Revisión literaria de aspectos de seguridad asociados al protocolo RPL en redes IEEE 802.15.4.

Oscar Enrique Medina Silva

Trabajo de Grado para Optar el título de Especialista en Telecomunicaciones

Director

Pedro Javier Trujillo Tarazona

Magíster en Informática

Universidad Industrial de Santander

Facultad de Ingenierías Fisicomecánicas

Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones

Especialización en Telecomunicaciones

Bucaramanga

2020

Contenido

Pág.

Lista de Tablas

Pág.

Lista de Figuras

Pág.

Glosario

Ad hoc On-Demand Distance Vector Routing (AODV): El protocolo de enrutamiento AODV está destinado a ser utilizado por nodos móviles en una red ad hoc. Ofrece una rápida adaptación a condiciones de enlace dinámico, bajo procesamiento y sobrecarga de memoria, baja utilización de la red y determina rutas de unidifusión a destinos dentro de la red. (Perkins, Belding-Royer, & Das, 2003)

Advanced Metering Infrastructure (AMI): Sistema integrado de medidores inteligentes, redes de comunicaciones y sistemas de administración de datos que permite la comunicación bidireccional entre los servicios públicos y los clientes. (Hakeem, Hady, & Kim, 2019)

Datagram Transport Layer Security (DTLS): DTLS es un protocolo utilizado para proteger el tráfico de red. Se basa en TLS y se puede usar con datagrama UDP. Por lo tanto, DTLS gestiona la pérdida de paquetes UDP, la reorganización de paquetes al momento de la recepción y opera en tramas más pequeñas. (Rescorla & Modadugu, 2012)

Hypertext Transfer Protocol (HTTP): Protocolo de la capa de aplicación para la transmisión de documentos hipermedia como HTML. Fue diseñado para la comunicación entre los navegadores y servidores web. (Fielding, y otros, 1999)

Intermediate System-to-Intermediate System (IS-IS): Es un protocolo de enrutamiento link-state del tipo IGP que permite una convergencia muy rápida con gran escalabilidad y cuyo uso ha sido generalizado por los proveedores de servicios. (Cisco Systems Inc., 2018)

Open Shortest Path First (OSPF): Es un protocolo de enrutamiento definido en el RFC 2328, de tipo IGP y que es utilizado para distribuir información de enrutamiento dentro de un único sistema autónomo. (Cisco Systems Inc., 2015)

Optimized Link State Routing Protocol version 2 (OLSRv2): OLSRv2 es una optimización del protocolo clásico de enrutamiento link-state y fue desarrollado para redes móviles ad hoc (MANET). Funciona como protocolo proactivo basado en el intercambio regular de tablas de enrutamiento con otros routers que forman parte de la red. (Clausen, Dearlove, Jacquet, & Herberg, 2014)

Routing Information Protocol (RIP): RIP es un protocolo de enrutamiento comúnmente utilizado en redes TCP/IP de pequeño a mediano tamaño. Es estable y usa un algoritmo tipo vector-distancia para calcular rutas. (Cisco Systems Inc., 2018)

Time Slotted Channel Hopping (TSCH): Método de acceso de canal para redes de medios compartidos. Fue diseñado especialmente para las redes de baja potencia y con pérdidas (LLN) y su implementación facilita el ahorro de energía por parte de los nodos y una mayor posibilidad de disponibilidad de uso de canales. (Wu, y otros, 2019)

Acrónimos

AES: Advanced Encryption Standard; Estándar de encriptación avanzado.

AMI: Advanced Metering Infrastructure; Infraestructura de Medición Avanzada.

AODV: Ad hoc On-Demand Distance Vector Routing; Encaminamiento de vector distancia según la demanda y ad hoc.

CC: Consistency Check; Verificación de Consistencia.

CoAP: Constrained Application Protocol; Protocolo de aplicación restringida.

DAO: Object of update to the destination; Objeto de actualización al destino.

DIO: Object of information of the DAG; Objeto de información del DAG.

DIS: Information request DODAG; Solicitud de información del DODAG.

DDoS: Distributed Denial of Service; Ataque de Denegación de Servicio Distribuido.

DODAG: Destination Oriented Directed Acyclic Graph; Grafo acíclico dirigido orientado hacia el destino.

DoS: Denial of Service Attack; Ataque de Denegación de Servicio.

ETX: Expected Transmission Count; Recuento de transmisión esperado.

FFD: Full Function Device; Dispositivo de Funcionalidad Completa.

IDS: Intrusion Detection System; Sistema de detección de intrusos.

IEEE: Institute of Electrical and Electronics Engineers; Instituto de Ingenieros Electricistas y en Electrónica.

IETF: Internet Engineering Task Force; Grupo de Trabajo de Ingeniería de Internet.

IoE: Internet of Everything; Internet del Todo.

IoT: Internet of Things; Internet de las Cosas.

IS-IS: Intermediate System to Intermediate System; Sistema Intermedio – Sistema Intermedio.

ISO: International Organization for Standardization; Organización Internacional de Normalización.

LAN: Local Area Network; Red de Área Local.

LLC: Logical Link Control; Control de enlace lógico.

LLN: Low Power and Lossy Networks; Redes de baja potencia y con pérdidas.

LoWPAN: Low power Wireless Personal Area Network; Red de área personal inalámbrica de baja potencia.

MAC: Media Access Control; Control de Acceso al Medio.

MP2P: Multipoint to Point; Multipunto a punto.

MQTT: Message Queue Telemetry Transport; Transporte de telemetría de mensajes en cola.

M2M: Machine to Machine; Máquina a Máquina.

OF: Objective Function; Función Objetivo.

OF0: Objective Function Zero; Función Objetivo Cero.

OLSRv2: Optimized Link State Routing Protocol Version 2; Protocolo de encaminamiento de estado del enlace optimizado versión 2.

OSPF: Open Shortest Path First; El primer camino abierto más corto.

PAN: Personal Area Network; Red de Área Personal.

PHY: Physical Layer; Capa Física.

P2MP: Point to Multipoint; Punto a multipunto.

P2P: Peer to Peer; Punto a punto.

QoS: Quality of Service; Calidad de Servicio.

RFC: Request for Comments; Petición de comentarios.

RFD: Reduced Function Device; Dispositivo de funcionalidad reducida.

RIFD: Radio Frequency Identification; Identificación por Radiofrecuencia.

RIP: Routing Information Protocol. Protocolo de información del encaminamiento.

ROLL: Routing Over Low Power and Lossy Networks. Encaminamiento en redes LLN (redes de baja potencia y con pérdidas).

RPL: Routing Protocol for Low-Power and Lossy Network; Protocolo de enrutamiento para redes inalámbricas de bajo consumo de energía y susceptibles a pérdidas.

UDP: User Datagram Protocol; Protocolo de datagrama de usuario.

VANET: Vehicular Ad Hoc Network; Red ad hoc vehicular.

WG: Working Group; Grupo de Trabajo.

WPAN: Wireless Personal Area Network; Redes Inalámbricas de Área Personal.

WSN: Wireless Sensor Networks; Redes de sensores inalámbricos.

6BR: 6LoWPAN Border Router. Enrutador de borde en 6LoWPAN.

6LoWPAN: IPv6 over Low-Power Wireless Personal Area Networks; IPv6 en redes de área personal inalámbricas de baja potencia.

Resumen

Título: Revisión literaria de aspectos de seguridad asociados al protocolo RPL en redes IEEE 802.15.4[*]

Autor: Oscar Enrique Medina Silva[**]

Palabras Clave: IoT, LLN, RPL, Seguridad, Ataques

Descripción:
Las redes de baja potencia y con pérdida (LLN) se caracterizan por estar compuestas de una gran cantidad de nodos con recursos limitados. Estos van desde una baja potencia de procesamiento y poca memoria de almacenamiento hasta escasa energía. Dichos dispositivos están interconectados por enlaces con pérdidas que solo admiten bajas velocidades de transferencia y suelen presentar una alta tasa de pérdidas de mensajes.

RPL fue propuesto por IETF como el estándar de enrutamiento IPv6 diseñado para las LLNs. RPL es un protocolo de enrutamiento ligero, proactivo, basado en una topología en forma de árbol, que cuenta con diversos mecanismos y técnicas optimizadas para permitir y facilitar el intercambio de datos entre dispositivos restringidos. Aunque es ampliamente considerado y utilizado por aplicaciones actuales, diferentes estudios han demostrado sus vulnerabilidades de seguridad.

Los ataques contra dispositivos y sensores integrados en aparatos no convencionales dentro de la red, han ido en aumento. Estos pueden incluir: routers, medidores inteligentes, estaciones de energía y hasta marcapasos. A medida que todo se vuelve más inteligente, la cantidad de servicios que podrían ser interrumpidos por malware u otro tipo de virus se torna significativa.

Este trabajo hace una revisión de la documentación referente a la seguridad en RPL y las redes LLN, con el objetivo de identificar y clasificar vulnerabilidades de seguridad, amenazas, ataques y consecuencias a las que está expuesto el protocolo RPL, utilizando como referencia el modelo AIC (Availability, Integrity, Confidenciality). Luego, se destacan soluciones que permitan contrarrestar estas ofensivas.

[*] Trabajo de Grado

[**] Facultad de Ingenierías Fisicomecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Director Pedro Javier Trujillo Tarazona, Mg. en Informática

Abstract

Title: Literary review of security aspects associated with RPL protocol in 802.15.4 IEEE networks[*]

Author: Oscar Enrique Medina Silva[**]

Key Words: IoT, LLNs, RPL, Security, Attacks

Description:
Low power and lossy networks (LLN) are characterized as being composed of a large sum of nodes with limited resources. These range from low processing power, reduced memory storage and scarce energy. These devices are interconnected by links with losses that only support low transfer speeds and yield a high loss message rate.

RPL was proposed by IETF as the IPv6 routing standard designed for LLNs. RPL is a lightweight, proactive routing protocol, based on a tree-shaped topology, which has various mechanisms and techniques optimized to allow and facilitate the exchange of data between constrained devices. Although widely considered and used by current applications, different studies have shown their security vulnerabilities.

Attacks against devices and sensors integrated in unconventional devices within the network have been increasing. These may include: routers, smart meters, power stations and even pacemakers. As everything gets smarter, the amount of services that could be interrupted by malware or another type of virus becomes significant.

This report reviews the documentation related to security in RPL and LLN networks, with the main objective of identifying and classifying the security vulnerabilities, threats, attacks and consequences to which the RPL protocol is exposed, using as reference the AIC model (Availability, Integrity, Confidentiality). Then, solutions that allow counteracting these aggressions are highlighted.

[*] Specialist Thesis
[**] Facultad de Ingenierías Fisicomecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Director Pedro Javier Trujillo Tarazona, Mg. en Informática

Introducción

En una era donde la tecnología se ha convertido en un factor transversal en todos los aspectos de la vida cotidiana, el tema de la ciberseguridad toma especial relevancia. Debido a una diversidad de factores, que van desde la interoperabilidad de tecnologías hasta las limitantes de recursos de sus componentes, el Internet de las Cosas (IoT, “Internet of Things”) representa un conjunto de desafíos para los cuales todavía la industria no tiene procesos totalmente estandarizados, destacando entre ellos los referentes a la seguridad.

Se presenta en este documento una revisión literaria que proporcione una visión de los problemas de seguridad actuales de las redes de baja potencia y pérdidas (LLN) asociados al protocolo RPL; así como también clasificar las amenazas o ataques a los que están expuestos, de acuerdo con los criterios de seguridad del modelo AIC (confidencialidad, integridad y autenticación) que permitan exponer métodos para contrarrestar agresiones.

Este documento se encuentra estructurado en tres partes. En la primera (capítulos 1 al 4) se plantea el problema y su justificación, los antecedentes de la investigación y se cierra con una serie de mapas conceptuales que ilustran los temas a tratar a lo largo de la monografía. En la segunda parte (capítulos 5 al 7), se describen las características generales del IoT, se ilustran: una pila de protocolos para IoT, las redes LLN, el estándar IEEE 802.15.4 y diversas deficiencias en seguridad relativas a RPL. Se finaliza esta segunda parte, con las exposiciones de seguridad que presenta RPL y detalles de los ataques que son capaces de tomar ventajas de estas. Acto seguido y por medio de los principios que integran el modelo de seguridad AIC, se clasifican estas amenazas con

el fin de presentar soluciones relevantes que ayuden a mitigar las agresiones. Y en la última parte (capítulos 8 y 9), se presentan las conclusiones y recomendaciones del trabajo.

1. Objetivos

1.1 Objetivo General

Realizar una revisión literaria de aspectos de seguridad asociados al protocolo RPL en redes IEEE 802.15.4.

1.2 Objetivos Específicos

1. Describir elementos relevantes de las redes de baja potencia y con pérdidas “LLN” (Low-Power and Lossy Network) inalámbricas de tipo IEEE 802.15.4.
2. Enunciar aspectos concernientes a la problemática de seguridad del Internet de las Cosas (IoT: Internet of Things) e Internet de Todo (IoE: Internet of Everything) relativos al protocolo RPL.
3. Explicar las principales características de la estructura y funcionamiento del protocolo de encaminamiento IPv6 para redes con pérdida y baja potencia “RPL” (IPv6 Routing Protocol for Low-Power and Lossy Networks, IETF RFC 6550).
4. Identificar escenarios de aplicación del protocolo RPL en redes de baja potencia y con pérdidas “LLN” en redes inalámbricas IEEE 802.15.4.
5. Clasificar las amenazas, ataques y deficiencias de seguridad a las cuales está expuesto el protocolo RPL utilizando como referencia el modelo AIC (Availability, Integrity, Confidenciality).
6. Exponer casos de problemas y soluciones de seguridad alrededor del uso del protocolo RPL en redes IEEE 802.15.4.

2. Planteamiento del Problema

Los dispositivos que integran el Internet de las Cosas (IoT) forman parte de la vida cotidiana y como conglomerado se encargan principalmente de enlazar los datos del mundo real con el mundo virtual, permitiendo así conectividad en cualquier momento y desde cualquier lugar para procesos pertinentes a los sectores de la salud, energía, agricultura, automotriz, seguridad, manufactura, servicios, entre muchas otras áreas. La popularidad que ha generado el IoT en la actualidad ha contribuido con nuevos desarrollos tecnológicos, entre cuales se destaca el despliegue a gran escala de redes de baja potencia y con pérdidas (LLNs).

Las redes LLN permiten interconectar una gran cantidad de dispositivos con recursos limitados en tamaño, almacenamiento, procesamiento y energía; formando una red inalámbrica tipo malla, útil para una amplia gama de aplicaciones. En lo que respecta a la conexión a Internet, varios enrutadores de borde sirven como puertas de enlace entre redes y la nube. El estándar IEEE 802.15.4-2011 se aplica en este tipo de redes, y define las capas física y de enlace a usar en redes inalámbricas de baja velocidad (IETF, 2018). De otra parte, el protocolo 6LowPAN define los mecanismos de encapsulación y compresión de encabezado entre IPv6 y tramas de redes IEEE 802.15.4 para poder manejar mensajes de gran tamaño.

El protocolo de encaminamiento para redes de baja potencia y con pérdidas (RPL) fue implementado en la capa de enrutamiento basada en IPv6 (Winter, y otros, 2012). RPL proporciona un mecanismo para propagar información a través de la topología de red formada dinámicamente. Dicho proceso permite una configuración mínima en los nodos, lo que hace que estos funcionen en su mayoría de forma autónoma (Tsao, y otros, 2015).

A pesar de las funcionalidades y ventajas que RPL ofrece, también se debe destacar que este protocolo es vulnerable a una serie de ataques. Diversas razones, entre las que se destacan la escasa energía y las limitaciones de procesamiento de los dispositivos IoT, hacen inviable la implementación de métodos criptográficos tradicionales para la protección contra ataques de enrutamiento. Por lo tanto, los desafíos de seguridad con respecto a los datos, privacidad, confidencialidad, identificación y el control de acceso son pertinentes.

Teniendo en cuenta lo anteriormente mencionado y basándose en varios aspectos como:

1. La vigencia del tema de la ciberseguridad en la actualidad debido a la creciente dependencia por parte de la sociedad de los sistemas informáticos, redes inalámbricas y el Internet.
2. El impulso que podría tener la paulatina adopción de IPv6 con las proyecciones de aumento exponencial de los dispositivos inteligentes y equipos IoT en general.
3. El análisis en estudios previos de varios de los ataques más relevantes sobre el protocolo RPL como Sinkhole, Wormhole, Sybil, Blackhole, entre otros.
4. La relevancia de las LLNs como una de las áreas de investigación más interesantes de los últimos años, así como el rol vital que juega el enrutamiento dentro de la arquitectura general del Internet de las cosas (IoT).

Por consiguiente, se plantea esta revisión literaria de los aspectos de seguridad asociados al protocolo RPL en redes IEEE 802.15.4, La cual busca identificar vulnerabilidades y categorizar los diversos ataques contra el protocolo RPL, además de explicar como suelen ocurrir dichas irrupciones y las prevenciones existentes.

3. Justificación

Según datos de la empresa estadounidense Gartner Inc., una de las principales compañías encargadas de consultoría e investigación de tecnologías de la información, se conectan 5.5 millones de “cosas” a Internet cada día (Bhardwaj, 2017) y de acuerdo a Cisco Systems Inc., organización pionera en la rama de las telecomunicaciones, se espera un aproximado de 26.300 millones de dispositivos conectados para finales del 2020, siendo el IoT uno de los principales responsables de la acelerada expansión. (Cisco Systems Inc., 2018)

Estos cálculos cimientan la presencia importante que tendrá el Internet de las Cosas en el futuro cercano, pero más allá de las grandes potencialidades, su penetración en todos los ámbitos también conlleva riesgos significativos en materia de seguridad.

Dichas vulnerabilidades ya han quedado demostradas tras varios ciberataques, los cuales no han pasado desapercibidos en esta era digital. Dentro de los casos más destacados se encuentran:

1. El BrickerBot malware, que con en su más reciente versión (BrickerBot.3) descubierta en abril de 2017, realizó 1295 ataques permanentes de negación de servicio (PDoS) durante 15 horas dejando inservibles miles de dispositivos IoT. (Goodin, 2017)
2. El ataque distribuido de denegación de servicio (DDoS) más grande hasta ahora, realizado por una Mirai botnet que paralizó a uno de los mayores proveedores de DNS (Dyn) en octubre de 2016. (Ducklin, 2016)

En lo que respecta a las áreas donde las LLNs tienen mayor presencia, como por ejemplo la domótica y las redes de sensores inalámbricos, RPL se muestra expuesto a una gran variedad de ataques simplemente por el hecho de ser menos robusto que el resto de los protocolos de enrutamiento tradicionales y debido a las mismas limitaciones (procesamiento, energía, memoria, altas tasas de pérdidas, bajo rendimiento) que por naturaleza presentan las redes de tipo 802.15.4 en donde se ejecuta.

Si bien es cierto que ya existe literatura en la que se ha registrado estudios referentes a las amenazas de seguridad que está propenso el protocolo RPL, se debe acotar que con la dinámica del mundo actual y mayor cantidad de dispositivos dependientes de conexión a una Internet insegura, estos peligros crecen exponencialmente cada día, creando la necesidad de mantenerse actualizado en el ámbito. De allí que se requiera revisar la documentación concerniente a las redes IEEE 802.15.4 y el protocolo RPL, con el fin de desarrollar un trabajo en el cual se puedan plasmar conceptos alineados a las recientes tendencias en materia de seguridad.

4. Antecedentes y Marco Conceptual

4.1 Antecedentes de la Investigación

Luego de realizar una búsqueda temática referente a las redes de baja potencia y con pérdidas (LLN) así como también del protocolo de encaminamiento RPL en los catálogos de la biblioteca

de la Universidad Industrial de Santander y de otras universidades de Colombia, se encontraron trabajos que abordaron temas afines que sirven como referencia al desarrollado en esta monografía.

En un trabajo perteneciente a Piñeres (2015) se efectuó la: "*Evaluación del rendimiento del protocolo 6LowPAN sobre una plataforma de hardware y software libre*". Este se centra en el estudio del rendimiento del direccionamiento IPv6 a través del protocolo 6LowPAN mediante la realización de pruebas sobre plataformas de hardware y software libre bajo escenarios con uno o dos nodos conectados a un sumidero que permitió evaluar el tiempo de transmisión de paquetes con enrutamientos estáticos y dinámicos (p.2).

En un segundo trabajo, Calderón (2014), realizó el: "*Diseño e implementación de un sistema genérico de monitoreo usando redes de sensores inalámbricos con el protocolo LowPAN*". En este trabajo de grado se presentó la implementación de una red de sensores inalámbricos usando los protocolos 6LowPAN y RPL con el fin de obtener un sistema de monitoreo que tenga la posibilidad de adaptar diferentes tipos de sensores a diferentes tipos de ambientes por medir (p.1).

