Análisis de vulnerabilidades en sistemas IEEE 802.15.4/ZigBee

Miguel Ángel Cazalla Barranco
Máster Universitario de Ingeniería de Telecomunicación - UOC
Telemática

José López Vicario
Xavi Vilajosana Guillen

Junio 2019


Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Análisis de vulnerabilidades en sistemas IEEE 802.15.4/ZigBee*
Nombre del autor:	*Miguel Ángel Cazalla Barranco*
Nombre del consultor/a:	*José López Vicario*
Nombre del PRA:	*Xavi Vilajosana Guillen*
Fecha de entrega (mm/aaaa):	06/2019
Titulación::	*Máster Universitario de Ingeniería de Telecomunicación - UOC*
Área del Trabajo Final:	*Telemática*
Idioma del trabajo:	***Castellano***
Palabras clave	*IoT, IEEE 802.15.4, ZigBee*

Resumen del Trabajo:

En el ecosistema de productos del Internet de las Cosas, cada día aparecen más dispositivos conectados a Internet y capaces de crear redes inalámbricas de área personal para integrarse en nuestro día a día y facilitar la vida a las personas, tanto en la automatización de tareas del hogar como en la implantación de nuevos tipos de sensores y actuadores en redes industriales.

Uno de los protocolos de comunicaciones más utilizados es el stack IEEE 802.15.4 / ZigBee, caracterizado por su bajo coste de implementación y el bajo consumo de energía.

En este TFM se han estudiado las características técnicas de ambos protocolos, haciendo un especial énfasis en los mecanismos de seguridad utilizados para proteger la información que transportan.

Mediante la creación de un escenario de pruebas, se han llevado a cabo una serie de ataques que han permitido comprobar el alcance y consecuencias para la confidencialidad, integridad y disponibilidad de la información transportada por redes ZigBee que hayan sido concebidas con una mala o nula implementación de medidas de seguridad en los dispositivos que la componen.

Se presentan, pues, las posibles vulnerabilidades que pueden llegar a producirse, los ataques llevados a cabo para su explotación, las contramedidas necesarias para mitigarlos o eliminarlos, así como un conjunto de conclusiones que ayuden a desarrolladores y fabricantes en la correcta implementación de la seguridad en el stack IEEE 802.15.4 / ZigBee.

Abstract:

In the ecosystem of Internet of Things products, every day there are more devices connected to the Internet and capable of creating wireless personal area networks to be integrated into our day to day and facilitate people's life, both in the automation of home tasks and in the implementation of new types of sensors and actuators in industrial networks.

One of the most used communication protocols is the IEEE 802.15.4 / ZigBee stack, characterized by its low implementation cost and low power consumption.

In this TFM, the technical characteristics of both protocols have been studied, with special emphasis on the security mechanisms used to protect the information they carry.

Through the creation of a test scenario, a series of attacks have been carried out that have allowed to verify the scope and consequences for the confidentiality, integrity and availability of the information transported in ZigBee networks that have been conceived with a bad or ineffective implementation of security measures in the devices that compose it.

Therefore, the possible vulnerabilities that may occur are presented, the attacks carried out for its exploitation, the necessary countermeasures to mitigate or eliminate them, as well as a set of conclusions that help developers and manufacturers in the correct implementation of security in the IEEE 802.15.4 / ZigBee stack.

Agradecimientos

A Jose y Xavi, por la ayuda y consejos durante este trabajo.
A mi familia, especialmente a mis padres y hermano, por su apoyo constante.
A mi mujer, Aurora, por su infinita ayuda y paciencia, por hacer suyo también la consecución de este gran objetivo.
A mi hija, Alba, por ser mi motivación cada día.

Índice de contenido

Índice de figuras

Índice de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

En un mundo tan globalizado, en el que el número de dispositivos conectados a Internet crece de forma desmesurada, se hace imprescindible conocer el estado de la seguridad de los dispositivos que, entre otras cosas, vamos introduciendo en los hogares para la automatización y ayuda en labores domésticas: hornos, tostadoras, cámaras de vigilancia, bombillas, enchufes, y un amplio abanico de dispositivos que componen lo que hoy día se conoce como el **Internet de las Cosas** (**IoT**, del inglés *Internet of Things*).

Ante tal escenario, los tipos de dispositivos disponibles y sus aplicaciones en entornos industriales y domésticos, nos surgen una serie de cuestiones que hemos tratado de resolver a lo largo de este trabajo: ¿qué clase de productos se utilizan en este tipo de entornos? ¿cuál es la topología de la red utilizada para interconectarlos? ¿qué características comunes y particulares tienen? ¿cómo se comunican entre ellos? ¿implementan algún mecanismo de seguridad para proteger tales comunicaciones? ¿existe la posibilidad de vulnerar o evadir estos mecanismos? ¿cómo? ¿cuál es el potencial de ataque en un entorno doméstico?

Con la realización de este Trabajo Final de Máster se ha perseguido estudiar y analizar las vulnerabilidades existentes en sistemas IEEE 802.15.4/ZigBee, ya sea aquellas inherentes a la tipología del medio de comunicación inalámbrico utilizado como aquellas debidas a implementaciones del protocolo o específicas de éste, de manera que pueda tenerse una instantánea del estado de la seguridad de dicho protocolo así como extraerse algunas recomendaciones y/o mejoras que ayuden en la adopción de medidas de mitigación o eliminación de tales vulnerabilidades.

1.2 Objetivos del Trabajo

El objetivo principal de este Trabajo Final de Máster consiste en el análisis de las vulnerabilidades existentes en sistemas IEEE 802.15.4/ZigBee mediante un el estudio de esta familia de protocolos, su tecnología y los distintos elementos que la componen.

El logro de este objetivo principal puede dividirse en la consecución de una serie de objetivos más concretos:

- Estudio del estándar IEEE 802.15.4 correspondiente al nivel físico y de control de acceso al medio de redes inalámbricas de área personal con tasas bajas de transmisión de datos (Low-Rate Wireless Personal Area Network, LR-WPAN).

- Estudio del protocolo de comunicación ZigBee, sus funcionalidad y características principales, el estado de su implementación y uso, así como los productos más conocidos que hacen uso de este protocolo.

- Estudio de la aplicación de esta familia de protocolos, principalmente centrada en Internet of Things (IoT), redes de sensores, sistemas de control industrial, etc.

- Estudio y análisis de las posibles vulnerabilidades específicas del protocolo.

- Explotación, en la medida de los posible, de las vulnerabilidades analizadas del protocolo mediante la creación de un escenario de pruebas donde se han utilizado un conjunto de dispositivos que utilizan este protocolo para sus comunicaciones inalámbricas.

- Establecer algunas mejoras o consejos que ayuden en la implementación segura del protocolo y que permitan minimizar o eliminar dichas vulnerabilidades.

1.3 Enfoque y método seguido

El desarrollo de este trabajo ha sido llevado a cabo teniendo en cuenta el objetivo final: el estudio y análisis de vulnerabilidades en sistemas IEEE 802.15.4/ZigBee. Para ello, previamente, ha sido necesario un trabajo de estudio y documentación de las características y aspectos fundamentales de dicha tecnología que nos ayude a comprender la naturaleza de su funcionamiento, los elementos que la componen, su arquitectura, así como las medidas de seguridad que implementan con el objetivo de proteger la información transmitida.

Así pues, primeramente, se ha elaborado un esquema o guion sobre los temas técnicos a abordar más relevantes, con el objetivo de dirigir el estudio en la adquisición de los conocimientos necesarios que permitan la consecución del objetivo final, llevando a cabo un trabajo de investigación, recopilación de información teniendo siempre presente los puntos necesarios para el trabajo, sintetizando los aspectos fundamentales en la presente memoria.

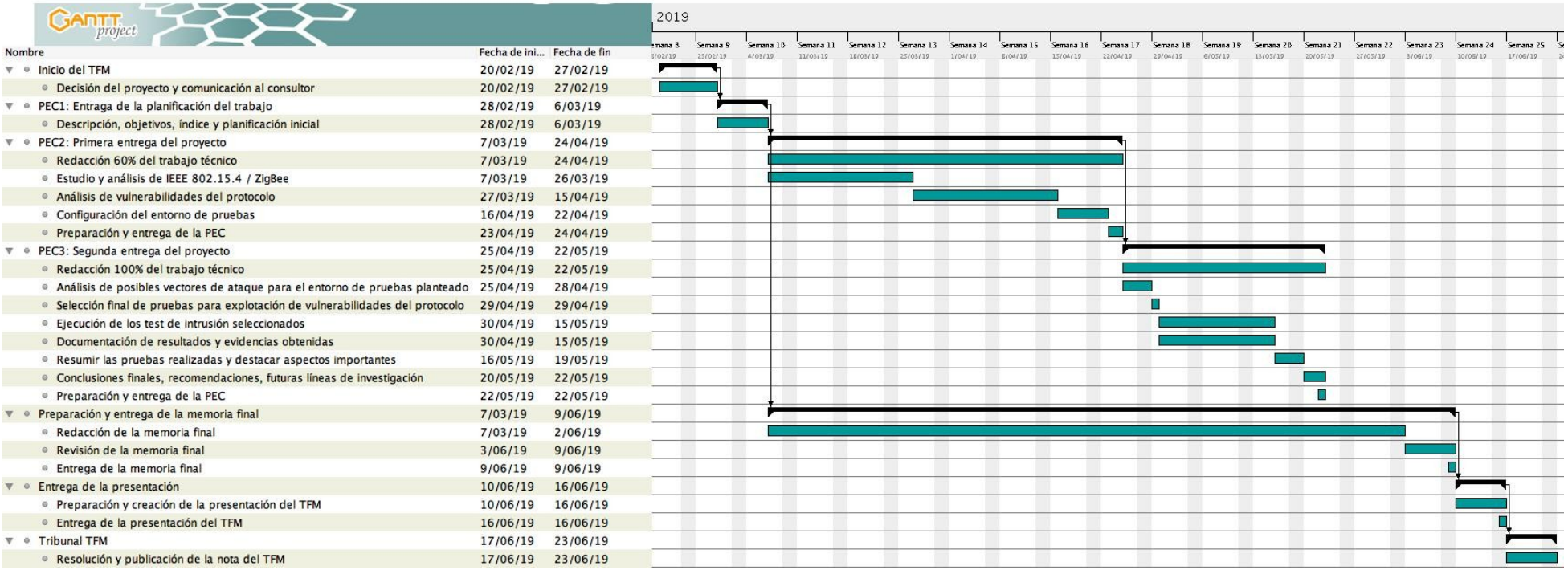
Posteriormente, se procedió a la creación de un pequeño laboratorio con dispositivos específicos 802.15.4/ZigBee con la intención de investigar y analizar su desempeño, centrando el estudio en el análisis de la seguridad y sus posibles vulnerabilidades.

Finalmente, se recogen los resultados obtenidos de la investigación realizada, resaltando los aspectos más importantes y que consideramos de mayor impacto en la seguridad de las comunicaciones de los dispositivos IEEE 802.15.4 ZigBee, así como una serie de recomendaciones y líneas de investigación futuras que ayuden a una adecuada securización en la utilización de esta tecnología.

1.4 Planificación del Trabajo

A continuación, se presenta la planificación seguida para este Trabajo Final de Máster, donde se recogen los hitos más importantes en los que se divide el trabajo, así como las tareas y objetivos a tener en cuenta en cada uno de ellos. En base a una planificación inicial establecida, ésta se ha ido adaptando según la valoración de esfuerzo necesaria en cada tarea a medida que se profundizaba en el estudio y se abordaban los trabajos técnicos, de manera que se produjera un alineamiento en las fechas finales de entrega establecidas para este trabajo.

Así pues, la planificación final llevada a cabo se recoge en el siguiente Diagrama de Gantt:


GANTT project
2019
Nombre
Fecha de ini...
Fecha de fin
Inicio del TFM 20/02/19 27/02/19
Decisión del proyecto y comunicación al consultor 20/02/19 27/02/19
PEC1: Entraga de la planificación del trabajo 28/02/19 6/03/19
Descripción, objetivos, índice y planificación inicial 28/02/19 6/03/19
PEC2: Primera entrega del proyecto 7/03/19 24/04/19
Redacción 60% del trabajo técnico 7/03/19 24/04/19
Estudio y análisis de IEEE 802.15.4 / ZigBee 7/03/19 26/03/19
Análisis de vulnerabilidades del protocolo 27/03/19 15/04/19
Configuración del entorno de pruebas 16/04/19 22/04/19
Preparación y entrega de la PEC 23/04/19 24/04/19
PEC3: Segunda entrega del proyecto 25/04/19 22/05/19
Redacción 100% del trabajo técnico 25/04/19 22/05/19
Análisis de posibles vectores de ataque para el entorno de pruebas planteado 25/04/19 28/04/19
Selección final de pruebas para explotación de vulnerabilidades del protocolo 29/04/19 29/04/19
Ejecución de los test de intrusión seleccionados 30/04/19 15/05/19
Documentación de resultados y evidencias obtenidas 30/04/19 15/05/19
Resumir las pruebas realizadas y destacar aspectos importantes 16/05/19 19/05/19
Conclusiones finales, recomendaciones, futuras líneas de investigación 20/05/19 22/05/19
Preparación y entrega de la PEC 22/05/19 22/05/19
Preparación y entrega de la memoria final 7/03/19 9/06/19
Redacción de la memoria final 7/03/19 2/06/19
Revisión de la memoria final 3/06/19 9/06/19
Entrega de la memoria final 9/06/19 9/06/19
Entrega de la presentación 10/06/19 16/06/19
Preparación y creación de la presentación del TFM 10/06/19 16/06/19
Entrega de la presentación del TFM 16/06/19 16/06/19
Tribunal TFM 17/06/19 23/06/19
Resolución y publicación de la nota del TFM 17/06/19 23/06/19

1.5 Breve sumario de productos obtenidos

A continuación se señalan una serie de puntos que resumen los productos obtenidos en este trabajo.

- Se han documentado las características técnicas del stack de protocolos IEEE 802.15.4 / ZigBee, estando enfocados, en gran medida, en los mecanismos de segurida que implementan para proteger tanto a dispositivos como a la información transmitida en este tipo de redes.

- Se han analizado las posibles vulnerabilidades que afectan al protocolo, principalmente, debidas a una escasa o nula implementación de seguridad en el diseño y creación de este tipo dispositivos.

- Se han llevado a cabo una serie de pruebas de explotación a un entorno de pruebas planteado, de manera que se ha podido demostrar la viabilidad y alcance de este tipo de ataques.

- Se especifican las contramedidas a tener en cuenta a la hora de mitigar o eliminar por completo este tipo de amenazas.

- Se recogen una serie de recomendaciones que ayuden en implementación segura del stack de comunicaciones IEEE 802.15.4 / ZigBee, de forma puedan ser tenidas en cuenta en la construcción de aplicaciones y dispositivos destinados a entornos domésticos e industriales.

- Se indican un conjunto de líneas de investigación que, en base al presente trabajo, podrían realizarse en un futuro con el objetivo de profundizar en el estudio de entornos y situaciones de uso del stack de protocolos.

1.6 Breve descripción de los otros capítulos de la memoria

Una breve descripción de los capítulos contenidos en esta memoria se indican a continuación:

- Capítulo 2: Estado del arte. Se trata del capítulo central en el que se recogen todos los detalles técnicos sobre los que se apoya el estudio y pruebas posteriores del protocolo. Así, se ha indicado en qué consiste el Internet de las Cosas y su enfoque en redes inalámbricas de área personal. Se han explicado y documentado los protocolos IEEE 802.15.4 y ZigBee, haciendo especial atención a las medidas de seguridad que, desde su diseño, adoptan para proteger la información transportada por ellos.

- Capítulo 3: Análisis de seguridad IEEE 802.15.4 / ZigBee. En base al estudio previo del Capítulo 2, se ha llevado a cabo un análisis de las posibles vulnerabilidades del stack de protocolos, detallando las herramientas software y hardware empleadas para la realización de dicho estudio. Se ha planteado un escenario de pruebas, compuesto por dos dispositivos configurables Xbee, que simulan un entorno de WPAN, y un dispositivo Api-Mote, con el que realizar la captura e inyección de paquetes de datos en dicha red.

- Capítulo 4: Detalle de las pruebas realizadas: Para una mayor claridad en la redacción del presente documento, se han documentado las pruebas y ataques realizados en un capítulo aparte, donde se recogen capturas de patalla de configuraciones de los dispositivos empleados, comandos y script ejecutados, así como capturas de tráfico que han determinado el éxito o fracaso en los ataques abordados.

- Capítulo 5: Conclusiones y líneas futuras. Se recogen una serie de conclusiones extraídas del estudio de la seguridad el stack IEEE 802.15.4 / ZigBee y los ataques realizados, de forma que se resaltan los aspectos más importantes del trabajo y el resultado de los análisis de capítulos anteriores. Además, se detallan algunas líneas futuras de investigación a tener en cuenta para trabajos posteriores y que puedan utilizar este mismo como punto de partida.

- Capítulo 6: Glosario. Se recogen los términos y acrónimos más importantes que aparecen en este trabajo.

- Capítulo 7: Bibliografía. Recoge el conjunto de referencias utilizadas en el estudio, documentación y pruebas se han llevado a cabo para dar forma y contexto a este documento.

2. Estado del arte

2.1 Proyectos y trabajos relacionados

Con el objetivo de poner en contexto el presente TFM y poder poner en perspectiva el valor aportado por el mismo, a continuación se señalarán algunos trabajos que comparten tecnología, objetivos o información relevante que ayuden a una correcta compresión del material presentado, así como a llenar los posibles huecos de información que puedan dejar al sintetizar y resumir gran parte del material teórico y práctico del trabajo.

