. Proporciona cobertura hasta 100 metros y comunicaciones seguras y fiables, aunque es más costosa y consume más energía que otras tecnologías.
- ✓ ZigBee: Estándar para redes personales inalámbricas (WPAN), con tasas de datos más bajas pero larga vida útil de la batería. Ofrece cobertura hasta 100 metros y puede extenderse a 1,000 metros en configuraciones de malla.
- ✓ Z-Wave: Tecnología de comunicación inalámbrica de bajo consumo diseñada para aplicaciones de control remoto en entornos residenciales. Soporta tasas de datos de hasta 40 kbps y cobertura hasta 30 metros, con redes en malla que mejoran la confiabilidad.
- ✓ Bluetooth: Estándar IEEE 802.15.1 para redes personales inalámbricas, con velocidades de hasta 721 kbps y alcance de hasta 100 metros. Utilizado principalmente en dispositivos personales portátiles.
- ✓ 6LoWPAN: Tecnología de red que permite transportar eficientemente paquetes IPv6 en marcos de capa de enlace pequeños, como los definidos por IEEE 802.15.4. Ideal para aplicaciones de automatización del hogar y sensores.
- ✓ IEEE 802.15.3a: Ultra-Wideband que proporciona tasas de datos de hasta 1.3 Gbps, pero con un rango corto de 10 metros.
- ✓ EnOcean: Tecnología de recolección de energía que permite interruptores y sensores inalámbricos y sin batería. Ofrece cobertura de hasta 30 metros en interiores y 300 metros en exteriores.
- ✓ Wave2M: Diseñado para transmisiones de baja potencia y largo alcance de datos y comunicaciones de bajo tráfico. Cubre hasta 1000 metros y opera en bandas de frecuencia sin licencia.

✓ RFID: Sistema de identificación por radiofrecuencia bidireccional con etiquetas y lectores. Operando en un amplio rango de frecuencias, ofrece una distancia de detección de hasta 200 metros.

✓ ONE-NET: Estándar de código abierto para redes inalámbricas de bajo costo y bajo consumo. Opera en las bandas de frecuencia UHF ISM y ofrece cobertura de hasta 500 metros en áreas abiertas y 100 metros en interiores.

La tabla 1 ofrece una comparación detallada de los valores de frecuencia, velocidad y rango aproximado, según lo presentado por Tulenkov et al. (2018). Es importante señalar que estos valores pueden mostrar variaciones sutiles entre distintos fabricantes, lo cual puede atribuirse a las diferentes especificaciones y estándares empleados por cada uno. Esta discrepancia en los datos subraya la importancia de considerar múltiples fuentes y realizar análisis comparativos exhaustivos al evaluar tecnologías de comunicación para aplicaciones en hogares inteligentes o edificios conectados.

Tabla 1: ***Comparación de los protocolos de comunicación inalámbricos más comunes***

Tecnología	Bluetooth	Zigbee	Z-Wave	6LoWPAN	Wi-Fi	RF
Frecuencia (GHz)	2.4	2.4, 0.915, 0.868	máx. 1.0	1.0, 2.4	2.4, 5.0	0.433, 0.315
Velocidad (Mbps)	máx. 24	máx. 0.25	máx. 0.1	máx. 0.250	máx. 300	máx. 0.01
Rango aprox. (m)	máx. 100	máx. 100	30	800	máx. 100	50

Fuente: The Features of Wireless Technologies por Tulenkov et al., 2018

La elección de enfocarse en ZigBee, Z-Wave y Wi-Fi en este trabajo responde a su amplia adopción en la domótica residencial y su relevancia en el contexto contemporáneo de la automatización del hogar. Estos protocolos representan un equilibrio entre eficiencia energética, facilidad de uso, interoperabilidad y rendimiento, lo que los hace particularmente adecuados para aplicaciones residenciales donde estos factores son importantes.

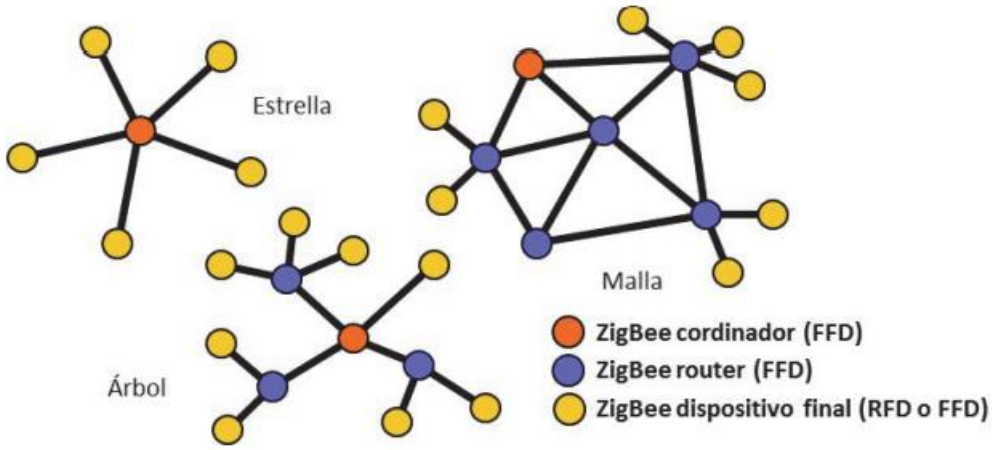
2.3. Protocolo de Comunicación Zigbee

Expandiendo en el punto anterior, Zigbee es un protocolo de comunicación inalámbrica de alta eficiencia energética, diseñado principalmente para aplicaciones de automatización del hogar y la empresa, así como para el Internet de las Cosas (IoT).

La tecnología ZigBee se encuentra principalmente integrada en productos que operan con acciones simples, como sensores de movimiento, detectores de temperatura, enchufes eléctricos, entre otros. ZigBee está diseñado para permitir la transferencia de paquetes de solicitud y respuesta de red de forma sencilla, con el fin de lograr una lectura de datos o acción de comando simple en un dispositivo ZigBee. Por lo tanto, esta tecnología tiene una presencia significativa en electrodomésticos para el hogar, desde bombillas de luz controladas de forma inalámbrica hasta cerraduras de puertas.

Es popular por su bajo consumo de energía y baja velocidad de datos, ya que se utiliza principalmente para la comunicación bidireccional entre sensores y sistemas de control. ZigBee tiene un rango de cobertura de comunicación similar al de Bluetooth y Wi-Fi, cubriendo hasta 100 metros en interiores. La diferencia principal es que Bluetooth y Wi-Fi son estándares de comunicación de alta velocidad que admiten la transferencia de estructuras complejas. Como resultado, es más adecuado para dispositivos que requieren baja potencia o larga vida útil de la batería implementar la tecnología de red ZigBee. (HKCERT y HKPC, 2020, p. 6)

Figura 2: *Topologías de comunicación para Zigbee*



Fuente: Redes Inalámbricas – Salazar, 2016

La red ZigBee permite la conexión de varias topologías red estrella, la red de árbol de clúster y la red en malla demostrado en la figura 2. La topología de Red Estrella es la más simple, involucrando solo un Coordinador ZigBee y un Dispositivo Final ZigBee. El Coordinador ZigBee actúa como el dispositivo central que inicia y gestiona los dispositivos dentro de la red. Esta topología se utiliza comúnmente en aplicaciones de Automatización del Hogar, donde la cobertura entre el Coordinador ZigBee y el Dispositivo Final ZigBee es suficiente para el entorno doméstico.

La topología de Red de Árbol de Clúster despliega Ruteadores ZigBee adicionales entre el Coordinador ZigBee y el Dispositivo Final ZigBee. Con la ayuda de los Ruteadores ZigBee, la cobertura puede extenderse aún más. Por ejemplo, cuando el Coordinador ZigBee y el Dispositivo Final ZigBee están físicamente ubicados a más de 100 metros, aún pueden comunicarse a través de los Ruteadores ZigBee. Esta topología se utiliza comúnmente en aplicaciones de Automatización Industrial, donde se despliegan numerosos Dispositivos Finales ZigBee en múltiples entornos de taller industrial más allá de las restricciones de distancia.

La topología de Red en Malla despliega múltiples Ruteadores ZigBee entre el Coordinador ZigBee y el Dispositivo Final ZigBee. Cada Ruteador ZigBee puede comunicarse entre sí, lo que permite extender aún más la cobertura. Por ejemplo, cuando el Coordinador ZigBee y el Dispositivo Final ZigBee están físicamente situados más allá de los 100 metros, aún pueden comunicarse al retransmitir a través de varios Ruteadores ZigBee. Esta topología se utiliza comúnmente en aplicaciones de Red Inteligente debido a la gran cantidad de Dispositivos Finales ZigBee que pueden desplegarse en múltiples regiones de la ciudad, permitiendo una comunicación en una amplia área. (HKCERT y HKPC, 2020, p. 7)

2.3.1. Origen

Zigbee fue desarrollado por el consorcio Zigbee Alliance, fundado en 2002. Este consorcio incluye empresas líderes en tecnología como Philips, Honeywell, Siemens, y Texas Instruments, entre otras. (HKCERT y HKPC, 2020, p. 8)

El objetivo principal de Zigbee era crear un estándar global para soluciones inalámbricas eficientes en energía, confiables y de bajo costo, adecuadas para controlar y monitorear aplicaciones donde el uso de Wi-Fi y Bluetooth no era práctico debido a su mayor consumo de energía. (Zohourian et al., 2023)

2.3.2. Características Técnicas

Zigbee se basa en el estándar IEEE 802.15.4 para redes inalámbricas de área personal (WPAN). Opera principalmente en bandas de frecuencia de 2.4 GHz, aunque también puede funcionar en 868 MHz en Europa y 915 MHz en América del Norte y Australia.

Una de las características más destacadas de Zigbee es su bajo consumo de energía, lo que lo hace ideal para dispositivos alimentados por batería.

Además, Zigbee utiliza una topología de red de malla, lo que permite que cada dispositivo se comunique con otros dispositivos cercanos, creando múltiples caminos para la transmisión de datos y aumentando la fiabilidad y el alcance de la red. A pesar de los esfuerzos por estandarizar, la interoperabilidad entre dispositivos de diferentes fabricantes sigue siendo un desafío en el ecosistema Zigbee. (Zohourian et al., 2023)

2.3.3. Adopción y Aplicaciones

Las tecnologías ZigBee han sido ampliamente utilizadas en la automatización del hogar, la automatización industrial, el monitoreo de redes inteligentes, entre otros. Se utilizan con diversos propósitos como la detección, monitoreo, seguimiento y etiquetado de objetos, que son medios para recopilar datos. Para facilitar la descripción del estudio de seguridad de ZigBee en diferentes aplicaciones, HKCERT y HKPC (2020) han categorizado los casos de uso de aplicación de la siguiente manera:

Sensor para Análisis de Datos: Se puede desplegar varios sensores en redes ZigBee para recopilar parámetros ambientales, como temperatura, humedad, presión y humedad, entre otros. Dentro de los casos de uso en la automatización del hogar, generalmente se proporciona un portal web central para que el consumidor monitoree la temperatura y humedad en diferentes áreas del entorno del Hogar Inteligente.