El tercer trabajo referenciado se llama "A survey: Attacks on RPL and 6LowPAN in IoT". Este artículo se centra en los posibles ataques a RPL y redes 6LowPAN, las consecuencias que generan los mismos y los métodos que se pueden aplicar para contrarrestarlos (Pongle & Chavan, 2018).

Un cuarto trabajo denominado "Survey on RPL enhancements: A focus on topology, security and mobility", es un artículo científico en el cual se revisan los trabajos recientes sobre RPL y destaca las principales contribuciones a su mejora, especialmente las relacionadas con la optimización de la topología, la seguridad y la movilidad. (Kamgueu, Nataf, & Djotio, 2018)

El quinto trabajo lleva por título "Security Vulnerabilities and Countermeasures in the RPL-Based Internet of Things", en este se estudian las vulnerabilidades del protocolo RPL y el impacto

de ciertos ataques con el fin de proponer acciones que puedan limitarlos. (Yang, Wang, Lai, Wan, & Cheng, 2018)

Por último, en el artículo “Securing the Internet of Things: Challenges, threats and solutions”, se proporciona un análisis de seguridad integral del IoT por medio de la evaluación de posibles amenazas y soluciones que ayuden a mitigarlas. (Panagiotis, Panagiotis, & Ioannis, 2018)

4.2 Marco Conceptual

Basado en la vigencia de las tecnologías del Internet de las cosas y las problemáticas de seguridad vinculadas con la implementación de ellas, por medio de esta monografía se plantea una revisión literaria de los aspectos de seguridad asociados a RPL en redes IEEE 802.15.4. Para ello, se hace necesario abordar en primer lugar la actualidad del IoT, los fundamentos que han impulsado su avance en diversos sectores, los protocolos en los que se basa y los retos que aún tienen por enfrentar. Uno de estos desafíos yace en el área de la seguridad, la cual por diferentes razones carece de la fiabilidad que amerita.

Como ya se ha mencionado anteriormente, el enfoque de este trabajo va dirigido a las falencias con las que cuenta el protocolo de enrutamiento RPL, cuya concepción giró en torno de las redes de baja potencia y perdida (LLN). Por esta razón, se dedican partes de varios capítulos para describir temas relacionados a las LLNs como el standard IEEE 802.15.4, sus características, funciones e importancia dentro del IoT.

En lo que respecta a RPL, en primera instancia se explican sus componentes, estructura, características, funcionamiento y campos de aplicación para luego dar paso al capítulo centrado en sus vulnerabilidades. Allí, se usa como referencia el modelo de seguridad AIC para ampliar los

criterios de seguridad que se deben tener en cuenta en todo sistema y clasificar los ataques y amenazas a los que está expuesto RPL. Por último, se describen soluciones de seguridad que van desde las básicas proporcionadas por el mismo protocolo, como los modos de seguridad, hasta sistemas de detección de intrusos (IDS) desarrollados para que en la mayoría de los casos ayuden a mitigar las agresiones.

A continuación, se presentan una serie de mapas conceptuales en los cuales se despliegan temas, subtemas y sus relaciones con el objeto de exponer una visión macro que ilustre los tópicos abordados a lo largo del trabajo.

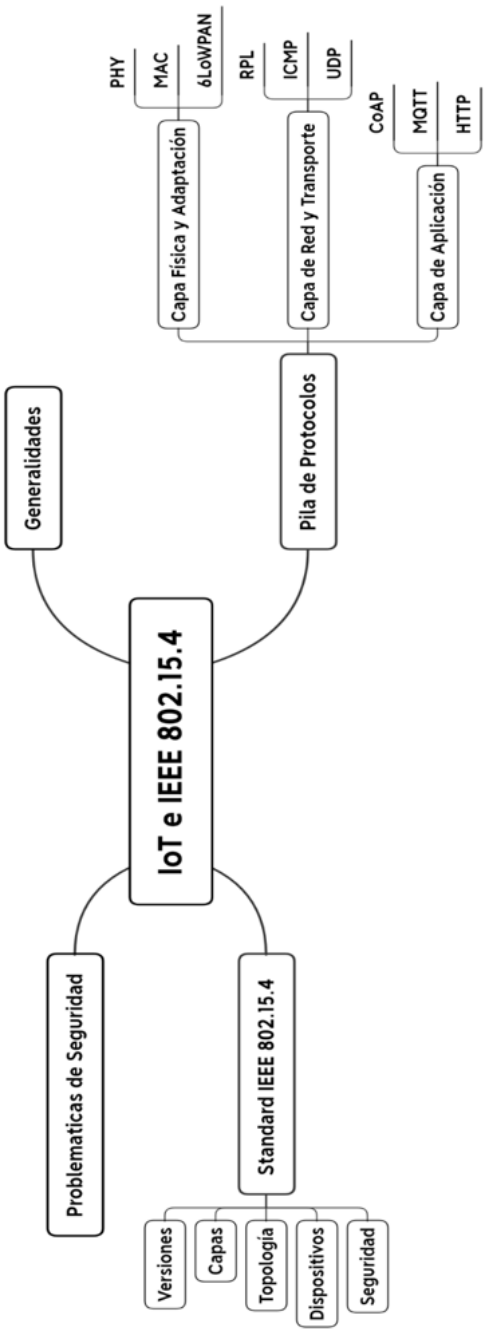

Figura 1. Mapa Conceptual General IoT e IEEE 802.15.4. Adaptado de Ashwini y Mohnami, (2015), Kivinen y Kinney, (2017), Panagiotis et al., (2018), Sebastian y Sivagurunathan, (2018) y Sharma y Gondhi, (2018).

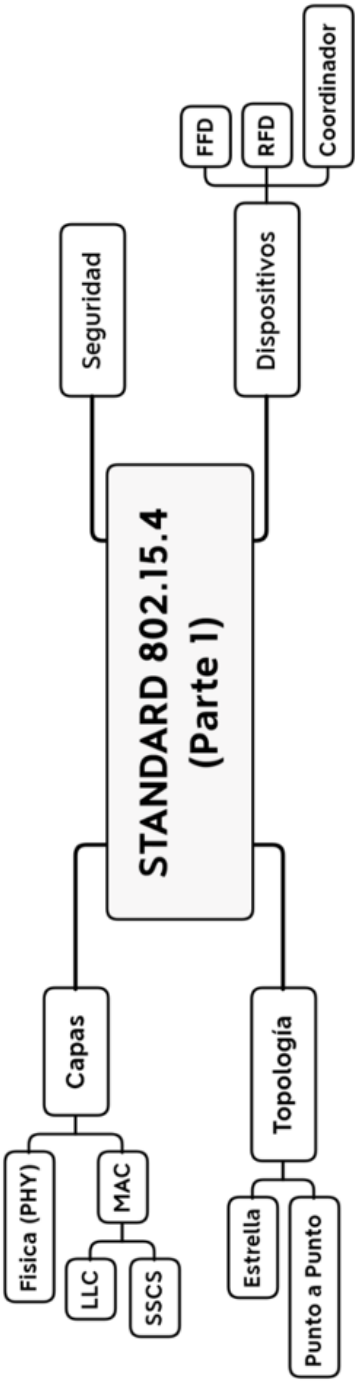

Figura 2. Mapa Conceptual Standard 802.15.4. Parte 1. Adaptado de Amin y Hamid, (2015), Kivinen y Kinney, (2017), Madan et al., (2014) y Panagiotis et al., (2018).

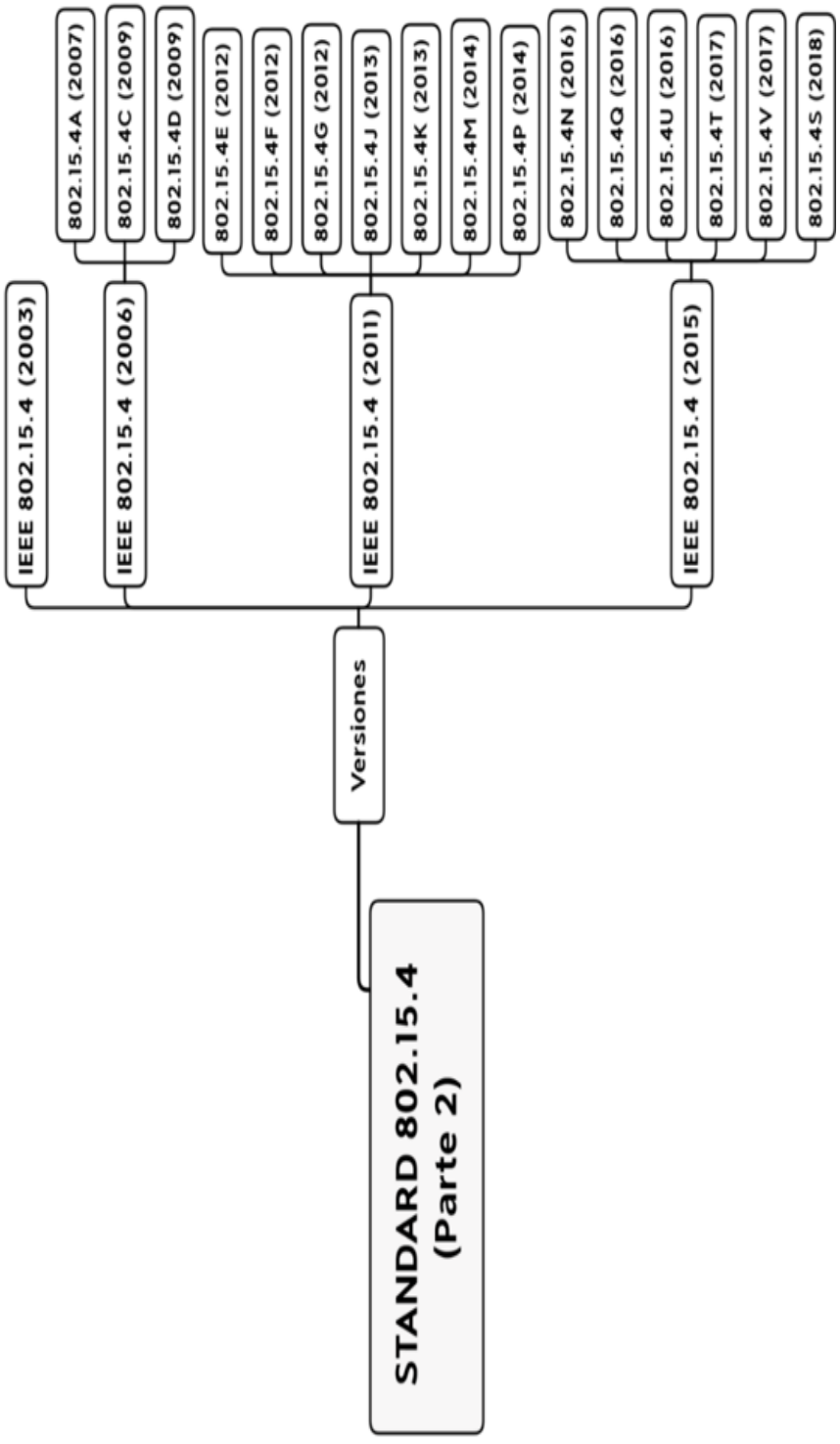

Figura 3. Mapa Conceptual Standard 802.15.4. Parte 2. Adaptado de Ramonet y Noguchi, (2019).

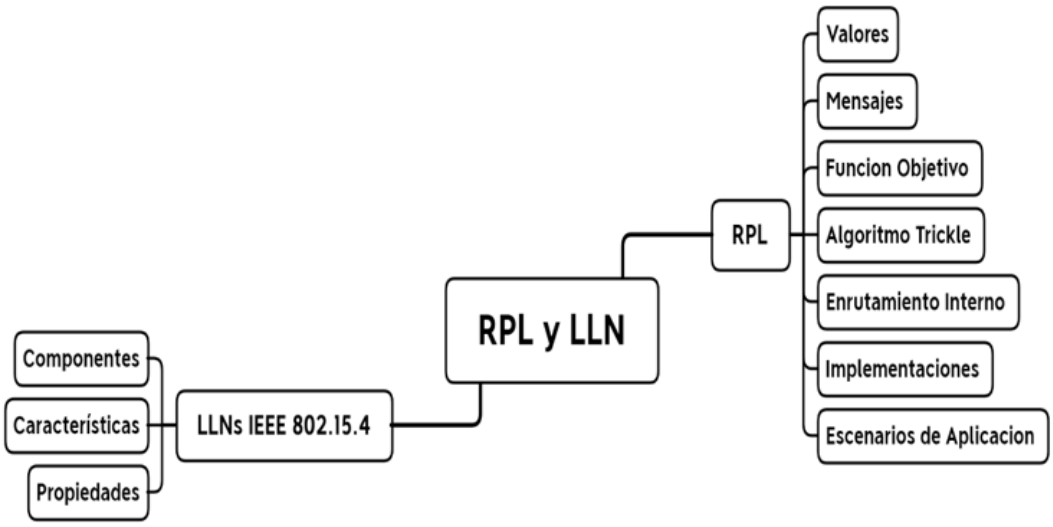

Figura 4. Mapa Conceptual General RPL y LLN. Adaptado de Gaddour y Koubaa, (2018), Perera et al., (2013), Robles, (2018) y Winter et al., (2012).

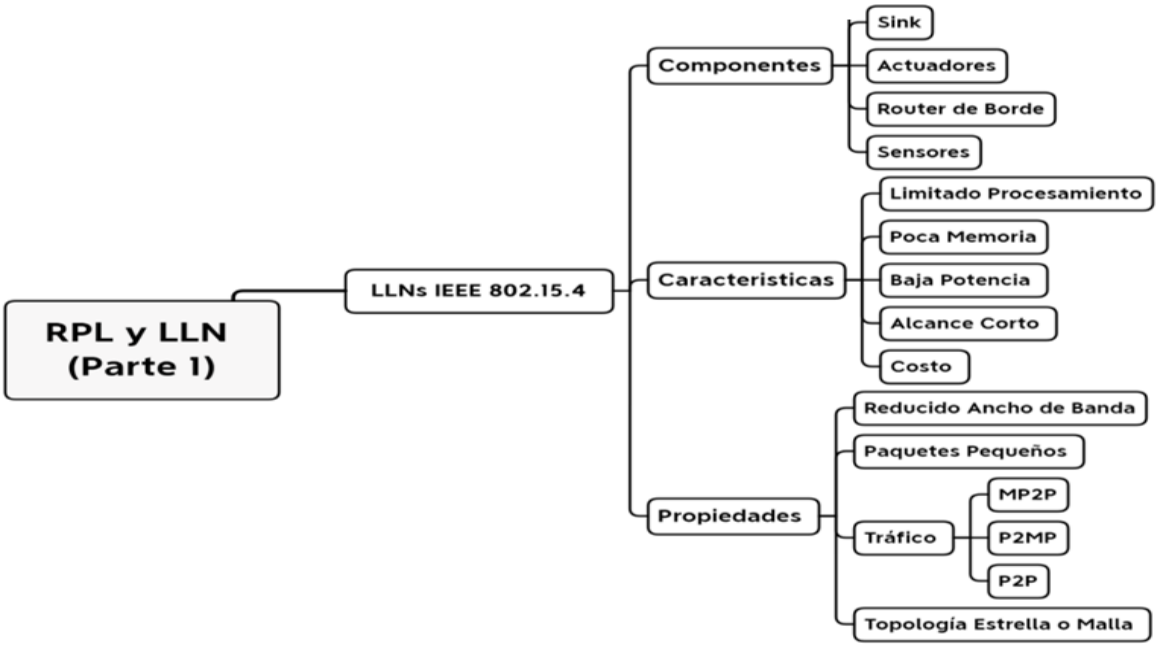

Figura 5. Mapa Conceptual LLNs IEEE 802.15.4. Adaptado de IEEE, (2003), IEEE, (2011) y Kushalnagar, (2007).

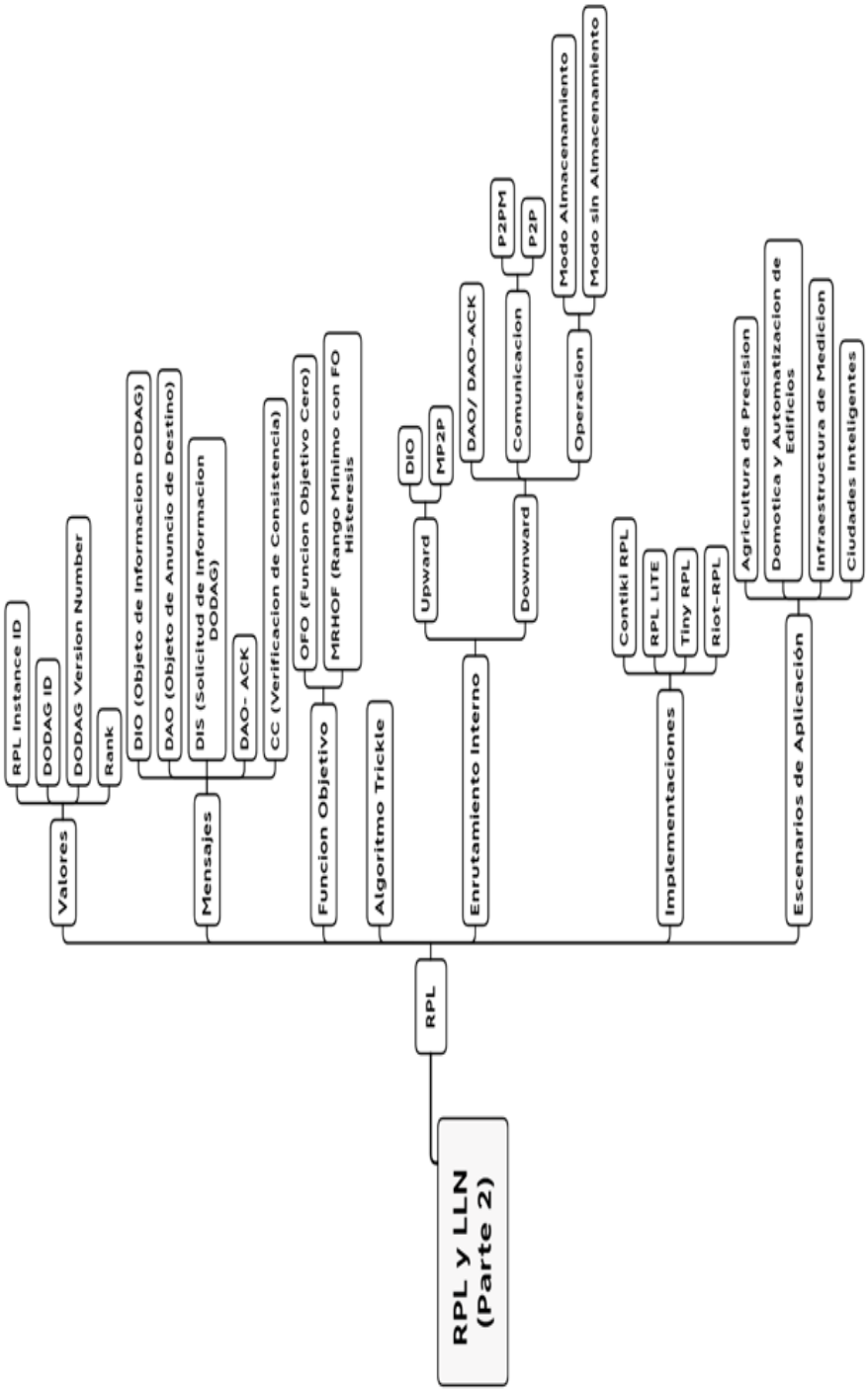

Figura 6. Mapa Conceptual RPL. Adaptado de Arena et al., (2019), Gaddour y Koubaa, (2018), Kamgueu et al., (2018), Levis et al., (2011), Thubert, (2012) y Winter et al., (2012).