✔ Trabajos final de Máster de la UOC relacionados [1]

Se han revisado algunos trabajos finales de máster presentados anteriormente en la UOC y cuya temática estuviese relacionada con la del presente trabajo. En este sentido, se pueden señalar los siguientes:

- Manuel Márquez Salas. *Demostrador de Internet of Things con la tecnologia IEEE 802.15.4e utilizando el sistema operativo OpenWSN, OpenSim y theThings.io.*
- Roberto Morago Martínez. *Demostrador de Internet of Things con la tecnologia IEEE 802.15.4e utilizando el sistema operativo OpenWSN, OpenSim y theThings.io.*
- Pablo Arriaga Pérez. *Seguridad en Internet de las Cosas Honeypot to capture IoT-attack methods.*
- Javier López Molinero. *Implementación del protocolo MQTT-S sobre IEEE 802.15.4e en plataformas OpenMOTE.*

✔ ZigBee Specification [2]

Se trata de la especificación del protocolo ZigBee. En ella se describen por completo las características técnicas del protocolo, así como la infraestructura y servicios disponibles para las aplicaciones que operen con él.

✔ IEEE Standard for Low-Rate Wireless Networks [13]

Se trata de la especificación del protocolo IEEE 802.15.4. Junto con la especificación de ZigBee, han sido los dos documentos principales a la hora del estudio y documentación de ambos protocolos.

✔ Zigbee Alliance. Zigbee: Securing the Wireless IoT [3]

En él se definen las medidas de seguridad implementadas por el protocolo Zigbee, haciendo especial hincapié en las novedades introducidas por la versión 3 del protocolo.

✔ Security Analysis of Zigbee [4]

En este trabajo aporta una visión general de la política de seguridad y arquitectura de ZigBee, además de intentar encontrar una serie de vulnerabilidades de seguridad en dispositivos comerciales que implementan este protocolo.

✔ *GTS Attack: An IEEE 802.15.4 MAC Layer Attack in WSN* [5]

Este artículo analiza los ataques conocidos en redes inalámbricas de sensores, centrándose en el ataque GTS (*Guaranteed Time Slot*) tomando como base el nivel MAC del protocolo IEEE 802.15.4, y sirviendo como base para conocer la seguridad implementada por este protocolo.

2.2 Internet de las Cosas (IoT)

2.2.1 Descripción

El **Internet de las Cosas** (**IoT**, del inglés *Internet of Things*) es uno de los términos más populares de los últimos años dentro de la industria tecnológica. Se trata de un concepto que se basa en la interconexión digital de objetos cotidianos con otros objetos de su alrededor y, a su vez, con Internet, extendiendo las capacidades de interconexión y procesamiento de dichos objetos. Este concepto fue propuesto en 1999 por Kevin Ashton, al realizar distintas investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores [6].

El Internet de las Cosas permite que los ordenadores interactúen con elementos de la vida real y ganen independencia de los seres humanos, dejándonos a nosotros al mando de lo realmente importante, logrando una mayor eficiencia y comodidad [7].

El auge de este concepto se explica atendiendo a las siguientes características [8]:

- **Protocolo de Internet versión 6 (IPv6)**: posibilita la identificación de todos los objetos conectados a Internet gracias a la disponibilidad de nuevos direccionamientos sin miedo a agotar el rango disponible, tal y como sucede con IPv4.

- **Abaratamiento de componentes**: con el avance de la tecnología se produce un abaratamiento de los procesadores y memorias necesarias en la construcción de estos dispositivos.

- **Reducción de tamaño de componentes**: de igual manera, los componentes electrónicos cada vez son más compactos, permitiendo la incorporación de nuevas capacidades, como la comunicación e interconexión, en un espacio menor. Según la conocida como Ley de Moore [9], se ha podido constatar que cada dos años se duplica el número de transistores en un microprocesador, lo que, consecuentemente, provoca que, para una misma capacidad de procesamiento, el espacio requerido sea menor. Con esto se consiguen dispositivos muchos más pequeños, pero con capacidades de procesamiento y comunicación mucho mejores.

- **Conectividad ubicua**: con el abaratamiento y miniaturización de componentes y dispositivos, se consigue una capacidad de conectividad de bajo coste y alta velocidad a través de tecnologías inalámbricas, haciendo posible la interconexión de dispositivos situados en cualquier parte.

- **Avances en el análisis de datos**: la creación de nuevos algoritmos y el rápido avance en la potencia de cómputo, capacidad de almacenamiento y servicios en la nube posibilitan la agregación, correlación y análisis de una gran cantidad

de datos, posibilitando la extracción de información y conocimiento a partir de conjuntos de datos grandes y dinámicos.

- **El aumento de la computación en la nube**: el aumento de los servicios de cloud computing permite que dispositivos pequeños y distribuidos interactúen con potentes capacidades de control y análisis de back-end.

Zigbee es uno de los estándares más utilizados para la comunicación inalámbrica entre diferentes dispositivos de IoT y ha sido adoptado por muchas de las compañías más importantes. Se trata de un estándar abierto para redes de área personal inalámbricas de bajo consumo (LR-WPAN) que conectan dispositivos principalmente para uso personal. El objetivo de la norma es proporcionar un protocolo de comunicación confiable y de doble vía para aplicaciones de corto alcance, generalmente de 10 a 100 metros. Se orienta a distintas áreas de aplicación, como puede ser la domesticación, la energía inteligente, el control remoto y la atención médica. Aunque Zigbee fue diseñado teniendo en cuenta la importancia de la seguridad, se han hecho algunas concesiones en esta materia debido a la orientación de su aplicación en dispositivos de bajo coste, bajo consumo de energía y buscando la interoperabilidad entre ellos, provocando que algunos de los controles de seguridad estén mal implementados y, consecuentemente, provocando un riesgo para la seguridad de estos dispositivos y sus comunicaciones.

2.2.2 Modelos de comunicación en el Internet de las Cosas

Desde una perspectiva operacional, los dispositivos IoT pueden conectar y comunicarse según los diferentes modelos [8]:

- **Comunicación Dispositivo a Dispositivo** (*Device-to-Device*): este modelo representa dos o más dispositivos que se conectan directamente y se comunican entre ellos sin utilizar un servidor de aplicaciones intermediario. Comúnmente, este tipo de dispositivos emplean protocolos como Bluetooth o Zigbee para el intercambio de mensajes, y es usado en aplicaciones como sistemas de automoción y dispositivos IoT domésticos (bombillas, termostatos o cerraduras inteligentes) en los que el tamaño de los paquetes de datos es reducido.

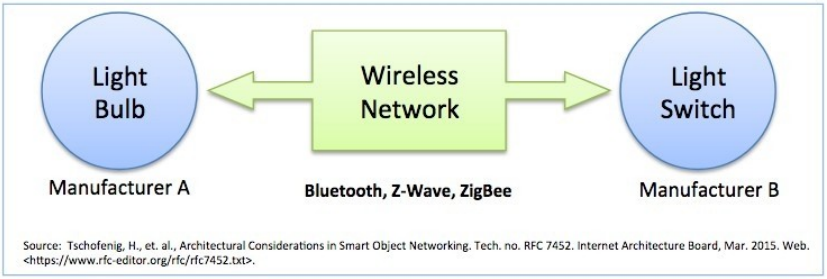


Figura 1. Ejemplo de modelo de comunicación Dispositivo a Dispositivo [8]

- **Comunicación Dispositivo a Nube** (*Device-to-Cloud*): el dispositivo IoT se conecta directamente a un servicio en la nube en Internet que proporciona un servicio de aplicación para el intercambio de datos. Se aprovecha de un mecanismo de comunicación existente como Ethernet o Wi-Fi para establecer

la conexión entre el dispositivo y la red IP, la cual, en última instancia, se conecta al servicio en la nube.

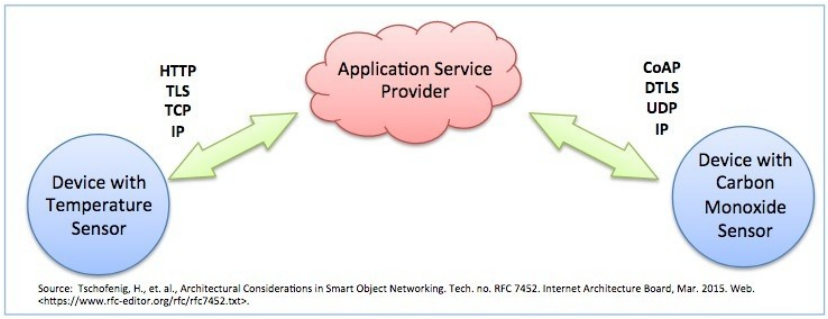


Figura 2. Diagrama del modelo de comunicación Dispositivo a Nube [8]

- **Comunicación Dispositivo a Pasarela** (*Device-to-Gateway*): en este modelo, existe un software de aplicación operando en un dispositivo pasarela local, el cual actúa de intermediario entre el dispositivo y el servicio en la nube, proporcionando seguridad y otras funcionalidades como interpretación de datos y protocolos.

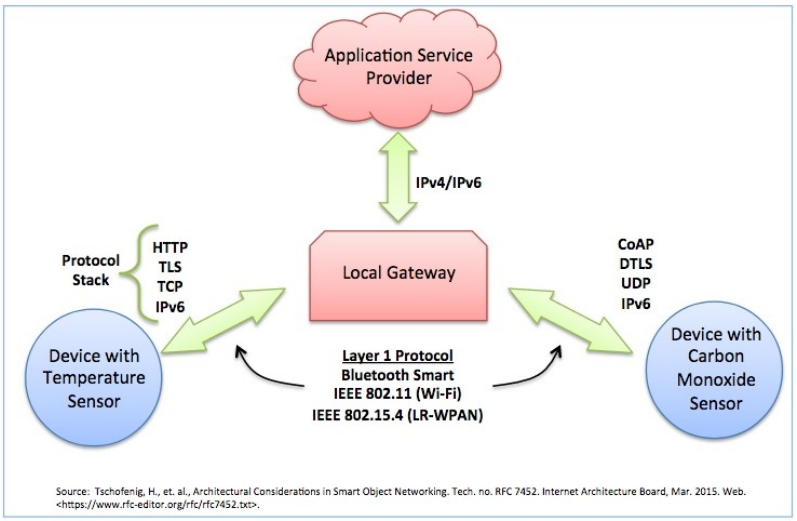


Figura 3. Diagrama del modelo de comunicación Dispositivo a Gateway [8]

- **Intercambio de datos de Back-End** (*Back-End Data-Sharing Model*): este modelo se refiere a una arquitectura de comunicación que posibilita a los usuarios el exportar y analizar datos de objetos inteligentes de un servicio en la nube en combinación con datos de otras fuentes.

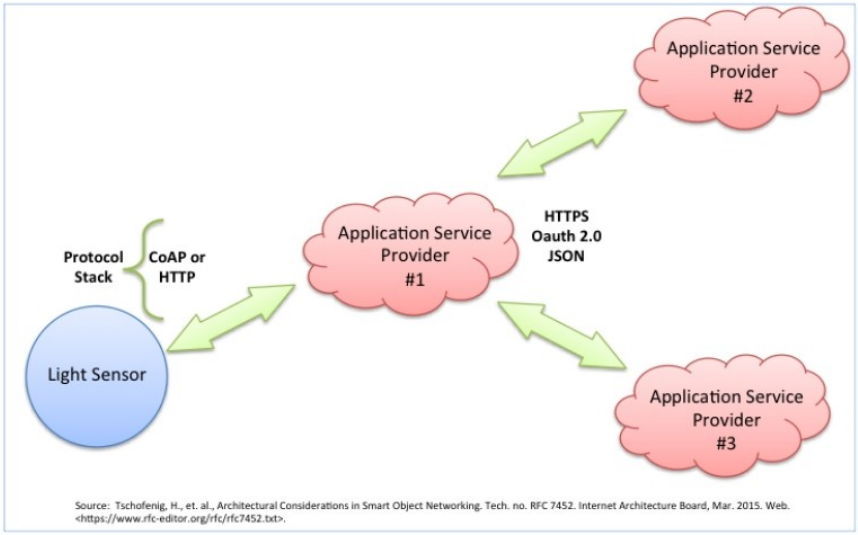


Figura 4. Diagrama del modelo de compartición de datos de Back-End [8]

2.2.3 Principales aplicaciones del Internet de las Cosas

Los dispositivos y tecnologías del IoT se utilizan en multitud de entornos y situaciones. Cada vez más podemos encontrar dispositivos conectados a Internet y que permiten ser configurados y utilizados desde una aplicación móvil cualquiera, en aplicaciones tan dispares que van desde la monitorización de datos de salud en pacientes hasta controles de tráfico en ciudades.

A modo de resumen, la siguiente tabla muestra las distintas configuraciones y aplicaciones en las que pueden emplease los sistemas IoT [8]:

Aplicación	Descripción	Ejemplos
Cuerpo humano	Dispositivos adheridos o en el interior del cuerpo humano	Dispositivos (wearables) para monitorizar y mantener la salud y bienestar, aumentar la productividad, manejo de enfermedades, etc.
Hogar	Edificios donde vive la gente	Controladores del hogar y sistemas de seguridad
Entornos minoristas	Espacios donde consumidores se dedican al comercio	Comprobaciones automáticas de identidad, ofertas y optimización de inventarios en tiendas, bancos, restaurantes y, en definitiva, cualquier sitio donde los consumidores puedan comprar
Oficinas	Espacios de trabajo	Gestión de la energía y seguridad en edificios, mejora de productividad, etc.
Industria	Entornos de producción estandarizados	Lugares con rutinas de trabajo repetitivas, incluidos hospitales y granjas, para mejorar las operaciones y optimizar el uso de equipos e inventarios
Lugar de trabajo	Entornos de producción personalizados	Minería, petróleo, gas, construcción, eficiencias operativas, mantenimiento predictivo, salud y seguridad
Vehículos	Sistemas dentro de vehículos en movimiento	Vehículos incluyendo coches, camiones, barcos, aviones y trenes, para el mantenimiento basado en condición, diseño basado en uso y análisis de preventa
Ciudades	Entornos urbanos	Espacios públicos e infraestructuras en entornos urbanos, para el control del tráfico adaptativo, medidores inteligentes, monitorización ambiental, gestión de recursos
Exteriores	Entre entornos urbanos	Vías férreas, vehículos autónomos (fuera de lugares urbanos) y navegación aérea, para el enrutamiento en tiempo real, navegación conectada y seguimiento de envíos

Tabla 1: Aplicaciones principales del Internet de las Cosas

2.2.4 Áreas y retos clave en el Internet de las Cosas

En lo que a tecnología se refiere, existen una serie de puntos que requieren una especial atención y énfasis por parte de toda la industria, con el objetivo de crear un ecosistema de productos en el que su usabilidad, seguridad e interoperabilidad sea máxima. Así pues, comúnmente se enumeran cinco áreas clave para IoT necesarias

para explorar los desafíos y necesidades más urgentes relacionados con la tecnología. Estos son [8]:

✔ Seguridad

La securización de los productos y servicios de IoT debe ser una prioridad fundamental para que los usuarios puedan confiar en los dispositivos de IoT y los servicios de datos relacionados estén protegidos contra vulnerabilidades, especialmente en estos tiempos en los que esta tecnología se ha vuelto más generalizada e integrada en nuestras vidas. Los dispositivos y servicios de IoT mal securizados pueden ser potenciales puntos de entrada a ataques cibernéticos y exponer datos de usuarios de forma flagrante.

Por lo tanto, se necesitará un enfoque de colaboración relativo a seguridad que ayude a desarrollar soluciones efectivas y apropiadas para que los desafíos de seguridad de IoT sean adecuados para la escala y complejidad de los problemas que se intentan abordar, dirigiendo los esfuerzos a una visión en la que la seguridad sea tenida en cuenta en todas las fases de producto o servicio, desde la concepción, pasando por la creación, implementación y utilización del mismo.

✔ Privacidad

El derecho a la privacidad y el respeto por las expectativas de privacidad del usuario son una parte integral para garantizar la confianza del usuario en Internet, los dispositivos conectados y los servicios relacionados, y más concretamente, en el Internet de las Cosas, ya que muchas implementaciones pueden cambiar dramáticamente las formas en que los datos personales se recopilan, analizan, utilizan y protegen.

Por lo tanto, será necesario desarrollar estrategias que permitan respetar las opciones de privacidad individuales al tiempo que se fomenta la innovación en nuevas tecnologías y servicios.

✔ Interoperabilidad / Estándares

Los compradores pueden dudar en comprar productos y servicios de IoT si no existe flexibilidad en la integración, una alta complejidad y preocupación sobre el bloqueo entre proveedores que fragmente y dificulte la interoperabilidad entre productos y servicios.

Así, aunque una interoperabilidad total no siempre es factible, el uso de estándares genéricos, abiertos y ampliamente disponibles aportará mayores beneficios para el usuario, la innovación y mayores oportunidades económicas.

✔ Legal, Regulación y Derechos

El frenético cambio continuo en la tecnología y, en particular, en la tecnología de IoT, a menudo supera la capacidad de las estructuras políticas, legales y regulatorias asociadas para adaptarse. Al crecer enormemente el número de dispositivos que recogen, utilizan y transmiten flujos de datos se amplifican los problemas legales existentes en Internet. De especial atención son aquellos casos correspondientes a los flujos de datos transfronterizos, donde los dispositivos de IoT recopilan datos sobre personas en una jurisdicción y la transmiten a otra jurisdicción con diferentes leyes de protección de datos para su procesamiento, llegando a poder ser usados de forma indebida o generar resultados discriminatorios para algunos usuarios.

La adopción de los principios rectores del Internet Society de promover la capacidad de un usuario para conectarse, hablar, innovar, compartir elegir y confiar son consideraciones para la evolución de las leyes y regulaciones de IoT que permiten los derechos de los usuarios.

✔ Economía emergente y problemas de desarrollo

El IoT es una herramienta prometedora para lograr los Objetivos de Desarrollo de las Naciones Unidas, donde se brinden beneficios sociales y económicos a las economías emergentes y en desarrollo en áreas como la agricultura sostenible, la calidad y uso del agua, la atención médica, la industrialización y gestión ambiental, etc.

En este sentido, será cuestión tanto de los países industrializados como de las regiones en desarrollo el responder para darse cuenta de los beneficios potenciales de IoT, abordando aquellas necesidades y desafíos únicos de la implementación en las regiones menos desarrolladas, incluida la preparación de infraestructura, los incentivos de inversión y de mercado, los requisitos de habilidades técnicas y los recursos de políticas.