Sensor para Decisión y Control Automatizado: Un ejemplo se puede encontrar en la automatización del hogar donde el sensor de temperatura ZigBee obtiene la temperatura ambiente en tiempo real para llevar a cabo el control automatizado del aire acondicionado en el área del hogar.

Relé de Electricidad y Control de Conmutación: Se pueden encontrar ejemplos en electrodomésticos para el hogar, como sistemas de control de iluminación para encender o apagar las luces.

Control Mecánico Directo: Algunos dispositivos ZigBee se utilizan para control mecánico directo, como cerraduras de puertas en aplicaciones de automatización del hogar. Dado que los paquetes de red de ZigBee están destinados a la simplicidad, se realizará una sola acción dentro de este campo, como realizar acciones de apertura y cierre de una cerradura de puerta ZigBee (p. 8 – 9).

2.3.4. Expansión y Estándares

Lanzado en 2016, Zigbee 3.0 unificó los perfiles de aplicación anteriores de Zigbee en un solo estándar, facilitando la compatibilidad y la interoperabilidad entre diferentes dispositivos y aplicaciones. Por ende, Zigbee continúa siendo un jugador clave en el creciente mercado de IoT, especialmente en aplicaciones que requieren redes de malla y bajo consumo de energía. La Zigbee Alliance sigue colaborando con otras organizaciones y consorcios para mejorar la interoperabilidad y la adopción de Zigbee en un espectro más amplio de aplicaciones. (Zohourian et al., 2023)

2.4. Protocolo de comunicación Z-Wave

Como fue mencionado anteriormente el trabajo se enfoca en tres protocolos específicos, incluyendo Z-Wave; es un protocolo de comunicación inalámbrica diseñado específicamente para la automatización del hogar.

2.4.1. Origen

El protocolo Z-Wave fue desarrollado por la empresa danesa Zensys en el año 2001. El protocolo fue diseñado como una solución inalámbrica para la automatización del hogar, enfocándose en la confiabilidad y el bajo consumo de energía.

El objetivo de Z-Wave era proporcionar una tecnología de comunicación inalámbrica que fuera más eficiente y menos costosa que las soluciones existentes, como Wi-Fi y Bluetooth, para aplicaciones de automatización del hogar. (Kim et al. 2020)

2.4.2. Características Técnicas

El protocolo Z-Wave utiliza una banda de frecuencia de radio de baja potencia (alrededor de 900 MHz, variando según la región geográfica) y es conocido por su bajo consumo de energía y su operación confiable a larga distancia. Al igual que Zigbee, Z-Wave utiliza una topología de red de malla, lo que permite que los dispositivos se comuniquen entre sí y extiendan el alcance de la red. (Kim et al. 2020)

2.4.3. Adopción y Aplicaciones

Z-Wave se ha convertido en uno de los estándares líderes en el mercado de la domótica, utilizado en dispositivos como termostatos, cerraduras, sensores y sistemas de iluminación. Además, existe un amplio ecosistema de dispositivos compatibles con Z-Wave, lo que permite a los usuarios una gran flexibilidad y opciones para configurar sus sistemas de hogar inteligente. (Kim et al. 2020)

2.4.4. Expansión y Estándares

Los dispositivos que utilizan Z-Wave deben pasar por un proceso de certificación, lo que garantiza un alto nivel de interoperabilidad y calidad. Aunque la certificación Z-Wave ayuda a garantizar la interoperabilidad, la integración con sistemas que utilizan otros protocolos puede ser un desafío.

Por otro lado, en 2016, Sigma Designs, el propietario de la tecnología Z-Wave, fue adquirido por Silicon Labs, una empresa que también posee tecnologías relacionadas con Zigbee. Esto podría llevar a una mayor integración y colaboración en el futuro. (Kambourakis et al. 2020)

2.5. Protocolo de comunicación Wi-Fi

Por último, el protocolo de comunicación Wi-Fi, aunque es un protocolo de comunicación inalámbrica ampliamente conocido y utilizado en muchos contextos, también juega un papel importante en el ámbito de la domótica.

2.5.1. Origen

El protocolo Wi-Fi, basado en los estándares IEEE 802.11, fue desarrollado en la década de 1990. Originalmente diseñado para redes de computadoras, rápidamente se expandió a una amplia gama de dispositivos y aplicaciones.

Con el auge del Internet de las Cosas (IoT) y la creciente demanda de hogares inteligentes, Wi-Fi ha encontrado un lugar significativo en la domótica, aprovechando su amplia disponibilidad y facilidad de conexión con Internet (Cabrera y Pérez, 2019).

2.5.2. Aplicaciones en Domótica

La red Wi-Fi es ideal para dispositivos de domótica que requieren transferencia de grandes cantidades de datos, como cámaras de seguridad, altavoces inteligentes y sistemas de entretenimiento. La mayoría de los dispositivos modernos de domótica son compatibles con Wi-Fi, lo que facilita la creación de un ecosistema de hogar inteligente integrado y accesible.

La alta familiaridad de los usuarios con Wi-Fi y la facilidad de configuración hacen que sea una opción popular para la domótica, especialmente para aquellos que buscan una solución sencilla y directa (Cabrera y Pérez, 2019).

2.5.3. Desafíos y Consideraciones

A pesar de su conveniencia, Wi-Fi puede ser susceptible a vulnerabilidades de seguridad, lo que es una preocupación particular en la domótica, donde la seguridad y la privacidad son críticas. Es esencial implementar prácticas de seguridad robustas, como el uso de contraseñas fuertes, redes seguras y actualizaciones regulares de firmware, para proteger los dispositivos de domótica conectados a Wi-Fi.

En la domótica, Wi-Fi a menudo coexiste con otros protocolos como Zigbee y Z-Wave. Mientras que Wi-Fi es adecuado para dispositivos de alto ancho de banda, Zigbee y Z-Wave son preferidos para dispositivos que requieren menor consumo de energía y redes de malla (Cabrera y Pérez, 2019).

2.5.4. Futuro de Wi-Fi en Domótica

Con el desarrollo continuo de nuevas tecnologías Wi-Fi, como Wi-Fi 6, se espera una mayor eficiencia, velocidad y capacidad, lo que podría ampliar aún más su aplicación en la domótica. Por ende, Wi-Fi seguirá siendo un componente clave en el creciente mercado de IoT, especialmente en aplicaciones de hogar inteligente que requieren conectividad de alta velocidad (Cabrera y Pérez, 2019).

2.6. Requisitos de Seguridad

El acelerado desarrollo del mercado de la domótica y la presión competitiva que enfrentan numerosas marcas por mantenerse a la vanguardia a menudo resultan en la negligencia de aspectos cruciales de seguridad. Esta tendencia subraya la importancia de enfocarse en los requisitos de seguridad en los sistemas domóticos, considerando los diferentes niveles operativos, tal como lo destacan Meneghello, Calore, Zucchetto, Polese y Zanella (2019): Información, Acceso y Funcional.

2.6.1. Nivel de Información

Este nivel define los requerimientos para la información, proporcionando las siguientes funcionalidades:

- ✓ Integridad: Los datos recibidos no deben haber sido alterados durante la transmisión.
- ✓ Anonimato: La identidad de la fuente de datos debe permanecer oculta a terceros.
- ✓ Confidencialidad: Los datos no deben ser accesibles para terceros. Se debe establecer una relación de confianza entre los dispositivos IoT para el intercambio de información protegida. Además, es necesario poder reconocer los mensajes replicados.

- ✓ Privacidad: La información privada del cliente no debe divulgarse durante el intercambio de datos. Debe ser difícil para los interceptores inferior información identificable.

2.6.2. Nivel de Acceso:

Este nivel especifica mecanismos de seguridad para controlar el acceso a la red, proporcionando las siguientes funcionalidades:

- ✓ Control de Acceso: Garantiza que solo los usuarios legítimos puedan acceder a los dispositivos y a la red para tareas administrativas (por ejemplo, reprogramación remota o control de los dispositivos y la red IoT).
- ✓ Autenticación: Verifica si un dispositivo tiene derecho a acceder a una red y si una red tiene derecho a conectar el dispositivo. Esta suele ser la primera operación realizada por un nodo al unirse a una nueva red. Es crucial que los dispositivos ofrezcan procedimientos de autenticación robustos para evitar amenazas de seguridad. Por ejemplo, si todos los dispositivos IoT de un mismo fabricante se configuran con las mismas credenciales de autenticación, el hackeo de un dispositivo podría comprometer todos los aspectos de seguridad a nivel de información.
- ✓ Autorización: Asegura que solo los dispositivos y usuarios autorizados accedan a los servicios o recursos de la red.

2.6.3. Nivel Funcional

Este nivel define los requisitos de seguridad en términos de los siguientes criterios:

- ✓ Resiliencia: Se refiere a la capacidad de la red para garantizar la seguridad de sus dispositivos, incluso en caso de ataques y fallos.
- ✓ Autoorganización: Denota la capacidad de un sistema IoT para ajustarse a sí mismo y seguir operativo incluso en caso de fallo de algunas de sus partes debido a malfuncionamientos ocasionales o ataques maliciosos.

La Escala Global sobre la Preocupación de la Privacidad de la Información (GIPC) identifica cuatro dimensiones críticas en la percepción general sobre la privacidad: la recopilación, el uso no autorizado por terceros, el acceso inapropiado y los errores. Aunque esta escala puede

evolucionar con el tiempo, proporciona un marco efectivo para abordar casos de privacidad de la información en la domótica. (Meneghello et al., 2019)

2.7. Privacidad de la Información

Para destacar la importancia de la ciberseguridad en los protocolos de comunicación inalámbricos es necesario explicar la privacidad de la información. La Escala Global sobre la Preocupación de la Privacidad de la Información (GIPC, por sus siglas en inglés) identifica cuatro dimensiones clave que reflejan las preocupaciones generales sobre la privacidad de la información. Estas dimensiones son:

- ✓ Recopilación: Se refiere a la inquietud sobre la extensión y el volumen de los datos personales que se recogen.
- ✓ Uso no autorizado por terceros: Esta dimensión aborda las preocupaciones sobre el uso indebido de la información personal por parte de entidades no autorizadas.
- ✓ Acceso inapropiado: Se centra en la preocupación por el acceso no autorizado o inadecuado a los datos personales.
- ✓ Errores: Esta dimensión considera la preocupación por los errores en el manejo de los datos personales, que pueden llevar a inexactitudes o malinterpretaciones.