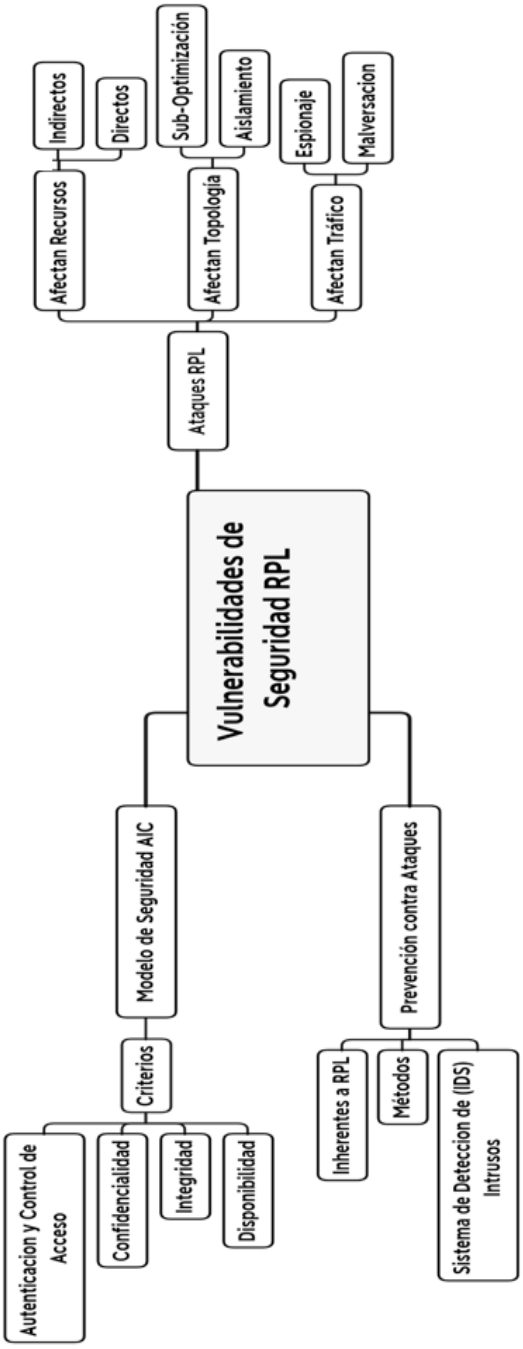

Figura 7. Mapa Conceptual Vulnerabilidades de Seguridad RPL. Adaptado de International Organization for Standardization, (2000), Mangelkar et al., (2018), Mayzaud et al., (2016), Razali et al., (2017) y Tsao et al., (2015).

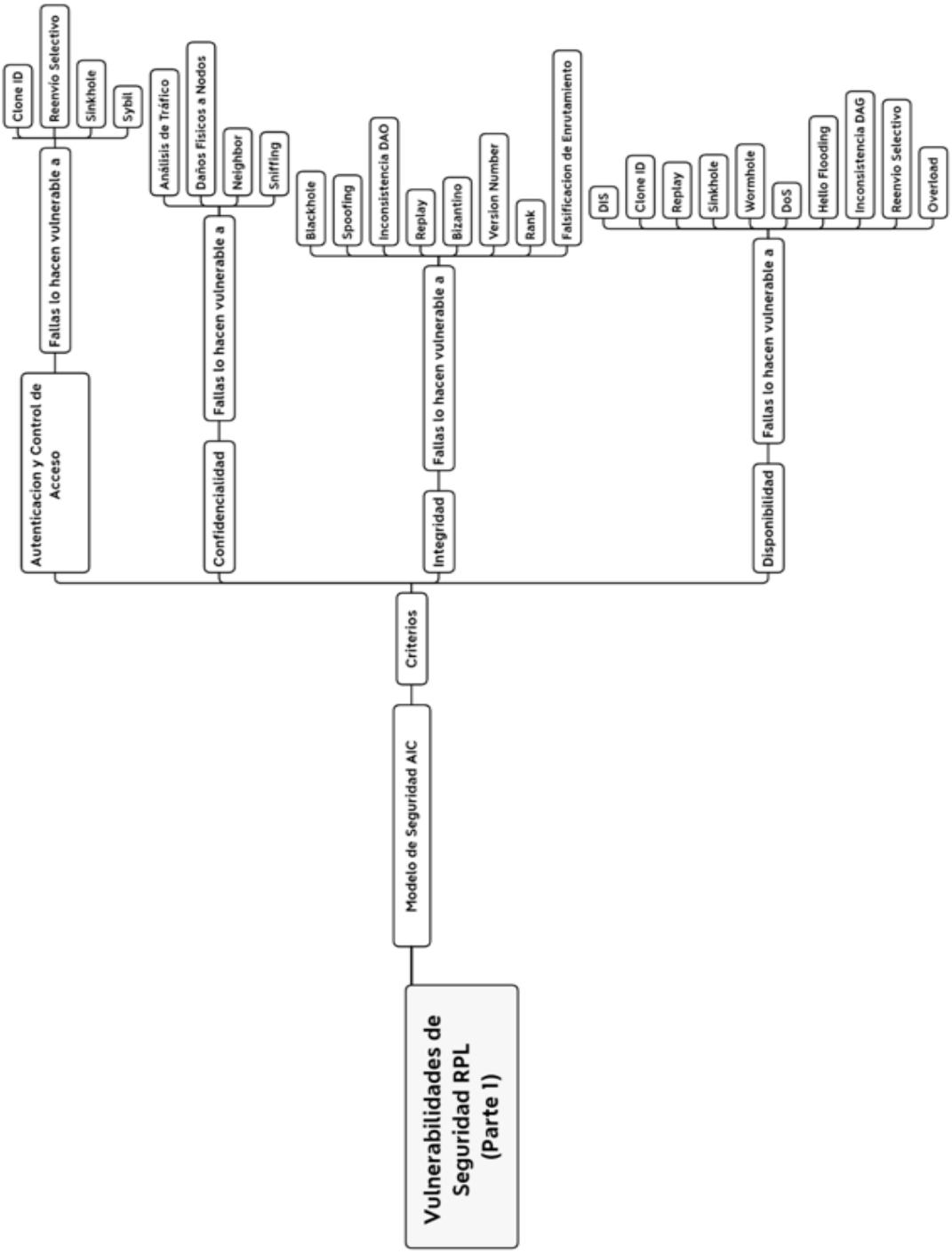

Figura 8. Mapa Conceptual de Seguridad AIC. Adaptado de Dohler et al., (2009), International Organization for Standardization, (2000) y Mangelkar et al., (2018).

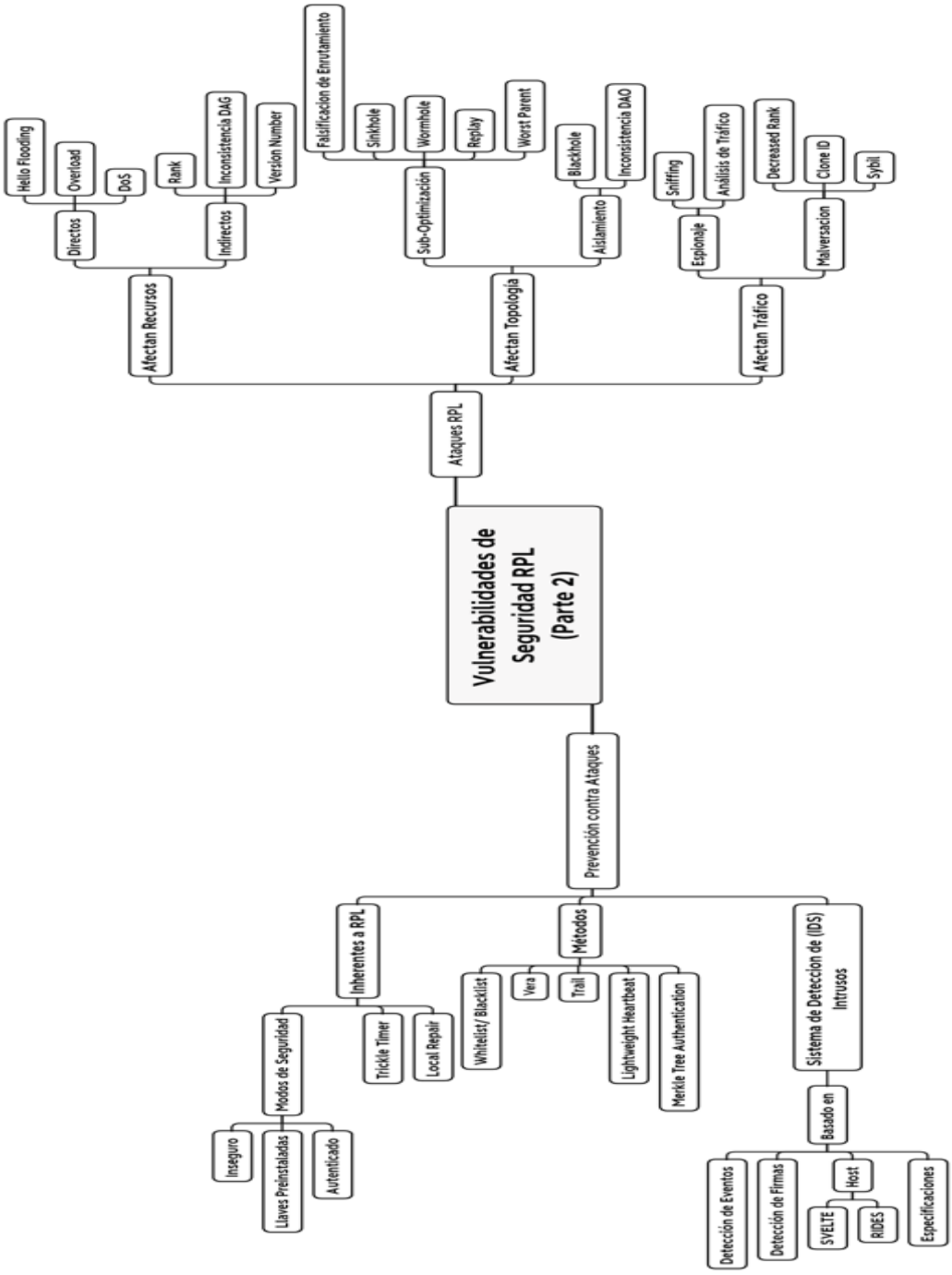

Figura 9. Mapa Conceptual Ataques RPL y Mecanismos de Prevención. Adaptado de Mayzaud et al., (2016), Pongle y Chavan, (2018), Razali et al., (2017), Tsao et al., (2015) y Wallgren et al., (2013).

5. Internet de las Cosas (IoT) e IEEE 802.15.4

5.1 Generalidades

A través de los años el término “Internet de las Cosas” (IoT) ha significado una variedad de conceptos. Sus orígenes se remontan a varias décadas atrás y su evolución ha demostrado que este principio en el cual convergen diversas tecnologías paso de ser una propuesta a convertirse en una realidad palpable.

Basta con regresar a mediados de los años 90 para reseñar un hecho significativo que empezó a pavimentar su camino. En ese tiempo la empresa Siemens conformo una división que se dedicó exclusivamente a desarrollar un módulo de datos GSM para aplicaciones industriales machine-to-machine (M2M), esto con el fin de permitir que las máquinas pudieran comunicarse a través de redes inalámbricas. (Press, 2014)

Luego, al darse la transición de redes dedicadas y propietarias, como la descrita anteriormente, a las redes basadas en el protocolo de Internet (IP), la integración de dispositivos en línea fue ganando popularidad. Esto llego al punto que el amplio alcance de sus funcionalidades dio pie al avance de nuevas áreas de investigación dedicadas a los objetos inteligentes.

El Internet de las cosas (IoT) formalmente se define como la interconexión de máquinas, dispositivos y personas a través de Internet, lo que permite generación de datos que pueden proporcionar información analítica y respaldar nuevas operaciones (Ashwini & Mohnami, 2015).

El IoT comprende múltiples tecnologías y capacidades que dependen de sensores inalámbricos, comunicaciones, redes, la nube, almacenamiento, actuadores, etc.

Desde una perspectiva más amplia, la confluencia de diferentes tendencias tecnológicas y de mercado han permitido propulsar paulatinamente la adopción e implementación de proyectos basados en el IoT, Ibarra et al., (2017) destaca: la adopción generalizada del protocolo IP, el progreso en el análisis de datos, la miniaturización de componentes, la mejora en las comunicaciones y el surgimiento de la computación en la nube. (Gilchrist, 2017)

El uso de dispositivos pertenecientes al Internet de las cosas ha aumentado sustancialmente en los últimos años y las proyecciones indican que el número continuará creciendo significativamente. En este entorno de rápida adopción tecnológica, el enfoque inclusivo y colaborativo es esencial para enfrentar los desafíos y aprovechar las oportunidades que surgen.

Las implementaciones del IoT utilizan diferentes modelos de conectividad, cada uno de estos poseen características que se adaptan a plenitud de escenarios, brindando así ventajas y flexibilidad según sea el caso. De acuerdo a Rose et al. (2015), "*los cuatro modelos de conectividad descritos por la Junta de Arquitectura de Internet (IAB) incluyen: device-to-device (dispositivo a dispositivo), device-to-cloud (dispositivo a la nube), device-to-gateway (dispositivo a puerta de enlace) y back-end data-sharing (intercambio de datos a través del back-end)*".

El IoT está compuesto por redes de baja potencia y pérdida (LLN), las cuales tienen la capacidad de proporcionar conectividad inalámbrica con una infraestructura limitada en características técnicas. Estas pueden tener un tamaño que va desde una docena hasta miles de sensores y enrutadores. Ejemplos de LLNs incluyen redes inalámbricas de sensores (WSN) y redes inalámbricas de área personal (WPAN).

Figura 10. Entornos para aplicaciones IoT. Adaptado de Rose et al. (2015). La Internet de las Cosas – Una breve reseña. *The Internet Society (ISOC)*,16-17. https://www.internetsociety.org/es/resources/doc/2015/iot-overview

Debido a la complejidad y limitaciones de dichas redes, la IETF ideó un protocolo de enrutamiento que se ajuste a los requerimientos específicos además de ser útil para otras aplicaciones dentro del entorno IoT, conocido como RPL (protocolo de enrutamiento para redes de baja potencia y con pérdida) (Robles, 2018). RPL se caracteriza por un enrutamiento proactivo y utiliza mensajes de control para estructurar una topología en forma de árbol, la cual cuenta con un nodo raíz que funciona como una especie de puerta de enlace y las hojas que están representadas por los nodos sensores.

En las siguientes secciones se describirá de manera más detallada la pila de protocolos que giran en torno a RPL y al IoT en general, el estándar que rige las redes de baja potencia y con pérdidas, así como también las problemáticas asociadas a los aspectos de seguridad en el Internet de las cosas.

5.2 Pila de protocolos para IoT alrededor RPL

En un sentido amplio, la arquitectura del Internet de las cosas consta de tres capas: capa física, capa de red y capa de aplicación (Sharma & Gondhi, 2018). La capa física o de detección, cuenta con sensores, actuadores, etiquetas RFID, medidores inteligentes y otros dispositivos de detección. Estos equipos perciben los parámetros físicos como temperatura, presión y humedad, e informan los datos al nivel superior.

En la capa de red, se ejecutan funciones como el enrutamiento optimizado y encapsulamiento. Por medio de la primera, se maneja la transferencia de paquetes desde el origen al destino, y a través de la segunda se encapsulan datagramas IPv6 para que sean procesados por la capa inferior. En lo que respecta a la capa de aplicación, en ella se proporcionan servicios al garantizar interacciones efectivas entre el usuario y los dispositivos IoT de recursos limitados y bajo consumo de energía. Cabe destacar que, en caso de tomar un enfoque más detallado de la arquitectura, se deben incluir capas alineadas de manera vertical que atraviesen otros niveles representando funciones como gestión de identidades o seguridad de datos.

Del mismo modo, la arquitectura del IoT basada en RPL también se puede explicar en tres capas, como se puede observar en la *Figura 3*. En la capa física y MAC, IEEE 802.15.4 por medio de sus niveles gestiona las operaciones físicas y de enlace de datos, mientras que 6LoWPAN hace labores de interconexión.

Siendo más específicos, el estándar IEEE 802.15.4 define las capas PHY y MAC, en donde la primera tiene como objetivo principal la transmisión y recepción de paquetes a través del medio físico, y la segunda, controla el acceso al canal de comunicación al tiempo que proporciona control de flujo por medio de acuse de recibos y retransmisiones (Amin & Hamid, 2015). Por su parte,

6LoWPAN (IPv6 de baja potencia WPAN) funciona dentro de la estructura como una capa de adaptación que utiliza mecanismos de compresión, fragmentación y encapsulación para transmitir los paquetes IPv6 modificados en la subcapa MAC. (Raza, Duquennoy, Hoglund, & Roedig, 2014)

En la capa de red y transporte, los protocolos RPL, ICMP, UDP gestionan las funciones de enrutamiento y transferencia. RPL (protocolo de enrutamiento IPv6 para redes de baja potencia y con pérdidas) fue diseñado específicamente para redes con recursos limitados, por lo que es el encargado de todas las labores de encaminamiento. Este es capaz de adaptarse a cambios topológicos, construir rutas rápidamente y transmitir la información de enrutamiento entre los nodos con una sobrecarga mínima (Gawade & Shekokar, 2017). Por su parte, ICMP (protocolo de control de mensaje de Internet) maneja el envío de mensajes con información de control, diagnóstico o respuesta a un error ocurrido.

En lo que respecta al transporte, UDP (User Datagram Protocol) está orientado a transacciones y proporciona un procedimiento para que las aplicaciones establezcan sesiones y se comuniquen por medio de mensajes de manera ligera con un mínimo de sobrecarga (Masirap, Amaran, Yusoff, Rahman, & Hashim, 2016). Además, ofrece multiplexación de aplicaciones por medio del uso de puertos.

Finalmente, en la capa de aplicación, se ejecutan las funciones de los protocolos HTTP, CoAP y MQTT. El protocolo de aplicación restringida (CoAP) se enfoca en las labores de transferencia web basado en el modelo cliente / servidor y fue diseñado con el propósito de ser usado en redes con dispositivos de recursos limitados. Es simple, ligero, soporta multidifusión y puede traducir fácilmente a HTTP. (Bormann, Castellani, & Shelby, 2012)

Por otro lado, MQTT (Message Queue Telemetry Protocol), es un protocolo de mensajería con soporte para la comunicación asíncrona entre los pares y que utiliza un modelo de publicación y

suscripción (Andy, Rahardjo, & Hanindhito, 2017). Es liviano, consume poca energía y minimiza los paquetes de datos, por lo cual es eficiente en implementaciones con dispositivos altamente restringidos.

En general, todos los protocolos de comunicación están diseñados para satisfacer las demandas de IoT de baja potencia, baja información, poca memoria y baja capacidad de procesamiento.

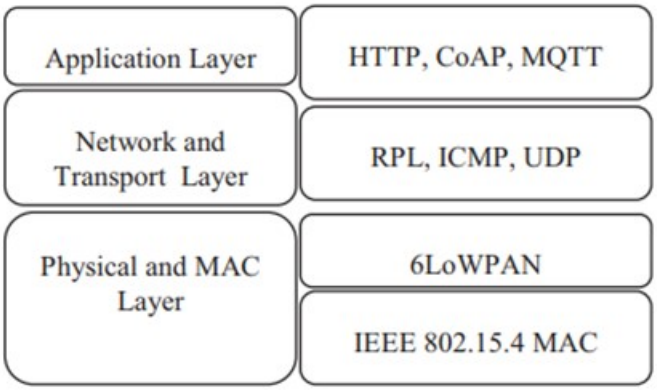

Figura 11. Arquitectura RPL en IoT. Adaptado de Sebastian y Sivagurunathan (2018), Multi DODAGs in RPL for Reliable Smart City IoT. *Journal of Cyber Security, 7*(1), 69-86. https://doi.org/10.13052/jcsm2245-1439.716

5.3 Estándar IEEE 802.15.4.

El estándar IEEE 802.15.4 especifica la capa física de comunicación y la del control de acceso al medio para redes inalámbrica con baja tasa de transferencia, enfocado a redes de área personal WPAN (Kivinen & Kinney, 2017). Está soportado por el grupo de trabajo IEEE 802.15 y su primera versión fue lanzada en 2003. Este define una interfaz inalámbrica para aplicaciones con

sistemas embebidos, proporciona comunicación ubicua de bajo costo con poca infraestructura subyacente, velocidades entre dispositivos altamente integrados y soporta varias topologías.

Entre las características generales más relevantes de IEEE 802.15.4 se pueden mencionar: comunicaciones con un rango de distancias entre 10 y 100 metros aproximadamente, velocidades máximas de transferencia de datos de 250 kbps, esquema de cifrado tipo AES para la seguridad e implementación del protocolo CSMA-CA para el control de acceso al medio.

El estándar IEEE 802.15.4 ha tenido varias versiones a través de los años y la mayoría de estas a su vez han sido complementadas con ciertas adiciones, por ejemplo, el estándar incluye una amplia colección de opciones de capa física y mejoras en la capa MAC que no están disponibles en todas las revisiones (Ramonet & Noguchi, 2019). Seguidamente, en la tabla 1 se presenta un compendio evolutivo del estándar.

Tabla 1.