2.3 Estándar IEEE 802.15.4

2.3.1 Descripción

IEEE 802.15.4 es un estándar que define el nivel físico (PHY) y el control de acceso al medio (MAC) de redes inalámbricas de área personal con tasas bajas de transmisión de datos (LR-WPAN, *Low-Rate Wireless Personal Area Network*), cuyo propósito principal es el de definir los niveles de red básicos para dar servicio a un tipo específico de red inalámbrica de área personal (WPAN) centrada en la habilitación de comunicación entre dispositivos ubicuos con bajo coste y velocidad [10], sin infraestructura o con muy poca, para favorecer aún más el bajo consumo.

Este protocolo opera en la capa 2 del modelo OSI, la capa de Enlace de Datos. Es en este lugar donde las unidades de información digital (bits) son gestionadas y organizadas para convertirse en impulsos electromagnéticos (ondas) en el nivel inferior del modelo, el nivel físico.

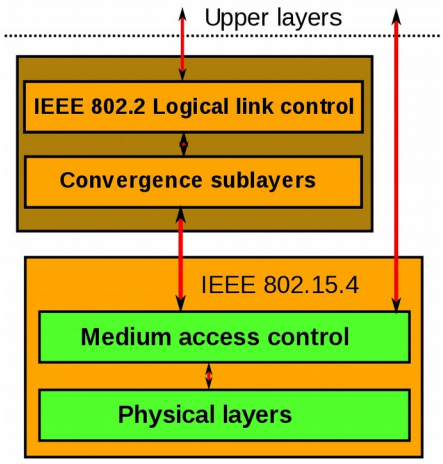


Figura 5. Pila de protocolos IEEE 802.15.4 [10]

La característica fundamental de 802.15.4 entre las WPANs es la obtención de costes de fabricación excepcionalmente bajos por medio de la sencillez tecnológica, sin perjuicio de la generalidad o la adaptabilidad.

Un dispositivo que implementa el 802.15.4 puede transmitir en una de tres posibles bandas de frecuencia de uso no regulado que se muestran en la siguiente tabla:

Frecuencia (MHz)	Tasa de datos (Kb/s)	Modulación	Número de canales	Región
868 - 868,6	20	BPSK	1 canal (revisión 2003) 3 canales (revisión 2006)	Europa
902 - 928	40	BPSK	10 canales (revisión 2003) 30 canales (revisión 2006)	EEUU
2400 - 2483,5	250	O-QPSK	16 canales	Todo el mundo

Tabla 2: Utilización del espectro radioeléctrico IEEE 802.15.4

Para el caso concreto de integración de IEEE 802.15.4 con el protocolo ZigBee, objeto de estudio de este trabajo, la banda de frecuencias utilizadas es aquella en el rango de los 2,4 GHz. Tal y como se recoge en la tabla, se definen hasta 16 canales, cada uno de ellos con un ancho de banda de 5 MHz, donde la frecuencia central de canal puede calcularse como [11]:

$$Fc = (2405 + 5(k - 11)) \text{ MHz, donde } k = 11, 12, \ldots, 26.$$

La estructura de canales para cada una de las bandas puede verse en la siguiente figura [12]:

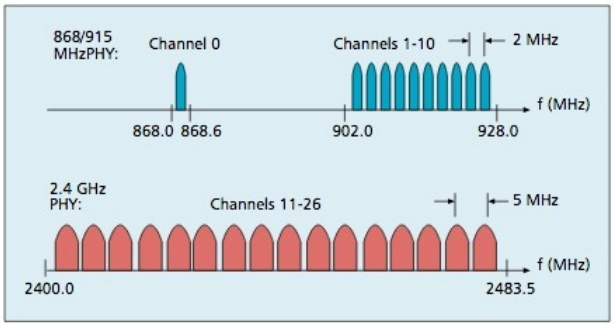


Figura 6: Estructura de canal IEEE 802.15.4 [12]

Dado que la banda de frecuencias ISM de 2,4 GHz es libre en todo el mundo y ampliamente utilizada por otros protocolos de comunicaciones, como Bluetooth y Wifi, es muy probable la existencia de varios tipos de redes inalámbricas en entornos de redes locales. Esto, unido al hecho de la posible existencia de interferencias no intencionadas, como ondas microondas, hacen que sea de gran importancia la implementación de mecanismos que ayuden a reubicar la red en el espectro. El estándar 802.15.4 incluye los mecanismos necesarios para implementar una selección dinámica de canal, aunque la selección del algoritmo específico se deja a la capa de red. A su vez, la capa MAC incluye una función de escaneo que le permite iterar entre los distintos canales en la búsqueda de beacons (balizas) que le ayuden a identificar y formar la red, mientras que el nivel físico contiene varias funciones de bajo nivel, como la detección de energía en recepción, indicadores de calidad del enlace, así como

cambiadores de canal, permitiendo una evaluación de canales y agilidad en frecuencia. Estas funcionalidades son usadas por la red para establecer su canal de operación inicial y cambiar de canal en caso de una desconexión prolongada [12].

El estándar no define niveles superiores ni subcapas de interoperabilidad. No obstante, existen extensiones, como las especificaciones ZigBee y Z-Wave, que lo utilizan como base para completar la pila de comuncicaciones y proponer soluciones más completas.

El estándar IEEE 802.15.4 define dos tipos de nodos en la red:

- **Dispositivo de funcionalidad completa** (FFD, *Full-Function Device*):
    - Puede funcionar como coordinador de una red de área personal (PAN) o como un nodo normal.
    - Implementa un modelo general de comunicación que le permite establecer un intercambio con cualquier otro dispositivo.
    - Puede, además, encaminar mensajes, en cuyo caso se le denomina coordinador (coordinador de la PAN si es el responsable de toda la red y no sólo de su entorno).
- **Dispositivos de funcionalidad reducida** (RFD, *Reduced-Function Device*).
    - Se plantean como dispositivos muy sencillos con recursos y necesidades de comunicación muy limitadas. Por ello, sólo pueden comunicarse con FFDs y nunca pueden ser coordinadores.

2.3.2 Arquitectura

La arquitectura de IEEE 802.15.4 se define en términos del número de bloques para simplificar el estándar. Estos bloques se llaman “niveles”. Cada nivel es responsable de una parte del estándar y ofrece servicios a los niveles superiores [13]. Un dispositivo LR-WPAN comprende al menos:

✔ Capa Física (PHY)

Contiene el transceptor de radiofrecuencia (RF) con su mecanismo de control de bajo nivel y proporciona un servicio de transmisión de datos y una interfaz de gestión de la propia capa, permitiendo funcionalidades como la activación y desactivación del transceptor de radio, detección de energía, indicación de calidad del enlace, selección de canal, así como transmitir y recibir paquetes a través del medio físico.

Las tasas de transferencia binaria son distintas, dependiendo de la frecuencia utilizada (ver Tabla 2). Así, en la banda de 2,4 GHz podemos alcanzar tasas binarias de hasta 250 Kbps, mientras que en 868 y 915MHz sólo podemos trabajar, respectivamente, con velocidades de 20Kbps y 40Kbps. Esta diferencia es debida, principalmente, a dos factores: al mayor orden del esquema de modulación O-QPSK (*Offset Quadrature Phase-Shift Keying*) utilizado en 2.4GHz respecto a BPSK (*Binary Phase-Shift Keying*), empleado en 868 / 915 MHz; y al mayor ancho de banda del que se dispone en 2,4 GHz.

✔ Capa MAC

La capa de Control de Acceso al Medio proporciona acceso al canal físico para todos los tipos de transferencias, además de la gestión de la propia capa. Entre las funciones principales de esta capa se encuentran la gestión de beacons, acceso al canal, gestión de slot temporales (GTS, del inglés *Guaranteed Time Slot*), validación de tramas, reconocimiento de entrega de tramas, asociación y disociación, además de ser la encargada de habilitar la implementación de mecanismos de seguridad apropiados para la aplicación.

La capa MAC será la encargada de filtrar las tramas recibidas, rechazando aquellas cuya verificación sea incorrecta, según el valor del FCS (*Frame Check Sequence*). En resumen, este campo se envía por el dispositivo emisor, habiéndose calculado previamente a partir de las cabeceras y el campo de datos (carga útil) de la trama MAC. Una vez llega la trama al dispositivo receptor, éste la calcula y compara el valor del FCS calculado con el de la trama recibida. Si coinciden se procesa la trama y se redirige a niveles superiores. Si no, la trama es descartada.

La siguiente figura muestra una representación gráfica de la interconexión de los niveles mencionados y sus interfaces correspondientes [13]:

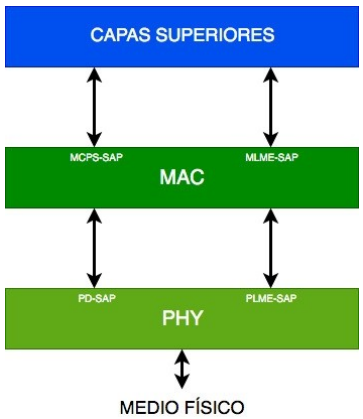


Figura 7: Arquitectura de dispositivo LR-WPAN

Las capas superiores mostradas en la figura consisten en la capa de red, que proporciona configuración y manipulación de red y encaminamiento de mensajes, y una capa de aplicación, la cual proporciona la funcionalidad propia del dispositivo. Estas capas están fuera del alcance del estándar IEEE 802.15.4, pudiendo ser implementadas por protocolos como Z-Wave [46] o ZigBee.

2.3.3 Topología de red

Las redes IEEE 802.15.4 están compuestas por grupos de dispositivos separados por distancias suficientemente reducidas, los cuales poseen un identificador único de 64 bits, esto es, su dirección MAC. Estas redes necesitan un FFD que actúe como coordinador y, dependiendo de los requerimientos de aplicación, pueden construirse como [5]:

- **Topología punto a punto**: cualquier dispositivo es capaz de comunicarse con otro siempre y cuando se encuentre en el su rango de cobertura, de forma que pueden formarse patrones arbitrarios de conexionado, permitiendo la

implantación de formaciones más complejas, como las redes en malla. Forman la base de redes ad-hoc auto-organizativas. El estándar no define un nivel de red, por lo que no se soportan funciones de enrutamiento de forma directa. No obstante, mediante el uso de alguna capa superior se permite el enrutamiento de mensajes desde un dispositivo a otro de la red en múltiples saltos.

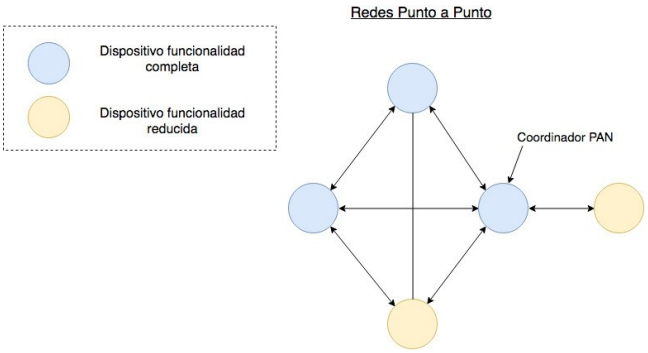


Figura 8: Red IEEE 802.15.4 Punto a Punto

- **Topología en estrella**: el coordinador va a ser siempre el nodo central. Una red así se forma cuando un FFD decide crear su PAN y se nombra a sí mismo coordinador, tras elegir un identificador de PAN único. Tras ello, otros dispositivos pueden unirse a una red totalmente independiente del resto de redes en estrella. El coordinador PAN, generalmente, está siempre conectado a la corriente eléctrica, mientras que el resto de dispositivos estarán alimentados por batería. Un ejemplo de aplicaciones que se benefician de este tipo de arquitectura son sistemas de automatización del hogar, dispositivos periféricos de un ordenador, juegos y sistemas de monitorización sanitaria. Un ejemplo de la estructura de este tipo de redes pueden verse en la siguiente figura:

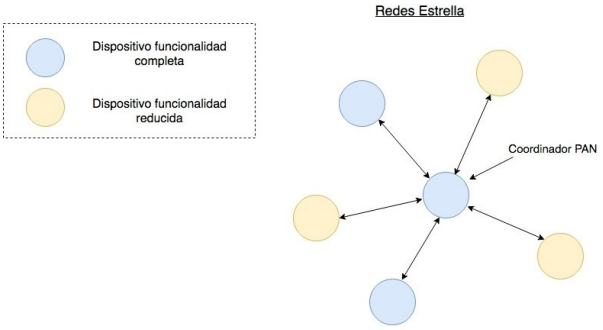


Figura 9: Red IEEE 802.15.4 Estrella

2.3.4 Modelos de transferencia de datos

Los modelos de transferencia de datos utilizados en el estándar IEEE 802.15.4 son los siguientes [13]:

✔ Transferencia de datos a un coordinador.

Cuando un dispositivo quiere enviar información a un coordinador en una PAN pueden darse dos casos:

1. **La red PAN utiliza transferencia de balizas** (beacons): en este caso, el dispositivo escucha el medio hasta que encuentra una baliza, momento en el que el dispositivo se sincroniza con la estructura de la supertrama (estructura utilizada por el coordinador para la sincronización en la PAN y que deben seguir todos los dispositivos, compuesta de dieciséis ranuras temporales de igual duración, la primera de las cuales estará ocupada por la trama baliza generada por el coordinador) y compite con el resto de los dispositivos de la red utilizando CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) hasta conseguir transmitir su información (puede esperar una trama de asentimiento de recepción por parte del coordinador, si está habilitada esta opción).

2. **La red no tiene habilitada la transferencia de balizas**: el dispositivo transmite la información directamente, empleando también CSMA/CA, pero sin a opción de ranurado temporal (también puede esperar una trama de aceptación por parte del coordinador si está activada dicha opción).

✔ Transferencia de datos desde un coordinador.

Al igual que en el caso anterior, este modelo de transferencia discierne entre la posibilidad de que la red implemente o no la transferencia de balizas:

1. **La red PAN utiliza transferencia de balizas**: el coordinador señaliza con un beacon que dispone de datos para transmitir a un dispositivo. Dado que dicho dispositivo se encuentra escuchando periódicamente la red, al descubrir que tiene datos pendientes para recibir, transmite un comando "*Data Request*". Entonces, el coordinador envía la trama de datos pendientes. Una vez finalizada satisfactoriamente la transacción de datos, el mensaje se elimina de la lista de mensajes pendientes en la baliza.

2. **La red no tiene habilitada la transferencia de balizas**: en este caso, el coordinado almacena los datos para que el dispositivo apropiado haga contacto y solicite los datos. Un dispositivo solicita datos mediante la transmisión de un comando "*Data Request*" a su coordinador. Si existe una trama con datos pendientes, el coordinador la envía. En caso de no existir ninguna información pendiente, el coordinador puede responder de dos formas:

    - Si se solicitó acuse de recibo por parte del dispositivo, se envía una trama *Ack* que sigue al comando "*Data Request*".

    - Si no se solicitó acuse de recibo, se envía una trama de datos con carga útil de longitud cero (sin datos útiles).

✔ Transferencia de datos entre pares (Peer-to-peer).

En este tipo de transferencias, si los dispositivos pueden actuar de dos formas:

1. Transmitir los datos directamente cuando dispone de acceso al canal, utilizando CSMA/CA.

2. Utilizando otra serie de medidas para conseguir una sincronización entre los distintos dispositivos que intentan comunicarse.

2.3.5 Características técnicas

El protocolo IEEE 802.15.4 se encuentra sobre la capa 2 del modelo de referencia OSI, la capa de Enlace de Datos. Aquí, de forma similar a lo que ocurre en otros protocolos como 802.11 (Wifi), las unidades de información digital (bits) se gestionan y organizan para convertirse en impulsos electromagnéticos (ondas) en el nivel inferior, el físico.

A continuación se analizarán las características técnicas que llevan al protocolo IEEE 802.15.4 a ser el estándar más utilizado en comunicaciones inalámbricas para la creación de redes en el Internet de las Cosas y ser la base sobre la que implementar otros protocolos de niveles superiores.

✔ Estructura de la trama

La estructura de la trama de IEEE 802.15.4 ha sido diseñada con el objetivo de mantener la complejidad al mínimo buscando al mismo tiempo hacerla lo suficientemente robusta para las transmisiones en canales ruidosos.

En la siguiente figura se puede apreciar un ejemplo del formato de las unidades de datos en los niveles MAC y PHY del protocolo:

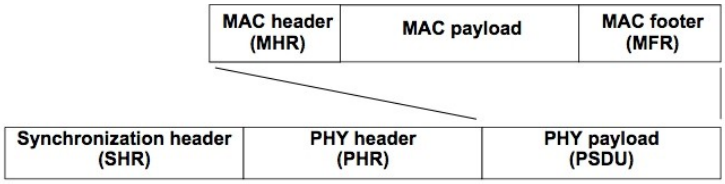


Figura 10: Vista esquemática del PPDU [13]

Tal y como se aprecia, los frames MAC se pasan al nivel físico como unidades de datos de servicio PHY (PSDU, PHY service data unit), componiendo la carga útil PHY. Finalmente, el nivel físico añade las cabeceras PHR (*PHY Header*) y SHR (*Synchronization Header*) para conformar la unidad de datos del protocolo PHY (PPDU, *PHY protocol data unit*).

✔ Protección frente a ruidos

IEEE 802.15.4 usa Espectro Ensanchado por Secuencia Directa (DSSS, *Direct Sequence Spread Spectrum*) para modular la información antes de ser enviada a la capa física. Mediante esta técnica, cada bit de información a ser transmitido se modula en cuatros señales diferentes, causando que la cantidad total de información a transmitir ocupe un mayor ancho de banda pero usa una densidad espectral de potencia menor para cada una de las señales. De esta manera, se reducen las interferencias en las bandas de frecuencia usadas y se mejora la Relación señal/ruido (SNR) en el receptor debido, principalmente, al hecho de que es más fácil detectar y decodificar el mensaje que está siendo transmitido por el transmisor [14].