Aunque la GIPC proporciona un marco útil para entender las preocupaciones generales sobre la privacidad, es importante reconocer que esta escala no es absoluta y puede evolucionar con el tiempo, especialmente en un entorno digital en constante cambio. (Solis, 2018, p. 31).

2.8. Principales Mecanismos de Seguridad en IoT

Para comprender adecuadamente las vulnerabilidades en la seguridad y privacidad que tienen los sistemas domóticos es importante conocer los principales mecanismos de seguridad utilizados en la industria, tal como lo destacan Meneghello, Calore, Zucchetto, Polese y Zanella (2019):

- ✓ Encriptación: Es la operación principal para garantizar la confidencialidad durante la comunicación. Cambia el mensaje real (texto plano) a uno diferente (texto cifrado) usando

una función hash que solo se puede revertir conociendo una clave secreta. Puede ser simétrica (misma clave para cifrar y descifrar) o asimétrica (claves públicas y privadas).

- ✓ Mecanismos de Encriptación Estándar: La encriptación puede ser de flujo (cifrando bit a bit) o de bloque (tratando un bloque de texto plano como un todo). El Estándar de Encriptación Avanzada (AES) es un cifrado de bloque simétrico común. Otros sistemas criptográficos asimétricos incluyen RSA, McEliece y ElGamal.
- ✓ Autenticación y Protección de Integridad: Se proporcionan mediante códigos de autenticación de mensajes (mecanismos simétricos), firmas digitales (mecanismos asimétricos) y funciones hash. Estos métodos combinan el texto plano con una etiqueta generada a partir de la clave privada.
- ✓ Criptografía Ligera: Diseñada para dispositivos IoT de baja complejidad y recursos limitados. Incluye nuevos cifrados de bloque y flujo, códigos de autenticación de mensajes y funciones hash. Ejemplos son los cifrados de bloque PRESENT y CLEFIA.
- ✓ Generadores de Números Aleatorios: Esenciales para la seguridad, generan números para diferentes propósitos como la creación de nonces y la generación de claves asimétricas. Los tipos comunes son los Generadores de Números Aleatorios Verdaderos (TRNG) y los Pseudoaleatorios (PRNG).
- ✓ Hardware Seguro: Para proteger contra ataques de capa de borde en dispositivos IoT. Incluye Funciones Físicamente Inclonables (PUFs) y otras soluciones de hardware y software para prevenir ataques de análisis de canal lateral.
- ✓ Sistemas de Detección de Intrusiones: Métodos ligeros para detectar ataques en curso en dispositivos IoT, utilizando parámetros del sistema como el uso de CPU, consumo de memoria y rendimiento de la red. El aprendizaje automático también se puede utilizar para la detección de intrusiones.

3. Descripción del TFM

En esta sección, se detallan los objetivos de la investigación y la metodología utilizada en el trabajo.

3.1. Objetivo General:

Realizar un análisis de los protocolos de transmisión de los sistemas domóticos residenciales mediante una revisión de literatura para la identificación de vulnerabilidades de seguridad.

3.2. Objetivo Específicos:

Determinar la metodología adecuada para llevar a cabo la revisión de literatura especializada en el ámbito de la domótica.

Identificar los protocolos de transmisión más utilizados en sistemas domóticos residenciales mediante un análisis de fuentes bibliográficas actuales para la categorización de tecnologías aplicadas en la domótica.

Evaluar las características de seguridad de los protocolos de transmisión identificados en la revisión de literatura para la identificación de posibles vulnerabilidades y riesgos asociados.

Desarrollar recomendaciones para la mitigación de las vulnerabilidades identificadas en los protocolos de transmisión de sistemas domóticos residenciales, basándose en las mejores prácticas de seguridad para el mejoramiento de la protección de los usuarios finales.

3.3. Metodología del Trabajo

El método PRISMA es reconocido internacionalmente por proporcionar un marco estandarizado y riguroso para realizar y reportar revisiones sistemáticas y metaanálisis. Esta estandarización asegura que la revisión sea rigurosa, transparente y replicable. Al seguir las directrices de PRISMA, se garantiza una cobertura de la literatura relevante, minimizando el sesgo en la selección de estudios y mejorando la calidad general de la revisión.

Por otro lado, Parsifal, como herramienta de apoyo, facilita significativamente la aplicación del método PRISMA. Ofrece una plataforma intuitiva para gestionar la gran cantidad de datos y referencias que se generan en una revisión sistemática. Esta herramienta permite organizar y documentar cada etapa del proceso de revisión de manera detallada, desde la definición de criterios de inclusión y exclusión hasta la selección final de estudios. Esto no solo mejora la eficiencia en la gestión de datos, sino que también refuerza la transparencia y la replicabilidad de la investigación.

3.4. Descripción General del Trabajo

La propuesta de este trabajo de fin de máster se enfoca en abordar los desafíos relacionados con la seguridad y la privacidad en sistemas de domótica basados en Internet de las Cosas (IoT). El proyecto busca analizar, evaluar y proponer soluciones para mejorar la protección de datos y la privacidad de los usuarios en entornos domésticos automatizados.

3.4.1. Alcance y limitaciones:

El trabajo se desarrolla en el contexto de la seguridad y la privacidad en sistemas de domótica e Internet de las Cosas (IoT) en entornos domésticos. En primer lugar, se llevará a cabo una revisión exhaustiva de la literatura científica y técnica relacionada con estos temas, con el objetivo de comprender a fondo los desafíos y las soluciones existentes. Asimismo, se llevará a cabo una evaluación crítica de las prácticas y estándares actuales en la industria de la domótica, enfocándose particularmente en la protección de datos y la privacidad de los usuarios. Finalmente, se extraerán recomendaciones y directrices basadas en la investigación y el análisis realizados, con el propósito de ofrecer soluciones prácticas para mejorar la privacidad en la utilización de sistemas de domótica en el hogar.

Esta investigación se centrará exclusivamente en cuestiones relacionadas con la seguridad y la privacidad en la domótica, excluyendo deliberadamente temas no relacionados. Además, se aplicará una restricción con respecto a la selección de documentos para la revisión de la literatura, limitándola a aquellos escritos en español e inglés. Por último, es relevante señalar que este proyecto se enfocará en un análisis totalmente teórico de la seguridad y la privacidad en la domótica, sin la inclusión de simulaciones ni implementaciones prácticas.

4. Desarrollo del Trabajo

En esta sección, se detallan los criterios de inclusión y exclusión aplicados en la investigación, así como la cadena de búsqueda utilizada para recopilar los datos relevantes.

4.1. Criterios de Inclusión

CI1. Se considerarán trabajos publicados entre 2018 y 2023 para abarcar investigaciones y desarrollos recientes en domótica, ciberseguridad y privacidad de datos.

CI2. Se aceptarán resúmenes analíticos, artículos científicos, tesis académicas y publicaciones en revistas científicas.

CI3. Se utilizarán bases de datos como Scopus y Web of Science, accesibles a través de la biblioteca de UNIR.

CI4. Se admitirán documentos redactados en español e inglés.

CI5. Los abstractos deben tratar al menos uno de los temas clave relacionados con la domótica residencial: Z-Wave, ZigBee o Wi-Fi; normativas de seguridad; vulnerabilidades y riesgos de seguridad en protocolos inalámbricos.

4.2. Criterios de Exclusión:

CE1. Se excluyen trabajos publicados antes de 2018 o después de 2023.

CE2. No se considerarán documentos que no sean artículos científicos, tesis académicas o publicaciones en revistas científicas.

CE3. Se rechazarán documentos en idiomas distintos al español e inglés.

CE4. Los documentos cuyos abstractos no aborden los temas clave especificados en los criterios de inclusión serán excluidos.

CE5. Se descartarán documentos no relacionados directamente con la domótica, la ciberseguridad o la privacidad de datos en la automatización.

4.3. Criterios de Calidad:

CC1. Los títulos de los trabajos seleccionados deben estar directamente relacionados con temas de domótica y protocolos de comunicación o ciberseguridad.

CC2. Los abstractos deben abordar temas específicos de ciberseguridad, como la identificación de riesgos, la protección de datos o la detección de intrusiones para protocolos de comunicación.

CC3. Se valorará la originalidad y la innovación en los enfoques y resultados presentados.

CC4. La claridad y coherencia en la presentación de los resultados y conclusiones.

CC5. El trabajo debe incluir el análisis de uno o más protocolos de comunicación relevantes, ZigBee, Wi-Fi o Z-Wave, en relación con la ciberseguridad y/o la domótica.

CC6. Se evaluará la robustez y la validez de los métodos utilizados en la investigación, incluyendo el diseño del estudio, la recopilación y análisis de datos, y la interpretación de los resultados.

4.4. Cadena de búsqueda:

Para llevar a cabo una revisión de literatura en el ámbito de la domótica residencial y los protocolos de comunicación inalámbrica, es necesario establecer una cadena de búsqueda precisa. Esta cadena de búsqueda es necesaria para dirigir la recopilación de información relevante y garantizar que la revisión cubra un rango adecuado de literatura. A continuación, se detalla la cadena de búsqueda empleada en este estudio.

La cadena de búsqueda se ha diseñado con el objetivo de abarcar una amplia variedad de publicaciones, que van desde aspectos técnicos específicos de los protocolos inalámbricos, como Wi-Fi, Z-Wave y ZigBee, hasta temas más generales relacionados con la seguridad y estrategias de mejora en el ámbito de la domótica. La selección cuidadosa de términos como "Estudio de Caso", "Análisis Comparativo" y "Revisión Sistemática" ha sido realizada con el fin de garantizar una investigación completa y pertinente en el área de estudio.