Versiones y adendas del estándar IEEE 802.15.4.

Versión	**Detalles**
802.15.4 - 2003	Versión original del estándar IEEE 802.15.4. Incluyó dos capas PHY diferentes: una para las bandas con frecuencias más bajas de 868 y 915 MHz, y la otra para 2.4 GHz.
802.15.4 - 2006	La versión 2006 del estándar proporcionó un aumento en las velocidades de datos alcanzables por parte de las bandas con frecuencia más bajas. Se actualizó la capa PHY para las franjas 868 y 915 MHz, y se definieron cuatro nuevos esquemas de modulación.
802.15.4a (2007) - Adenda1	Esta versión definió dos capas PHY nuevas: una usaba tecnología UWB y el otro preveía el uso del espectro extendido chirp (CSS) a 2.4 GHz.

Tabla 1. *(Continuación)*

Versión	Detalles
802.15.4c (2009) - Adenda 2	Actualizaciones para 2.4 GHz, 868 MHz y 915 MHz, UWB y la banda china 779-787 MHz.
802.15.4d (2009) - Adenda 3	Actualizaciones para 2.4 GHz, 868 MHz, 915 MHz y la banda japonesa 950 - 956 MHz.
802.15.4 – 2011	En esta versión de 2011, el estándar eliminó el concepto de subcapa de convergencia específica de servicio (SSCS) y en su lugar se centra exclusivamente en temas de capa PHY y MAC. Debido a la falta de una capa MAC flexible a este punto, la revisión de 2011 dio origen a numerosas propuestas alternativas de capa MAC que satisfacen los requisitos de diferentes tipos de aplicaciones.
802.15.4e (2012) - Adenda 1	Esta versión define mejoras en la capa MAC en apoyo de la aplicación ISA SP100.11a.
802.15.4f (2012) - Adenda 2	Este complemento define nuevas capas PHY para UWB, banda de 2.4 GHz y también 433 MHz
802.15.4g (2012) - Adenda 3	Esto complemento define nuevas capas PHY para redes neighbourhood inteligentes, abarcando así la inclusión de aplicaciones para Smart Grid.
802.15.4j (2013) - Adenda 4	Presenta una sola capa PHY para la banda de 2380 MHz con una velocidad máxima de 250 kb/s. Su uso está restringido a la transmisión de datos (sin voz) en dispositivos para monitoreo, diagnóstico y tratamiento de pacientes.

Tabla 1. *(Continuación)*

Versión	Detalles
802.15.4k (2013) - Adenda 5	Esta enmienda agregó dos capas PHY más: una PHY DSSS con esquemas de modulación BPSK u O-QPSK y una FSK PHY con 3 posibles modulaciones (GFSK, P-FSK, P-GFSK). Estos PHY fueron diseñados para aplicaciones de monitoreo de infraestructura crítica de baja energía (LECIM).
802.15.4m (2014) - Adenda 6	El objetivo de esta adenda era reutilizar el espacio de frecuencia dejado entre los canales de televisión en las bandas UHF. Originalmente, este espacio no se usó para evitar que los canales de televisión interfieran entre sí.
802.15.4p (2014) - Adenda 7	Abordó la necesidad de un estándar de comunicación en los sistemas de control de comunicaciones ferroviarias (RCC). Este estándar permitió velocidades de datos de hasta 1 Mb/s sobre frecuencias en las bandas VHF, UHF y SHF que operan en anchos de banda de canal contiguos y no contiguos tan estrechos como 12.5 kHz y tan amplios como 2Mhz.
802.15.4 – 2015	Tercera revisión de la norma. Como sus predecesores, esta combina todas las adiciones de capas PHY y las mejoras de capa MAC desde la revisión de 2011 en un solo documento.
802.15.4n (2016) - Adenda 1	Introduce otra alternativa de capa PHY para la transmisión de información médica en China. La China Medical Band (CMB) define las bandas: 174-216 MHz, 407-425 MHz y 608-630 MHz para este propósito y restringe su uso para aplicaciones de voz.
802.15.4q (2016) - Adenda 2	Añadió dos capas PHY para 2.4 GHz y múltiples bandas Sub-GHz con velocidades de datos de hasta 1 Mb/s. Estos niveles fueron diseñados para aplicaciones de ultra bajo costo (baja complejidad) y ultra bajo consumo.

Tabla 1. *(Continuación)*

Versión	Detalles
802.15.4u (2016) - Adenda 3	Agregó la capa PHY para 866 Mhz en la India. Este nivel definió la banda de 865-867 MHz con una opción para elegir múltiples velocidades de bits y 3 posibles modulaciones: SUN FSK, OFDM, O-QPSK.
802.15.4t (2017) - Adenda 4	Se introdujo una nueva capa PHY en esta enmienda, la cual fue diseñada para operar en dispositivos que requieren una breve ráfaga de información a altas velocidades (hasta 2 Mb/s) seguido de largos períodos de suspensión, lo que contribuye a una mayor duración de la batería.
802.15.4v (2017) - Adenda 5	Se cambiaron varios rangos de frecuencia de SUN PHY, incluidos sus rangos de canales. Los cambios admitieron el uso de 870-876 MHz y 915-921 Mhz en Europa, 902-928 MHz en México, 902-907.5 en Brasil y 915-928 MHz en Australia, Brasil y Nueva Zelanda.
802.15.4s (2018) - Adenda 6	Última enmienda hasta la fecha. Se agregaron varias primitivas y comandos de la capa MAC como parte del kit de herramientas Spectrum Resource Measurements (SRM). Estos cambios son las adiciones más significativas a la capa MAC desde la versión 802.15.4e-2012. SRM permite la medida, transmisión y solicitud de información sobre el estado del canal.

Nota: Extracto de "IEEE 802.15.4 Historical Evolution and Trends", por A. Ramonet y T. Noguchi, (2019), *21st International Conference on Advanced Communication Technology*, p. 351-359 (https://doi.org/10.23919/ICACT.2019.8702040).

5.3.1 Capa Física. La capa física (PHY), se caracteriza principalmente por permitir la transmisión de datos, seleccionar el canal, gestionar la potencia de la señal de salida y manejar el transceptor de radiofrecuencia (RF) (IEEE, 2003). El estándar también define la unidad de datos de esta capa como PPDU y su operación dentro de los siguientes rangos de frecuencia:

- **868 - 868.8 MHz:** Este rango es utilizado según normativa europea y tiene un (1) canal con velocidad de transferencia de 20 kbps.
- **902-928 MHz:** Esta franja es utilizada según normativa norteamericana y tiene hasta diez (10) canales con tasa de transferencia de 40 kbps.
- **2400-2483.5MHz:** Es la franja mundialmente aceptada para ISM y tiene hasta dieciséis (16) canales con velocidad de transferencia de 250 kbps.

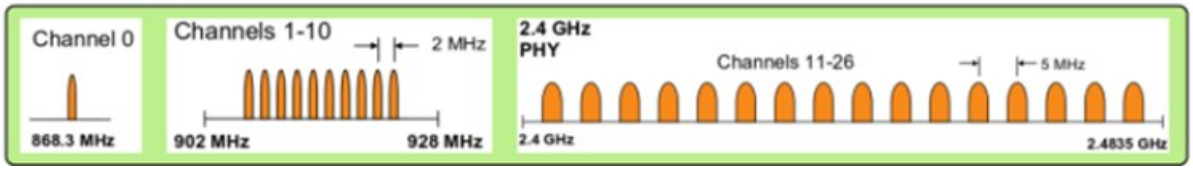

Figura 12. Frecuencias de operación de la capa física. Adaptado de Octavio Taladriz (2016) *Resumen visual del estándar 802.15.4.* http://elb105.com/resumen-visual-del-estandar-802-15-4/

5.3.2 Capa MAC. El control de acceso al canal o MAC, se encarga de permitir el envío de tramas a través del medio físico, garantizar intervalos de tiempo para evitar colisiones y la asociación de nodos (IEEE, 2003). Entre la capa MAC y el nivel inmediatamente superior, se encuentran definidas las subcapas control de enlace lógico (LLC) y convergencia específica de servicio (SSCS), las cuales contribuyen con el flujo de información.

El estándar IEEE 802.15.4 también define la unidad de información de la capa MAC como MPDU, la cual se ilustra en la *Figura 13*. Esta se encuentra conformada por el encabezado (MHR), la carga útil o payload de la trama y el campo de secuencia de verificación.

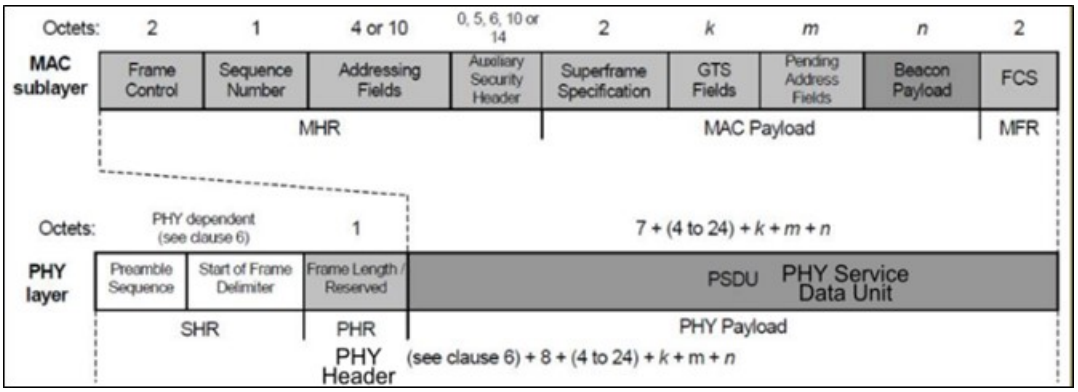

Figura 13. Trama beacon y paquete capa física. Adaptado de Octavio Taladriz (2016) *Resumen visual del estándar 802.15.4.* http://elb105.com/resumen-visual-del-estandar-802-15-4/

5.3.3 Topologías de red IEEE 802.15.4. Dentro de IEEE 802.15.4 se destaca la formación de dos tipos principales de topologías. Estas se caracterizan principalmente por su flexibilidad y sencillez de implementación, brindando así diversas ventajas a una gran gama de aplicaciones (Madan, Bagavathi, & Shalini, 2014). A continuación, se detallan:

a. **Topología en estrella**: esta se encuentra constituida por un nodo central denominado coordinador PAN, con el cual se comunican todos los demás dispositivos.

b. **Topología punto a punto**: en esta se añade la capacidad de que los diversos nodos puedan comunicarse entre ellos más allá de que se cuente con el coordinador dentro de la estructura. Son capaces de formar patrones arbitrarios de conexiones y su extensión solo está limitada por la distancia entre cada par de nodos. Su objetivo es servir de base para redes ad hoc capaces de realizar autogestión y organización.

El estándar define que dichas topologías de red están conformadas por varios dispositivos, entre ellos se encuentran los siguientes:

a. **Dispositivo de función completa (FFD):** como su nombre lo indica, se refiere a un nodo que tiene niveles completos de funcionalidad. Son capaces de enviar y recibir información, además de enrutar datos provenientes de otros nodos.

b. Dispositivo de función reducida (RFD): hace referencia a un terminal que tiene un nivel reducido de funcionalidad, como por ejemplo un sensor. Debido a su simpleza, no son capaces de enrutar tráfico y en función de administrar su energía, entran en modo de suspensión (sleeping mode) cuando no están en uso.

c. Coordinador: como se mencionó anteriormente, este se encarga de realizar todas las funciones del administrador de la red.

5.3.4 Seguridad en IEEE 802.15.4. IEEE 802.15.4 solo incluye mecanismos de seguridad en la subcapa MAC y su activación es opcional. Como se muestra en la Figura 13, en el encabezado de la MPDU se incluye un campo llamado frame control, el cual consta de un bit identificado como security enable bit (SEB) que determina la implementación de los servicios de seguridad incluidos en el campo authentication security header (ASH). (IEEE, 2011)

ASH determina la combinación de los algoritmos de seguridad y define el procedimiento de construcción de claves para el cifrado simétrico. A continuación, se muestran las opciones disponibles dependiendo del o los servicios que se requiera aplicar (Panagiotis, Panagiotis, & Ioannis, 2018):

- **Confidencialidad:** estándar de cifrado avanzado (AES) en modo de seguridad *counter* (AES-CTR).
- **Integridad y Autenticidad:** estándar de cifrado avanzado (AES) en el modo de seguridad *cypher block chaining* (AES-CBC).
- **Confidencialidad, Integridad y Autenticidad:** modo de seguridad *counter combinado* con CBC (AES-CCM).

Vale la pena acotar que IEEE 802.15.4 comprende soluciones contra ataques de repetición y también admite capacidades de control de acceso basadas en listas ACL. Más allá de estos servicios de seguridad, la protección no deja de ser limitada, por ejemplo, un ataque DoS puede tomar fácil ventaja de las exposiciones presentadas por los mensajes ACK ligados con la integridad y confidencialidad. (Granjal, Monteiro, & Silva, 2015)

5.4 Problemáticas de Seguridad en IoT

Con el objeto de cumplir con los estándares básicos de seguridad, toda tecnología de comunicación y sistemas de redes informáticas debe garantizar la implementación de los principios del modelo AIC (confidencialidad, integridad, disponibilidad y autenticación). A raíz de la implementación del IoT, surgen nuevos desafíos de seguridad que se fundamentan en las limitaciones de recursos de los dispositivos y su naturaleza ubicua, la heterogeneidad e interoperabilidad de las redes que lo componen y los amplios campos de aplicación; lo cual hace que la ejecución de los criterios sea más complicada y difícil de abordar.

De acuerdo a Panagiotis et al. (2019), las principales problemáticas de seguridad concernientes al Internet de las cosas giran en torno a los siguientes aspectos: gestión y protección de claves de autenticación, definición de soluciones de seguridad escalables, manejo del gran volumen de información confidencial y privada, restricción de hardware, configuraciones autónomas, limitados mecanismos de actualización y contraseñas débiles o por defecto.

Pasando de una perspectiva general a un enfoque más específico y teniendo en cuenta la importancia de la pila de protocolos en la cual está fundamentado el IoT, se hace necesario detallar las deficiencias de seguridad asociadas a estos y su susceptibilidad para con ciertos ataques a continuación:

En la base de la pila, irrupciones complejas pueden afectar las capas PHY y MAC del standard 802.15.4 debido a características inherentes como el uso del medio inalámbrico, la topología de red dinámica, la limitación de recursos en los nodos y el tamaño de la red. Amenazas de seguridad como el ataque de conflicto PANId y el ataque del intervalo de tiempo garantizado (GTS) han sido perpetrados (Amin & Hamid, 2015). En el primero, un adversario abusa del procedimiento de resolución de conflictos para transmitir notificaciones PANId falsas al coordinador PAN impidiendo la comunicación entre nodos y por medio del segundo, se hace un uso inadecuado del esquema de gestión GTS afectando las ventanas de tiempo para acceder al medio por parte de los nodos.

Para admitir la transmisión de paquetes IPv6 que exceden el tamaño máximo de trama de la capa inferior, 6LoWPAN dentro de la capa de adaptación, define un mecanismo de fragmentación de paquetes. Sin embargo, los procesos internos para ejecutar las transmisiones de fragmentos, la falta de autenticación en este nivel y los escasos recursos de memoria de los dispositivos en la red hacen que el diseño del mecanismo de segmentación sea vulnerable. El ataque de duplicación de

fragmentos y el ataque de reserva de espacio en el buffer (Hummen et al., 2013) se han encargado de explotar dichas vulnerabilidades. El primero se aprovecha de que la dirección de destino se menciona solo en el primer fragmento, creando la posibilidad de inundar fácilmente la red duplicando los siguientes fragmentos y el segundo, reserva espacio en el búfer con el objeto malicioso de evitar la reconstrucción de paquetes.

En las labores de enrutamiento, RPL presenta una proactividad y adaptabilidad que lo hacen ideal para las condiciones restringidas de la red. Este cuenta con algunas medidas y modos de seguridad, además de un mecanismo de recuperación automática para garantizar la estabilidad de las operaciones, no obstante, está lejos de ser exento a presentar deficiencias tanto en su funcionamiento como implementación que lo hacen objeto de agresiones. El standard de RPL menciona que el cifrado asimétrico no es soportado, la autenticación de nodos es bastante condicionada y los enlaces son poco confiables (Winter, y otros, 2012), abriendo así la oportunidad para que un atacante pueda acceder a información importante como datos en tablas de enrutamiento, estructuras de topologías e información específica de nodos padres e hijos, originando consecuencias como redireccionamiento de tráfico, suplantación de identidad de nodos y suboptimización de la red, entre muchas otras que serán abordadas más a fondo a lo largo de los siguientes capítulos.

En la capa de aplicación, el protocolo CoAP presenta limitaciones de seguridad con el procesamiento de URLs, modo proxy, almacenamiento en caché, gestión de credenciales y análisis sintáctico, haciéndolo propenso a ataques como spoofing y cross protocol. Para proteger los mensajes de CoAP, se usa el protocol DTLS (Datagram Transport Layer Security), aunque este también posee algunas restricciones de implementación en dispositivos restringidos y carece de un framework estandarizado para el control de acceso y autorización (Naik, 2017). Por último y en lo

que respecta a MQTT, este es un protocolo que no cuenta con un mecanismo de seguridad general, solo posee un componente de autenticación sin capacidad de cifrado, razón por la cual es propenso a espionaje y ataques de modificación de paquetes exponiendo la privacidad e integridad de la red. (Andy, Rahardjo, & Hanindhito, 2017)

Debido a las problemáticas de seguridad alrededor del IoT y sus protocolos más relevantes, cualquier red empresarial que no cuente con una ciberseguridad apropiada puede incurrir en riesgos que comprometan la operatividad y continuidad del negocio. Seguidamente se detallan los riesgos más destacados juntamente con ataques de notoriedad pública que tomaron ventaja de cada exposición mencionada.

Acceso a datos confidenciales: un gran número de equipos IoT cuentan con amplia gama de funcionalidades que le permiten entre otras cosas grabar, almacenar, acceder y transmitir datos confidenciales. Elementos comunes en la infraestructura de redes pequeñas como access points, cámaras e impresoras representan una oportunidad para capturar información relevante en caso de ser hackeados.

Dentro de los casos más impactantes de acceso no autorizado a información sensible, se encuentra el del malware denominado VPNFilter, el cual en el año 2018 se encargó de infectar a cientos de miles de dispositivos de red y almacenamiento para el hogar y pequeñas empresas con el objeto de extraer información privada (Largent, 2018). El FBI atribuyó públicamente esta actividad a un grupo de hackers apoyado por el gobierno de Rusia y tomó medidas posteriores para desmantelar dicha red de bots. Por medio de comunicados, se instó a los usuarios a establecer controles de seguridad básicos o actualizaciones de firmware adecuados con el propósito de evitar la reinfección.

Sabotaje: Sin importar la magnitud o el entorno de un dispositivo IoT**,** al este ser vulnerado**,** el agresor tiene acceso total a sus funciones y puede hacer uso de ellas para crear interrupciones en el desenvolvimiento del negocio. Las industrias que están expuestas a este tipo de riesgos son aquellas en las que los dispositivos de IoT no solo se usan como herramientas para ayudar a la productividad, sino que se están integrando en el núcleo de la operación del negocio. Por ejemplo, el uso de equipos del Internet de las cosas en la fabricación puede proporcionar enormes beneficios para la eficiencia, pero cuando los procesos de producción se vuelven completamente dependientes de la tecnología inteligente, un solo ataque tiene el potencial de hacer que una fábrica no funcione por un período determinado de tiempo.

Tal es el caso del virus Stuxnet, que en 2010 infectó una planta de enriquecimiento de uranio en Irán y causó daños permanentes en las centrífugas (Holloway, 2015). Mención aparte merece el malware llamado BrickerBot, en su última versión 3, el cual se encargó en abril de 2017 de destrozar miles de dispositivos IoT, entre los que se destacaron routers, webcams y smart tvs, solo en cuestión de horas (Goodin, 2017). El autor intelectual apodado Janit0r, mencionó que la razón del ataque fue eliminar muchos terminales IoT inseguros que están conectados a Internet antes de que estos fueran infectados por otros agentes maliciosos, a pesar de que esto representara un daño de gran magnitud a propiedad privada.

Botnets: Estas redes están constituidas por una gran cantidad dispositivos pirateados que pueden estar ubicados en cualquier parte del mundo y son generalmente utilizadas para la ejecución de ataques de denegación de servicio distribuido (DDoS). Los dispositivos infectados funcionan de manera normal, pero al momento de que el agresor decida iniciar la ofensiva, éste activa rutinas de fondo que originan un flujo de solicitudes de red desde cada equipo hackeado hacia un objetivo

específico. Al existir demasiadas solicitudes de conexión, el destino rebasa su capacidad de manejo y se bloquea, ocasionando así la suspensión temporal de sus servicios.