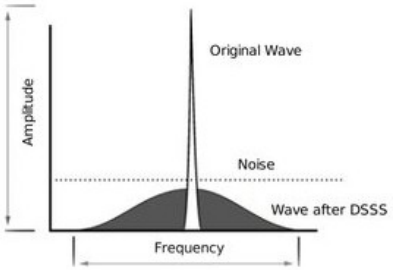


Figura 11: DSSS, Direct Sequence Spread Spectrum [14]

Existen diferentes modulaciones DSSS dependiendo de las limitaciones físicas hardware del circuito y número de símbolos que pueden ser procesados en un momento dado. Las modulaciones BPSK (*Binary Phase Shift Keying*), O-QPSK (*Offset Quadrature Phase Shift Keying*) y PSSS (*Parallel Sequence Spread Spectrum*) permiten la comunicación desde anchos de banda entre 20 y 250 Kb/s.

✔ Protección frente a interferencias

Como se ha podido deducir al explicar el modelo de transferencia de datos, 802.15.4 usa dos técnicas para evitar que todos los nodos comiencen a emitir al mismo tiempo y facilitar la sincronización entre ellos, evitando las interferencias y colisiones en el envío de información:

- **CSMA/CA** (*Carrier Sense Multiple Access-Collision Avoidance*): en este método, cada nodo escucha el medio antes de transmitir. Si la energía encontrada es mayor que un nivel especificado, el nodo espera durante un tiempo aleatorio (incluido en un intervalo) y, posteriormente, lo intenta de nuevo. Existe un parámetros definido en el estándar: *macMinBE*, el cual especifica el exponente de retroceso (*back-off*) que se utilizará al calcular este intervalo de tiempo.

- **GTS** (*Guarantee Time Slot*): este sistema usa un nodo centralizado (coordinador PAN) que proporciona slots de tiempo a cada uno de los nodos, de manera que cada uno de ellos conoce cuando tienen que transmitir. Existen dieciséis slots de tiempo posibles. Como paso inicial, un nodo debe enviar al coordinador PAN un mensaje de petición GTS. Como respuesta, el coordinador enviará un mensaje de baliza que contiene el slot asignado y el número de slots que puede utilizar.

Con el objetivo de ahorrar energía escogiendo los canales libres al configurar la red, a la hora de enfrentarse a problemas de detección de energía y comenzar a utilizar un canal en concreto, 802.15.4 implementa los siguientes mecanismos:

- **Detección de energía**: escanea los canales e informa de la energía encontrada. No importa si es causado por otros nodos, por otra tecnología o ruido. Sólo se informa si el espectro está siendo utilizado. Únicamente cuando el valor recibido esté por debajo de un cierto umbral, se procederá a transmitir.

- **Detección de portadora** (CCA, *Clear Channel Assessment*): escanea el medio e informa si hay transmisiones 802.15.4. Sólo cuando el canal está libre se procederá a transmitir.

- **CCA + Energía**: escanea el medio e informa si hay transmisiones 802.15.4 por encima del umbral de energía especificado. Si no, se procede a usar dicho canal.

✔ Bajo consumo

IEEE 802.15.4 está listo para trabajar con ciclos de poca potencia, por lo que el transceptor puede estar durmiendo la mayor parte del tiempo (99% en promedio), mientras que las tareas de recepción y envío pueden configurarse para tomar solo una pequeña parte de la energía de los dispositivos. Este porcentaje depende del tipo de modelo de comunicación utilizado. Así, si se usa el modo baliza (redes en estrella o PAN), la cantidad mínima de tiempo utilizada para transmitir / recibir estas tramas aumentará el tiempo total durante el cual se usa el transceptor.

En este sentido, el estándar establece la cantidad mínima de energía necesaria para transmitir en -3 dBm (0,5 mW) y la mínima sensibilidad en el receptor en -85 dBm para 2,4 GHz y -92 dBm para las bandas de 868/915MHz. Estos valores incluyen un margen suficiente para cubrir las tolerancias de fabricación así como para permitir implementaciones de muy bajo coste.

2.3.6 Seguridad en IEEE 802.15.4

El estándar IEEE 802.15.4 soporta los siguientes servicios de seguridad:

- Confidencialidad de los datos.
- Autenticidad de los datos.
- Protección contra repetición.

La subcapa MAC es la responsable de proporcionar estos servicio de seguridad a las tramas salientes y entrantes cuando se demanda por los niveles superiores. No obstante, la implementación de seguridad de un dispositivo es opcional, comportándose de una de las siguientes formas [13]:

- **Cuando un dispositivo no implementa seguridad**, no debe proporcionar un mecanismo a la subcapa MAC para realizar ninguna transformación criptográfica en tramas salientes o entrantes ni requerir ningún atributo asociado con seguridad.
- **Si un dispositivo implementa seguridad**, debe proporcionar un mecanismo a la subcapa MAC para proporcionar transformaciones criptográficas con seguridad sólo si el atributo *macSecurityEnabled* está puesto a TRUE.

Así, cuando se ofrece servicios de seguridad, existen tres campos en la trama MAC que están relacionados con esta [15]:

- **Control de trama** (*Frame Control*), ubicado en el encabezado MAC.
- **Control de Seguridad Auxiliar** (*Auxiliary Security Control*, también en el encabezado MAC).
- **Carga útil de datos** (*Data Payload*), en el campo de carga útil del MAC.

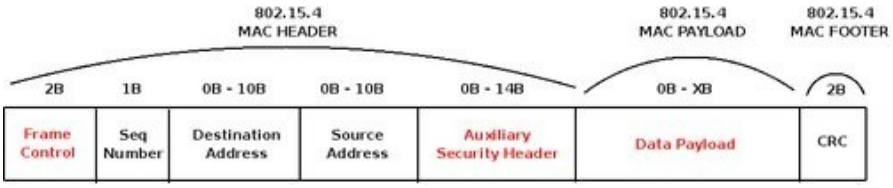


Figura 12: Trama subcapa MAC con información de seguridad [15]

La Trama de Seguridad Auxiliar (*Auxiliary Security Frame*) solo se habilita si el subcampo *Security Enabled* de la Trama de Control está activo. Este encabezado especial tiene tres campos:

- **Security Control** (1 byte), especifica qué clase de protección se usa (ver más abajo).
- **Frame Counter** (4 bytes), es un contador dado por el origen de la trama actual para proteger el mensaje de ataques de repetición. Por esta razón, cada mensaje tiene un ID de secuencia único representado por este campo.
- **Key Identifier** (0 - 9 bytes), especifica la información necesaria para conocer qué clave se está usando con el nodo con el que nos estamos comunicando.

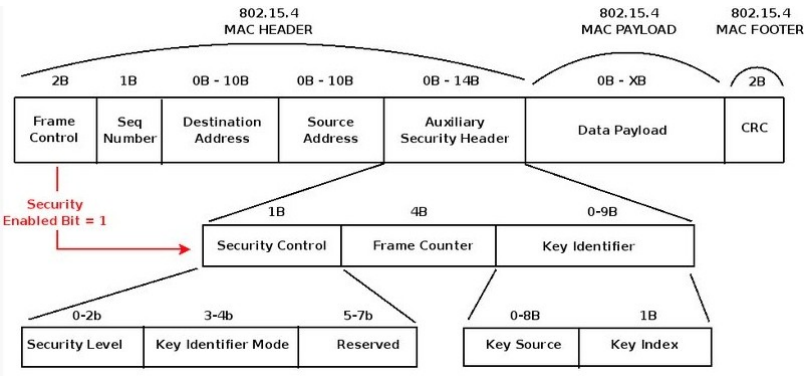


Figura 13: Campos de Cabecera de Seguridad Auxiliar IEEE 802.15.4 [15]

El *Security Control* es el lugar donde se especifica nuestra Política de Seguridad (*Security Policy*) global. Usando los primeros 2 bits (campo *Security Level*) elegimos qué vamos a cifrar y cual será la longitud de la clave: el valor 0x00 significa sin cifrado, de manera que los datos ni se cifran (ausencia de confidencialidad de los datos) ni se valida su autenticidad (ausencia de validación de integridad de los datos). Desde 0x01 a 0x03, los datos se autentican usando el Código de Autenticación de Mensaje (MAC). El valor 0x04 cifra la carga útil asegurando la confidencialidad de los datos. Los valores en el rango 0x05 a 0x07 aseguran tanto confidencialidad de los datos como su integridad (autenticidad).

El campo de datos de carga útil puede tener tres configuraciones diferentes, dependiendo de los campos de seguridad definidos:

- **AES-CTR**: todos los datos se cifran usando el algoritmo AES con una clave definida de 128 bits, el contador de trama establece un ID de mensaje único, y el Key Counter (campo Key Control) se usa por la capa de aplicación si se alcanza el máximo valor de Frame Counter.

- **AES-CBC-MAC**: el Código de Autenticación de Mensaje (MAC) se añade al final del payload, con una longitud que depende del nivel de seguridad especificado en el campo Security Policy. El MAC se crea cifrando la información de la cabecera MAC 802.15.4 y la carga útil de datos.

- **AES-CCM**: Es la mezcla de los dos métodos anteriores, donde los subcampos se corresponden con el modo AES-CTR más el subcampo AES-CBC-MAC cifrado.

En la siguiente figura se puede ver el formato que adoptaría el campo de carga útil según los subcampos de seguridad incluidos:

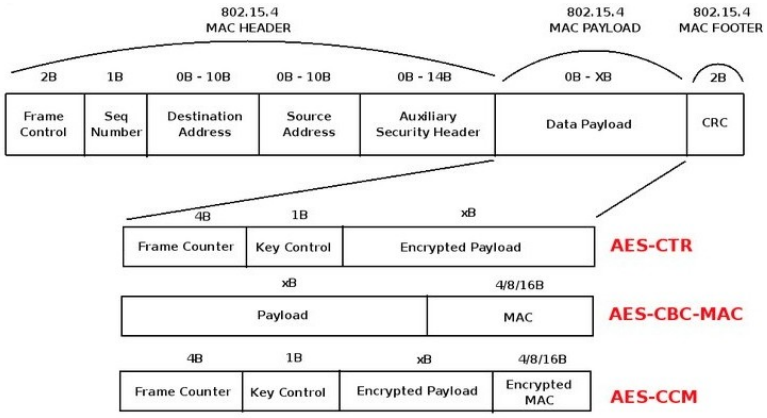


Figura 14: Carga útil según configuración de seguridad [15]

Aparte de proporcionar los servicios de seguridad formateando las tramas salientes e interpretando y gestionando las entrantes, cada transceptor 802.15.4 tiene que controlar su propia lista de control de acceso (ACL, *Access Control List*) para controlar los pares "de confianza", junto con la política de seguridad correspondiente para cada uno. Esta lista, entre otras cosas, contiene la siguiente información:

- **Dirección**: del nodo con el que se quiere comunicar.

- **Suite de seguridad** (*Security Suite*): la política de seguridad que está siendo aplicada ((AEC-CTR, AES-CCM-64, AES-CCM-128, etc.).

- **Clave**: la clave de 128 bits usada en el algoritmo AES.

- **Último vector de inicialización** (IV, *Initialization Vector*) y contador de repeticiones (*Replay Counter*), para evitar ataque de repetición.

Cuando un nodo quiere recibe un mensaje de otro nodo (o quiere enviar un paquete a un nodo específico), primeramente, comprueba que dicho nodo se encuentra en su ACL (se trata de un nodo de confianza). En caso afirmativo, utiliza los datos de configuración específicos extraídos de la lista y aplica las medidas de seguridad adecuadas; en caso contrario (no es un nodo de confianza), o bien rechaza el mensaje o comienza un proceso de autenticación con el nodo remoto.

2.4 ZigBee

2.4.1 Descripción

ZigBee es estándar desarrollado por la ZigBee Alliance para comunicaciones digitales inalámbricas bidireccionales, de bajo consumo y bajo coste destinado a dispositivos embebidos empleados en electrónica de consumo, automatización de hogares y edificios, control industrial, periféricos de PC, aplicaciones de sensores médicos, juguetes y juegos. Está basado en el estándar IEEE 802.15.4 y su objetivo principal es la transmisión de comunicaciones seguras con baja tasa de envío de datos, maximizando de la vida útil de baterías [11].

Las características que diferencian al protocolo ZigBee y lo hacen ideal para su implementación en redes inalámbricas de área personal son [11]:

- Una red Zigbee puede constar de un máximo de 65535 nodos distribuidos en subredes de 255 nodos.
- Los dispositivos ZigBee requieren un menor consumo eléctrico que los dispositivos con otros protocolos, ya que pueden permanecer durmiendo la mayor parte del tiempo. En términos exactos, Zigbee tiene un consumo de 30 mA transmitiendo y de 3 µA en reposo.
- Tiene una velocidad de hasta 250 kbit/s, en la banda de frecuencias de 2,4 GHz (definida por el protocolo subyacente IEEE 802.15.4). Esta velocidad del Zigbee es suficiente para aplicaciones empleadas en domótica, los productos dependientes de baterías, los sensores médicos y en artículos de juguetería, ya que la transferencia de datos es menor.
- La potencia de salida suele ser de 0 dBm (1 mW), teniendo unos rangos de transmisión que oscilan entre los 10 y 75 metros, aunque depende bastante del entorno.

ZigBee se sustenta en el nivel físico (PHY) y de control de acceso al medio (MAC) del protocolo IEEE 802.15.4, proporcionando el nivel de red (NWK) y el framework (AF, *Application Framework*) para el nivel de aplicación (APL). Este framework del nivel de aplicación consiste en las subcapas de soporte de aplicación (APS, *Application Support Sublayer*) y de objetos de dispositivo ZigBee (ZDO, *ZigBee Device Objects*). Los objetos de aplicación definidos por el fabricante utilizan el framework y comparten los servicios de seguridad y APS con el ZDO [2].

A continuación se puede ver un esquema general de la pila del protocolo ZigBee, además de una serie de cuestiones que ayudan a extraer la funcionalidad implementada en cada capa del stack:

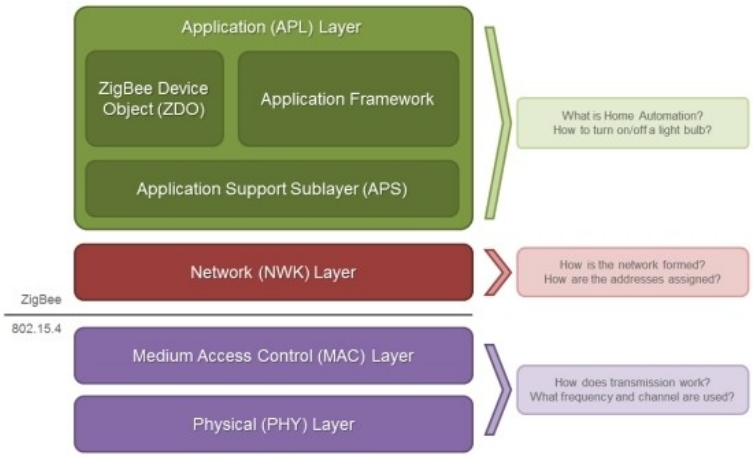


Figura 15: Capas del stack ZigBee [16]

Tal y como se aprecia, este estándar define una de comunicación en el nivel tres y superiores en el modelo OSI. Su objetivo principal es crear una topología de red (jerárquica) para permitir que varios dispositivos se comuniquen entre ellos y establecer funciones de comunicación adiciones, como autenticación, cifrado, asociación y servicios de aplicación en la capa de superior.

En la siguiente tabla se resume la funcionalidad principal de cada capa del stack ZigBee [16]:

Capa ZigBee	Descripcion
ZDO	Nivel de Aplicación que proporciona funcionalidades de descubrimiento de dispositivos y servicios y capacidades de gestión de red avanzadas.
APS (AF)	Nivel de Aplicación que define varios objetos de direccionamiento incluyendo perfiles, clusteres y endpoints.
NWK	Añada capacidades de enrutamiento que permiten a los paquetes de datos de radiofrecuencia atravesar múltiples dispositivos (múltiples saltos) para enrutar los datos desde el origen al destino (peer-to-peer).
MAC	Gestiona las transacciones de datos de radiofrecuencia entre dispositivos vecinos (punto a punto), incluyendo servicios como el reintento de transmisión y gestión de confirmación, y técnicas para evitar colisiones (CSMA/CA)
PHY	Define la operación física del dispositivo ZigBee, incluyendo la sensibilidad en recepción, rechazo de canal, potencia de salida, número de canales, modulación del chip, y especificaciones de tasa de transmisión. La mayoría de las aplicaciones ZigBee operan en la banda ISM 2.4 GHz a una tasa de datos de 250 kb/s.

Tabla 3: Funcionalidad capas ZigBee

La ZigBee Alliance es un consorcio formado por más de 300 empresas tecnológicas entre las que se encuentran empresas como Philips, Siemens, Samsung, Mitsubishi Electrics, Amazon, entre otras, con el objetivo de crear una especificación

abierta que permita definir y crear redes inalámbricas de área personal con baja tasa de bits (LR-WPAN) que implementen distintas tipologías y se favorezca la interoperabilidad y usabilidad de sistemas y dispositivos de control remoto. Además, ofrece la capacidad de estudiar la compatibilidad e implementación del estándar en cualquier dispositivo y expedir la certificación acreditativa que indica su correcto cumplimiento con el estándar.

Para lograr la compatibilidad entre productos y favorecer la interoperabilidad entre ellos, ZigBee define Perfiles de Aplicación (*Application Profiles*), los cuales describen cómo las aplicaciones (*Application Objects*) de distintos dispositivos pueden conectarse entre sí y cooperar entre ellos para llevar a cabo una acción concreta.