En español: ("Domótica Residencial" OR "Automatización Residencial" OR "Automatización del Hogar" OR "Casa Inteligente" OR "Hogar Inteligente") AND ("Protocolos de comunicación inalambrico" OR "Wi-Fi" OR "Z-Wave" OR "ZigBee") AND ("Estudio de Caso" OR "Análisis Comparativo" OR "Revisión Sistemática" OR "Estándares de Seguridad" OR "Cumplimiento normativo" OR "Recomendaciones" OR "Estrategias" OR "Mejoras" OR "Sugerencias" OR

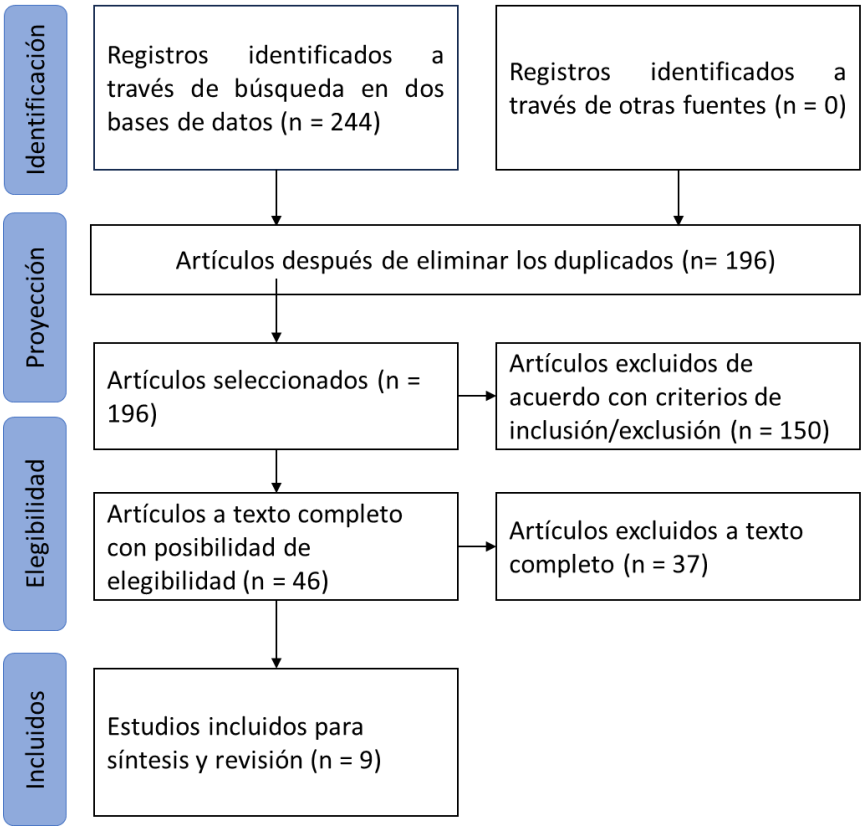
"Seguridad de Red" OR "Amenazas" OR "Inseguridades" OR "Puntos Débiles" OR "Riesgos" OR "Vulnerabilidades")

En ingles: ("Residential Domotics" OR "Residential Automation" OR "Home Automation" OR "Smart Home" OR "Intelligent Home") AND ("Wireless Communication Protocols" OR "Wi-Fi" OR "Z-Wave" OR "ZigBee") AND ("Case Study" OR "Comparative Analysis" OR "Systematic Review" OR "Security Standards" OR "Regulatory Compliance" OR "Recommendations" OR "Strategies" OR "Improvements" OR "Suggestions" OR "Network Security" OR "Threats" OR "Insecurities" OR "Weak Points" OR "Risks" OR "Vulnerabilities")

4.5. Selección de Registros:

Para la selección de estudios, inicialmente se identificaron un total de 244 registros a través de la búsqueda, utilizando la cadena de búsqueda, en las bases de datos Scopus y Web of Science.

Figura 3: *Diagrama de Flujo de PRISMA - Elaboración propia*



Luego, se utilizó la herramienta de gestión de referencias, Parsifal, para eliminar 46 registros duplicados. Posteriormente, se realizó una evaluación preliminar de los títulos y resúmenes de los 198 registros restantes utilizando criterios de calidad predefinidos. Se rechazaron 136 registros debido a que no cumplían con los criterios de inclusión y calidad establecidos. Lo que resultó en un total de 46 registros evaluados para la elegibilidad.

Después de la evaluación completa de los 46 registros, se seleccionaron 21 registros que cumplían con los criterios de inclusión y calidad establecidos en el texto completo para su inclusión en la revisión sistemática.

4.6. Evaluación de la Calidad de los Estudios:

La evaluación de la calidad de los estudios se realizó mediante un conjunto de criterios de calidad predefinidos. Únicamente se consideraron para el análisis aquellos estudios que cumplían con un criterio de calidad superior a 4.0 (tablas 3 a 11 para las publicaciones seleccionadas), según los criterios de calidad establecido. Cada estudio fue evaluado en función de estos criterios, asignando puntos en una escala de 0, 0.5 o 1, dependiendo del grado en que cumplían con los requisitos establecidos. Los criterios se utilizaron para determinar la idoneidad metodológica y la relevancia de cada estudio para la revisión sistemática. Esta evaluación rigurosa permitió identificar los estudios de mayor calidad y relevancia para la síntesis de datos y la generación de conclusiones en el contexto de la revisión PRISMA. La Tabla 2 se muestra la publicación para cada protocolo de comunicación.

Tabla 2: ***Lista de las publicaciones para los protocolos seleccionados***

Protocolo de Comunicación	Publicación
Zigbee	1, 4, 9
Z-Wave	1, 3
Wi-Fi	6, 7, 8
Recomendaciones de seguridad	2, 3, 4, 5, 7, 8, 9

4.7. Análisis de las publicaciones revisadas

Las publicaciones presentadas fueron seleccionados en base a los criterios previamente definidos. La información está centrada en dos áreas principales: vulnerabilidades de los

protocolos de comunicación Z-Wave, Zigbee y/o Wi-Fi, así como recomendaciones de seguridad para los protocolos de comunicación utilizados en sistemas de domótica.

Publicación 1: A State-of-the-Art Review on the Security of Mainstream IoT Wireless PAN Protocol Stacks.
Autores: Georgios Kambourakis, Constantinos Kolias, Dimitrios Geneiatakis, Georgios Karopoulos, Georgios Michail Makrakis e Ioannis Kounelis

Tabla 3: ***Criterios de Calidad para la Publicación 1***

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
0.5	1	1	1	1	1	5.5

4.7.1. Vulnerabilidades de Zigbee

ZigBee, aunque ofrece servicios de seguridad como el establecimiento de claves y la protección de la confidencialidad e integridad de los datos mediante AES-CCM, tiene algunas vulnerabilidades importantes. Por ejemplo, en la versión S0 del protocolo, la fase de emparejamiento está protegida por una clave predeterminada codificada de ceros, lo que facilita a los atacantes obtener la clave de red y acceder al tráfico de datos. Esto significa que los dispositivos ZigBee más antiguos pueden ser vulnerables a diversos ataques si no se actualizan con las últimas medidas de seguridad.

Además, aunque ZigBee cuenta con un modelo de confianza entre dispositivos, donde se asume que las diferentes capas del conjunto y las aplicaciones en el mismo dispositivo son confiables entre sí, esto puede representar un riesgo si un dispositivo se ve comprometido. Un atacante podría aprovechar una aplicación comprometida para acceder a otras aplicaciones en el mismo dispositivo, lo que podría comprometer la seguridad de los datos en toda la red ZigBee. (Kambourakis et al. 2020)

4.7.2. Vulnerabilidades de Z-Wave

Z-Wave ha introducido mejoras significativas en la seguridad con la versión S2 del protocolo. Esta versión utiliza el esquema de acuerdo de clave Diffie-Hellman elíptica (ECDH) para el emparejamiento, lo que hace que los ataques de intermediarios sean prácticamente inútiles.

Sin embargo, existen preocupaciones sobre la seguridad de las implementaciones específicas de Curve25519, que pueden ser vulnerables a ataques de canal lateral.

Una preocupación importante es que las versiones anteriores de Z-Wave, como S0, no requieren cifrado en el enlace de comunicación, lo que las hace vulnerables a ataques como el espionaje, la manipulación e inyección de mensajes. Esto significa que los dispositivos Z-Wave certificados con S0 pueden representar un riesgo de seguridad para toda la red si no se actualizan a las últimas medidas de seguridad S2. (Kambourakis et al. 2020)

4.7.3. Discusión de la investigación

A pesar de que la investigación incluye la presentación de varios protocolos de comunicación nos enfocamos solamente en Zigbee y Z-Wave, que son los protocolos previamente establecidos para el análisis. Los autores Kambourakis et al. (2020) presentan las siguientes observaciones:

Los protocolos que respaldan la infraestructura de redes de malla, como ZigBee y Z-Wave, destacan por su robustez en términos de conectividad y disponibilidad de servicios, superando a otras arquitecturas. Esta ventaja radica en su capacidad para crear redes que se autoorganizan y autorreparan, lo que aumenta la fiabilidad y la cobertura de la red. Aunque se han introducido mejoras en los mecanismos de seguridad en las nuevas versiones de los protocolos, como Z-Wave S2, aún persisten posibles vulnerabilidades que los atacantes podrían aprovechar para interceptar o manipular comunicaciones.

Tanto ZigBee como Z-Wave proporcionan servicios de seguridad básicos, como confidencialidad, autenticación de origen e integridad de datos. Sin embargo, la implementación efectiva de estas medidas puede variar entre dispositivos y fabricantes. Utilizar una clave de red única para proteger las comunicaciones entre dispositivos puede aumentar el riesgo de ataques si la clave se ve comprometida. Para mitigar este riesgo, los protocolos implementan la segmentación de redes y procedimientos de establecimiento de claves seguros. Además, cambiar las claves de red con regularidad puede reducir el riesgo de compromiso de seguridad.

Por otro lado, los dispositivos con certificaciones antiguas pueden representar un riesgo de seguridad, ya que es menos probable que reciban actualizaciones de seguridad del fabricante. La fragmentación en la elección de tecnologías de comunicación inalámbrica en el entorno IoT dificulta la interoperabilidad y puede introducir vulnerabilidades de seguridad. Aunque se han realizado intentos para abordar este problema, como 6LoWPAN, aún queda trabajo por hacer para lograr una interoperabilidad segura en el ámbito del IoT.

Muchos ataques pueden ser el resultado de una configuración incorrecta o decisiones de implementación deficientes por parte de los fabricantes de dispositivos. Es crucial que los fabricantes implementen prácticas de seguridad sólidas y actualicen regularmente el firmware de sus dispositivos para abordar estas vulnerabilidades. Proteger los datos importantes almacenados en los dispositivos IoT, como información de red, material de seguridad y datos de autenticación, contra compromisos de seguridad es fundamental. Esto requiere medidas de seguridad sólidas, como el borrado seguro de datos cuando un dispositivo abandona la red y la autenticación de mensajes de salida para prevenir ataques de suplantación. Si una red WPAN utiliza servicios en la nube, todos los nodos pueden ser vulnerables a ataques de Internet si la conexión a la nube no está segura de extremo a extremo. Es crucial implementar medidas de seguridad sólidas para proteger los datos en tránsito hacia y desde la nube. (Kambourakis et al. 2020)

Publicación 2: “Network Sentiment” Framework to Improve Security and Privacy for SmartHome.
Autores: Tommaso Pecorella, Laura Pierucci y Francesca Nizzi

Tabla 4: *Criterios de Calidad para la Publicación 2*

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
1	1	1	1	0.5	1	5.5

Este articulo aborda la creciente importancia de la ciberseguridad en entornos de Hogar Inteligente, donde una amplia gama de dispositivos de automatización del hogar necesita comunicarse con redes externas y están expuestos a vulnerabilidades. Se destaca cómo los

ataques maliciosos pueden comprometer tanto la seguridad de la red como la seguridad física de los usuarios, lo que subraya la necesidad de soluciones efectivas y dinámicas de protección.