En octubre de 2016 tuvo lugar el que hasta ahora debido a su alcance ha sido catalogado por expertos como el mayor ataque de DDoS en la historia del Internet. El malware Mirai infectó a cientos de miles de dispositivos, entre ellos cámaras, routers caseros e impresoras, creando así un ejército botnet que utilizó para atacar a la empresa Dyn, proveedora de servicios DNS, inhabilitando sus funciones por horas y sacando de línea algunos de los sitios más grandes en el Internet como twitter y netflix (Ducklin, 2016). Los autores intelectuales de Mirai: Paras Jha, Josiah White y Dalton Norman, tenían para ese entonces entre 18 y 20 años.

Antes de Mirai, no se habían visto tantos ataques de tipo telnet simplemente porque los administradores de sistemas se han encargado de limitar los protocolos inseguros de administración remota a través de Internet. De manera rampante los dispositivos IoT comenzaron a implementarse y exponencialmente se ha visto el aumento en los ataques de este tipo. Esto valida que la diversidad de los dispositivos IoT también ofrece a los atacantes una amplia gama de puertos potenciales a los cuales apuntar.

Es claro que existe una necesidad de un enfoque más amplio con respecto a las tecnologías del IoT en general. Tanto los equipos de seguridad de las organizaciones necesitan ser más conscientes de todas las amenazas descritas anteriormente, como los fabricantes de dispositivos de IoT están en la obligación de proporcionar un mejor soporte empresarial, tal cual como se hace con los dispositivos de IT convencionales, y capacidades de monitoreo para facilitar a los equipos de seguridad la defensa de sus redes.

6. El protocolo RPL y las redes inalámbricas de baja potencia y pérdidas

6.1 Características y funcionamiento de las LLNs tipo IEEE 802.15.4.

Un componente vital del IoT es la tecnología de comunicación inalámbrica. Las redes de sensores inalámbricos (WSN) proporcionan la capacidad para detectar distintas variables relacionadas con el entorno en el que se insertan los dispositivos. (Sobral, Rodrigues, Rabelo, Al-Muhtadi, & Korotaev, 2019)

Una WSN es un tipo específico de LoWPAN, que como su nombre lo indica, está integrada por nodos equipados con diversos tipos de sensores, por ejemplo, de temperatura, humedad, luminosidad, etc. A su vez, una LoWPAN representa un ejemplo particular de LLN formada por dispositivos que se adhieren al estándar 802.15.4 de la IEEE.

La estructura de las redes de baja potencia y con pérdidas (LLN) cuenta con nodos que cumplen diferentes roles, entre los que se destacan:

• **Nodos sensores:** tienen como función principal la captura de información de su entorno para luego realizar la transmisión de las mismas a un nodo raíz o sink. Un sensor cuenta con capacidades de procesamiento, comunicación y de detección autónomas.

• **Nodos recolectores (sink):** como su nombre lo indica, estos se encargan de recibir las lecturas procedentes de los sensores y transferirlas para su posterior análisis.

• **Actuadores:** son dispositivos que responden a las lecturas de los sensores con el propósito de ejecutar alguna acción sobre un terminal remoto.

Cabe destacar que también forman parte de esta arquitectura los routers de borde que se encargan de almacenar las lecturas o datos provenientes de los sensores para enrutarlos través del Internet con el objetivo de que sean analizados y procesados.

De acuerdo al estándar IEEE 802.15.4, las características más resaltantes de los dispositivos anteriormente mencionados son las siguientes:

1. Capacidad limitada de procesamiento: procesadores de distintos tipos y diferentes velocidades.
2. Alcance corto: dependiendo de la implementación va desde 10 hasta 100 metros máximo cuando hay línea de vista.
3. Poca capacidad de memoria: desde unos pocos kilobytes de RAM hasta unas docenas de kilobytes de ROM o memoria flash.
4. Baja potencia: alrededor del orden de decenas de milivatios.
5. Bajo costo.

La adopción de las LLN en diversidad de ámbitos como el de la salud, industrial y automatización, han contribuido con un creciente despliegue de las mismas a nivel mundial. Más allá de los requerimientos particulares que puedan tener entornos como los anteriormente mencionados, las principales propiedades de las LLN según Kushalnagar et al., (2007) se resumen a continuación:

1. Paquetes pequeños: Se soportan tramas con un tamaño máximo de 127 bytes, incluidos 25 bytes de encabezado MAC y 102 bytes de payload.

2. Soportan dos tipos de direcciones: las extendidas de 64 bits del IEEE o las cortas de 16 bit.

3. Reducido ancho de banda: velocidad de datos de 250 kbps, 40 kbps y 20 kbps respectivamente para cada una de las capas físicas definidas (2.4 GHz, 915 MHz y

868 MHz).

4. Soporte para dos tipos de topología: estrella y malla.

5. Baja potencia: generalmente funcionan con baterías.

6. La ubicación de los dispositivos no está predefinida ya que la tendencia es desplegarlos de manera ad hoc. Por consiguiente, las locaciones pueden ser de difícil acceso según sea el caso.

7. Poca fiabilidad de los dispositivos debido a conectividad inestable de los radios, baterías descargadas, exposición a vandalismo, etc.

8. Los dispositivos pueden permanecer en modo “durmiente” (sleeping mode) por largos periodos para ahorrar energía.

Por último, cabe destacar que los patrones de tráfico y el flujo de datos dentro de una LLN son altamente direccionales. Estos se pueden definir en tres tipos: tráfico multipunto a punto (MP2P), tráfico punto a multipunto (P2MP) o tráfico punto a punto (P2P). (Iova, Picco, Istomin, & Kiraly, 2017)

La IETF (*Internet Engineering Task Force*) tiene diferentes grupos de trabajo (WGs) que han desarrollado estándares para su implementación con las LLN, entre ellos se destacan:

6LoWPAN: IPv6 sobre Redes Inalámbricas de Área Personal y Baja Potencia (*Low-power Wireless Personal Area Networks)* es un grupo que fue creado en octubre de 2004 con el objetivo de crear formas para permitir el uso de IPv6 en redes IEEE 802.15.4. Por lo tanto, 6LoWPAN

definió la inclusión de una capa de adaptación en la pila de protocolos, específicamente entre la capa de red y la capa de enlace de datos. Este nuevo nivel de adaptación permite la fragmentación y desfragmentación de paquetes IPv6 en tramas IEEE 802.15.4, realizando la compresión del encabezado de IPv6 (Ishaq et al., 2013). Las redes 6LoWPAN se conectan a Internet a través del router de borde (6BR) que es análogo a un sink en una WSN.

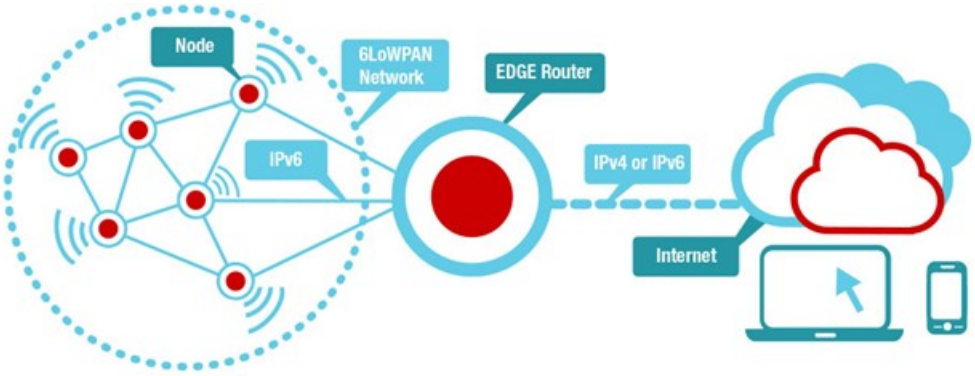

Figura 14. Red 6LoWPAN. Adaptado de Texas Instruments wiki. *Contiki-6LoWPAN* http://processors.wiki.ti.com/index.php/Contiki-6LOWPAN

ROLL: Enrutamiento en Redes de Baja Potencia con Pérdidas (*Routing Over Low power and Lossy networks*) es un grupo de trabajo que maneja temas de enrutamiento de Internet de las cosas (IoT) (IETF, 2018). ROLL comenzó su trabajo en febrero de 2008 con el objetivo de desarrollar un protocolo de enrutamiento adecuado a todos los requisitos específicos de las áreas de aplicación de las redes de baja potencia y con pérdida (LLN). Sus objetivos solo se enfocan en enrutamiento para IPv6.

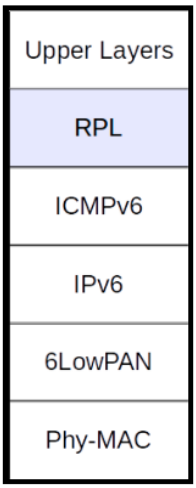

Figura 15. RPL Stack. Adaptado de Robles, I. (2018). *ROLL on a roll!* IETF Journal. Disponible en: https://www.ietfjournal.org/roll-on-a-roll/

6.2 RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks

Luego de la realización de estudios a través de los cuales se evaluó el rendimiento y adaptabilidad en diferentes entornos de los protocolos de enrutamiento IETF como OSPF, IS-IS, OLSRv2, AODV y RIP; el grupo de trabajo ROLL llegó a la conclusión de que ninguno cumplía con sus expectativas de aplicación. En consecuencia, desarrollaron un protocolo de enrutamiento tipo distance vector y source-routing denominado Protocolo de enrutamiento IPv6 para redes de baja potencia y con pérdida (RPL). (Robles, 2018)

A través de las especificaciones de RPL en el documento RFC 6550 *RPL: Protocolo de enrutamiento IPv6 para redes de baja potencia y pérdida*, la IETF define un modelo proactivo de encaminamiento en el cual el enrutamiento y el reenvío se implementan en la capa de red de acuerdo con la arquitectura IP (Winter, y otros, 2012). El protocolo proporciona un mecanismo a través del cual se admite tráfico multipunto a punto (MP2P), punto a multipunto (P2MP) y punto

a punto (P2P). RPL fue diseñado de acuerdo con los requisitos de enrutamiento para las redes LLNs, más sin embargo su uso no se limita solo a ellas. Las rutas RPL están optimizadas para el tráfico hacia o desde una raíz que actúa como un sumidero / estación base para la topología. En términos más específicos, los objetivos principales del protocolo son los siguientes:

• Operar en redes a gran escala formadas por pequeños dispositivos que se conectan a través de tecnologías de comunicación de bajo consumo y bajo costo.

• Adoptar mecanismos de enrutamiento y reenvío de datos de baja complejidad para facilitar la implementación en microcontroladores simples con capacidades limitadas.

• Distribuir información de enrutamiento compacta para admitir tecnologías de capa de enlace con tamaños de trama restringidos.

• Minimizar los requisitos de memoria con el fin de mantener toda la información concerniente al enrutamiento.

• Reducir los gastos generales de señalización de enrutamiento con el propósito de limitar el uso de ancho de banda y el consumo de energía.

• Descubrir enlaces de manera eficiente y asociarse con nodos vecinos que sean adecuados para redes que no poseen una topología predefinida.

En lo que respecta a su estructura, RPL está basado en la construcción de un Gráfico Acíclico Dirigido (DAG), que consiste en uno o más DODAG (DAG orientados al destino), para cada raíz de un DODAG (Gaddour & Koubaa, 2012). Con el objeto de identificar una topología, RPL utiliza cuatro valores claves:

1. *RPL Instance ID* o ***Instancia de RPL***: Por medio de este se establece arreglos de red de al menos un DODAG. Básicamente, todos los DODAG dentro de la misma instancia comparten información de enrutamiento. Como se observa en la *Figura 16*, varias instancias de RPL pueden ejecutarse de forma independiente dentro de una sola topología de red.

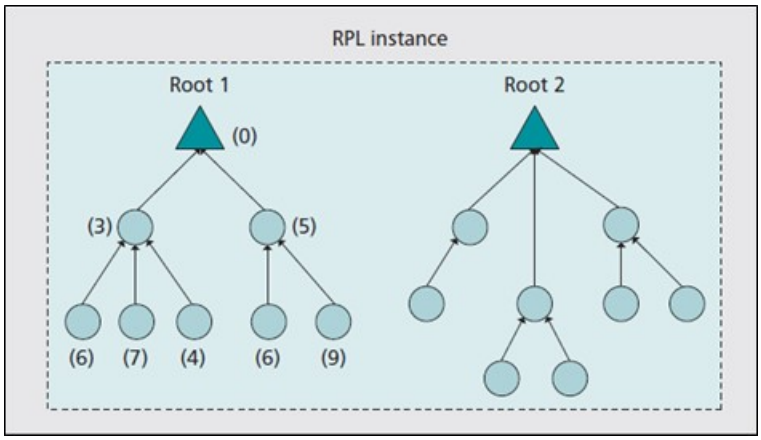

Figura 16. Instancia de RPL conformada por dos DODAGs. Adaptado de Ancillotti et al. (2013). The roles of the RPL routing protocol for smart grid communications. *IEEE Communications Magazine, 51,* 75-83. Disponible en: https://doi.org/10.1109/MCOM.2013.6400442

2. *DODAG ID:* Es usado como identificador único de un DODAG en el sistema. Este surge mediante la combinación de los valores del ***RPL Instance ID*** y el ***DODAG ID***.

3. *DODAG Version Number:* Este valor es incrementado cada vez que la red pasa por un proceso de reinicio o reconstrucción. Es de suma ayuda para reconocer la versión del DODAG cuando se usa en combinación con los valores del ***RPL Instance ID*** y el ***DODAG ID***.

4. *Rank* o ***Rango***: Es utilizado para definir la posición de un nodo individual con respecto a la raíz del DODAG.

Adicionalmente, RPL utiliza cuatro mensajes de control ICMPv6 (Gaddour y Koubaa, 2018) para crear y mantener tanto el DODAG como la tabla de enrutamiento:

• **Objeto de información DODAG (DIO):** Usado principalmente para formar la estructura del DODAG. Como se muestra en la *Figura 17*, cada nodo comienza a enviar este mensaje a sus adyacentes hasta que se completa la topología. En el mensaje DIO se incluye información vital que contribuye a que un nodo pueda aprender los parámetros de la red, seleccionar un padre preferido, entre otros.

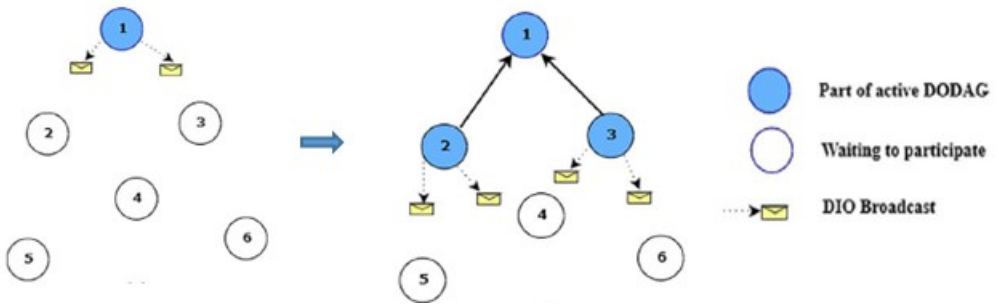

Figura 17. Formación del DODAG a través de DIO broadcast. Adaptado de Kamgueu et al. (2018). Survey on RPL enhancements: A focus on topology, security and mobility. *Computer Communications, 120*, 10-21.Disponible en: https://doi.org/10.1016/j.comcom.2018.02.011

• **Objeto de anuncio de destino (DAO):** En concordancia con la *Figura 18*, este tipo de mensaje se utiliza para propagar información de destino hacia arriba a lo largo del DODAG.

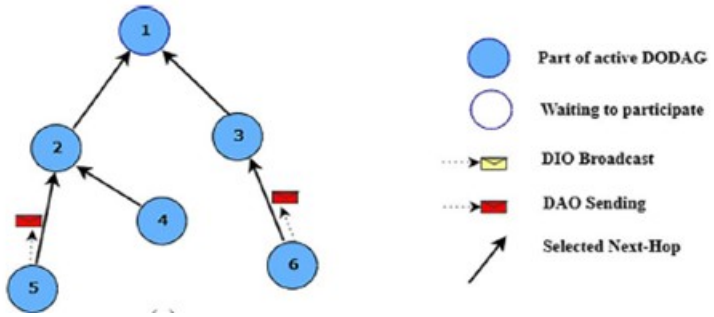

Figura 18. Despliegue de mensajes DAO a través del DODAG. Adaptado de Kamgueu et al. (2018). Survey on RPL enhancements: A focus on topology, security and mobility. *Computer Communications, 120,* 10-21. Disponible en: https://doi.org/10.1016/j.comcom.2018.02.011

• **Solicitud de información de DODAG (DIS):** Como se representa en la *Figura 19*, este mensaje es usado por un nodo externo para solicitar un DIO que le permita unirse a la estructura del DODAG.

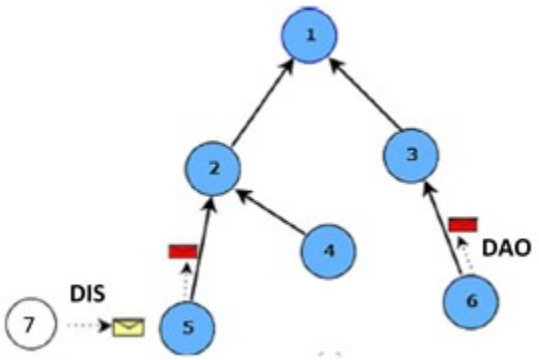

Figura 19. Envío de DIS por nodo para unirse al DODAG. Adaptado de Kamgueu et al. (2018). Survey on RPL enhancements: A focus on topology, security and mobility. *Computer Communications, 120,* 10-21. Disponible en: https://doi.org/10.1016/j.comcom.2018.02.011

• **DAO-ACK:** Usado como confirmación de una respuesta enviada por un nodo padre a un nodo hijo luego de un mensaje DAO.

Aunque los mensajes descritos anteriormente son los principales dentro de la estructura de RPL, es importante mencionar que cuando el protocolo funciona en modo seguro, también se emplea otro mensaje denominado *Verificación de consistencia* (CC). Como su nombre lo indica, este revisa e informa a un nodo destino acerca de los contadores de mensajes seguros y también emite respuestas tipo desafío.

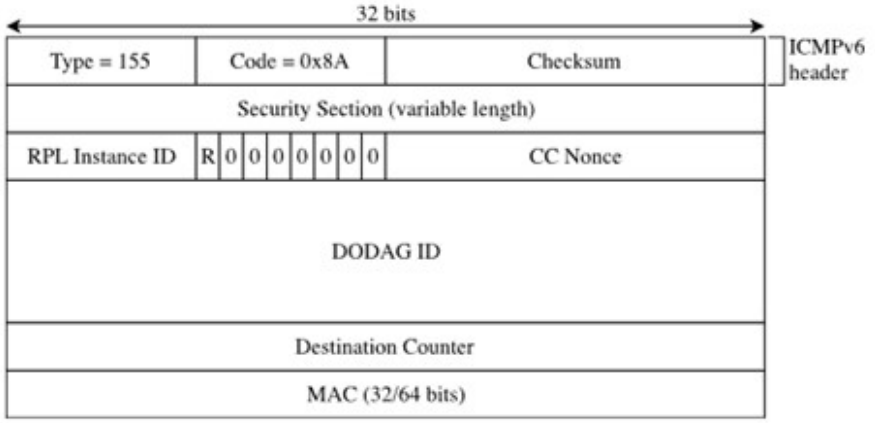

Figura 20. Formato del mensaje de Verificación de Consistencia (CC). Adaptado de Arena et al. (2019). Evaluating and improving the scalability of RPL security in the Internet of Things. *Computer Communications, 151,* Disponible en: 119-132. https://doi.org/10.1016/j.comcom.2019.12.062

Durante el proceso de construcción del gráfico DODAG, uno de los principales objetivos de RPL es que cada nodo que intenta formar parte de la red, seleccione un padre preferido entre un grupo de dispositivos existentes.

La fase anteriormente descrita, se lleva a cabo por medio del cálculo de una Función Objetivo (OF). Esta se encarga de interpretar métricas, reglas y restricciones en el valor del ***Rank***, modelando así la distancia del nodo desde una raíz DODAG y optimizando los enlaces dentro de la topología de red. La OF también permite la selección de un DODAG al cual unirse y la identificación de un número de nodos pares en ese DODAG como padres (Thubert, 2012).