Además, con el propósito de aumentar aún más esta interoperabilidad entre los productos certificados, la ZigBee Alliance ha definido una serie de versiones del stack para permitir a los fabricantes poder implementar funcionalidades dependiendo del mercado en el que enfocar el producto. Así, se encuentra la especificación de 2003-2006 ZigBee, y la de 2007 ZigBee PRO. Sus principales diferencias se recogen en la siguiente tabla [17]:

Especificaciones	ZigBee	ZigBee PRO
Año de estandarización	2006	2007
Direccionamiento	Basado en árbol	Estocástico
Enrutamiento	Árbol o malla	Malla
Agregación de ruta	No disponible	Sí
Manejo enlaces asimétricos	No disponible	Sí
Agilidad de frecuencia	Opcional	Disponible
Resolución conflicto PAN ID	No disponible	Sí
Provisión de seguridad básica	Residencial	Estándar
Cifrado nivel APS	Funcionalidad opcional	Funcionalidad opcional
Modo seguridad alta	No disponible	Funcionalidad opcional
Fragmentación	Funcionalidad opcional	Funcionalidad opcional
Puesta en servicio de clúster	Funcionalidad soportada	Funcionalidad soportada
Puesta en servicio segura	No disponible	Disponible

Tabla 4: ZigBee vs ZigBee PRO

2.4.2 Componentes Zigbee

La siguiente figura muestra los diferentes elementos que pueden componer una red Zigbee:

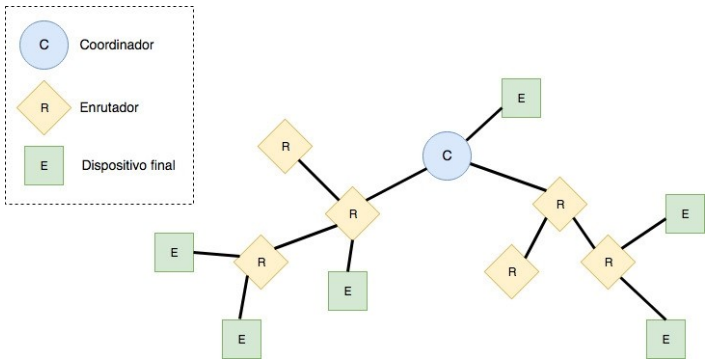


Figura 16: Visión general de una red ZigBee

Tal y como se aprecia en la imagen anterior, existen tres tipos de dispositivos:

✔ Coordinador

Cada red ZigBee debe tener un coordinador que gestione el conjunto de la red [18]. Un coordinador funciona, normalmente, como centro de confianza (TC, *Trust Center*) que proporciona el control de seguridad de la red, siendo responsable de establecer la misma. En este proceso, elige el canal que se usará en la red por los dispositivos para comunicarse, y otorga permisos a otros dispositivos para unirse o dejar la red, haciendo un seguimiento de todos los dispositivos y routers. Además, configura los dispositivos y habilita la seguridad extremo a extremo entre ellos. Y lo que es más importante, el coordinador almacena y distribuye las claves de red. Este tipo de dispositivos no pueden dormir y necesitan estar alimentados constantemente

✔ Enrutador (router)

Dentro de una red ZigBee, actúan como nodos intermedios entre el coordinador y los dispositivos finales, pudiendo redirigir el tráfico entre unos y otros, así como retransmitir y recibir datos. Estos dispositivos tienen que unirse a la red primero con el permiso del coordinador, siendo capaces de permitir a otros enrutadores y dispositivos finales unirse a la red. Al igual que el coordinador, los enrutadores no pueden dormir siempre y cuando la red esté establecida [19].

✔ Dispositivo final

Se trata del elemento más simple que existe dentro de una red Zigbee. Normalmente son dispositivos de baja potencia y están alimentados por batería. A este grupo pertenecen aquellos dispositivos como sensores de movimiento, bombillas inteligentes, sensores de contacto, etc. No obstante, este tipo de dispositivos no enrutan ningún tipo de tráfico y no son capaces de permitir que otros dispositivos se unan a la red. En consecuencia, tan sólo pueden comunicarse en la red a través de sus nodos “padre”, siendo, normalmente, los enrutadores. A diferencia de los otros dos tipos de dispositivos, los dispositivos finales pueden reducir drásticamente el consumo de energía gracias a que pueden permanecer dormidos la mayor parte del tiempo (incluso muchos días seguidos). Cuando se requiere su uso, el nodo es capaz de despertar en un tiempo mínimo, para volverse a dormir cuando deje de ser requerido.

2.4.3 Arquitectura

Como se indicó más arriba, ZigBee se sustenta en las capas física (PHY) y de control de acceso al medio (MAC) del protocolo IEEE 802.15.4. En base a ellas, se construye el stack del protocolo añadiendo una serie de capas y funcionalidades, las cuales describiremos a continuación.

2.4.3.1 Capa de Red (NWK)

La capa de red es requerida para proporcionar la funcionalidad necesaria que asegure una correcta operación de la subcapa MAC de IEEE 802.15.4, así como proporcionar una interfaz de servicio adecuada a la capa de aplicación [2]. Para interactuar con la capa de aplicación, la capa de red, conceptualmente, incluye dos entidades de servicio que proporcionan la funcionalidad necesaria:

- **Entidad de servicio de datos** (**NLDE**, del inglés *NWK layer data entity*): proporciona el servicio de datos que permite a una aplicación transportar unidades de datos del protocolo de aplicación (APDU) entre dos o más dispositivos, los cuales deben estar ubicados en la misma red. Esta entidad se encarga de ofrecer los siguientes servicios:
  - Generación de PDU de nivel de red (NPDU, del inglés *Network Protocol Data Unit*): es capaz de generar un NPDU a partir de un PDU de la subcapa de soporte de aplicación (APS) a través de la adición de una cabecera de protocolo apropiada.
  - Enrutamiento específico de la topología: es capaz de transmitir un NPDU a un dispositivo apropiado que o bien es el detino final de la comunicación o el siguiente paso hasta el destino final en la cadena de comunicación.
  - Seguridad: tiene la capacidad de asegurar tanto autenticidad como confidencialidad de una transmisión.
- **Entidad de servicio de gestión** (**NLME**, del inglés *NWK layer management entity*): debe proporcionar un servicio de gestión para permitir a una aplicación interactuar con el stack. Ofrece los siguiente servicios:
  - Configuración de un dispositivo nuevo: configurar suficientemente el stack para operar tal y como se requiere, como iniciar una operación como coordinador ZigBee o unirse a una red existente.
  - Crear una red: capacidad para establecer una nueva red.
  - Unirse, re-unirse y abandonar una red: proporciona la capacidad para unirse, volver a unirse o abandonar una red a un dispositivo. También, ofrece la capacidad a un coordinador o enrutador ZigBee de pedir a un dispositivo que abandone la red.
  - Direccionamiento: permite a coordinadores y enrutadores ZigBee asignar direcciones a dispositivos que ingresan en la red. Los dispositivos ZigBee disponen de dos tipos de direcciones: por un lado disponen de una dirección única de 64 bits a nivel de enlace (MAC) asignada por el

fabricante durante el proceso de instalación, y, por otro, de una dirección de red de 16 bits (dirección lógica o de red). Esta dirección de red es la que se asigna por el coordinador ZigBee cuando el dispositivo se une a la red. Dependiendo de la versión del estándar, esta dirección puede reflejar la posición del dispositivo dentro de la red. Así, en ZigBee, la dirección 0x0001 reflejaría el primer enrutador ZigBee que se ha unido a la red. En cambio, en ZigBee PRO, las direcciones se asignan aleatoriamente.

- Descubrimiento de vecinos: capacidad para descubrir, guardar y reportar información pertinente a los vecinos de un dispositivo que se encuentran a un salto de distancia.

- Descubrimiento de ruta: proporciona la capacidad de descubrir y guardar caminos a través de la red, de manera que se realice un enrutamiento eficiente del tráfico.

- Control en recepción: permite a un dispositivo controlar cuándo el receptor está activado y durante cuanto tiempo, permitiendo sincronización de la subcapa MAC o recepción directa.

- Enrutamiento: es la capacidad de usar diferentes mecanismos de encaminamiento, como unicast, multicast, broadcast y muchos a uno (source routing), para el intercambio eficiente de datos en la red.

La primera cosa que un nodo (router o dispositivo final) que quiere unirse a la red tiene que hacer es preguntar al coordinador por una dirección de red (16 bits) como parte del proceso de asociación. Toda la información en la red es enrutada usando esta dirección y no la dirección MAC de 64 bits. Es este paso se realizan los procedimientos de autenticación y cifrado.

Una vez que un nodo se ha unido a la red, puede enviar información a sus hermanos a través de los enrutadores que se encuentran siempre disponibles ("despiertos") esperando los paquetes. Cuando el enrutador recibe el paquete y el destino está en su radio de señal, el enrutador primero mira si el dispositivo final de destino está despierto o dormido. En el primer caso, el enrutador envía el paquete al dispositivo final. Sin embargo, si está inactivo, el enrutador almacenará el paquete en un búfer hasta que el nodo del dispositivo final se despierte y le pregunte por novedades al enrutador.

2.4.3.2 Capa de Aplicación (APL)

La capa de aplicación (APL) se compone de tres componentes principales: la subcapa de soporte de aplicación (APS), objetos de dispositivo ZigBee (ZDO), y el marco de aplicación (AF):

- **La subcapa APS** se encarga de proporcionar proporciona una interfaz entre la capa de red (NWK) y la capa de aplicación (APL) a través de un conjunto de servicios generales que son usado tanto por el ZDO y los objetos de aplicación definidos por el fabricante. Estos servicios son proporcionados por dos entidades [2]:

  - **Entidad de datos de la subcapa APS** (**APSDE**, *Application Support Sub-Layer Data Entity*): proporciona un servicio de datos tanto a la

capa de red como al ZDO y los objetos de aplicación para habilitar el transporte de PDUs de aplicación entre dos o más dispositivos, los cuales deben estar en la misma red. Ofrece:

- Generación de unidades de datos del nivel de aplicación (APDU, *Application Protocol Data Unit*): esta entidad debe coger un APDU y genera un APS PDU mediante la adición de la cabecera adecuada del protocolo.

- Asociación (*binding*): una vez que dos dispositivos son asociados, la APSDE debe ser capaz de transferir un mensaje desde un dispositivo a otro.

- Filtrado de direcciones de grupo: proporciona la capacidad de filtrar mensajes dirigidos a grupos basados en pertenencia de dispositivos a dichos grupos.

- Transporte confiable: aumenta la confiabilidad de las transacciones por encima de la disponible solo desde la capa NWK al emplear reintentos de extremo a extremo.

- Rechazo de duplicados: no se permite la recepción del mismo mensaje enviado más de una vez.

- Fragmentación: habilita la segmentación y el reemsamblado de mensajes mayores que la carga útil de un único paquete NWK.

- **Entidad de gestión de la subcapa APS** (**APSME**, *Application Support Sub-Layer Management Entity*): proporciona un servicio de gestión que permite a una aplicación interactuar con el stack. Además, ofrece:

  - Gestión de asociación: asocia dos dispositivos basándose en sus servicios y necesidades.

  - Seguridad: capacidad de establecer relaciones auténticas entre dispositivos mediante el uso de claves seguras.

  - Gestión de grupos: ofrece la capacidad de declarar una única dirección compartida por múltiples dispositivos y añadir y eliminar nodos del grupo.

- El **marco de aplicación (AF)** es el entorno en el cuál se albergan las distintas aplicaciones (objetos de aplicación) de un dispositivo ZigBee y es el encargado de gestionarlas. Se pueden definir hasta 254 objetos de aplicación distintos, del 1 al 254, cada uno de los cuales dispone de un punto de acceso (endpoint). El endpoint 0 se reserva para la interfaz de datos con el ZDO, y el 255 para la función de interfaz de datos para enviar mensajes de broadcast a todas las aplicaciones de un dispositivo.

  Para llevar a cabo la gestión de las aplicaciones de un dispositivo de forma eficiente, el marco de aplicación utiliza los dos siguiente conceptos:

- **Perfiles de aplicación**: son acuerdos para mensajes, formatos de mensajes, y acciones de procesamiento que permiten a los desarrolladores crear una aplicación distribuida e interoperable empleando entidades de aplicación que residen en dispositivos separados. Estos perfiles de aplicación permiten a las aplicaciones enviar comandos, pedir datos, y procesar comandos y respuestas.

- **Clústeres**: son identificados por un identificador de clúster, el cual está asociado con un flujo de datos desde o hacia un dispositivo. Estos identificadores son únicos en el alcance de un perfil de aplicación particular.

- Los **objetos de dispositivo ZigBee** (**ZDO**) representan una clase base de funcionalidad que proporciona una interfaz entre objetos de aplicación, perfiles de dispositivo y el APS. Se localiza entre el marco de aplicación y el APS, siendo responsable de:

  - Inicializar la subcapa de soporte de aplicación (APS), la capa de red (NWK), y el Proveedor de servicio de seguridad (SSP, *Security Service Provider*).

  - Ensamblar información de configuración desde la aplicación final para determinar e implementar descubrimiento de servicios y dispositivos, gestión de seguridad, gestión de enrutamiento y gestión de asociación. El descubrimiento de dispositivos es la capacidad de determinar la identidad de otros dispositivos de la PAN, mientras que con el descubrimiento de servicios el dispositivo puede solicitar a otro dispositivo de la PAN que le proporcione información detallada sobre las aplicaciones que implementa o los puntos de acceso que tiene asignados.

  De manera similar a los perfiles de aplicación definidos en el AF, existe un perfil definido para el ZDO denominado Perfil de Dispositivo ZigBee (**ZDP**, *ZigBee Device Profile*), el cual contiene los descriptores del dispositivo y los clústeres con los que puede operar.

2.4.4 Topologías de red

El protocolo ZigBee permite el empleo de tres topologías de red [11]:

- **Topología en estrella**: la red es controlada por un único dispositivo, el coordinador ZigBee, siendo responsable de inicial y mantener los dispositivos en la red.

- **Topología en árbol**: el coordinador ZigBee será la raíz del árbol, siendo el responsable de iniciar la red y elegir ciertos parámetros de red claves. La red puede ser extendida con el uso de enrutadores ZigBee, los cuales mueven los datos y controlan los mensajes a través de la red usando una estrategia de encaminamiento jerarquizada.

- **Topología de malla** (*mesh*): es la topología más habitual utilizada, en la que al menos uno de los nodos tendrá más de dos conexiones. Es el equivalente a la denominada punto a punto en IEEE 802.15.4 (Figura 8). En ella, cada dispositivo puede comunicarse directamente con cualquier nodo de la red. Para ello, se requiere que un FFD actúe como coordinador para inicializar la red y

gestionar el proceso de comunicación, gestionando los caminos que puede seguir un paquete para prevenir un mal funcionamiento de la red en caso de fallo de uno de los nodos. En este tipo de redes, los dispositivos que participan en la retransmisión de los mensajes son siempre FFDs. Los RFDs pueden formar parte de la red pero únicamente pueden comunicarse con un dispositivo en particular (coordinador o enrutador).

2.4.5 Medidas de seguridad en el protocolo ZigBee

Zigbee implementa dos capas de seguridad extra sobre la capa 802.15.4: las capas de seguridad de Red y Aplicación. Todas las políticas de seguridad se basan en el algoritmo de cifrado AES 128 bits, por lo que la arquitectura de hardware implementada anteriormente para el nivel de enlace (capa MAC) sigue siendo válida [15].

Hay tres tipos de claves: claves maestras, de enlace y de red.

- **Claves Maestras** (*Master Keys*): se encuentran pre-instaladas en cada uno de los nodos. Su función es la de mantener confidencial el intercambio de Claves de Enlace (Link Keys) entre dos nodos durante el Procedimiento de Establecimiento de Claves (*Key Establishment Procedure* (SKKE)).

- **Claves de Enlace** (*Link Keys*): Son únicas entre cada par de nodos. Estas claves se gestionan por el nivel de Aplicación. Se usan para cifrar toda la información entre cada par de dispositivos, por lo que se necesitarían más recursos de memoria en cada dispositivo (no se utilizan en el modo residencial, explicado más abajo).

- **Claves de Red** (*NWK Keys*): se trata de una clave única de 128 bits compartida entre todos los dispositivos de la red. Es generada por el Centro de Confianza y re-generada en diferentes intervalos de tiempo. Cada nodo tiene que obtener dicha clave para poder unirse a la red. Una vez que el centro de confianza decide cambiar la Clave de Red, la nueva clave se difunde a través de la red usando la vieja Clave de red (la nueva clave se cifra con la antigua). Una vez la nueva clave es actualizada en un dispositivo, su Contador de Trama (*Frame Counter*) se inicializa a cero. Por lo general, el centro de confianza es el Coordinador. Sin embargo, puede ser un dispositivo dedicado. Debe autenticar y validar cada dispositivo que intenta unirse a la red.

Existen dos clases de políticas de seguridad que un Centro de Confianza puede seguir:

- **Modo Comercial**: el Centro de Confianza comparte las claves Master y de Enlace con cualquier dispositivo en la red. Este modo requiere recursos de memoria elevados. Este modo ofrece un modelo centralizado completo para el control de la seguridad de claves (*Key Security*).

- **Modo Residencial**: el Centro de Confianza comparte únicamente la Clave de Red (es el modo ideal cuando los dispositivos integrados tienen que hacer frente a esta tarea debido a los bajos recursos que poseen). Este es el modo elegido normalmente para modelos de redes de sensores inalámbricos.

Como protocolo de bajo costo, Zigbee asume un modelo de "confianza abierta" en el que las capas de la pila de protocolos confían entre sí. Por lo tanto, la protección criptográfica solo existe entre los dispositivos, pero no entre las diferentes capas en un dispositivo. Además, establece el principio: "l*a capa que origina una trama es responsable de su seguridad inicial*" [4]. Además, cada comando Zigbee incluye un contador de tramas para detener los ataques de repetición o replay (en los que un atacante puede grabar y reproducir un mensaje anteriores). El punto extremo receptor siempre verifica el contador de trama e ignora los mensajes duplicados. Zigbee también es compatible con lo que se conoce como *agilidad de frecuencia*, en la cual la red se reubica en caso de la existencia de un ataque de interferencias (jamming) [20].