El trabajo propone una arquitectura llamada SHIELD que integra firewalls distribuidos y un sistema de análisis de amenazas, con la idea de que todos los elementos de seguridad deben trabajar juntos de manera coordinada y reactiva frente a nuevas amenazas. Se enfatiza la importancia de una evaluación dinámica del riesgo, denominada análisis de sentimiento de red, para adaptar las medidas de seguridad según la situación. Además, se presenta un banco de pruebas que demuestra la viabilidad de la arquitectura SHIELD y se discuten posibles direcciones futuras para abordar los desafíos de seguridad y privacidad en entornos de Hogar Inteligente.

4.7.4. Recomendaciones de seguridad

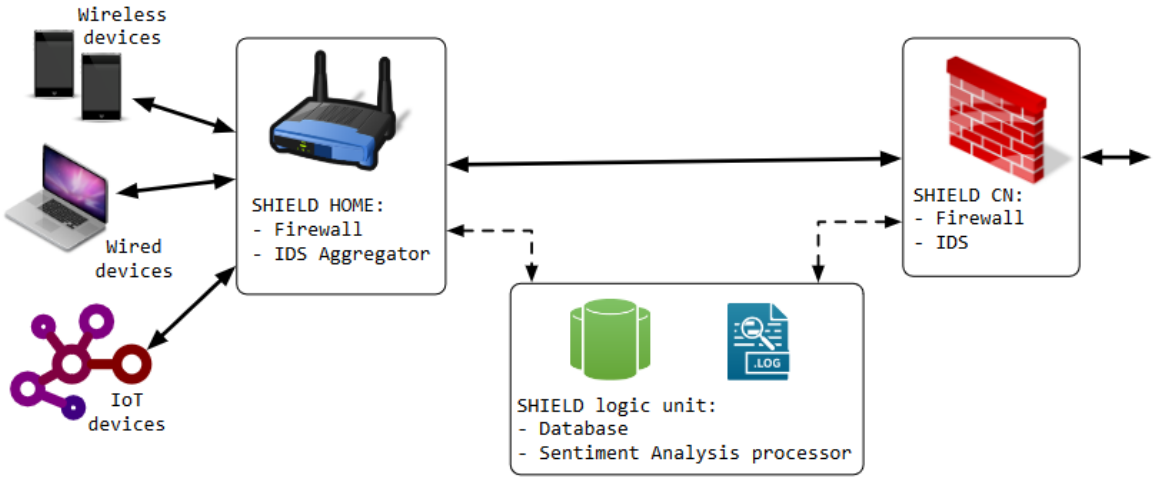
SHIELD (Security and Home Integrated Environment for IoT anD Smarthome) es un marco de seguridad diseñado para proteger los entornos de Hogar Inteligente contra amenazas cibernéticas. Se centra en la integración de firewalls y sistemas de detección de intrusiones (IDS) distribuidos para garantizar una protección completa y dinámica contra una amplia gama de ataques, incluidos ataques de repetición, retardo, denegación de servicio (DoS) y denegación de servicio distribuido (DDoS).

El marco SHIELD, como se muestra en la figura 4, se basa en la idea de distribuir la inteligencia de seguridad entre el proveedor de servicios de Internet (ISP) y el hogar inteligente. En el lado del ISP, se implementa un dispositivo denominado SCN (Security Control Node), que actúa como un firewall para proteger tanto la red del ISP como la red del usuario. El SCN también analiza el tráfico para identificar actividades sospechosas y recopila datos de los IDS instalados en el hogar inteligente.

Por otro lado, en el hogar inteligente, se despliega un dispositivo llamado SH (SHIELD Home), que actúa como un firewall y un agregador de IDS. El SH es responsable de filtrar el tráfico entre el hogar inteligente y el ISP, así como de coordinar y armonizar los diferentes IDS instalados en la red doméstica. Además, el SH puede tomar medidas correctivas, como

modificar las reglas del firewall, en respuesta a las amenazas detectadas (Pecorella, Pierucci y Nizz, 2018).

Figura 4: *Arquitectura Shield*



Fuente: "Network Sentiment" Framework to Improve Security and Privacy for Smart por Pecorella, Pierucci y Nizz, 2018

Publicación 3: Evaluation of security regarding Z-Wave wireless protocol.

Autores: Muneer Bani Yassein, Wail Mardini y Taha Almasri

Tabla 5: ***Criterios de Calidad para la Publicación 3***

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
1	1	0.5	0.5	1	0.5	4.5

El presente estudio se centra en evaluar la seguridad del protocolo Z-Wave. El uso de sensores inalámbricos ha aumentado, especialmente en aplicaciones como la automatización del hogar.

4.7.5. Análisis de Vulnerabilidades

El análisis de vulnerabilidades en el protocolo Z-Wave revela una serie de posibles puntos débiles que podrían ser explotados por los atacantes. Estos incluyen la posibilidad de ataques de inyección de paquetes, donde un atacante puede introducir paquetes maliciosos en la red

para llevar a cabo diversas acciones perjudiciales. Además, se han identificado vulnerabilidades en la capa de seguridad del protocolo, lo que podría comprometer la confidencialidad y la integridad de los datos transmitidos a través de la red Z-Wave. Estas vulnerabilidades pueden ser especialmente preocupantes en entornos donde la seguridad y la privacidad son críticas, como en aplicaciones de hogares inteligentes donde se controlan sistemas de seguridad y dispositivos domésticos conectados.

4.7.6. Estrategias de Mitigación:

Para abordar estas vulnerabilidades y fortalecer la seguridad en las redes Z-Wave, se proponen varias estrategias de mitigación. Una de las estrategias clave es ocultar el SSID WLAN, lo que dificulta que los atacantes identifiquen y accedan a la red. Además, se recomienda el uso de contraseñas robustas para proteger el acceso a la red y evitar ataques de fuerza bruta. Filtrar direcciones MAC también puede ayudar a restringir el acceso a dispositivos autorizados, mientras que el uso de un servidor proxy inverso proporciona una capa adicional de autenticación y seguridad para las comunicaciones entrantes. Por último, monitorear los archivos de registro en busca de actividades sospechosas puede ayudar a detectar y responder rápidamente a posibles ataques.

Publicación 4: IoT Device (Zigbee) Security Study [Estudio de seguridad de dispositivos IoT (Zigbee)].
Autores: HKCERT y el Consejo de Productividad de Hong Kong (HKPC)

Tabla 6: ***Criterios de Calidad para la Publicación 4***

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
1	1	1	1	1	1	6

ZigBee, al formar parte de las tecnologías inalámbricas con bajo consumo de energía, puede transportar solo pequeños paquetes de red que no permiten la implementación de dispositivos de seguridad de alta gama. La mayoría de la seguridad dentro de la tecnología ZigBee se ha realizado en las secciones de emparejamiento y de redes, que incluyen cifrado.

La Alianza ZigBee ha anunciado estándares de seguridad para que los fabricantes desarrollen productos ZigBee con estándares de seguridad adecuados.

4.7.7. Características de seguridad

En cuanto a las características de seguridad dentro del entorno de redes ZigBee, ZigBee proporciona servicios de seguridad basados en IEEE 802.15.4, como el establecimiento seguro de claves, el transporte seguro de claves, la protección de tramas a través de criptografía simétrica y la gestión segura de dispositivos. Estos servicios de seguridad se han implementado al emparejar y en la red en los dispositivos ZigBee.

Hay dos tipos diferentes de modelos de seguridad que admite la red ZigBee, Modelo de Seguridad Centralizado y Modelo de Seguridad Distribuido. La seguridad de la red ZigBee depende principalmente de las claves de red y las claves de enlace al implementar tanto el Modelo de Seguridad Centralizado como el Modelo de Seguridad Distribuido. La clave de red de 128 bits se utiliza para asegurar la comunicación de difusión, que se comparte entre todos los dispositivos en la red. (HKCERT y HKPC, 2020)

4.7.8. Protección y Cifrado

El estudio de seguridad en la tecnología ZigBee por HKCERT y HKPC destaca varios aspectos clave:

- ✓ Estándar de Cifrado: ZigBee utiliza AES (Estándar de Cifrado Avanzado) con una longitud de clave de 128 bits, ofreciendo robustez contra interferencias y protección de tramas de red mediante AES-CCM, una variación de AES con un modo modificado.
- ✓ Protección contra Ataques de Repetición: La red ZigBee implementa protección contra ataques de repetición mediante un contador de tramas de 32 bits, que se incrementa en cada transmisión de paquetes, previniendo así ataques inalámbricos.
- ✓ Cifrado en la Capa de Red: Durante la autenticación del nodo en la red, se envía una clave de cifrado al dispositivo que se une, llamada Clave de Red, para cifrar o descifrar datos de protocolo intercambiados.

- ✓ Cifrado en la Capa de Aplicación: Además del cifrado en la capa de red, los nodos pueden establecer comunicaciones cifradas de extremo a extremo en la capa de aplicación mediante una clave única llamada clave de aplicación o clave de enlace.
- ✓ Claves de Código de Instalación: Una alternativa a las claves de enlace preconfiguradas son las Claves de Código de Instalación, que requieren interacción manual en el Centro de Confianza y en los dispositivos ZigBee.
- ✓ Cifrado con Clave Basada en Certificado: Los perfiles de aplicación ZigBee emplean el Establecimiento de Clave Basado en Certificado (CBKE), donde cada dispositivo debe almacenar un certificado emitido por una autoridad de certificación de confianza.
- ✓ Estándares de Seguridad de la Alianza ZigBee: La Alianza ZigBee introduce "ZigbeeAlliance09" como el valor predeterminado de la Clave de Enlace del Centro de Confianza, permitiendo la interoperabilidad entre dispositivos de diferentes fabricantes.

Publicación 5: Is your Smart Home a Secure Home? - Analysis of Smart Home Breaches and an Approach for Vulnerability Analysis and Device Isolation.
Autores: Gokila Dorai, Eleason A. Williams, Hongmei Chi y Richard A. Alo

Tabla 7: ***Criterios de Calidad para la Publicación 5***

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
1	1	1	1	1	1	6

El artículo aborda la creciente popularidad de los dispositivos inteligentes en el hogar y los riesgos de seguridad asociados con ellos. Los dispositivos inteligentes están conectados a la red Wi-Fi del hogar, lo que significa que una vulnerabilidad en uno de ellos podría tener repercusiones graves en toda la red del hogar, especialmente en entornos médicos inteligentes.