Las dos funciones objetivo más comunes son la Función Objetivo cero (OF0) y la denominada rango mínimo con función objetivo de histéresis (MRHOF). En miras de encontrar un potencial padre que esté más cerca de la raíz, la primera emplea el principio de ***grounded root*** más cercana, el cual está compuestos por varios parámetros. En cambio, la segunda utiliza el recuento de transmisión esperado (ETX) como la métrica predeterminada (Thubert, 2012).

Con la premisa de garantizar la escalabilidad del enrutamiento, RPL emplea el algoritmo Trickle, por medio del cual se regula la propagación de mensajes de control DIO dentro de la red. De acuerdo a Levis et al., (2011) la lógica detrás de Trickle es la siguiente: cada nodo programa una transmisión de difusión DIO de forma periódica. Este flujo de paquetes es administrado de dos maneras, ya sea por la suspensión temporal de la emisión o por un ajuste dinámico que dependerá de la consistencia o falta de integridad de la información que atraviesa la red. De esta manera se logra un equilibrio que establece datos de enrutamiento actualizados sin consumir excesivos recursos.

En lo que respecta a la operación del protocolo, RPL emplea dos modos de enrutamiento dentro de la topología: ***upward routing mode*** o enrutamiento hacia arriba, en el cual se admite el patrón de comunicación MP2P, y el ***downward routing mode*** o enrutamiento hacia abajo, para el esquema de comunicación P2PM y P2P.

Durante el upward routing mode, el proceso de transmisión se asemeja al de la construcción del DODAG, en donde se hace un envío multicast de los mensajes tipo DIO desde el sumidero atravesando los nodos intermedios hasta llegar a los ubicados en el fondo de la estructura en forma de árbol.

Por medio del enrutamiento hacia abajo, las rutas se construyen utilizando mensajes tipo DAO y DAO-ACK. Cuando un nodo ha seleccionado a su padre preferido, este enviará un mensaje DAO a su padre, que a su vez continuará con el reenvío a través de su padre y así sucesivamente hasta la raíz. Dentro de este se admiten dos modos de operación: modo de almacenamiento o sin almacenamiento.

En el modo de almacenamiento, cada nodo mantiene una tabla de enrutamiento que guarda el mapeo entre los destinos accesibles a través de su sub-DODAG y los nodos que representan el siguiente salto; todos aprendidos por medio de la recepción de los mensajes DAO. Por otra parte, en el modo sin almacenamiento, la raíz es el único nodo de red que mantiene la información de enrutamiento; la raíz toma ventaja de la “visión global” que tiene de la topología de red para el enrutamiento de origen, como por ejemplo, al incluir información de ruteo directamente en el paquete.

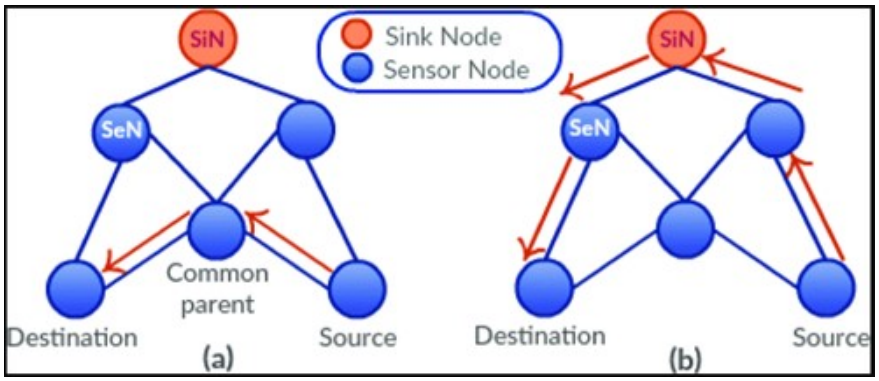

Figura 21. DODAG en nodo de almacenamiento (a) y sin almacenamiento (b). Adaptado de Abbou et al. (2019). Routing over Low Power and Lossy Networks protocol: Overview and performance evaluation. *International* Conference of Computer Science and Renewable Energy, 1-6. Disponible en: https://doi.org/10.1109/ICCSRE.2019.8807584

Ambos modos de operación afectan el proceso de comunicación punto a punto entre dos nodos de la red, esto debido a que el mismo se logra como una combinación de las técnicas utilizadas para los dos tipos de tráfico mencionados anteriormente. En el modo de almacenamiento, los paquetes de datos viajan hacia arriba hasta que alcanzan un nodo con información de enrutamiento sobre su destino, es decir, un ancestro común; a partir de ese momento, continúan hacia abajo, siguiendo las rutas establecidas previamente por los paquetes DAO. La misma técnica se utiliza en el modo sin almacenamiento; no obstante, en este escenario los paquetes deben viajar hasta la raíz (el único nodo que mantiene la información de enrutamiento) antes de ser redirigidos a su destino.

Durante el proceso de estandarización de RPL, el draft del protocolo se implementó en varias plataformas. Estos sistemas operativos de código abierto se han desarrollado para ejecutarse en dispositivos con recursos limitados, posibilitando el desarrollo aplicaciones que se enfocan en

maximizar el uso del hardware al tiempo que proporcionan una herramienta importante para simulaciones dentro de estudios de investigación.

Entre los más populares se encuentran Contiki OS, Tiny OS y RIOT. Contiki conecta pequeños microcontroladores de bajo costo y baja potencia a Internet, en este se ejecuta ContikiRPL el cual implementa ETX como OF predeterminado más allá de permitir la configuración de otras funciones (ContikiOS Org., 2019). TinyRPL es una implementación de RPL para TinyOS y también utiliza la función objetivo ETX por defecto. Es comúnmente integrado en los campos de informática ubicua, redes LAN, edificios y medidores inteligentes (TinyOS Wiki, 2013). En el caso de Riot-RPL (Riot-OS Org, 2019), este está diseñado de manera muy ligera para operar especialmente en dispositivos integrados con escasa memoria. Por último,

RPL Lite es ejecutado por defecto en Contiki–NG y surgió como una actualización en 2017 de la versión original de ContikiRPL, mejorando aspectos de funcionabilidad y estabilidad (Contiki-NG Wiki , 2019). A continuación, se muestra una tabla donde se resumen las diferentes implementaciones:

Tabla 2.

Implementaciones de RPL

Nombre	Sistema Operativo	Versión de Protocolo
ContikiRPL	Contiki	RFC 6550
RPL Lite	Contiki-NG	N/D
TinyRPL	TinyOS	Draft-ietf-roll-rpl-17
Riot-RPL	RIOT	N/D

6.3 Escenarios de Implementación y Aplicación de RPL

Las LLN y RPL tienen diversos campos de aplicación, entre los cuales se destacan: ciudades inteligentes, sistemas de defensa, aplicaciones biomédicas, detección de terremotos, agricultura de precisión, sistemas de control automático a nivel industrial, redes vehiculares ad-hoc (VANET).

Teniendo en cuenta el potencial y ventajas que ambos pueden aportar al ser ejecutados dentro de los entornos mencionados anteriormente, se han realizado muchos trabajos de investigación en los cuales se documentan experimentos reales y simulaciones que evalúan su desempeño general dentro de situaciones particulares, así como también aportan conocimiento para futuros desarrollos y en mejoras de sus limitaciones. A continúan se describen algunos trabajos que se enfocan en la implementación del protocolo RPL en redes LLN tipo IEEE 802.15.4:

En primer lugar, Wu et al., (2019) desarrollan e implementan tecnologías de red claves para construir una arquitectura inalámbrica del Internet de las cosas industrial (IIoT) y stacks de protocolos de comunicación basadas en el modo de acceso de IEEE 802.15.4-2015 TSCH. Con el propósito de lograr el objetivo, diseñaron un mecanismo de programación sensible al retraso y un algoritmo dinámico de asignación de ancho de banda, el cual no se encuentra especificado dentro del estándar IEEE 802.15.4-2015 TSCH. Estos se implementaron y pusieron en marcha por medio de una aplicación para administrar la red, 8 nodos sensores Texas Instrument modelo CC2538 SoC y un router de borde.

La topología de red construida y configurada por RPL fue monitoreó desde el aplicativo. Adicionalmente, el rendimiento de la demora de transmisión de paquetes y la tasa de entrega de paquetes (PDR) fueron presentados para validar la efectividad de la implementación de lograr los

requisitos de QoS de bajo retraso, alta confiabilidad y bajo consumo de energía impuestos por el entorno IIoT.

En lo que respecta al área de seguridad, Arena et al., (2019) realizaron una evaluación exhaustiva del impacto de los mecanismos de seguridad RPL en el rendimiento de las topologías de red a gran escala mediante simulaciones y pruebas reales. En primera instancia, se ejecutaron simulaciones de las funcionalidades de seguridad de RPL en COOJA, un emulador del sistema operativo Contiki. Dentro de dicho entorno de simulación realista, se configuró una red con nodos constituidos por un hardware de sensor genérico equipado con una interfaz de radio IEEE 802.15.4. Luego, con el propósito de validar y fundamentar los resultados obtenidos en los experimentos de simulación, se realizaron un conjunto de mediciones en un banco de pruebas real facilitado por el FIT IoT-LAB. Esta plataforma abierta, multiusuario y con una infraestructura de gran escala se presta para experimentaciones con sistemas IoT en entornos existentes. Allí, se constituyó una red de 54 nodos M3 Open, los cuales están basados en Cortex M3 con un chip de radio Atmel AT86RF231 compatible con IEEE 802.15.4. Estos son compatibles con ContikiOS, por lo que pudieron ejecutar el mismo código utilizado en la simulación y están equipados con una herramienta que monitorea el consumo de energía.

Los resultados tanto de la simulación como del experimento real demostraron que la configuración de seguridad ligera no tiene un impacto relevante en los procedimientos críticos de la red, como por ejemplo, la creación de la topología y los procedimientos de formación de rutas descendentes. Además, también se destacó que la configuración de seguridad completa ofrece un mecanismo de protección ante ciertas eventualidades y mejora la optimización de las rutas, a cambio de una ligera disminución del tiempo de formación de la red.

Por último, Hakeem et al., (2019) realizó tanto una implementación real como simulada del comportamiento de RPL con modificaciones adecuadas para admitir los requisitos de enrutamiento de redes inalámbricas basadas en una infraestructura de medición avanzada (AMI).

El experimento se llevó a cabo con una topología de 140 nodos M3 Open desplegados en el interior de una sede del FIT IoT-LAB ubicada en Lille. Los ensayos se realizaron alrededor de 70 veces con los nodos distribuidos uniforme y aleatoriamente e intercambiando alta cantidad de paquetes por un período de un par de horas. En lo que respecta a la emulación, esta se ejecutó en COOJA con una red a gran escala de 1000 nodos Tmote Sky que asemejaban a los medidores inteligentes y adoptando ETX y OF0 como métricas de enrutamiento.

7. Vulnerabilidades de Seguridad en RPL

7.1 Clasificación según modelo AIC

Haciendo referencia al RFC 4949, una amenaza es definida como "*una posibilidad de violación de la seguridad, la cual está latente cuando existe una circunstancia, capacidad, acción o evento que podría quebrantar la seguridad y a su vez causar daños*" (Shirey, 2007).

Como se ha indicado anteriormente, las redes LLN tipo IEEE 802.15.4 están expuestas a varias amenazas. A lo largo de este capítulo se procederá a identificarlas, describirlas y clasificarlas con el objeto de proponer soluciones que en la medida de lo posible garanticen que tanto la red en general como el protocolo de enrutamiento funcionen correctamente. Estas medidas deben

ejecutarse acorde a estándares de seguridad tales como el modelo de referencia de seguridad ISO 7498-2 (International Organization for Standardization, 2000) el cual está basado en los criterios AIC (Confidencialidad, Integridad, Autenticación y Disponibilidad).

Debido a las peculiaridades ya conocidas de estas redes, las implementaciones de dichas medidas de seguridad se enfocan en problemas bastante concretos y complejos. A continuación, se definirán cada uno de los principios del modelo de seguridad. Luego, y en referencia al contexto de RPL, se describirán las vulnerabilidades cuyas características aplican para cada criterio del modelo, así como también se enunciarán los ataques que entran dentro de cada una de las categorías. Cabe destacar que, debido a la naturaleza u objetivos de los ataques, estos pueden integrar uno o más principios del estándar.

7.1.1 Principios del modelo de Seguridad ISO 7498-2

7.1.1.1 Autenticación y Control de Acceso. Este concepto plantea el proceso a través del cual por medio de ciertos mecanismos se verifica la identidad de un nodo antes de que este acceda a un recurso o ejecute cualquier función dentro de la red. Según el RFC 5548, las LLN son susceptibles a desperdiciar energía por la aparición de nodos maliciosos no autenticados, incluso mucho antes de alcanzar la etapa de intercambio de información. (Dohler, Watteyne, Winter, & Barthel, 2009)

7.1.1.2 Confidencialidad. La confidencialidad se basa en la protección de información relevante para que esta no sea accedida por agentes no autorizados. Teniendo en cuenta que el medio principal de transporte de las LLN es de acceso público compartido, toda data referente a la topología, dispositivos y enrutamiento debe estar bien resguardada.

7.1.1.3 Integridad. La integridad, al igual que la recién señalada confidencialidad, hace referencia a la protección de la información. De manera más específica, con este criterio se busca garantizar la veracidad de la data que se transmite a través de la red evitando así modificaciones no autorizadas.

7.1.1.4 Disponibilidad. Como su nombre lo indica, este principio es garante del acceso a recursos, adecuado funcionamiento de los servicios y operación eficiente del sistema en general.

7.1.2 Amenazas basadas en las vulnerabilidades de los principios de seguridad

7.1.2.1 Amenazas debido a fallas en la autenticación. Dentro de estas se pueden incluir aquellas que se caractericen principalmente por la usurpación de identidad, esto con el objetivo de asumir el rol de un nodo legítimo dentro de la estructura. Luego de lograr esto, se pueden observar por parte del nodo malicioso alguno de los siguientes comportamientos:

1. Despliegue de información falsa y mensajes de control alterados.
2. Redirigir tráfico hacia sí mismo originando ralentización, filtrado y descarte de paquetes.
3. Duplicación de entidades con identificaciones falsas.
4. Agotamiento de recursos físicos de los nodos legítimos de la red.

Los ataques que cumplen con las tácticas mencionas son Clone ID, Sybil, Sinkhole y Reenvío Selectivo.

7.1.2.2 Amenazas debido a fallas de confidencialidad. Están representadas por aquellos ataques que comprometan cualquier tipo de información relevante para el correcto funcionamiento y desempeño de la red. Tanto los nodos como el medio de transporte suponen puntos de fallas, los cuales al ser vulnerados, originarían consecuencias como las siguientes:

1. Divulgación de la información de enrutamiento y topología.
2. Exposición de los datos de accesibilidad hacia los nodos con mayor relevancia dentro del DODAG.
3. Captura de paquetes que describan el estado y recursos específicos de los nodos vecinos.
4. Acceso y gestión remota de dispositivos al placer del atacante.
5. Riesgo físico de equipos.

Los ataques que realizados con la función de apropiarse de la información de manera indebida son Sniffing, Análisis de tráfico, Sybil, Clone ID, Reenvío selectivo, entre otros.

7.1.2.3 Amenazas y ataques a la integridad. Su alcance abarca desde la apropiación de dispositivos legítimos hasta la suboptimización de una red en general. Las características más comunes de estos ataques son las siguientes:

1. Manipulación de las rutas en las tablas de enrutamiento.
2. Fragmentación de la red al aislar la comunicación entre nodos y routers.
3. Reenvío o repetición de información de enrutamiento afectando la convergencia de los protocolos.

4. Falsificación de identidades de los nodos encargados del enrutamiento.
5. Explotación de dispositivos por medio de accesos remotos.

Dentro de los ataques concebidos para afectar la integridad podemos encontrar al Local Repair, Bizantino, Repetición de información de enrutamiento, Clone ID, Neighbor, Rank, Version number y Sybil.

7.1.2.4 Amenazas y ataques contra la disponibilidad. Dentro de este apartado se incluyen ataques que interrumpen los procesos de la red, inhabilitando de esta manera el acceso y correcto funcionamiento de sus recursos. Las acciones típicas de estos son las siguientes:

1. Obstaculización del tráfico de red.
2. Ruptura de los canales de comunicación entre los nodos.
3. Interferencia en el intercambio de la información de enrutamiento.
4. Agotamiento de los recursos físicos de los nodos.

Estas ofensivas son llevadas a cabo por ataques como Hello flooding, DoS, Sobrecarga de tabla de enrutamiento, Sinkhole, Wormhole, Reenvío selectivo, Inconsistencia del DAG y DIS. En la Tabla 3 se resumen y clasifican los ataques y amenazas a RPL basadas en el modelo de seguridad AIC.

Tabla 3.

Clasificación de amenazas y ataques a RPL

Amenazas debido a vulnerabilidades de	**Ataques**	**Tipo de ataque según taxonomía**
Autenticación	Sybil Clone ID Reenvío selectivo Sinkhole	Despliegue de información falsa / Filtrado de tráfico
Confidencialidad	Análisis de tráfico Neighbor Sniffing Daño físico de nodos	Exposición de la información de enrutamiento
Integridad	Blackhole Inconsistencia de DAO Spoofing Repetición de información de enrutamiento	Manipulación de la información de enrutamiento
	Bizantino Version Number Rank, Decreased Rank Falsificación de tabla de enrutamiento	Apropiación indebida de la identidad de nodos

Tabla 3. *(Continuación)*

Amenazas debido a vulnerabilidades de	**Ataques**	**Tipo de ataque según taxonomía**
Disponibilidad	Basado en DIS Sybil Clone ID Repetición de información de enrutamiento Sinkhole Wormhole	Interrupción del flujo del tráfico de red
	Denial of Service (DoS) Sobrecarga de tablas de enrutamiento Reenvío selectivo Hello flooding Inconsistencia de DAG	Agotamiento de recursos

Nota: Extracto de "A comparative study on RPL attacks and security solutions", por S. Mangelkar, S. N. Dhage y A.V. Nimkar, 2017, *International Conference on Intelligent Computing and Control*, p. 1-6 (https://doi.org/10.1109/I2C2.2017.8321851).

7.2 Identificación de Ataques

A través del análisis del modelo de enrutamiento y la revisión asociada a literatura existente, se han determinado la amplia gama de agresiones a las cuales son propensos el protocolo RPL y las redes LLNs.

Dependiendo de los objetivos del intruso y de la taxonomía de los ataques (Mayzaud et al, 2016), estos pueden ser de diferentes tipos: los que se enfocan en alterar el rendimiento de la red

y agotar sus recursos, los que apuntan a modificar la topología de la red y los que secuestran o espían el tráfico.

En lo que respecta a las fuentes de los ataques, estas pueden ser internas y externas. Los internos normalmente se caracterizan por desplegarse desde nodos manipulados dentro de la estructura y su alcance es considerable. Sin embargo, no llegan a ser tan invasivos como aquellos que se generan desde el exterior, los cuales en la mayoría de los casos no están limitados en recursos como memoria, procesamiento, energía o almacenamiento (Mangelkar et al, 2018). A continuación, se describen los ataques más relevantes:

7.2.1. Sinkhole. Toma lugar cuando un nodo malicioso modifica su número de rango para así obtener un mejor valor dentro de la topología. Esto le permitirá ser un potencial candidato a padre preferido que terminará atrayendo mayor de cantidad de tráfico que puede descartar para degradar el funcionamiento de la red. (Wallgren, Raza, & Voigt, 2013)

7.2.2. Reenvío Selectivo. Es llevado a cabo por un nodo maligno que de manera selectiva escoge mantener o descartar paquetes. Es indiferente si el tráfico contiene información relevante y principalmente se gesta para alterar el flujo de comunicación dentro de la red. Posee dos variaciones, una en la que se reenvían paquetes para desencadenar un ataque de DoS, y otra en donde la data filtrada va dirigida a otro nodo malicioso (Sharma et al., 2012).

7.2.3. Ataques de repetición de información de enrutamiento. Normalmente son ejecutados por un nodo fraudulento que se encarga de repetir transmisiones de información válida a destiempo. Esto es bastante perjudicial ya que altera la integridad de las tablas de enrutamiento y el funcionamiento general de la red al crear topologías ficticias (Mayzaud et al, 2016).