2.4.5.1 Modelo de Seguridad

Para satisfacer una amplia gama de aplicaciones, al mismo tiempo que mantiene bajo costo y potencia, Zigbee afirma ofrecer dos arquitecturas de red y los modelos de seguridad correspondientes: modelos distribuidos y centralizados. Se diferencian en cómo admiten nuevos dispositivos en la red y cómo protegen los mensajes en la red. [3]

- Un **modelo de seguridad distribuido** proporciona un sistema menos seguro y más simple. Tiene dos tipos de dispositivos: enrutadores y dispositivos finales. Aquí, un enrutador puede formar una red de seguridad distribuida cuando no puede encontrar ninguna red existente. Cada enrutador puede emitir claves de red. A medida que más enrutadores y dispositivos se unen a la red, los enrutadores anteriores en la red envían la clave. Para participar en redes de seguridad distribuidas, todos los enrutadores y finales deben estar preconfigurados con una clave de enlace que se utiliza para cifrar la clave de red al pasarla de un enrutador "padre" a un nodo recién unido. Todos los dispositivos en la red cifran mensajes con la misma clave de red.

- Un **modelo de seguridad centralizado** proporciona mayor seguridad. También es más complicado ya que incluye un tercer tipo de dispositivo, el Centro de Confianza, que generalmente también es el coordinador de la red. El Centro de Confianza forma una red centralizada, configura y autentica enrutadores y dispositivos para que se unan a una red. El TC establece una Clave de Enlace de Centro de Confianza (TCLK, *Trust Center Link Key*) única para cada dispositivo de la red a medida que se unen y vinculan las claves para cada par de dispositivos según se solicite. El TC también determina la clave de red. Para participar en un modelo de red de seguridad centralizada, todas las entidades deben preconfigurarse con una clave de enlace que se utiliza para cifrar la clave de red al pasarla desde el TC a una entidad recién unida. Ambos sistemas se ilustran en la siguiente figura.

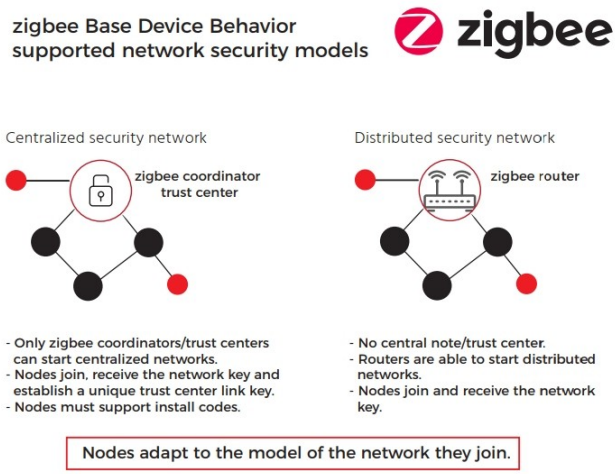


Figura 17: Modelos de Seguridad ZigBee [3]

2.4.5.2 Presunciones sobre la seguridad de ZigBee

Aparte del modelo de confianza abierta entre capas, la seguridad de ZigBee depende en última instancia de las suposiciones siguientes [2]:

- **La custodia de claves simétricas.** ZigBee asume que las claves secretas no están disponibles fuera del dispositivo de forma no segura, lo que significa que toda la transmisión de claves debe estar cifrada. Sin embargo, durante la configuración previa de un nuevo dispositivo se produce un intercambio de claves en la que, si un adversario tiene acceso físico al dispositivo, podría llegar a vulnerar esta suposición y acceder a información confidencial. No obstante, la política de seguridad de ZigBee no protege contra ataques al hardware debido a su naturaleza de bajo coste.

- **La protección del mecanismo empleado**. Todos los nodos del enrutador y del dispositivo final deben admitir la seguridad centralizada y la seguridad distribuida adaptándose al esquema de seguridad empleado por la red a la que se unen.

- **La implementación adecuada del mecanismo criptográfico y las políticas de seguridad asociadas involucradas**. Aquí, se supone que los desarrolladores de ZigBee siguen el protocolo completo en la práctica.

2.4.5.3 Claves de Seguridad

Tanto la red ZigBee como los dispositivos que hay en ella utilizan una claves de red y de enlace para comunicarse. La parte receptora siempre conoce qué claves son usadas en la protección de los mensajes.

Una clave de enlace es una clave de 128 bits compartida por dos dispositivos. Existen dos clases de claves de enlace: global y única, determinadas por cómo el dispositivo maneja los mensajes del Centro de Confianza (comandos APS). En una red con seguridad centralizada, existen tres clases de claves de enlace:

1. **Clave de enlace global**, usada por el Centro de Confianza y todos los nodos de la red.

2. **Clave de enlace única**, usada para relaciones uno a uno entre el Centro de Confianza y un nodo, la cual se reemplaza, posteriormente, por la clave de enlace del Centro de Confianza.

3. **Clave de enlace de aplicación**, la cual se usa entre un par de dispositivos de la red ZigBee.

Las claves de enlace relacionadas con el Centro de Confianza normalmente se encuentran configuradas usando algún método sin conexión o de fábrica, cómo códigos QR en el embalaje. Por su parte, las claves de enlace entre entidades son generadas por el centro de confianza y cifradas usando la clave de red. En redes con seguridad distribuida, estas claves de enlace únicamente existen en las comunicaciones existentes entre un par de dispositivos.

Dependiendo del modelo de seguridad empleado en una red ZigBee, pueden existir diferentes tipos de claves de seguridad empleadas para proteger las comunicaciones entre los dispositivos involucrados. A continuación pasamos a describirlas.

✔ Modelo de Seguridad Centralizada.

En una red con seguridad centralizada, las claves utilizadas en la capa de red se detallan a continuación:

- **Clave de red**: se trata de una clave compartida de 128 bits compartida por todos los dispositivos de la red, la cual es usada en comunicaciones de broadcast. Existen dos tipos de claves de red: estándar y de alta seguridad, dependiendo de cómo se distribuye dicha clave por la red, en claro o cifrada, respectivamente. Esta clave debería protegerse mediante cifrado cuando se le pasa a un nodo que intenta unirse a la red utilizando una clave de enlace (también llamada clave de Transporte) preconfigurada, la cual es conocida tanto por el Centro de Confianza como por el dispositivo que intenta unirse a la red en redes centralizadas. Para el caso de redes con seguridad distribuida, esta clave debe ser conocida por todos los nodos de la red.

- **Clave de enlace global pre-configurada**: se usa para cifrar la clave de red cuando es distribuida desde el Centro de Confianza a los dispositivos. Esta clave de enlace es la misma para todos los nodos de la red. Puede ser de dos tipos:

  - Definida por Zigbee, su valor es bien conocido (**0x5A 0x69 0x67 0x42 0x65 0x65 0x41 0x6C 0x6C 0x69 0x61 0x6E 0x63 0x65 0x30 0x39** (*ZigbeeAlliance09*)) y permite la adición a la red de nodos de diferentes fabricantes.

  - Definida por el fabricante, haciendo que únicamente los nodos del fabricante específico se unan a la red.

- **Clave de enlace única pre-configurada**: se utiliza para cifrar la clave de red cuando se transmite desde el Centro de Confianza a un nodo. Esta clave es exclusiva para cada para Centro de Confianza – Nodo, y se encuentra pre-

configurada o pre-programada en los nodos relevantes, ya sea en su fabricación o durante su puesta en servicio [2]. En la nueva versión, ZigBee 3.0, la clave de enlace única pre-configurada se proporciona en forma de un código de instalación, compuesta por un número aleatorio de 128 bits protegido por un CRC de 16 bits (Comprobación de Redundancia Cíclica) pre-instalado en los dispositivos [20].

En una versión anterior del protocolo ZigBee, los nodos, normal,ente, usan la clave de enlace global pre-configurada. No obstante, la mayor parte de los dispositivos compatibles con Zigbee 3.0 usan la clave de enlace única pre-configurada o la clave de enlace global pre-configurada definida por el fabricante.

Una vez se ha establecido la seguridad a nivel de red, se puede configurar la seguridad a nivel de aplicación para comunicaciones más seguras. Las claves utilizadas en este caso son:

- **Clave de enlace global pre-configurada**: explicada más arriba, se utiliza para comunicaciones entre el Centro de Confianza y todos los demás nodos.

- **Clave de enlace único pre-configurada**: explicada más arriba, también se utiliza para comunicaciones entre el Centro de Confianza y el resto de nodos.

- **Clave de Enlace del Centro de Confianza (TCLK)**: utilizada entre el centro de Confianza y cualquier otro nodo, se trata de una clave de 128 bits derivada de la clave de enlace única pre-configurada usando la función hash de Matyas-Meyer-Oseas (MMO) o generada aleatoriamente por el Centro de Confianza. Esta clave se pasa, desde el Centro de Confianza al nodo relevante, cifrada usando la clave de red y, si existe, la clave de enlace única pre-configurada para dicho dispositivo. Posteriormente, esta TCLK se usa para cifrar todas las comunicaciones subsecuentes entre el Centro de Confianza y el nodo, reemplazando a la clave de enlace única pre-configurada. Sin embargo, el nodo guarda la clave de enlace única pre-configurada en caso de que necesite volver a unirse a la red en en futuro.

- **Clave de Enlace de Aplicación:** se utiliza entre un par de nodos cualesquiera para comunicarse (no interviene el Centro de Confianza). Esta clave se pide al Centro de Confianza por uno de los dos dispositivos finales, y se genera por éste mediante la asociación de las direcciones MAC de los dos nodos. Posteriormente, el Centro de Confianza cifra dicha clave con la clave de red y, si existe, con la clave de enlace única pre-configurada para cada uno de los nodos.

En un modelo de seguridad centralizado, el Centro de Confianza periódicamente crea, distribuye y cambia la clave de red para limitar el tiempo que un atacante puede adquirirla. La nueva clave de red es cifrada con la Clave de Enlace Del Centro de Confianza (TCLK) generada por este. Cuando la nueva clave, primero, alcanza los nodos, la clave transportada es automáticamente guardada, pero no activada. Un nodo puede almacenar más de una clave de red mientras identifica a la clave actual con un único “número de secuencia de clave” asignado por el Centro de Confianza. Igualmente, la clave de enlace de aplicación puede ser reemplazada con la nueva clave de enlace generada por el Centro de Confianza.

A modo de resumen, las claves usadas en un modelo de seguridad centralizado del protocolo ZigBee se recoge en la siguiente tabla:

Claves de Seguridad	Descripción	
Seguridad Nivel de Red		
Clave de red	• Clave esencial para cifrar las comunicaciones entre todos los nodos de la red. • Generada aleatoriamente por el Centro de Confianza. • Distribuida a los nodos entrantes, cifrada con una clave de enlace pre-configurada.	
Seguridad Nivel de Aplicación		
Clave de Enlace Global (pre-configurada)	• Usada entre el Centro de Confianza y el resto de nodos. • Pre-configurada en todos los nodos (excepto cuando se pre-configura una clave de enlace única). • Usada al unirse nuevos dispositivos para cifrar la clave de red transportada desde el Centro de Confianza a los nodos. • Si es definida por ZigBee, permite la adición a la red de nodos de distintos fabricantes. • Si es definida por el fabricante, permite la adición de nodos pertenecientes a dicho fabricante.	
Clave de Enlace Única	Clave opcional utilizada para cifrar las comunicaciones entre un par de nodos. Puede ser de los siguientes tipos:	
	Clave de enlace única pre-configurada	• Usada entre el Centro de confianza y cualquier otro nodo. • Pre-configurada en el Centro de Confianza y el nodo. • Se usa también para cifrar la clave de red cuando se transporte desde el Centro de Confianza al nodo cuando intenta unirse.
	Clave de Enlace del Centro de Confianza (TCLK)	• Utilizada entre el Centro de Confianza y cualquier otro nodo. • Se genera aleatoriamente por el Centro de Confianza. • Distribuida al nodo cifrada con la clave de red y la clave de enlace pre-configurada (si existe). • Reemplaza a la clave de enlace pre-configurada (si existe) pero la aplicación debe guardar la clave pre-configurada en caso de que necesite volver a unirse a la red.
	Clave de enlace de Aplicación	• Usada entre un par de nodos, sin incluir al Centro de Confianza. • Generada aleatoriamente por el Centro de Confianza. • Distribuida a cada uno de los nodos cifrada con la clave de red y la clave de enlace pre-configurada (si existe).

Tabla 5: Claves de Seguridad en un modelo centralizado

✔ Modelo de Seguridad Distribuida.

Las claves utilizadas para las capas de Red y Aplicación en un modelo de seguridad distribuida son las siguientes:

- **Clave de red**, como se describió más arriba.

- **Clave de Enlace Global para Seguridad Distribuida**, la cual se usa para cifrar las comunicaciones entre el Enrutador padre y un nodo que se une a la red. Esta clave viene fijada de fábrica en todos los nodos [21].

- **Clave de Enlace Pre-configurada**, la cual se usa también para cifrar la comunicación entre el Enrutador padre y el nodo que se une a la red. Al igual que la anterior, también viene programada de fábrica en todos los nodos usando alguna herramienta de configuración. Existen tres tipos:

  - **Clave de Desarrollo**, usada durante el desarrollo anterior a una certificación ZigBee.

  - **Clave Maestra**, usada después de una certificación ZigBee válida.

  - **Clave de Certificación**, usada durante las pruebas en una certificación ZigBee [21].

Al final, la clave de enlace usada debería ser la clave maestra que muestra una certificación ZigBee válida.

2.4.5.4 Arquitectura de Seguridad

Tal y como se ha mencionado anteriormente, ZigBee construye las capas de Red (NWK) y Aplicación (APL) encima de las capas IEEE 802.15.4 Física (PHY) y de Control de Acceso al Medio (MAC). La capa de aplicación incluye la subcapa APS, la de Objeto de Dispositivo ZigBee (ZDO) y la de aplicaciones ZigBee (AF).

Una visión más detallada del esquema de la arquitectura de la pila del protocolo ZigBee se presenta a continuación:

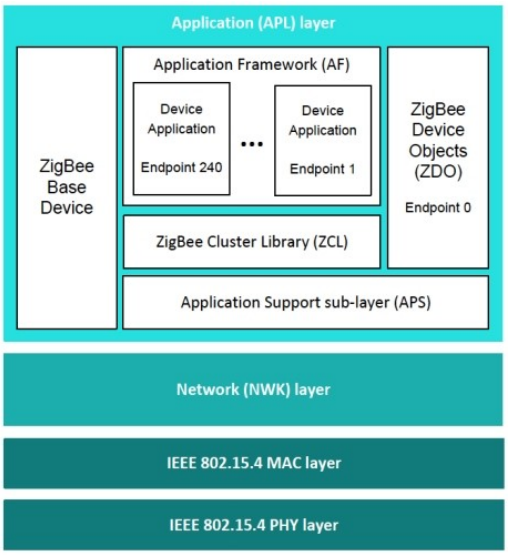


Figura 18: Esquema de la arquitectura del stack de ZigBee

Atendiendo a la seguridad del protocolo, la arquitectura incluye mecanismos de seguridad en tres capas del stack: las capas MAC, NWK y APS.

✔ Seguridad en la Capa MAC.

La seguridad de la capa MAC se basa en la seguridad de IEEE 802.15.4 aumentada con CCM*. CCM es un contador mejorado con un esquema de cifrado utilizando el modo de operación CBC-MAC, mientras CCM* es CCM con capacidades de sólo cifrado y sólo integridad. La capa MAC usa una sola clave para todos los niveles de seguridad CCM* (CCM* a lo largo de las capas MAC, NWK y APS) [4].

Como parte del modelo de confianza abierta, la capa MAC es responsable de su propio procesamiento de seguridad, pero las capas superiores determinan qué claves o niveles de seguridad usar. La capa superior hace que coincida la clave por defecto para la capa MAC con la clave de red activa, y las claves de enlace de la capa MAC con cualquiera de las claves de enlace de la capa superior.

La siguiente figura muestra una trama MAC saliente en el protocolo ZigBee con su procesamiento de seguridad:

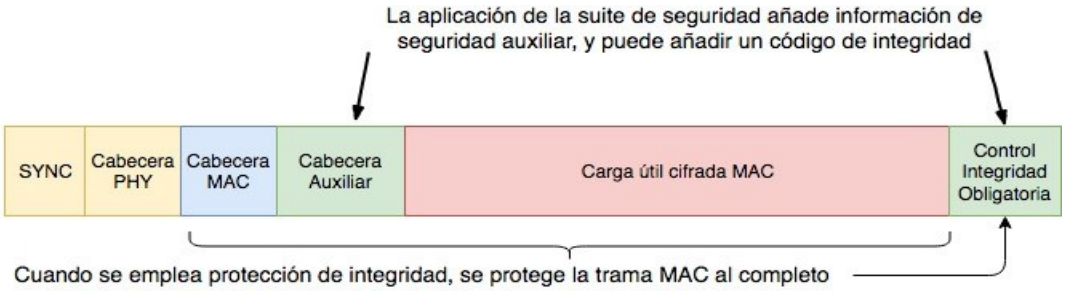


Figura 19: Trama ZigBee con seguridad en la capa MAC

✔ Seguridad en la Capa NWK (Red).

La capa NWK es responsable de los pasos de procesamiento necesarios para transmitir los paquetes salientes de forma segura, al igual que recibir también de forma segura los paquetes entrantes. Similar a la capa MAC, las capas superiores establecen las claves apropiadas y el contador de paquete, y establece qué nivel de seguridad usar [2].

La capa NWK a veces transmite mensajes de solicitud de ruta y procesa los mensajes de respuesta de ruta recibidos. Al hacerlo, la capa NWK utiliza claves de enlace si están disponibles; de lo contrario, utiliza su clave de red activa. En todo caso, se indica explícitamente la clave utilizada para proteger el paquete mediante el formato de este.

En la siguiente figura se recoge un ejemplo de un paquete de capa NWK cifrado:

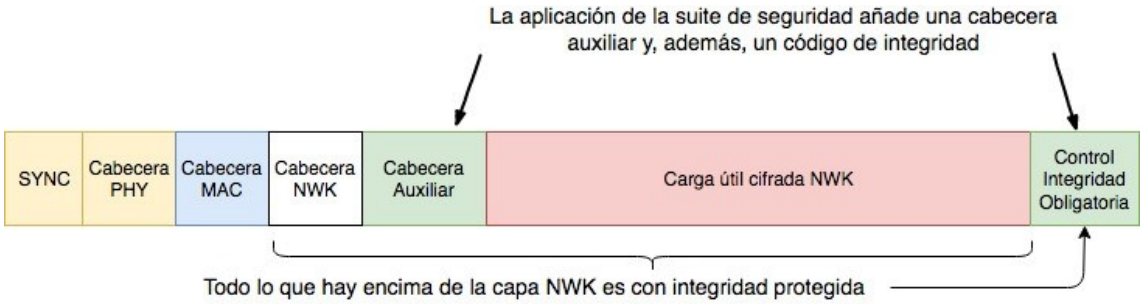


Figura 20: Trama ZigBee con seguridad en la capa NWK

✔ Seguridad en la Capa APL (Aplicación).