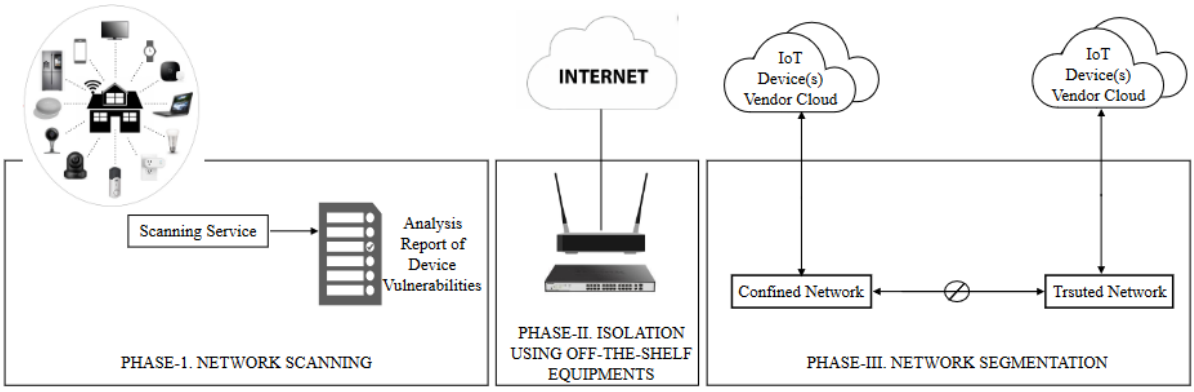
El estudio se centra en la detección de vulnerabilidades en un entorno experimental de hogar inteligente utilizando diversos dispositivos conectados, proponiendo soluciones para aislar los dispositivos vulnerables y proteger así el hogar inteligente. Se emplea la herramienta de escaneo de red Nmap para identificar todos los dispositivos conectados y sus vulnerabilidades.

Se proponen dos enfoques para aislar dispositivos vulnerables: el uso de routers en cascada y la creación de redes VLAN (Virtual Local Area Network).

El análisis revela que, en promedio, existen más de 25 defectos de seguridad en dispositivos IoT comúnmente utilizados, lo que subraya la importancia de abordar las vulnerabilidades en estos dispositivos.

4.7.9. **Técnicas de aislamiento de** dispositivos

Figura 5: *Un Enfoque para el Aislamiento de Dispositivos*



Fuente: Analysis of Smart Home Breaches and an Approach for Vulnerability Analysis and Device Isolation por Dorai et al., 2020

En cuanto a las técnicas de aislamiento de dispositivos, como se muestra en la figura 5, se describen detalladamente dos enfoques: el uso de routers en cascada y la configuración de VLAN. Ambos enfoques se prueban experimentalmente, demostrando su eficacia para aislar dispositivos vulnerables en una red de hogar inteligente.

El enfoque de routers en cascada implica la conexión de múltiples routers en secuencia, lo que crea subredes separadas dentro de la red principal. Este método se implementa colocando un router adicional entre el router principal y los dispositivos vulnerables, lo que permite segmentar la red y aislar los dispositivos susceptibles de manera efectiva. Durante los experimentos, se demuestra la capacidad de este enfoque para crear una red confinada donde los dispositivos vulnerables pueden operar sin interactuar con el resto de la red.

Por otro lado, la configuración de VLAN proporciona una solución más avanzada y robusta para el aislamiento de dispositivos. Mediante la creación de redes locales virtuales separadas, la VLAN permite que los dispositivos se asignen a grupos específicos y se les impida comunicarse con otros dispositivos fuera de su grupo designado. Este método ofrece un mayor nivel de control sobre el tráfico de red y garantiza una separación completa entre los dispositivos vulnerables y los dispositivos seguros. Durante las pruebas experimentales, se confirma la efectividad de la configuración de VLAN para mantener los dispositivos vulnerables completamente aislados y protegidos dentro de la red de hogar inteligente. (Dorai et al., 2020)

Publicación 6: A Quantitative Study of DDoS and E-DDoS Attacks on Wi-Fi Smart Home Devices.
Autores: Bhagyashri Tushir, Yogesh Dalal, Behnam Dezfouli y Yuhong Liu

Tabla 8: ***Criterios de Calidad para la Publicación 6***

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
1	1	1	1	1	1	6

El amplio uso de Wi-Fi en dispositivos IoT domésticos es debido a su amplio despliegue y bajo costo, el Wi-Fi es una tecnología ampliamente utilizada para la conectividad inalámbrica de dispositivos IoT. Esta tecnología se utiliza para la conectividad de dispositivos en el hogar inteligente, como asistentes de voz, cámaras de seguridad, sistemas de entretenimiento y electrodomésticos.

4.7.10. Ataques DDoS y E-DDoS

DDoS significa "Denegación de Servicio Distribuido" (en inglés, Distributed Denial of Service). Es un tipo de ataque informático donde múltiples sistemas comprometidos se utilizan para dirigir tráfico malicioso hacia un objetivo, como un servidor, red o sistema, con el objetivo de sobrecargarlo y hacer que sea inaccesible para los usuarios legítimos. Estos sistemas comprometidos, también conocidos como "bots" o "zombies", pueden ser computadoras, dispositivos IoT u otros dispositivos conectados a Internet que han sido previamente infectados con malware diseñado para participar e11n el ataque.

E-DDoS, o "Denegación de Servicio de Energía Distribuida" (en inglés, Energy Distributed Denial of Service), es una variante del ataque DDoS que tiene como objetivo agotar los recursos de energía de los dispositivos objetivo. En lugar de simplemente abrumar los recursos computacionales, como en un ataque DDoS tradicional, un ataque E-DDoS busca consumir la mayor cantidad posible de energía del dispositivo objetivo. Esto puede tener consecuencias graves, especialmente en dispositivos alimentados por batería o dispositivos con limitaciones energéticas, como dispositivos IoT en un hogar inteligente.

A pesar del aumento significativo en el uso de dispositivos domésticos inteligentes, estos dispositivos muestran vulnerabilidades a diversos ataques de seguridad y privacidad, como ataques DDoS y E-DDoS. Estas vulnerabilidades pueden deberse a la falta de atención a la seguridad por parte de los fabricantes, la falta de educación del consumidor sobre los problemas de seguridad potenciales y el uso compartido de un punto de acceso Wi-Fi para la conexión a Internet y la interconexión local.

Los ataques DDoS y E-DDoS en dispositivos IoT domésticos pueden tener un impacto significativo en los dispositivos IoT del hogar, incluyendo la interrupción de servicios y el aumento de los costos de electricidad para los usuarios. Los dispositivos IoT comprometidos pueden utilizarse para lanzar ataques DDoS y E-DDoS, lo que resulta en una mayor interrupción del servicio y consumo de energía.

Importancia de comprender y defenderse contra los ataques DDoS y E-DDoS: Dado el aumento en el uso de dispositivos IoT en el hogar inteligente y el potencial impacto de estos ataques, es esencial comprender y defenderse contra ellos. Se destaca la necesidad de soluciones de defensa efectivas y estándares de seguridad para garantizar el funcionamiento seguro de los dispositivos IoT en el hogar. (Tushir et al., 2020)

Publicación 7: Securing the wireless environment of IoT.

Autores: Fanzeng Xia, Huancheng Song y Chunting Xu

Tabla 9: *Criterios de Calidad para la Publicación 7*

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
1	1	0.5	0.5	1	0.5	4.5

El Internet de las cosas (IoT) puede ser considerado como una infraestructura de red compuesta por numerosos dispositivos conectados que proporcionan actividades de detección, actuación, control y monitoreo. Estos dispositivos pueden intercambiar datos entre sí o recopilar información de otros dispositivos para procesarla localmente o enviarla a servidores centralizados. La tecnología rudimentaria para IoT es la identificación por radiofrecuencia (RFID), que permite la transmisión de información a través de la comunicación inalámbrica, mientras que las redes de sensores inalámbricos (WSNs) son otra tecnología fundamental que utiliza sensores programáticos para detectar y monitorear el entorno. Además, los protocolos de comunicación IoT son cruciales para definir los formatos de intercambio de datos, y el trabajo presenta un enfoque principal en IEEE 802.11 (Wi-Fi), que es una colección de estándares de comunicación de Red de Área Local Inalámbrica (WLAN).

4.7.11. Medidas de seguridad

El entorno de redes inalámbricas IoT presenta desafíos únicos, y los mecanismos de seguridad existentes son insuficientes. Los tradicionales mecanismos de seguridad integrados en la capa física, como firewall e IDS, ya no son adecuados para asegurar la próxima generación de Internet debido a preocupaciones ilimitadas sobre el control de acceso a la red, la verificación de software y el consumo de energía. Muchas soluciones propuestas se basan en modelos de red específicos, pero se requiere una solución distribuida y económica que garantice la seguridad de manera efectiva.

La tecnología de redes definidas por software (SDN) se propuso en 2015 para bloquear o cuarentenar dinámicamente dispositivos a nivel de red, lo que extendió el perímetro de

seguridad a los dispositivos de acceso a la red. Desde entonces, identificar y bloquear las amenazas a nivel de red resultó ser más factible y efectivo.

También, se han propuesto sistemas como IoT SENTINEL en 2017, capaces de identificar automáticamente los tipos de dispositivos conectados a una red IoT y hacer cumplir reglas de seguridad. En 2018, se propuso un enfoque basado en reglas donde cada dispositivo conectado proporciona una especificación de comunicación requerida para los servicios deseados. Se reconoció que la seguridad en la red puede complementarse con técnicas de aprendizaje automático para reaccionar dinámicamente a los ataques y ajustar las reglas de comunicación durante la operación.

Investigaciones recientes han demostrado el potencial del aprendizaje automático para la detección de anomalías. Se aplicaron algoritmos como el bosque aleatorio a características extraídas de datos de tráfico de red, logrando una detección perfecta de dispositivos IoT no autorizados en 2017. Además, se logró una alta precisión en la detección distribuida de denegación de servicio (DDoS) en el tráfico entre dispositivos Wi-Fi con una variedad de algoritmos de aprendizaje automático en el mismo año. Estos resultados muestran que los algoritmos de aprendizaje automático pueden ser efectivos para mantener un entorno seguro de Wi-Fi IoT en el futuro (Xia, Song y Xu, 2018).

Publicación 8: SecWIR: Securing smart home IoT communications via wi-fi routers with embedded intelligence.
Autores: Xinyu Lei, Guan-Hua Tu, Chi-Yu Li, Tian Xie y Mi Zhang

Tabla 10: ***Criterios de Calidad para la Publicación 8***

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
1	1	0.5	1	1	1	5.5

La investigación presenta un estudio sobre la seguridad de dispositivos de IoT para el hogar conectados a través de Wi-Fi. Se destaca que muchos de estos dispositivos carecen de protocolos de seguridad adecuados, lo que los hace vulnerables a ataques cibernéticos. Para

abordar este problema, proponen un marco llamado SecWIR, diseñado para implementarse en los routers Wi-Fi existentes de los usuarios, proporcionando así a los dispositivos IoT una capacidad de comunicación segura.