7.2.4. Neighbor. El nodo malicioso establece su ataque al replicar mensajes DIO que recibió de sus vecinos con anterioridad, pero sin agregar información referente a el mismo. De esta manera, los próximos nodos que reciben este paquete pueden considerar que se trata de un nuevo dispositivo adyacente, cuando en realidad está fuera de alcance, o de un potencial candidato a padre preferido. Cambios en la topología y rutas inexistentes quedarían como resultado. (Kamgueu, Nataf, & Djotio, 2018)

7.2.5. Worst Parent. A través de la manipulación de los mecanismos que definen las reglas de escogencia de un nodo padre por medio de la información del parámetro rank, un nodo malicioso condiciona la escogencia para que esta se decante por el peor candidato posible. En consecuencia, se generan rutas de bajo rendimiento y con retrasos a través de los nodos maliciosos (Le, y otros, 2013)

7.2.6. Wormhole. Ocurre cuando se crea un túnel entre dos nodos intrusos y se transmite tráfico selectivo a través del mismo. Si estos nodos se encuentran separados dentro de la misma red, cualquiera es capaz de replicar y redirigir información de un área a la otra por medio del túnel, causando alteraciones en la topología y distorsión del patrón natural de tráfico. (Nagrath & Gupta, 2011)

7.2.7. Blackhole. Por medio de este, un nodo comprometido actúa silenciosamente y empieza a descartar todos los paquetes que recibe en vez de darle continuidad a las rutas establecidas dentro de la topología. Como consecuencia, sectores de la red son propensos a quedar aislados causando la pérdida significativa de tráfico. Este ataque puede aumentar su alcance y magnitud a niveles peligrosos si actúa en conjunto con el sinkhole. (Razali, Rusli, Jamil, Ismail, & Yussof, 2017)

7.2.8. Ataques de inconsistencia DAO en modo de almacenamiento. Las inconsistencias de DAO ocurren cuando en un enlace entre nodos padre e hijo, el segundo provoca que el primero descarte rutas descendentes totalmente válidas en su tabla de enrutamiento. Siendo más específico, luego de recibir un paquete, el nodo hijo retorna un mensaje con un flag de error que manifiesta la incapacidad para seguir reenviando tráfico, lo cual ocasiona que el padre remueva de cache ese trazado en particular. RPL ofrece un mecanismo para mejorar esta inconsistencia, llamado recuperación de bucle de inconsistencia DAO. (Pu, 2019)

7.2.9. Hello Flooding. Por medio de la emisión masiva de mensajes DIO engañosos, un nodo maligno externo a la estructura del DODAG puede convencer a dispositivos legítimos de que es su vecino. Esto causa que los nodos malgasten su energía al dar respuesta a los constantes mensajes de tipo HELLO y que en la topología impere un estado de confusión. (Pongle & Chavan, 2018)

7.2.10. Ataques de sobrecarga de tablas de enrutamiento en el modo de almacenamiento. Este ataque se enfoca en llenar tabla de enrutamiento de un nodo específico con rutas falsas dentro de la red y puede ser llevado a cabo por uno o varios dispositivos maliciosos a través de la emisión

de mensajes DAO. Al vulnerar la integridad de las rutas, el atacante garantiza que los paquetes no lleguen a los destinos que corresponden o peor aún que se desborde la memoria del nodo legítimo.

7.2.11. Ataque basado en DIS. Ocurre cuando un nodo malicioso difunde periódicamente mensajes DIS con identidades falsas a vecinos que forman parte de una estructura legítima. Esto ocasiona en los nodos receptores el restablecimiento del algoritmo trickle, lo que trae como consecuencia la emisión considerable de mensajes DIO y el agotamiento de la energía (Pu, 2019).

7.2.12. Local Repair. Un atacante invoca el método de reparación local al modificar los valores del rango o del DODAG ID de un nodo. Al detectarse estos cambios dentro de la red, se hace necesario actualizar la topología de la red. Si este proceso es realizado de manera constante en varios nodos dentro la estructura, la generación de mensajes de control aumenta, la energía de los equipos se agota y la operación de la red se degrada al perder paquetes. (Gaddour & Koubaa, 2012)

7.2.13. Increased Rank. Al aumentar el valor del rank, un atacante puede atraer más tráfico. Teniendo en cuenta este fin, el nodo malicioso debe primero actualizar la lista de hijos su padre, eliminando los dispositivos que tienen un rango mayor que el nuevo rango deseado. La modificación de dicho parámetro origina la formación de bucles e inconsistencias en las tablas de enrutamiento. Mientras mayor sea el número de nodos afectados, más tiempo tardaran los mecanismos de reparación para entrar en acción (Wallgren, Raza, & Voigt, 2013).

7.2.14. Inconsistencia del DAG. Ocurre cuando agentes maliciosos modifican parámetros en las extensiones del encabezado de mensaje de RPL, específicamente los valores del rango del remitente y el flag denominado ‘O’.

Esta inconsistencia busca tomar ventaja de la activación de los mecanismos de auto reparación de RPL, ejecutando reinicios del trickle timer de los nodos, lo que trae como consecuencia mayor uso de recursos, generación de mensajes de control, perdida de paquetes e inestabilidad en la red que puede evolucionar en un DoS. (Sfar, Natalizio, Challal, & Chtourou, 2018)

7.2.15. Version Number. Se fundamenta en la modificación ilegal del parámetro identificado como número de versión, el cual está contenido en el mensaje de control DIO. Al realizar esta alteración, el atacante provoca una reconstrucción innecesaria y constante de todo el gráfico DODAG que suboptimiza el funcionamiento de la red (Mayzaud et al, 2014).

7.2.16. Denial of Service (DoS). El ataque de negación de servicio, como se indicó en capítulo previo, se enfoca en orquestar una ofensiva que inhabilite un nodo objetivo y los servicios que este provee. El extenso número de nodos con los que cuenta las redes LLN facilita el escenario para que técnicas empleadas como inundación de paquetes UDP tenga éxito. (Goodin, 2017)

7.2.17. Sniffing. Este ataque se ejecuta de manera pasiva y básicamente realiza labores de espionaje inspeccionando el contenido los mensajes de control RPL que atraviesan la red. Al realizar esta técnica se termina agrupando una cantidad considerable de información que puede revelar parámetros vitales de la estructura como direcciones, DODAG ID, el número de versión, rangos, entre otros (Alabsi et al, 2018).

7.2.18. Análisis de Tráfico. Este ataque se basa en la recopilación de información dentro la red RPL, la cual luego de ser sometida a un extenso procesamiento puede arrojar datos útiles que expongan la ubicación de los nodos, funciones de enrutamiento y el flujo del tráfico dentro de la topología (Goyal & Goyal, 2017). Al violentar la confidencialidad de esta manera, se da pie a la ejecución de ataques más sofisticados y dañinos. Si bien ciertas técnicas de encriptación de paquetes pueden limitar este tipo de brechas de seguridad, la misma naturaleza restringida de los dispositivos impide que sean robustas.

7.2.19. Decreased Rank. Al atacante disminuir el valor del rango de un nodo, automáticamente garantiza que este avance dentro de la estructura de la topología ubicándose más cerca del sink. Esto lo logra por medio de la falsificación de mensajes DIO y tal posición le otorga privilegios como un mayor manejo del tráfico de red o control de nodos hijos legítimos, de los que puede tomar ventaja para desencadenar diversas agresiones (Le, y otros, 2013)

7.2.20. Clone ID y Sybil. A través de un ataque de clonación, el agente malicioso se apodera de un dispositivo legítimo con el fin de replicar varios clones que contengan su identidad. Una vez el proceso de copia haya finalizado, los nodos se distribuyen estratégicamente a lo largo de la red para orquestar ofensivas de gran impacto en el funcionamiento de la red (Wallgren, Raza, & Voigt, 2013).

En lo que respecta a los ataques Sybil, estos también se basan en la duplicación de identidades, aunque sus métodos no solamente dependen de la apropiación física de un nodo, sino que además son capaces de fabricar entidades lógicas impostoras que se asemejen al original. (Zhang, Liang, Lu, & Shen, 2014)

7.2.21. Byzantine. Este ataque se gesta cuando uno o varios nodos legítimos dentro de la red se encuentran comprometidos, pero continúan operando de manera encubierta por un período de tiempo. De esta manera el agresor se aprovecha de las credenciales de seguridad de red válidas para manipular la información de enrutamiento y alterar el funcionamiento general de la red (Geetha y Sreenath, 2016).

7.3 Soluciones y prevención contra ataques

Teniendo en cuenta la exposición del protocolo RPL debido a las vulnerabilidades de seguridad que lo rodean, se hace de vital importancia destacar las técnicas existentes para prevenir y mitigar la ocurrencia de agresiones en su contra. En primer lugar, se describirán los mecanismos de protección inherentes a RPL, luego se presentarán varios métodos para contrarrestar ataques específicos y por últimos se listarán los diferentes tipos de sistemas de detección de intrusos (IDS) usados para identificar eventos maliciosos en la red o en un dispositivo.

7.3.1 Mecanismos de protección inherentes a RPL. Los mecanismos de auto recuperación incluidos dentro de RPL aseguran que el protocolo funcione de manera segura y pueda superar ciertas inconsistencias básicas por sí mismo. En lo que respecta a los modos de seguridad, estos proporcionan algunas técnicas básicas que añaden otra capa de protección a la red.

7.3.1.1 Modos de seguridad. RPL cuenta con tres modos de soporte de seguridad opcionales, desarrollados mayormente con un enfoque a la autenticación de los mensajes de control DIO, DIS y DAO-ACK, utilizados por los nodos para la construcción de la topología e intercambio de información. Estos mensajes incluyen en su formato un campo con una bandera o *flag* que indica si la seguridad está habilitada. A continuación, y de acuerdo a Razali et al (2017), se listan los modos de seguridad disponibles para los mensajes de RPL:

- **Modo inseguro:** Es el predeterminado dentro del protocolo y como su nombre lo indica, a través de esta modalidad los paquetes de enrutamiento son transferidos sin componentes de seguridad.
- **Modo con llaves preinstaladas:** Estipula que para un nodo se integre a una instancia de RPL, sin importar la función que vaya a ejecutar dentro de la estructura (host o router), este debe contar con una clave preinstalada, proporcionando así mayor seguridad durante el intercambio de mensajes. La protección básica de dicha clave es posible por medio del esquema de cifrado por bloques AES.
- **Modo con autenticación:** Al igual que el anterior, los nodos también cuentan con credenciales preinstaladas, pero en esta modalidad la clave existente solo puede ser usada para unirse a una instancia de RPL como host. Este modo está reservado para futuras implementaciones

y por el momento las especificaciones del estándar describen que no debe ser compatible con criptografía simétrica.

Estas características básicas de seguridad de RPL pueden proteger la red contra ataques externos como se indica en Tsao et al. (2015). Sin embargo, se ha de resaltar que en el caso de que un dispositivo con una clave preinstalada sea manipulado desde el interior de la red, información vital de enrutamiento y de la topología lógica quedaría totalmente expuesta. He allí donde las limitaciones de las LLNs juegan un papel determinante al dificultar la implementación de mecanismos de autenticación más robustos.

7.3.1.2 Local repair y Trickle timer. RPL tiene mecanismos de reparación tanto globales como locales y estos pueden ejecutarse a raíz de alguna de las siguientes situaciones: fallas en la topología lógica de enrutamiento, desconexiones de enlaces entre nodos o simplemente problemas internos de un nodo.

La reparación local se encarga comúnmente del restablecimiento de links entre nodos padre e hijo y la reparación global se enfoca en solucionar los conflictos internos que puede sufrir un nodo, al punto de tener la capacidad de activar una reconstrucción de todo el DODAG. (Levis, Clausen, Hui, Gnawali, & Ko, 2011)

En lo que respecta al Trickle timer, como se describió en el capítulo anterior, este se reinicia cuando se detecta información de enrutamiento incongruente o eventos como modificaciones repentinas del parámetro rango de ciertos nodos dentro de la red. Logrando de esta manera combatir ciertas inconsistencias en el DODAG.

7.3.2 Métodos

Número de versión y Autenticación de rango (VeRA): Es un sistema de seguridad concebido con el objetivo de evitar que un nodo malicioso propague falsos valores de rango y número de version dentro de la red. Esto lo logra al generar una cadena por medio de una función hash que recibe como entrada un número aleatorio elegido por el nodo raíz. (Dvir, Holczer, & Levente, 2011)

TRAIL (TRust Anchor Interconnection Loop): Es un esquema de seguridad desarrollado para la autenticación de topología en RPL. TRAIL verifica rutas ascendentes hacia la raíz por medio de mensajes con el fin de detectar suplantaciones de rango y modificaciones en el número de version del DODAG. (Perrey, Landsmann, Ugus, Schmidt, & Wahlisch, 2015)

Protocolo Heartbeat: Es empleado en redes con enrutamiento IPv6, en el que se monitorea el estado de los nodos por medio del envío de una solicitud de eco ICMPv6 desde un router. En caso de no recibir respuesta del eco, se puede asumir que el tráfico está siendo filtrado en el trayecto a un nodo en particular o que el dispositivo está fuera de línea por alguna razón. Heartbeat es capaz de detectar ataques de reenvío selectivo, flooding y blackhole. (Kent, 2005)

Merkle tree authentication: Es un método que emplea una estructura de datos autenticada que asemeja la forma de un árbol. Su construcción inicia luego de la formación del DODAG y el arreglo categoriza a los nodos hijos como hojas y a los padres como ramas. Por medio de la clave pública y el ID del nodo se calcula un hash criptográfico, el cual sirve para validar la relación

legítima entre nodos padres e hijos. Este es comúnmente usado para evitar la ejecución del ataque Wormhole. (Khan, Shon, Lee, & Kim, 2014)

Whitelist / Blacklist: Con el objetivo de identificar y limitar el alcance de la suplantación de direcciones IP y MAC llevadas a cabo por ataques de clonación o sybil, se implementan listas blancas o negras. Por medio de estas se pueden agrupar nodos legítimos o maliciosos y su implementación es determinada por el tamaño de la red y la capacidad de administración del escenario.

7.3.3 Sistemas de detección de intrusos (IDS). Un sistema de detección de intrusos (IDS) se encarga principalmente de detectar y notificar actividades maliciosas e intrusiones no autorizadas en la red por medio de la constante monitorización de sus procesos. Este puede basarse en un software o un dispositivo dedicado y debido al extenso análisis que realiza sobre todos los patrones de actividad, es propenso a generar alertas por sospecha de ataques que en realidad no son, denominados falsos positivos (Chen & Chen, 2014). En general, existen cuatro categorías de IDS: basadas en detección de eventos, basadas en detección de firmas, basadas en host y basadas en especificaciones.

7.3.3.1 IDS basados en detección de eventos. A través de este sistema se detectan anomalías que aparte de ser notificadas de manera instantánea, contribuyen con la identificación de ataques particularmente desconocidos o nuevos. Por medio del almacenamiento de estos eventos en bases de datos que son continuamente actualizadas, el sistema es capaz de conformar patrones que dictaran pauta al momento de cotejar futuras ocurrencias maliciosas.

7.3.3.2 IDS basados en detección de firma. Las detecciones basadas en firmas identifican ataques al contrastar el tráfico y actividades en la red con patrones predefinidos denominados firmas. Estas pueden evaluar detalles como el número total de bytes de un archivo con el fin de verificar si corresponde con un evento malicioso conocido. La principal desventaja es que no son capaces de detectar nuevas amenazas ya que los patrones de las mismas pueden ser desconocidos.

7.3.3.3 IDS basados en host. Este tipo de sistema IDS utiliza un modelo de arquitectura híbrida y se enfoca en analizar las actividades y funcionalidades que residen en el interior de un dispositivo. Entre los sistemas más eficaces se encuentran los siguientes:

SVELTE, fue desarrollado específicamente para el IoT y ejecuta RPL. Está compuesto por un 6LoWPAN Mapper que hace las funciones de detección de intrusiones y un firewall. Este sistema detecta ataques de rango, inconsistencias de topología, sinkhole y reenvío selectivo. (Raza, Wallgren, & Voigt, 2013)

RIDES (Robust Intrusion Detection System), combina mecanismos de detección basados en firmas y eventos, los cuales implementa en redes de sensores con recursos limitados (Amin, Siddiqui, & Hong, 2009). Por medio de filtros Bloom y módulos capaces de identificar anomalías, los nodos dentro de la estructura analizan y alertan acerca del contenido de los paquetes.

7.3.3.4 IDS basados en especificaciones. Está fundamentado en la generación de alarmas al momento en que el comportamiento de los componentes que integran la red se desliga de lo preestablecido. Las técnicas más usadas por este sistema para definir los patrones de

reconocimiento son aprendizaje automatizado y transiciones de máquina de estado finito (FSM) (Le et al., 2012). Si bien el proceso de identificación de ataques varía dependiendo del tipo de amenaza, hay que destacar que son bastante efectivos con ofensivas de rango y local repair. En la Tabla 4 se resumen los mecanismos de acción que se pueden implementar para mitigar o contrarrestar ataques al protocolo RPL.

Tabla 4.

Ataques y Mecanismos de Prevención

Ataques	Implicaciones en la Red	Mecanismo de Prevención
Sinkhole	Tráfico comprometido al ser filtrado por el nodo atacante	SVELTE
Reenvío Selectivo	Alteración de rutas	Heartbeat Protocol
Repetición de información de enrutamiento	Afectación de nodos alrededor del atacante	Sequence Number (Winter, y otros, 2012)
Neighbor	Uso excesivo de recursos,	Ninguno hasta los momentos
Worst Parent	Suboptimización de la red	Ninguno hasta los momentos
Wormhole	Alteración del flujo del tráfico	Merkle tree authentication
Blackhole	Congestión y pérdida de paquetes	Trust Based (Airehrour, Gutierrez, & Ray, 2016)
Inconsistencia de DAO	Modificación de tablas de enrutamiento	Discarding Routing State (Huir & Vasseur, 2012)
Sinkhole	Tráfico comprometido al ser filtrado por el nodo atacante	SVELTE

Tabla 4. *(Continuación)*

Ataques	Implicaciones en la Red	Mecanismo de Prevención
Reenvío Selectivo	Alteración de rutas	Heartbeat Protocol
Repetición de información de enrutamiento	Afectación de nodos alrededor del atacante	Sequence Number (Winter, y otros, 2012)
Neighbor	Uso excesivo de recursos,	Ninguno hasta los momentos
Worst Parent	Suboptimización de la red	Ninguno hasta los momentos
Wormhole	Alteración del flujo del tráfico	Merkle tree authentication
Blackhole	Congestión y pérdida de paquetes	Trust Based (Airehrour, Gutierrez, & Ray, 2016)
Inconsistencia de DAO	Modificación de tablas de enrutamiento	Discarding Routing State (Huir & Vasseur, 2012)
Hello Flooding	Uso excesivo de energía	Local Repair
Sobrecarga de tablas de enrutamiento	Agotamiento de recursos como me	Ninguno
Basado en DIS	Rendimiento limitado de la red	TRAIL
Local Repair	Afectación del tráfico de red	Sistema basado en IDS
Rank	Loops, retrasos y pérdidas de datos	VERA, Sistema basado en IDS
Inconsistencia del DAG	Agotamiento de recursos	Limitar los reinicios del timer
Version Number	Retrasos y perdidas de paquetes	VERA
Denial of Service (DoS)	Inhabilitación de recursos	Sistema basado en IDS

Tabla 4. *(Continuación)*

Ataques	Implicaciones en la Red	Mecanismo de Prevención
Sniffing	Divulgación de datos críticos	Tunnelling (Tsao, y otros, 2015)
Análisis de Tráfico	Apropiación de información	Tunnelling (Tsao, y otros, 2015)
Clone ID / Sybil	Desestabilización de rutas	Sistema basado en IDS
Byzantine	Alteraciones de la red	Ninguno hasta los momentos

Nota: Extracto de "A comparative study on RPL attacks and security solutions", por S. Mangelkar, S. N. Dhage y A.V. Nimkar, 2017, *International Conference on Intelligent Computing and Control*, p. 1-6 (https://doi.org/10.1109/I2C2.2017.8321851).

8. Conclusiones

Trabajos previos han investigado las principales amenazas y ataques que afectan al protocolo RPL y las LLN, esto con el fin de formular ciertas propuestas que ofrezcan medidas para mitigarlas. Dichas soluciones generalmente conllevan sobrecargas adicionales que en mayor o menor grado alteran el funcionamiento de la red en general.

Dentro del grupo de agresiones más comunes se encuentran: DoS, sinkhole, reenvío selectivo, wormhole, modificación de DIS, Blackhole y las combinaciones que frecuentemente se ven entre ellas. Por medio de la variedad de estos ataques, un nodo malicioso puede aprovechar los mismos componentes y herramientas que integran la estructura y funcionamiento de RPL, como por ejemplo el trickle timer, el rango o el número de versión, para poner en peligro la operación de la red y su vida útil.