Toda la seguridad relativa a las capas APL es gestionada por la subcapa APS (soporte de aplicación). La capa APS es responsable del los pasos de procesamiento necesarios para transmitir de forma segura los paquetes salientes, recibir de forma segura los paquetes entrantes y establecer y gestionar las claves de cifrado también de forma segura. Los niveles superiores controlan el nivel de seguridad o la gestión de las claves de cifrado proporcionando primitivas a la capa APS. La siguiente imagen muestra un ejemplo de capa APS cifrada:

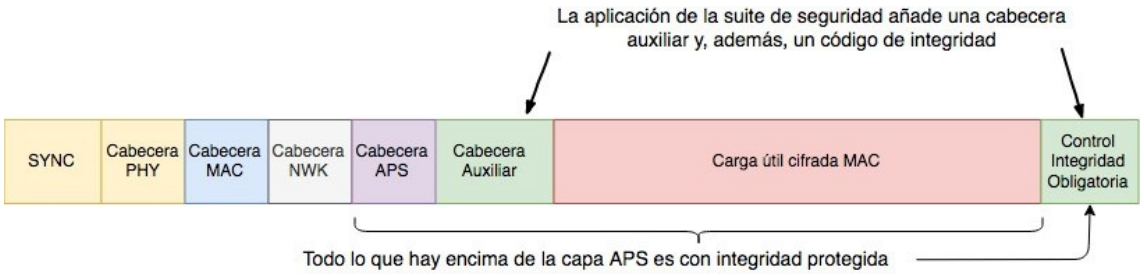


Figura 21: Trama ZigBee con seguridad en la capa APS

2.4.6 Novedades en ZigBee 3.0

El protocolo ZigBee, en su versión 3.0, implementa algunas capacidades de seguridad nuevas diseñadas para adaptarse al estado actual de la tecnología y a los nuevos riesgos. Estas novedades incluyen:

- ✔ Autenticación única por dispositivo al unirse a la red.

Existe un momento de "inseguridad" en la especificación de ZigBee 1 y 2 que usa una clave de cifrado simétrica bien conocida (*TCLK*) para distribuir una clave de red única cuando un nuevo dispositivo se une a la red. Esto fue establecido así por la ZigBee Alliance para realizar un balance entre seguridad y usabilidad, pensando en el impacto moderado que un atacante tendría al tener que estar capturando el tráfico de red ZigBee al mismo tiempo que un nuevo dispositivo se está uniendo a la red [4].

Este método ha sido eliminado de la especificación ZigBee 3.0 y reemplazado por un proceso que requiere un código de instalación por dispositivo que se utiliza para generar una clave única para el proceso de unión a redes con seguridad centralizada. Este código puede ser impreso en el dispositivo (o en su embalaje), bien mediante un número o código QR (para ser escaneado por una cámara) o bien mediante cualquier otro método "fuera de línea" (donde no se utilice un mensaje ZigBee). Este código, posteriormente, se insertará o escaneará en un smartphone o tablet conectado al Centro de Confianza (por ejemplo, usando NFC o Bluetooth) [3]. Todos los dispositivos ZigBee deben contener un código de instalación único, el cual se trata de un número aleatorio de 128 bits protegido con un CRC de 16 bits. Entonces, el dispositivo que intenta unirse y el Centro de Confianza derivan una Clave de Enlace del Centro de Confianza (TCLK) única usando la función de hash Matyas-Meyer-Oseas (MMO).

- ✔ Actualización de claves en tiempo de ejecución durante la operación.

En redes con seguridad centralizada, el Centro de Confianza periódicamente crea, distribuye y cambia a una nueva clave de red. Por lo tanto, un atacante que adquiera una clave de red dispondrá de un tiempo limitado antes de que ésta expire. Estas claves actualizadas se envían cifradas con la Clave de Enlace generada por el Centro de Confianza, explicada más arriba.

- ✔ Actualizaciones seguras de firmware over-the-air (OTA).

Existen, también, actualizaciones OTA (Over-The-Air) que permiten al fabricante añadir nuevas funcionalidades, arreglar defectos en el producto y aplicar parches de seguridad a medida que se encuentran nuevas amenazas. Este tipo de actualizaciones introducen una vulnerabilidad de seguridad potencial si el protocolo no proporciona suficiente protección o el fabricante del dispositivo no usa todas las medidas de protección disponibles. ZigBee proporciona seguridad multi-nivel para actualizar dispositivos y asegurar la integridad de las imágenes con la actualización. Para ello, se cifran todas las imágenes transferidas mediante OTA con una única clave, se firma dicha imagen con otra clave única, cifrando la imagen durante la fabricación, de manera que únicamente el dispositivo final puede descifrarlo. La imagen puede estar almacenada en una memoria on-chip, la cual se configura deshabilitando la lectura de depuración para evitar ingeniería inversa con aplicaciones de debugging comunes. Una vez se recibe la imagen cifrada, el bootloader descifra la imagen, valida las firmas y actualiza el dispositivo. El bootloader también comprueba la validez de cada imagen cada vez que se inicia el dispositivo, de manera que se pueda volver a utilizar una buena imagen conocida anterior si la imagen no es válida

(detección de la corrupción imagen de forma rápida para poder tomar las acciones pertinentes) [4].

- ✔ Cifrado lógico basado en enlace.

En ZigBee 3.0, el protocolo puede también crear un enlace seguro a nivel de aplicación entre un par de dispositivos en la red mediante el establecimiento de un único set de claves de cifrado AES-128, soportando los enlaces privados virtuales entre un par de nodos que requieran una seguridad mayor. Un ejemplo de esto ocurre cuando se dispone de una red ZigBee local que conecta multitud de dispositivos, entre los que se encuentran cerraduras para puertas y sensores para apertura de garajes. Aquí, se hace necesaria una capa extra de seguridad que limite la capacidad de un posible atacante de conseguir la clave de red e inyectar mensajes que pudieran abrir las puertas, necesitando, además, la clave de enlace a nivel de aplicación necesaria para abrirlas [20].

- ✔ Técnicas adicionales

Para parar los ataques de repetición (en los que un atacante puede capturar y replicar un mensaje de comando), cada comando ZigBee incluye un contador de paquetes. El dispositivo receptor comprueba este contador de paquetes e ignora mensajes duplicados.

Además, Zigbee soporta agilidad de frecuencia, la cual permite a la red reubicarse en un canal diferente (frecuencia) si el canal actual está dañado, por ejemplo, por un ataque de interferencia (jamming).

2.4.7 Productos ZigBee

La cantidad de productos Zigbee certificados crece cada día. Cada vez más fabricantes centran el desarrollo de sus productos en la implementación de dicho protocolo, dada su versatilidad, su cuota de mercado y la previsión de crecimiento en los próximos años. Esto provoca que el ecosistema de dispositivos destinados al IoT y el IIoT se expanda, a la vez que se facilita la interoperabilidad entre ellos.

Un ejemplo de este tipo de dispositivos puede encontrarse en la web de la Zigbee Alliance [22], junto con información relativa a su función principal, así como referencias a hojas de características de fabricantes y enlaces para su compra. Así, entre ellos podemos encontrar desde sistemas industriales de medición de gas [23] hasta bombillas inteligentes de capaces de modificar tanto la intensidad de la luz como su color [24] o altavoces con sistemas gestión inteligente como el Echo Plus de Amazon [25].

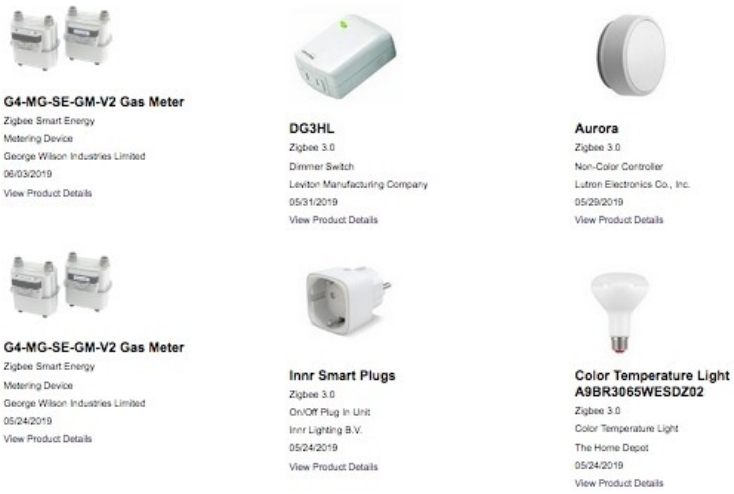


Figura 22: Productos ZigBee certificados [22]

Dado el crecimiento en el uso e implementación del protocolo por gran parte de la industria y la orientación de los productos lanzados al mercado, principalmente, sistemas domóticos y gestión industrial, se hace de especial importancia que se llevan a cabo las medidas necesarias que permitan un correcto uso de la tecnología, así como la adopción de acciones que eliminen o limiten en gran medida las posibles amenazas que puedan aparecer en el uso de dicha tecnología.

Factores como el deseo de reducir el time-to-market, implementar compatibilidad hacia atrás, favorecer la usabilidad o reducir los costes por unidad de los dispositivos llevan a los fabricantes a relajar e, incluso, eliminar por completo las controles de seguridad, con el consiguiente aumento del riesgo de sufrir un posible ciberataque.

La seguridad no deberá ser una consideración más justo antes de lanzar un producto al mercado, sino que deberá estar presente desde la concepción misma del producto, pasando por las fases de diseño, construcción, validación y testeo, hasta su puesta en producción. Sólo así se podrán anticipar y prever los posibles ataques a los que será sometido el producto durante un periodo de tiempo que, en el caso de sistemas industriales, podrá ser de varios años. Esto, unido a una política de seguridad adecuada, permitirá la adopción de medidas que, en caso de un posible incidente de seguridad, permitan mitigar o eliminar las amenazas en el menor tiempo posible.

3. Análisis de seguridad de IEEE 802.15.4/ZigBee

Llegados a este punto, y basados en la información previa sobre el protocolo, llevaremos a cabo un análisis de seguridad del protocolo ZigBee con el principal objetivo de conocer sus debilidades en cuanto a diseño y arquitectura, funcionamiento e implementación que nos permita obtener una serie de conclusiones que ayuden en la correcta utilización de éste, minimizando todos los riesgos de seguridad posibles.

3.1 Herramientas hardware

Los dispositivos utilizados en este trabajo para llevar a cabo el análisis de seguridad del protocolo IEEE 802.15.4/ZigBee son los siguientes.

✔ XBee Serie 2

Se han utilizado dos módulos ZigBee de la serie 2 XBee (S2C) con antena cableada integrada para establecer una comunicación entre ambos, de manera que podamos estudiar y analizar dicha comunicación y, más concretamente, su seguridad. Este tipo de dispositivos pueden ser utilizados para la creación de redes punto a punto, punto a multipunto y malladas.

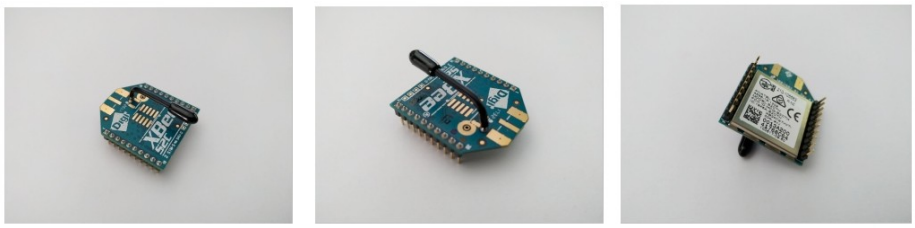


Figura 23. Diferentes vistas del módulo XBee S2C

Las especificaciones técnicas más importantes del XBee S2C se muestran a continuación [26]:

- Corriente pico en transmisión: 40 mA
- Corriente en recepción: 40 mA (@3.3 V)
- Corriente en corte: < 1 µA
- Alcance entorno urbano / indoor: hasta 40 m
- Alcance al aire libre (visión directa): hasta 120 m
- Potencia de transmisión: 2 mW (3 dBm)
- Sensibilidad en recepción: -96 dBm
- Dimensiones: 24mm x 28mm x 9mm
- Peso: 3.24g

✔ Adaptador XBee USB

Este tipo de placas permiten conectar y utilizar cualquier módulo XBee directamente mediante un puerto USB. Se trata de una tarjeta de comunicación UART que admite conectividad XBee, cuenta con interfaz UART, interfaz USB y botones y LED integrados, y proporciona una manera fácil de desarrollar y depurar [27].

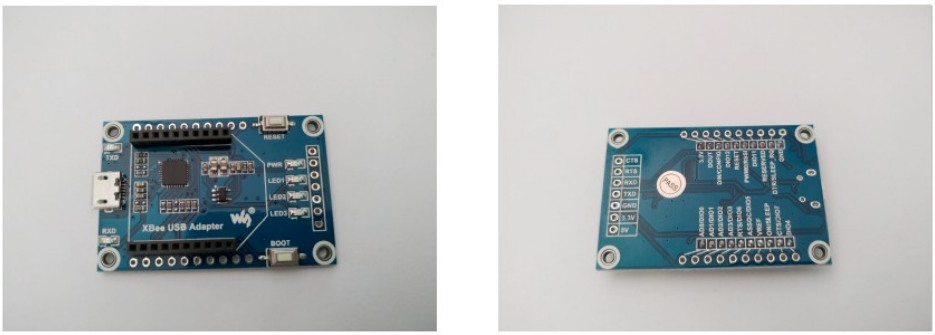


Figura 24. XBee USB Adapter

Este adaptador realiza dos funciones, principalmente:

- Proveer de una conexión entre el PC y el módulo XBee mediante un cable mini USB para poder acceder a los pines serie del dispositivo para programarlo y utilizarlo, convirtiendo y traduciendo los datos de USB a serie.
- Realizar la adaptación de voltaje a 3.3 V necesaria para alimentar los módulos XBee.

A continuación se muestra la imagen con la definición de los pines de este adaptador:

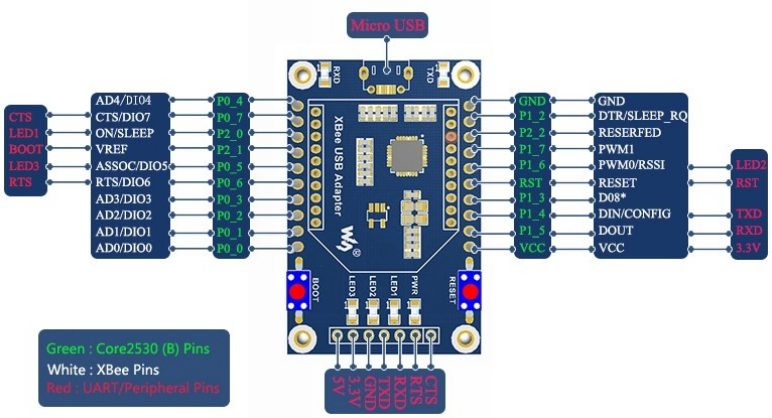


Figura 25. Definición de pines XBee USB Adapter

✔ Api-Mote

El Api-Mote es una placa hardware utilizada para ayudar a conocer y evaluar la seguridad de los sistemas IEEE 802.15.4 / ZigBee [28]. Se trata de un dispositivo basado en un chip diseñado específicamente para la interacción de bajo nivel con IEEE 802.15.4 / ZigBee PHY (nivel físico), el cual se suministra flasheado con la última versión de firmware KillerBee [29] por defecto. Este dispositivo es capaz tanto de escuchar y capturar información en canales ZigBee (funcionalidad pasiva) como inyectar y transmitir datos en dichos canales (funcionalidad activa).

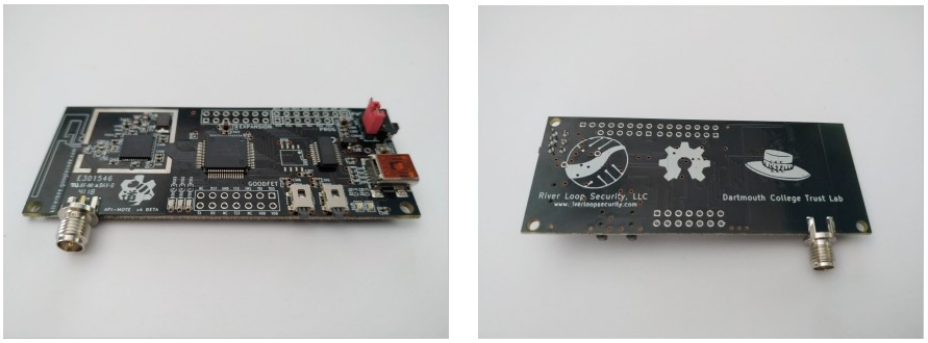


Figura 26. Placa Api-Mote (v4 Beta) IEEE 802.15.4 / ZigBee

Las especificaciones técnicas más importantes de esta placa son:

- Transceptor de RF compatible con IEEE 802.15.4 de 2.4 GHz y ZigBee™ Ready (CC2420).
- Interoperabilidad con otros dispositivos IEEE 802.15.4.
- MCU de 16 bits de potencia ultrabaja (116kB Flash, 8KB RAM) (MSP430F2618), con ADC integrado, DAC, supervisor suministro de voltaje y controlador DMA.
- Circuito integrado FTDI USB a serie.
- Programación y recolección de datos vía USB.
- Antena integrada (posibilidad de conexión de antena externa mediante conector SMA).
- Bajo consumo.
- Se soporta cifrado y autenticación hardware de enlace de datos.
- Soporte de firmware básico basado en GoodFET.