4.7.12. SecWIR

La falta de recursos de hardware/software en muchos dispositivos dificulta la instalación de parches de seguridad. Por lo tanto, SecWIR se propone como una solución que no requiere la modificación de los dispositivos existentes ni la compra de hardware adicional. El marco SecWIR se basa en el enrutador Wi-Fi del hogar del usuario y utiliza recursos de cómputo incorporados en el enrutador para proporcionar comunicaciones de IoT seguras.

El diseño de SecWIR es un marco de seguridad basado en software para asegurar dispositivos IoT utilizando enrutadores Wi-Fi comerciales fuera de la estantería (COTS, por sus siglas en inglés). SecWIR apunta a dos tipos particulares de dispositivos IoT, a saber, dispositivos NonSecIoT que carecen de soporte para protocolos de seguridad estándar, y dispositivos InSecIoT que ofrecen soporte de seguridad, pero tienen implementaciones defectuosas. SecWIR proporciona a los dispositivos NonSecIoT soporte para protocolos de seguridad convencionales para facilitar comunicaciones seguras con los servidores IoT, y protege contra comunicaciones inseguras para los dispositivos InSecIoT identificando conflictos entre el comportamiento del dispositivo y los estándares de protocolo de seguridad.

La arquitectura de SecWIR consta de cuatro módulos: (1) túneles seguros para IoT, (2) validación de seguridad de flujo, (3) monitoreo de recursos y (4) filtrado de paquetes. Todos los paquetes entrantes al enrutador Wi-Fi primero ingresan al módulo de filtrado de paquetes. Los paquetes de IoT se envían al módulo de túneles seguros para IoT o al módulo de validación de seguridad de flujo, mientras que los paquetes no IoT se reenvían directamente a sus destinos. El módulo de túneles permite a los dispositivos NonSecIoT comunicarse de forma segura con sus servidores IoT a través de túneles SSL/TLS específicos para IoT. Mientras tanto, el módulo de validación examina las operaciones SSL/TLS de los dispositivos InSecIoT en tiempo de ejecución utilizando una técnica eficiente de procesamiento de flujo, permitiendo que las conexiones SSL/TLS se establezcan solo si sus operaciones se verifican como compatibles con los estándares de protocolo de seguridad implementados.

Además, hay un módulo de monitoreo de recursos que rastrea el estado de los dispositivos no IoT y las estadísticas de recursos del sistema, y luego asigna dinámicamente recursos al marco de SecWIR de manera que mantenga sus operaciones normales. (Lei et al., 2020)

4.7.13. Ataques de seguridad en la red Wi-Fi

Ataques dentro de la red Wi-Fi doméstica:

- Compromiso de IoT/Ataques de denegación de servicio (DoS)/Ataques de canal lateral: Los dispositivos IoT pueden ser atacados internamente de diversas maneras, como compromisos de seguridad, ataques de denegación de servicio y ataques de canal lateral. Estos ataques requieren acceso a la red Wi-Fi doméstica del usuario de IoT. SecWIR implementa una política de seguridad para prevenir la comunicación de los dispositivos IoT con cualquier host interno que no sea SecWIR.
- Ataques de suplantación de IoT: Los adversarios pueden comprometer dispositivos no IoT dentro de la red Wi-Fi doméstica y hacerse pasar por auténticos dispositivos IoT, enviando datos basura al servidor IoT para agotar sus recursos. SecWIR puede detectar estos ataques y reportarlos a los usuarios de IoT, ya que asigna una clave de seguridad única a cada dispositivo asociado al enrutador Wi-Fi.
- Ataques maliciosos/comprometidos de IoT: Si un dispositivo comprometido comparte el mismo túnel SSL/TLS que otros dispositivos IoT, puede afectar el rendimiento de estos últimos. Sin embargo, SecWIR puede proteger a los dispositivos IoT de compromisos remotos y mitigar ataques físicos mediante un límite de velocidad por dispositivo.
- Ataques de denegación de servicio de IoT (DoIS): Los adversarios pueden comprometer dispositivos no IoT para consumir recursos del enrutador Wi-Fi y lanzar ataques de denegación de servicio contra los dispositivos IoT del usuario. SecWIR puede defenderse asignando recursos garantizados y utilizando routers Wi-Fi que soporten el reparto equitativo de ancho de banda. (Lei et al., 2020)

Ataques fuera de la red Wi-Fi doméstica:

- Ataques al protocolo SSL/TLS: Recientemente, los investigadores han explotado las vulnerabilidades de SSL/TLS para desarrollar varios ataques MITM, incluidos BEAST,

CRIME, TIME, RC4 BIASES, Renegociación SSL y ataques de degradación. Sin embargo, dado que estos ataques se basan principalmente en algoritmos de seguridad inseguros e implementaciones problemáticas, pueden ser fácilmente frustrados por SecWIR.

- Ataques de canal lateral: Los investigadores han demostrado que los adversarios pueden inferir el uso de IoT de los usuarios mediante el análisis de los datos de IoT cifrados. Sin embargo, SecWIR protege en gran medida a los usuarios de IoT de tales ataques mediante el mecanismo de tunelización. (Lei et al., 2020)

Publicación 9: Zigator: Analyzing the security of Zigbee-enabled smart homes.
Autores: Dimitrios-Georgios Akestoridis, Madhumitha Harishankar, Michael Weber y Patrick Tague

Tabla 11: ***Criterios de Calidad para la Publicación 9***

Criterios de Calidad						Total
CC1	CC2	CC3	CC4	CC5	CC6	
1	1	1	1	1	1	6

El ultimo registro presenta la herramienta Zigator, es un software diseñado específicamente para evaluar la seguridad de las redes Zigbee, un estándar de comunicación inalámbrica ampliamente utilizado en aplicaciones de domótica y automatización del hogar. Su función principal es analizar el tráfico de red Zigbee, permitiendo a los usuarios examinar tanto los paquetes capturados como los forjados para inyección en la red.

4.7.14. Funcionamiento de Zigator

Una de las capacidades destacadas de Zigator es su capacidad para analizar paquetes Zigbee, incluso aquellos que están encriptados. Puede desglosar los campos de encabezado no encriptados y utilizar algoritmos criptográficos para desencriptar y verificar la autenticidad de los paquetes encriptados. Esta capacidad es crucial para comprender la seguridad de una red Zigbee y detectar posibles vulnerabilidades.

Además de analizar paquetes, Zigator también puede forjar y enviar paquetes Zigbee manipulados para realizar pruebas de seguridad. Esto incluye ataques de spoofing y jamming,

que son fundamentales para evaluar la resistencia de una red Zigbee a diferentes tipos de ataques. Esta funcionalidad permite a los usuarios simular situaciones de amenaza y evaluar la capacidad de respuesta de la red.

Para facilitar el análisis y la comprensión de los datos Zigbee, Zigator almacena la información detallada de los paquetes capturados en una base de datos SQLite. Esto permite realizar consultas SQL detalladas para obtener información valiosa sobre el tráfico Zigbee y sus patrones. Además, proporciona una interfaz de línea de comandos rica en funciones que permite a los analistas de seguridad visualizar datos y enviar paquetes forjados para inyección sobre UDP.

4.8. Discusión

En base a la literatura analizada, a continuación se discuten las vulnerabilidades de cada protocolo y recomendaciones de seguridad para la mejora de la domótica residencial.

4.8.1. Vulnerabilidades en Zigbee, Z-Wave y Wi-Fi

La elección del protocolo de comunicación inalámbrica para un sistema de domótica es crucial para garantizar tanto la funcionalidad como la seguridad del hogar inteligente. Cada protocolo, ya sea Zigbee, Z-Wave o Wi-Fi, tiene sus propias ventajas y vulnerabilidades, y es importante considerarlas detenidamente antes de tomar una decisión.

Las vulnerabilidades en Zigbee abarcan diversas áreas preocupantes. Por un lado, existe la posibilidad de inserción de tráfico no deseado debido a su naturaleza de red de malla abierta. Además, la falta de implementación consistente de cifrado en todos los dispositivos puede crear brechas de seguridad significativas. Esta situación facilita que los paquetes de datos sean interceptados y manipulados por atacantes, lo que aumenta los riesgos de seguridad en esta plataforma de comunicación inalámbrica.

Por otro lado, una vulnerabilidad adicional en Zigbee radica en el uso de una clave predeterminada débil en versiones antiguas, lo que permite ataques de intermediario.

Además, el modelo de confianza inseguro entre dispositivos podría dar lugar a la propagación de compromisos, aumentando aún más los riesgos asociados con esta tecnología.

Las debilidades en Z-Wave incluyen la vulnerabilidad a ataques de rejugado en versiones antiguas, donde un atacante puede capturar y retransmitir comandos legítimos para provocar efectos no deseados. Además, las versiones más antiguas de Z-Wave utilizaban formas de cifrado menos seguras, lo que las hacía susceptibles a ser descifradas, aumentando el riesgo de comprometer la seguridad de la red. Además, los dispositivos Z-Wave pueden ser desvinculados de la red por atacantes, lo que interrumpe su funcionamiento normal y potencialmente compromete la integridad del sistema doméstico.

Las vulnerabilidades en las redes Wi-Fi incluyen la posibilidad de ataques de fuerza bruta a contraseñas, especialmente si estas son débiles, lo que puede comprometer la seguridad de la red y permitir el acceso no autorizado. Además, los atacantes pueden llevar a cabo ataques de intermediarios (MitM) al interceptar la comunicación entre dispositivos Wi-Fi, lo que les permite robar o manipular información transmitida, comprometiendo así la privacidad y la integridad de los datos. Asimismo, a pesar de la robustez del protocolo WPA2, ha sido vulnerable a ataques como KRACK, que explotan debilidades en la negociación de claves de cifrado, lo que resalta la importancia de mantenerse al tanto de las actualizaciones de seguridad y de implementar medidas adicionales para proteger las redes Wi-Fi contra tales amenazas.

Al tomar en cuenta estos factores, es esencial encontrar un equilibrio entre las funcionalidades ofrecidas por cada protocolo y las consideraciones de seguridad asociadas. La adopción de medidas de protección adecuadas, como la implementación de cifrado sólido y la gestión segura de contraseñas, es fundamental para mitigar los riesgos de seguridad y garantizar la integridad del hogar inteligente.

4.8.2. Recomendaciones para Zigbee, Z-Wave y Wi-Fi

En base a la literatura analizada a continuación se presentan recomendaciones de seguridad cada protocolo. Igualmente se presentaron herramientas para el análisis de la seguridad de alguno de los protocolos de comunicación inalámbrica como Zigator. Y técnicas como el uso

de routers en cascada y VLAN permiten aislar efectivamente dispositivos IoT vulnerables en la red doméstica para limitar su exposición.

Además, soluciones como IoT SENTINEL, SDN y algoritmos de aprendizaje automático han demostrado potencial para identificar y aislar dispositivos no autorizados o anomalías en el tráfico de red IoT. Por su parte, el framework SHIELD integra firewalls y sistemas IDS distribuidos para proteger el hogar inteligente. En este sentido, se destaca la importancia de realizar una evaluación de riesgo dinámica o "análisis de sentimiento de red".