RPL proporciona algunos mecanismos de seguridad como la autenticación de sus mensajes de control por medio de la activación opcional del modo con llaves preinstaladas. Esto con el fin de establecer canales de comunicación segura entre nodos internos del DODAG y evitar que ciertos embates de agentes externos manipulen o capturen el tráfico legítimo. Además, existen medidas de auto reparación como el global repair y el trickle timer, que incrementan la capacidad de recuperación del protocolo para hacer frente a ciertas inconsistencias. Sin embargo, con todo y estos mecanismos de protección básicos, los nodos no están totalmente a salvo de la mayoría de las amenazas que se originan tanto desde afuera como desde adentro de la propia red RPL.

Las arquitecturas de monitoreo y los IDS han demostrado ser soluciones adecuadas para contrarrestar los ataques internos, no obstante, pueden inducir costos de implementación significativos ya que involucran infraestructura dedicada y nodos más potentes dentro de su concepción. Debido a los costos elevados para aplicar estas medidas de seguridad, la gestión de riesgos ofrece la opción de evaluar dinámicamente los peligros a los que se está expuesto antes de definir una solución.

La protección de los nodos del mundo exterior depende del cifrado de datos, que combina algoritmos criptográficos y gestión de claves. La criptografía asimétrica sigue siendo un desafío abierto para las LLN y actualmente queda fuera del proceso de estandarización. Por lo tanto, los futuros documentos complementarios de los estándares deberían definir claramente cómo abordar este y otros retos.

9. Recomendaciones

1. Es necesaria la realización de estudios de investigación más profundos con el objetivo de encontrar soluciones para contrarrestar ataques sobre RPL y redes LLN que todavía no han sido evaluados.

2. Es esencial adaptar y diseñar subsistemas relacionados que refuercen los esquemas de autenticación en RPL como gestión de claves, credenciales y encriptación.

3. Se deben ejecutar periódicamente auditorías de configuración y parches actualizados en dispositivos IoT implementados dentro del entorno empresarial.

4. Tomar conciencia y evaluar la relación entre beneficios y exposiciones de seguridad que conlleva el uso en general del IoT.

Referencias Bibliográficas

Airehrour, D., Gutierrez, J., & Ray, K. (2016). *Securing RPL routing protocol from Blackhole attacks using a trust-based mechanism.* Obtenido de 26th International Telecommunication Networks and Applications Conference (ITNAC), 115-120.: https://doi.org/10.1109/ATNAC.2016. 7878793

Amin, S., Siddiqui, M., & Hong, C. (2009). *A novel coding scheme to implement signature based IDS in IP based Sensor Networks.* . Obtenido de Integrated Network Management Workshops IFIP/IEEE International Symposium. : https://10.1109/INMW.2009.5195973

Amin, Y., & Hamid, A. (2015). *Classification and analysis of IEEE 802.15.4 MAC layer attacks.* Obtenido de International Conference on Innovations in Information Technology (IIT), 74-79.: https://doi.org/10.1109/INNOVATIONS.2015.7381518

Ancillotti, E., Bruno, R., Conti, M. (2013). The roles of the RPL routing protocol for smart grid communications. *IEEE Communications Magazine, 51,* 75-83. https://doi.org/10.1109/MCOM.2013.6400442

Andy, S., Rahardjo, B., & Hanindhito, B. (2017). *Attacks scenarios and security analysis of MQTT Communication protocol in IoT system.* Obtenido de 4th International Conference on Electrical Engineering, Computer Science and Informatics, 1-6: https://doi.org/10.1109/EECSI.2017. 8239179

Anthea, M., Badonnel, R., Chrisment, I. (2016). A Taxonomy of Attacks in RPL-based Internet of Things. *International Journal of Network Security, 18*(3), 459-473. Obtenido de https://hal.inria.fr/hal-01207859/

Anthea, M., Sehgal, A., Badonnel, R., Chrisment, I, Schonwalder, J. (2014). A study of RPL DODAG version attacks. Monitoring and Securing Virtualized Networks and Services, 8508, 92-104. Obtenido de https://doi.org/10.1007/978-3-662-43862-6_12

Arena, A., Perazzo, P., Vallati, C., Dini, G., & Anastasi, G. (2019). *Evaluating and improving the scalability of RPL security in the Internet of Things.* Obtenido de Computer and Communications, 151, 119-132. https://doi.org/10.1016/j.comcom.2019.12.062

Ashwini, R., & Mohnami, P. (2015). *Application of Wireless Sensor Network in Home Automation.*. Obtenido de International Journal of Computer & Organization Trends, 4(3), 64-71: http://www.ijcotjournal.org/

Bhardwaj, M. (23 de Septiembre de 2017). *IoT device security: A comprehensive look, from edge to cloud*. Obtenido de https://www.iotworldtoday.com/2017/09/23/iot-device-security-comprehensive-look-edge-cloud/

Bormann, C., Castellani, A., & Shelby, Z. (2012). *CoAP: An Application Protocol for Billions of Tiny Internet Nodes.* Obtenido de IEEE Internet Computing, 16(2), 62-67. https://doi.org/10.1109/MIC. 2012.29

Calderón, W. (2014). *Diseño e implementación de un sistema genérico de monitoreo usando redes de sensores inalámbricos con el protocolo 6LowPAN (tesis de maestría).* . Bogotá, Colombia: Universidad Nacional de Colombia.

Chen, J., & Chen, C. (2014). *Design of Complex Event-Processing IDS in Internet of Things.* Obtenido de Sixth International Conference on Measuring Technology and Mechatronics Automation, 226-229. : https://doi: 10.1109/ICMTMA.2014.57

Cisco Systems Inc. (2015). *OSPF Design Guide*. Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Cisco Systems Inc. (2018). *Cisco Visual Networking Index: Forecast and Trends, 2017-2022 White Paper (1551296909190103).* Obtenido de https://www.cisco.com/c/en/us/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

Clausen, T., Dearlove, C., Jacquet, P., & Herberg, U. (2014). *The Optimized Link State Routing Protocol Version 2. RFC 7181.* . Obtenido de https://tools.ietf.org/html/rfc7181

Contiki OS Org. (2019). *The Contiki Operating System*. https://github.com/contiki-os/contiki

Contiki-NG Wiki . (2019). *Contiki Documentation.* Obtenido de https://github.com/contiki-ng/contiki-ng/wiki

Dohler, M., Watteyne, T., Winter, T., & Barthel, D. (2009). *Routing Requirements for Urban Low – Power and Lossy Networks. RFC 5548.* Obtenido de https://tools.ietf.org/html/rfc5548

Ducklin, P. (5 de Octubre de 2016). *Mirai "Internet of things" malware from DDoS attack goes open Source. Naked security by Sophos.* Obtenido de https://nakedsecurity.sophos.com/2016/10/05/mirai-Internet-of-things-malware-from-krebs-ddos-attack-goes-open-source/

Dvir, A., Holczer, T., & Levente, B. (2011). *VeRA – version number and rank authentication in RPL*. Obtenido de IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 709-714. https://10.1109/MASS.2011.76

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. (1999). *Hypertext Transfer Protocol – HTTP/1.1. RFC 2616.* Obtenido de https://tools.ietf.org/html/rfc2616

Gaddour, O., & Koubaa, A. (2012). *RPL in a nutshell: A survey.* Obtenido de Computer Networks, 56(14), 3163-3178: https://www.sciencedirect.com/science/article/abs/pii/S1389128612002423

Gawade, A., & Shekokar, N. (2017). *Lightweight Secure RPL: A need in Iot.* Obtenido de International Conference on Information Technology, 214-219. https://doi.org/10.1109/ICIT.2017.31

Gilchrist, A. (2017). *IoT Security Issues.* . Obtenido de De Gruyter Press. ISBN: 9781501505621. https://books.google.com.co/books?id=xipDDgAAQBAJ

Goodin, D. (2017). *BrickerBot, the permanent denial-of-service botnet, is back with a vengeance.* Obtenido de https://arstechnica.com/information-technology/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/

Goyal, P., & Goyal, A. (2017). *Comparative study of two most popular packet sniffing tools - Tcpdump and Wireshark.* Obtenido de 9th International Conference on Computational Intelligence and Communication Networks (CICN), 77-81: https://doi.org/10.1109/CICN.2017.8319360

Granjal, J., Monteiro, E., & Silva, J. (2015). *Security for the Internet of Things: A Survey of Existing Protocols and Open Research.* Obtenido de IEEE Communications Surveys & Tutorials, 17(3), 1294 - 1312: https://doi.org/10.1109/COMST.2015.2388550

Hakeem, S., Hady, A., & Kim, H. (2019). *RPL Routing Protocol Performance in Smart Grid Applications Based Wireless Sensors: Experimental and Simulated Analysis.* Obtenido de Electronics 2019, 8(2), 186. https://doi.org/10.3390/electronics8020186

Holloway, M. (16 de Julio de 2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities.* Obtenido de Department Of Physics Stanford University. http://large.stanford.edu/courses/2015/ph241/holloway1

Huir, J., & Vasseur, J. (2012). *The Routing for Low-Power and Loosy Network (RPL) Option for Carrying RPL Information in Data-Plane Datagrams. RFC 6553.* Obtenido de ttps://tools.ietf.org/html/rfc6553h

Ibarra, J., Gónzalez, F., Flores, B., Burtseva, L., & Astorga, M. (2017). *Tracking the Evolution of the Internet of Things Concept Across Different Application Domains.* Obtenido de Sensors an Open Access Journal, 17(6), 1379 - 1404. : https://doi.org/10.3390/s17061379

IEEE (2016). Errata to IEEE Standard for Low-Rate Wireless Personal Area Networks (WPANs). Recuperado de https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/erratas/802.15.4-2015_errata.pdf

IEEE. (2003). *Standard for Telecommunications and Information Exchange and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 15: Wireless Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal*. Obtenido de Area Networks (WPAN). IEEE Std 802.15.4-2003, 1-680. https://doi.org/10.1109/IEEESTD.2003.94389

IEEE. (2011). *Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPAN). IEEE Std 802.15.4-2011(Revision of IEEE Std 802. 15.4-2006),1-314.* Obtenido de https://doi.org/10.1109/IEEESTD.2011.6012487

IETF. (2018). *Routing Over Low power and Lossy networks (roll).* Obtenido de https://datatracker.ietf.org/wg/roll/about/

International Organization for Standardization. (2000). *ISO 7498-2:1989 Security Architecture Standard.* Obtenido de https://www.iso.org/obp/ui/#iso:std:iso:7498:-2:ed-1:v1

Iova, O., Picco, G., Istomin, T., & Kiraly, C. (2017). *RPL, the Routing Standard for the Internet of Things. Or Is It?*. Obtenido de IEEE Comunications Magazine, Institute of Electrical and Electronics Engineers, 54(12), 16-22. Obtenido de https://hal.archives-ouvertes.fr/hal-01647152

Kamgueu, P., Nataf, E., & Djotio, T. (2018). *Survey on RPL enhancements: A focus on topology, security and mobility.* Obtenido de Computer Communications, 120, 10-21. https://doi.org/10.1016/j.comcom.2018.02.011

Kent, S. (2005). *IP Encapsulating Security Payload (ESP). RFC 4303.* Obtenido de https://tools.ietf.org/html/rfc4303

Khan, F., Shon, T., Lee, T., & Kim, K. (2014). *Merkle tree-based wormhole attack avoidance Mechanism in low power and lossy network based networks.* Obtenido de Security and Communication Networks, 7, 1292-1309. https://doi: 10.1002/sec.1023

Kivinen, T., & Kinney, P. (2017). *IEEE 802.15.4 Information Element for the IETF. RFC 8137.* . Obtenido de https://tools.ietf.org/html/rfc8137

Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, And Goals. RFC 4919.* Obtenido de https://tools.ietf.org/html/rfc4919

Largent, W. (23 de Mayo de 2018). *New VPNFilter targets at least 500K networking devices worldwide.* Obtenido de Cisco Talos Blog. https://blog.talosintelligence.com/2018/05/VPNFilter.html

Le, A., Loo, J., Lasebae, A., Aiash, M., Luo, Y. (2012). 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection. *International Journal of Communication Systems, 25*(9), 1189-1212. Obtenido de https://doi.org/10.1002/dac.2356

Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., Chai, M. (2013). The impact of rank attack on network topology of RPL networks. *IEEE Sensor, 13*(10), 3685-3692. Obtenido de https://doi.org/10.1109/JSEN.2013.2266399

Levis, P., Clausen, T., Hui, J., Gnawali, O., & Ko, J. (2011). *The Trickle Algorithm. RFC 6206.* Obtenido de https://tools.ietf.org/html/rfc6206

Madan, K., Bagavathi, C., & Shalini, K. (2014). *A power efficient MAC protocol for quality of service evaluation in wireless sensor networks.* Obtenido de International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 2(11), 2154-2158. Obtenido de https://ijireeice.com

Masirap, M., Amaran, M., Yusoff, Y., Rahman, A., & Hashim, H. (2016). *Evaluation of reliable UDP based transport Protocols for Internet of Things (IoT).* Obtenido de IEEE Symposium on Computer Applications & Industrial Electronics, 200-205: Obtenido de https://doi.org/10.1109/ISCAE.2016.7575063

Nagrath, P., & Gupta, B. (2011). *Wormhole attacks in wireless adhoc networks and their counter measurements: a survey.* Obtenido de 3rd International Conference on Electronics Computer Technology, 6, 245-250. https://doi/10.1109/ICECTECH.2011.5942091

Naik, N. (2017). *Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP And HTTP*. Obtenido de IEEE International Systems Engineering Symposium, 1-7: https://doi.org/10.1109/SysEng.207.8088251

Panagiotis, I., Panagiotis, G., & Ioannis, M. (2018). *Securing th-e Internet of Things: Challenges, threats and solutions.* Obtenido de Internet of Things, 5, 41-70. https://doi.org/10.1016/j.iot.2018.11.003

Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561.* . Obtenido de https://tools.ietf.org/html/rfc3561

Perrey, H., Landsmann, M., Ugus, O., Schmidt, T., & Wahlisch, M. (2015). *TRAIL: Topology Authentication in RPL. Cornell University.* Obtenido de https://arxiv.org/abs/1312.0984

Piñeres, G. (2015). *Evaluación del Rendimiento del Protocolo 6LowPAN sobre una plataforma de hardware y Software libre (tesis de maestría).* Cartagena de Indias, Colombia: Universidad Tecnológica de Bolívar.

Pongle, P., & Chavan, G. (2018). *A Survey: Attacks on RPL and 6LowPAN in IoT.* . Obtenido de International Journal of Advance Research in Science and Engineering, 7(3), 55-69.: http://www.ijarse.com

Press, G. (18 de Junio de 2014). *A Very Short History Of The Internet Of Things. Forbes.* Obtenido de https://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/#4fla05d110de

Pu, C. (2018). Mitigation DAO inconsistency attack in RPL-based low power and lossy networks. *IEEE 8th Annual Computing and Communication Workshop and Conference*, 570-574. Obtenido de https://doi/10.1109/CCWC.2018.8301614

Pu, C. (2019). *Spam DIS Attack Against Routing Protocol in the Internet of Things.* . Obtenido de 2019International Conference on Computing, Networking and Communications (ICNC), 73-77. : https://doi.org/10.1109/ICCNC.2019.8685628

Ramonet, A., & Noguchi, T. (2019). *IEEE 802.15.4 Historical Evolution and Trends.* Obtenido de 2019 21st International Conference on Advanced Communication Technology, 351-359.: https://doi.org/10.23919/ICACT.2019.8702040

Raza, S., Duquennoy, S., Hoglund, J., & Roedig, U. (2014). *Secure communication for the Internet of Things – A comparison of link-layer security and IPsec for 6LoWPAN. Security and Communication Networks, 7(12), 2654-2668.* Obtenido de https://doi.org/10.1002/sec.406

Raza, S., Wallgren, L., & Voigt, T. (2013). *SVELTE: Real-Time Intrusion Detection in the Internet of Things. Ad Hoc Networks, 11(8), 2661-2674.* Obtenido de https://10.1016/j.adhoc.2013.04.014

Razali, M., Rusli, M., Jamil, N., Ismail, R., & Yussof, S. (2017). *The authentication techniques for enhacing the RPL security mode: A survey*. Obtenido de Proceedings of the 6th International Conference on Computing & Informatics, 119, 735-743. https://www.uum.edu.my

Rescorla, E., & Modadugu, N. (2012). *Datagram transport layer security version 1.2. RFC 6347.* Obtenido de https://tools.ietf.org/html/rfc6347

Rghiout, A. Khannous, A., Bouhorma, M. (2014). Denial-of-service attacks on 6LowPAN-RPL networks: issues and practical solutions. *Journal of Advanced Computer Science & Technology, 3*(2), 143-153. Obtenido de https://doi.org/10.14419/jacst.v3i2.3321

Riot-OS Org. (2019). *RIOT: The friendly Operating System for the Internet of Things.* Obtenido de https://doc.riot-os.org/index.html

Robles, I. (24 de Abril de 2018). *ROLL on a roll! IETF Journal.* Obtenido de https://www.ietfjournal.org/roll-on-a-roll/

Rose, K., Eldridge, S., & Chapin, L. (2015). *La Internet de las Cosas – Una breve reseña.* Obtenido de https://www.Internetsociety.org/es/resources/doc/2015/iot-overview

Sánchez, G. (2019, Febrero 22). *¿A dónde nos llevará la agricultura de precisión?* Agro negocios. Obtenido de https://www.agronegocios.co/analisis/gabriel-sanchez-2830947/a-donde-nos-llevara-la-agricultura-de-precision-2830945

Sebastian, A., Sivagurunathan, S. (2018). Multi DODAGs in RPL for Reliable Smart City IoT. *Journal of Cyber Security, 7*(1), 69-86. Obtenido de https://doi.org/10.13052/jcsm2245-1439.716

Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). *A roadmap for security challenges in the Internet of Things*. Obtenido de Digital Communications and Networks, 4(2), 118-137. https://www.sciencedirect.com/science/article/pii/S2352864817300214

Sharma, C., & Gondhi, N. (2018). *Communication Protocol Stack for Constrained IoT System.* Obtenido de 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, 1-6. http://doi.org/10.1109/IoT-SIU.2018.8519904

Sharma, D., Mishra, I., Jain, S. (2017). A Detailed Classification of Routing Attacks against RPL in Internet of Things. *International Journal of Advance Research, Ideas and Innovations in Technology*, *3*(1), 692-703. Obtenido de https://www.ijariit.com

Shirey, R. (2007). *Internet Security Glossary, Version 2. RFC 4949.* Obtenido de https://tools.ietf.org/html/rfc4949

Sobral, J., Rodrigues, J., Rabelo, R., Al-Muhtadi, J., & Korotaev, V. (2019). *Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications. .* Obtenido de Sensors an Open Access Journal, 19(9), 21-44.: https://doi.org/10.3390/s19092144

Taladriz, O. (2016, Marzo 7). *Resumen visual del estándar 802.15.4.* Obtenido de http://elb105.com/resumen-visual-del-estandar-802-15-4/

Thubert, P. (2012). *Objective Function Zero for The Routing Protocol for Low-Power and Lossy Networks (RPL). RFC 6552.* Obtenido de https://tools.ietf.org/html/rfc6552

TinyOS Wiki. (12 de Mayo de 2013). *TinyOS Overview.* Obtenido de http://tinyos.stanford.edu/tinyos-wiki/index. php/TinyOS_Overview

Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., & Richardson, M. (2015). *A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). RFC 7416, 4.* . Obtenido de https://tools.ietf.org/html/rfc7416

Wallgren, L., Raza, S., & Voigt, T. (2013). *Routing Attacks and Countermeasures in the RPL-Based Internet of Things.* Obtenido de International Journal of Distributed Sensor Networks, 9(8), 13-24. https://doi.org/10.1155/2013/794326

Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., . . . Alexander, R. (2012). *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550, 8.* Obtenido de https://tools.ietf.org/html/rfc6550

Wu, H., Ke, K., Wang, S., Chen, P., Lee, G., Tseng, C., & Ho, C. (2019). *The implementation of Wireless Industrial Internet of Things (IIoT) Based Upon IEEE 802.15.4-2015 TSCH Access Mode. IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl C.* Obtenido de Intl Conf on Cyber Science and Technology Congress, 367-369. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00075

Yang, W., Wang, Y., Lai, Z., Wan, Y., & Cheng, Z. (2018). *Security Vulnerabilities and Countermeasures in the RPL-Based Internet of Things. 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 49-495.* Obtenido de https://doi.org/10.1109/CyberC.2018.00020

Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). *Sybil attacks and their defenses in the Internet of things.* Obtenido de IEEE Internet of Things Journal, 1(5), 372-383. https://doi.org/10.1109/JIOT.2014. 2344013