Zigbee:

- ✓ Cambiar regularmente las claves de red y asegurar su complejidad.
- ✓ Mantener actualizados los dispositivos para aplicar parches de seguridad.
- ✓ Segmentación de Red: Dividir la red en segmentos más pequeños para limitar el impacto de posibles ataques.
- ✓ Supervisar constantemente la red para detectar actividades sospechosas.

Z-Wave:

- ✓ Uso de la versión más reciente, actualizar a la versión más reciente del protocolo Z-Wave para aprovechar mejoras de seguridad.
- ✓ Verificar la identidad de los dispositivos durante la inclusión en la red.
- ✓ Examinar periódicamente los dispositivos para detectar comportamientos inusuales.
- ✓ Ajustar la red Z-Wave con configuraciones óptimas de seguridad.
- ✓ Mantener actualizados los dispositivos para aplicar parches de seguridad.

Wi-Fi:

- ✓ Establecimiento de contraseñas fuertes y únicas, utilizar contraseñas complejas y cambiarlas regularmente.
- ✓ Un firewall robusto y otras medidas de seguridad de red.
- ✓ Mantener actualizados todos los dispositivos conectados a la red Wi-Fi.
- ✓ SecWIR implementado en routers Wi-Fi comerciales puede proporcionar comunicación segura a dispositivos IoT mediante túneles SSL/TLS específicos y validación de conexiones SSL/TLS.

5. Conclusiones y trabajos futuros

Este trabajo ha abordado la problemática de la seguridad en los protocolos de comunicación Zigbee, Z-Wave y Wi-Fi utilizados en sistemas de domótica residencial. Un área de constante crecimiento tecnológico, pero con riesgos potenciales para la privacidad y seguridad de los usuarios finales.

Una de las limitaciones de este trabajo fue la falta de acceso gratuito a todas las publicaciones que podrían haber sido elegibles para texto completo, a pesar de usar los recursos de la biblioteca de UNIR. En particular, 8 publicaciones no estuvieron disponibles de forma gratuita, lo que podría haber afectado la exhaustividad del análisis y la comprensión de ciertos aspectos relacionados con la investigación.

EL primer objetivo específico se cumple al identificar un protocolo para la revisión de literatura se logró mediante la utilización de la metodología PRISMA, que permitió la evaluación sistemática de las publicaciones y la selección de los protocolos relevantes (Apartado 4.1).

Al analizar detalladamente publicaciones recientes, se evidencia la proliferación de dispositivos IoT domésticos y su vulnerabilidad ante diversas amenazas, desde ataques DDoS hasta comprometimiento de dispositivos y suplantación de identidad. Esto se debe principalmente a falencias en el cifrado, autenticación débil e implementaciones defectuosas de los protocolos (objetivo específico 3). La interoperabilidad a menudo se valora más que la seguridad en los protocolos de comunicación. Sin embargo, es importante destacar que cuando los protocolos de comunicación sufren ataques de seguridad, todos los datos se encuentran en riesgo.

Sin embargo, la investigación ha avanzado significativamente en soluciones innovadoras para mitigar estos riesgos, como el uso de redes VLAN para segmentar tráfico, routers con inteligencia de seguridad incorporada, y herramientas especializadas de análisis como Zigator. Estos avances representan un progreso importante para proteger el entorno de hogares inteligentes (objetivo específico 4). Destacando la necesidad de educar y concientizar a los

usuarios finales de las soluciones existentes para promover buenas prácticas, dado que los avances tecnológicos por sí solos son insuficientes.

No obstante, se requiere trabajo adicional para implementar dichas soluciones a gran escala y garantizar su adopción por parte de los usuarios finales. La educación y concienciación de los usuarios resulta fundamental, ya que, sin importar los avances tecnológicos, las malas prácticas como el uso de contraseñas débiles persistirán como una vulnerabilidad crítica.

Finalizando, este trabajo aporta una evaluación de los riesgos actuales y las vulnerabilidades de los protocolos de comunicación en hogares inteligentes. Brindando un mapeo de soluciones de seguridad emergentes para Zigbee, Z-Wave y Wi-Fi y sentando las bases para continuar avanzando hacia entornos domóticos residenciales confiables y seguros.

5.1. Trabajos Futuros

Investigar técnicas eficientes de actualización remota de firmware en dispositivos IoT con recursos limitados. Esta investigación facilitaría la aplicación de parches de seguridad y actualizaciones críticas de manera oportuna, ayudando a mitigar vulnerabilidades y mantener la seguridad de los dispositivos a lo largo del tiempo.

También sería de interés el análisis de seguridad de protocolos emergentes como Thread y Alexa Smart Home. Asimismo, se puede realizar un estudio del impacto del cifrado y la autenticación en el rendimiento de redes inalámbricas domóticas.

Otra área de investigación prometedora es el perfeccionamiento del uso de aprendizaje automático para la detección de anomalías y amenazas en entornos IoT. Mejorar la capacidad de detección de amenazas ayudaría a prevenir y responder de manera más efectiva a posibles ataques cibernéticos en dispositivos y redes domésticas.

Finalmente, se sugiere explorar el potencial de técnicas criptográficas integradas en los dispositivos domóticos, para mejorar la confidencialidad, integridad y autenticación en protocolos de comunicación para la domótica.

Referencias bibliográficas

Akestoridis, D.-G., Harishankar, M., Weber, M., & Tague, P. (2020, julio 21). Zigator: Analyzing the security of zigbee-enabled smart homes. *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*.

Bani Yassein, M., Mardini, W., y Almasri, T. (2018, junio). Evaluation of security regarding Z-Wave wireless protocol. *Jordan University of Science and Technology.* doi.org/10.1145/3234698.3234730

Cabrera, K. M., y Pérez, S. M. (2019). *Ampliación de cobertura Wi-Fi para un ambiente domótico*. (Disertación Doctoral, Universidad Andrés Bello).

Domínguez, H. M., y Vacas, F. S. (2006, junio). Domótica: un enfoque sociotécnico. *E.T.S.I. de Telecomunicación (UPM) eBooks.* oa.upm.es/25581/

Dorai, G., Williams, E. A., Chi, H., y Alo, R. A. (2020, octubre 13). "Is your Smart Home a Secure Home?" - Analysis of Smart Home Breaches and an Approach for Vulnerability Analysis and Device Isolation. *IEEE Access*. doi.org/10.1109/ACCESS.2022.3209355

Flórez de la Colina, M. A. (2004, diciembre 30). Hacia una definición de la domótica. *Informes De La Construcción*, *56*(494), 11–17. doi.org/10.3989/ic.2004.v56.i494.444

HKCERT y el Consejo de Productividad de Hong Kong (HKPC) (2020, abril). IoT Device (Zigbee) Security Study [Estudio de seguridad de dispositivos IoT (Zigbee)].

Kambourakis, G., Kolias, C., Geneiatakis, D., Karopoulos, G., Makrakis, G. M., y Kounelis, I. (2020, abril 6). A State-of-the-Art Review on the Security of Mainstream IoT Wireless PAN Protocol Stacks. *Symmetry*, 12(4), 666. doi.org/10.3390/sym12040666

Khan, N. A., Awang, A., y Abdul Karim, S. A. (2022, octubre 7). Security in Internet of Things: A Review. *IEEE Xplore*. doi.org/10.1109/ACCESS.2022.3209355

Kim, K., Cho, K., Lim, J., Jung, Y. H., Sung, M. S., Kim, S. B., & Kim, H. K. (2020, mayo 5). What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol. *Pervasive and Mobile Computing* (66). doi.org/10.1016/j.pmcj.2020.101211

Kuzlu, M., Pipattanasomporn, M., y Rahman, S. (2015, noviembre 6). Review of Communication Technologies for Smart Homes/Building Applications. *IEEE Innovative Smart Grid Technologies Conference.* ieeexplore.ieee.org/document/7437036

Lei, X., Tu, G.-H., Li, C.-Y., Xie, T., y Zhang, M. (2020). SecWIR: Securing smart home IoT communications via wi-fi routers with embedded intelligence. *18th International Conference on Mobile Systems, Applications, and Services*.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., y Zanella, A. (2019). *IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices.* IEEE Internet of Things Journal, *6*(5), 8182-8201. doi.org/10.1109/jiot.2019.2935189

Mordor Intelligence (2023). Smart Home Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029). www.mordorintelligence.com/industry-reports/global-smart-homes-market-industry

Ojeda-Crespo, L. G. y Cabrera-Mejía, J. B. (2020). Análisis de las estrategias aplicadas en el desarrollo de sistemas domóticos de seguridad. *Dialnet*. dialnet.unirioja.es/servlet/articulo?codigo=7539682

Pecorella, T., Pierucci, L., y Nizzi, F. (2018). "Network Sentiment" Framework to Improve Security and Privacy for Smart Home. *Future Internet*, 10(12), Articulo 120. doi.org/10.3390/fi10120120

Salazar, J. (2016). Redes Inalámbricas. *TechPedia*. techpedia.eu/topic/9

Solis, D. F. (2018, 26 abril). La privacidad de la información generada por dispositivos de domótica en el internet de las cosas. *Universidad de San Carlos de Guatemala*. repositorioslatinoamericanos.uchile.cl/handle/2250/1397688

Statista. (2022, noviembre 7). *Tasa de penetración de los smart homes en el mundo 2017 2025*. es.statista.com/estadisticas/1166176/tasa-de-penetracion-de-los-smart-homes-en-el-mundo/

Tulenkov, A., Parkhomenko, A., Sokolyanskii, A., Stepanenko, A., y Zalyubovskiy, Y. (2018, septiembre 1). The Features of Wireless Technologies Application for Smart House Systems. *IEEE*. ieeexplore.ieee.org/document/8525842

Tushir B., Dalal Y., Dezfouli B. y Liu Y. (2021, abril 15). A Quantitative Study of DDoS and E-DDoS Attacks on Wi-Fi Smart Home Devices. *IEEE Internet of Things Journal* 8(8)

Vida domótica (2023, 12 de junio). *Conectividad, comunicaciones y protocolos en la domótica*. www.vidadomotica.com/conectividad-y-comunicaciones/

Xia, F., Song, H., y Xu, C. (2018, diciembre). Securing the wireless environment of IoT. 2018 *IEEE International Conference of Safety Produce Informatization (IICSPI)*, 315–318.

Zohourian, A., Dadkhah, S., Pinto Neto, E. C., Mahdikhani, H., Kyei Danso, P., Molyneaux, H., y Ghorbani, A. A. (2023). IoT Zigbee device security: A comprehensive review. *Internet of Things*. www.sciencedirect.com/science/article/abs/pii/S2542660523001142