Los componentes estándar base del Api-Mote y sus conexiones lógicas se muestran a continuación [30]:

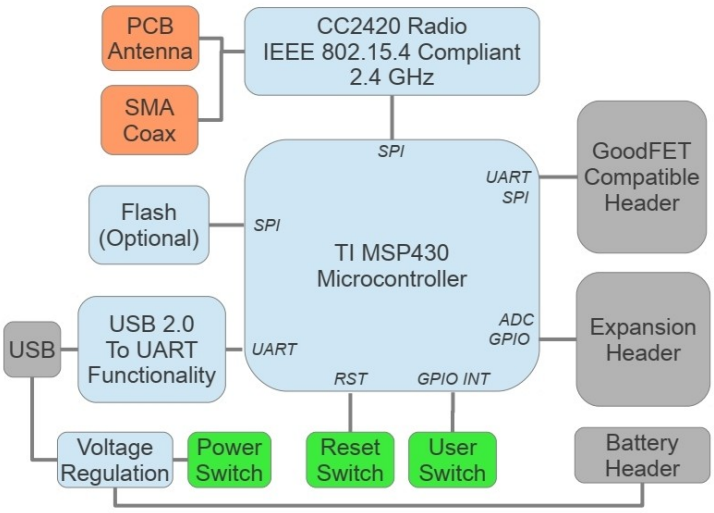


Figura 27. Diagrama de bloques del Api-Mote

3.2 Herramientas software

Para la realización de este trabajo y, más concretamente, en la puesta en funcionamiento del entorno de pruebas y el estudio y análisis de vulnerabilidades del protocolo ZigBee, han sido necesarias una serie de herramientas software que recogemos a continuación.

✔ XCTU

Se trata de una aplicación gráfica multiplataforma desarrollada por Digi que nos ha permitido interactuar con los módulos XBee para poder configurarlos y usarlos [31]. Entre las muchas funcionalidades que ofrece, con esta herramienta hemos podido:

- Conectar y actualizar el firmware de los módulos XBee S2C a la última versión disponible.
- Configurar los módulos XBee S2C, especificando el canal utilizado, el PAN ID (Personal Area Network Identifier), el modo de funcionamiento (Transparente o API), habilitación de cifrado, clave de red (en el nodo coordinador) y verificación de canal (en el nodo enrutador).
- Comunicar los módulos XBee mediante el envío de información entre ellos.

Para el correcto reconocimiento y funcionamiento de los XBee, ha sido necesario la instalación previa de los drivers de puerto virtual COM (Virtual COM Port (VCP)) que hacen que el dispositivo conectado como USB aparezca como un puerto COM adicional disponible en el PC. De esta forma, la aplicación puede acceder al dispositivo USB de la misma manera que lo haría a un puerto COM estándar [32]. Dado que se ha utilizado un equipo con Windows 10, la versión existente a fecha de entrega de este trabajo es la 2.12.28 para equipos de 64 bits (x64) [47].

✔ KillerBee

KillerBee es un framework (conjunto de herramientas) desarrollado en Python y diseñado especialmente para atacar y explotar vulnerabilidades en redes ZigBee y IEEE 802.15.4 [29]. Mediante las herramientas de KillerBee y una interfaz de radio IEEE 802.15.4 compatible, se puede escuchar en las redes ZigBee, reproducir el tráfico capturado, atacar sistemas criptográficos, etc. Además, ofrece la posibilidad de extender el framework con la creación de herramientas propias mediante el uso de su API.

Algunas de las herramientas utilizadas en este trabajo son:

- zbid: Identifica todas las interfaces disponibles.
- zbfind: Permite seguir y localizar transmisores IEEE 802.15.4.
- zbgoodfind: Busca archivos para averiguar la clave de cifrado de un SNA.
- zbassocflood: Intenta saturar una red definida enviando constantes peticiones (“inundación” o flood) de asociación.
- zbreplay: Reenvía el tráfico de red ZigBee/802.15.4 desde ficheros libpcap o Daintree.
- zbdsniff: Descifra las claves ZigBee entregadas en claro desde un archivo.
- zbdump: Permite capturar el tráfico de red ZigBee y IEEE 802.15.4 y registrarlo en un archivo para su posterior análisis.

Tal y como se indica en su repositorio de Github, es necesario tener instaladas un mínimo de dependencias software como módulos Python , como serial, usb, crypto, pygtk, cairo y scapy. A excepción de scapy, el resto de librerías pueden encontrarse en los repositorios oficiales de la distribución Linux que se use. Por ejemplo, en nuestro caso, para Fedora Linux:

```
# dnf install pygtk2 pycairo pyusb pycrypto pyserial python-de-
vel libgcrypt-devel
```

Para el caso de scapy, tendremos que clonar el repositorio oficial y, posteriormente, instalarlo:

```
# git clone https://github.com/secdev/scapy
# cd scapy
# python setup.py install
```

Finalmente, para la instalación de KillerBee clonamos su repositorio y lo instalamos según las instrucciones proporcionadas:

```
# git clone https://github.com/riverloopsec/killerbee
# cd killerbee
# python setup.py install
```

- ✔ Attify Zigbee Framework

Se trata de una aplicación gráfica para utilizar las herramientas de KillerBee, de manera que se facilita su uso al automatizar algunas de las acciones necesarias en el uso de la herramienta.

Para instalar la aplicación, tan sólo hay que clonar su repositorio de Github [40] y lanzar el script installer.sh, el cual instala KillerBee junto con las dependencias necesarias para utilizarlo (explicado más arriba) y la herramienta analizadora de Wireshark:

```
# git clone https://github.com/attify/Attify-Zigbee-Framework
# cd Attify-Zigbee-Framework
# chmod 755 installer.sh
# ./installer.sh
```

Para ejecutar la aplicación:

```
# python main.py
```

- ✔ Wireshark

Se trata de un conocido analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica, permitiendo ver todo el tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark [33].

Esta herramienta permitirá capturar y analizar el tráfico de red IEEE 802.15.4 / ZigBee transmitido entre los nodos XBee, de forma que se compruebe la correcta comunicación entre ellos, la aplicación de las medidas de seguridad configuradas, así

como extraer información confidencial transmitida cuando se consigan vulnerar tales mecanismos de seguridad.

Wireshark es una aplicación multiplataforma. Para GNU/Linux, se encuentra disponible en los repositorios oficiales de la mayoría de distribuciones. En nuestro caso, para Fedora, se instalaría como sigue:

```
# dnf install wireshark-qt
```

3.3 Entorno de pruebas

Para el estudio de la seguridad del protocolo ZigBee, y utilizando los dispositivos hardware y herramientas software detalladas anteriormente, hemos planteado la creación del siguiente escenario:

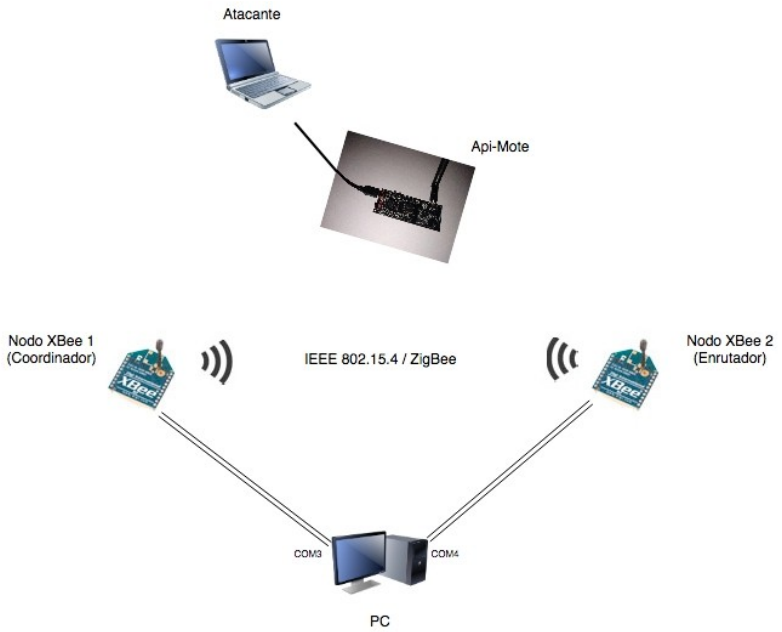


Figura 28. Esquema de red utilizado en el trabajo

Tal y como se extrae en la imagen, se dispone de un entorno de pruebas con las siguientes particularidades:

- Se han comunicado dos módulos XBee, utilizando los modos “Transparente” y “API” [34], en el que uno de ellos tendrá el rol de Coordinador y el otro de Enrutador.

- Ambos dispositivos XBee se encuentran conectados mediante cable USB a un ordenador con Windows 10 que ejecuta el programa XCTU, utilizado para realizar la configuración de estos y ejecutar los comandos a través de la interfaz Serial que serán transmitidos de un dispositivo a otro.

- Se ha simulado la existencia de un atacante (en adelante, “nodo Atacante”) que utiliza un equipo con Fedora Linux al que se encuentra conectado la placa Api-Mote con el que se ha capturado e inyectado tráfico entre los dos dispositivos XBee según el tipo de ataque en ejecución.

3.4 Ataques al protocolo IEEE 802.15.4 / ZigBee

Utilizando los componentes hardware y software detallados en el punto anterior, a continuación se recoge el análisis de vulnerabilidades del protocolo IEEE 802.15.4 / ZigBee para el entorno de pruebas definido que ha sido llevado a cabo. Concretamente, en este apartado se explicarán en qué consiste cada ataque, qué pruebas se han realizado, cuáles son los resultados esperados y cuáles son los obtenidos. Además, se señalarán el impacto que tienen cada uno de estos posibles ataques para las comunicaciones en este tipo de redes. Los detalles y pasos realizados para abordar los ataques han sido recogidos en el capítulo 4.

3.4.1 Sniffing

En este tipo de ataques el objetivo principal es el robo o la interceptación de datos al capturar el tráfico de la red utilizando un sniffer (herramienta destinada a capturar paquetes de red) cuando los datos se transmiten entre dos o más dispositivos [35]. Algunas redes ZigBee no utilizan el cifrado adecuado y permiten a un atacante, que utilice un equipo adecuado, interceptar y acceder a la información transmitida durante la comunicación, pudiendo hacer lo que se conoce como ataque de rastreo, donde se intenta recopilar toda la información disponible en la red. Esto es posible en redes que implementan protocolos estándar con un nivel genérico de seguridad.

En este apartado se ha establecido una comunicación entre dos dispositivos ZigBee, diferenciando entre comunicación cifrada y no cifrada. Una vez establecida, se ha transmitido información de un nodo a otro y se ha intentado capturar la información mediante el nodo atacante para comprobar el impacto que para la confidencialidad de las comunicaciones tendría este tipo de ataque.

✔ **Comunicación no cifrada.**

1. **Configuración del enlace**: el estado de configuración del enlace entre los dos dispositivos XBee se recoge en la siguiente tabla:

	Coordinador	Enrutador
Comunicación	Modo Transparente	Modo Transparente
Canal de comunicación	25	-
Identificador PAN	4444	4444
Cifrado	*No*	No
Verificación de canal	-	Sí
Mensaje enviado	-	*«HelloMiguel»*

Tabla 6: Configuración enlace para ataque de sniffing no cifrado

Como se puede ver, no se utiliza cifrado para proteger la información transmitida, el canal de comunicaciones elegido es el 25 (principalmente, para evitar un solapamiento con redes Wifi domésticas) y el identificador PAN es el 4444. Se enviará el mensaje “HelloMiguel” desde el nodo enrutador al

coordinador. Una visión más detallada de la configuración utilizada puede verse en la sección 4.1 del documento.

2. **Objetivo**: el objetivo principal que se persigue es la captura del mensaje "*HelloMiguel*" enviado entre los nodos enrutador y coordinador.

3. **Resultado esperado**: al no implementar ningún tipo de cifrado en la comunicación, se espera poder capturar el mensaje enviado entre los dos dispositivos en texto plano.

4. **Resultado obtenido**: se ha podido capturar el tráfico transmitido en la red ZigBee y obtenerse el mensaje "*HelloMiguel*" enviado entre los dos dispositivos (ver sección 4.1).

5. **Consecuencias**: se produce una vulneración de la confidencialidad de la información de la red, pudiendo extraer cualquier dato que sea transportado en ésta sin mayor problema.

✔ **Comunicación cifrada.**

1. **Configuración del enlace:** procedemos ahora a configurar los módulos de la misma manera que en el caso anterior a excepción de que, esta vez, las comunicaciones se cifrarán utilizando el algoritmo AES con una clave de red (NWK) simétrica. Esta clave se especificará en el Coordinador, y se transmitirá al Enrutador cuando éste se una a la red. Las características principales del enlace entre estos dispositivos son:

	Coordinador	Enrutador
Comunicación	Modo Transparente	Modo Transparente
Canal de comunicación	25	-
Identificador PAN	4444	4444
Clave red AES	*0xABCD*	-
Verificación de canal	-	Sí
Mensaje enviado	-	«EncryptedHelloMiguel»

Tabla 7: Configuración enlace comunicación cifrada modo Transparente

2. **Objetivo**: capturar el mensaje *EncryptedHelloMiguel* enviado desde el enrutador al coordinador.

3. **Resultado esperado**: como la información va cifrada, se espera no poder acceder al texto en claro y, consecuentemente, no poder obtener el mensaje.

4. **Resultado obtenido**: no se ha podido obtener el mensaje en claro ya que la comunicación va cifrada mediante AES 128 bits (ver sección 4.1).

5. **Consecuencias**: no se vulnera la seguridad de las comunicaciones de la red ZigBee.

Ahora bien. Partiendo del diseño y definición del estándar de ZigBee, la clave de red con la que se cifran las comunicaciones podría llegar a obtenerse y, por consiguiente, descifrar el tráfico dentro de la red debido a las siguientes premisas:

- El encargado de configurar la clave de red es el nodo Coordinador.

- Cuando un nuevo nodo se une a la red, el nodo Coordinador o Centro de Confianza (TC) le hace llegar la clave de red de la siguiente forma:

    - Supuesto 1: Si no existe configurada una clave de enlace, la clave de red se envía en claro al dispositivo.

    - Supuesto 2: Si existe configurada una clave de transporte (*Key-Transport Key,* también conocida como Clave de Enlace (*Link Key*)), se suministra la clave de red cifrada con la clave de transporte. El nuevo dispositivo que intenta unirse a la red debe también conocer la misma clave de transporte utilizada por el Centro de Confianza para poder descifrar la clave de red (cifrado simétrico AES). Según la Especificación Zigbee, una Clave de Transporte es una "clave utilizada para proteger los mensajes de transporte clave" [2] . Según la bibliografía consultada, esta Clave de Transporte o Enlace está siendo configurada en los dispositivos ZigBee en una de las siguientes formas:

        - Familias de dispositivos pertenecientes a la misma marca o compañía pueden configurarse de fábrica con la misma Clave de Transporte (pre-instalada), de manera que sea trivial la construcción de redes ZigBee y la adición de nuevos componentes a dichas redes.

        - Normalmente, los dispositivos que pueden operar y configurarse como Centro de Confianza tienen una Clave de Enlace o Transporte predeterminada y se conoce públicamente, siendo la codificación en hexadecimal de **ZigbeeAlliance09** [2].

Por lo tanto, para comprobar cómo de fácil sería para un posible atacante obtener la clave de red con la que se cifran las comunicaciones, hemos configurado la red ZigBee según los supuestos descritos para, posteriormente, intentar conseguir la clave de red.

A) Supuesto 1: Clave de Transporte no configurada.

1. **Configuración del enlace**: los datos con los que se han configurado los dispositivos XBee se recogen en la siguiente tabla:

	Coordinador	Enrutador
Comunicación	Modo API	Modo API
Canal de comunicación	25	-
Identificador PAN	4444	4444
Clave red AES	32 caracteres hexadecimales "*A*"	-

Tabla 8: Configuración enlace modo API sin clave de enlace

2. **Objetivo**: Capturar la clave de red enviada desde el coordinador al nodo enrutador cuando intenta unirse a la red.

3. **Resultado esperado**: como se ha analizado en el capítulo 2, en redes con seguridad centralizada, cuando un nodo intenta unirse a una red pero no dispone de clave de enlace, el centro de confianza (coordinador) envía la clave de red en claro. Por lo tanto, se espera poder obtenerla a partir de una captura de tráfico desde el nodo atacante.

4. **Resultado obtenido**: efectivamente, se ha podido acceder a la clave de red al ser enviada en claro desde el nodo coordinador al enrutador (ver sección 4.1).

5. **Consecuencias**: una vez se obtiene la clave de red, se puede acceder a cualquier información que circule por la red ZigBee, con lo que se produce una vulneración en la confidencialidad de las comunicaciones de la red.

B) Supuesto 2: Clave de Transporte configurada.

1. **Configuración del enlace**: en este caso, se configurará la clave de enlace en ambos nodos, enrutador y coordinador, de forma que el intercambio de la clave de red se haga de forma segura.

	Coordinador	Enrutador
Comunicación	Modo API	Modo API
Canal de comunicación	25	-
Identificador PAN	4444	4444
Clave red AES	32 caracteres hexadecimales "*A*"	-
Clave de enlace	0xABCDE	0xABCDE

Tabla 9: Configuración enlace modo API con clave de enlace

2. **Objetivo**: acceder a la información transmitida entre los nodos y obtener la clave de red.

3. **Resultado esperado**: como la comunicación se protege con la clave de enlace configurada, se espera no poder obtener la clave de red actual.

4. **Resultado obtenido**: el tráfico enviado entre los dispositivos de la red está correctamente cifrado y, consecuentemente, no se ha podido obtener la clave de red (ver sección 4.1).

5. **Consecuencias**: no se produce una vulneración en la confidencialidad de las comunicaciones de la red IEEE 802.15.4 / ZigBee.

3.4.2 Ataques de Repetición (Replay attacks)

También llamado ataque de playback, en español ataque de reproducción, o ataque de reinyección, es una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado [36]. En el caso de ZigBee, intenta evadir el uso e implementación de un número de secuencia introducido en los paquetes de datos para evitar este tipo de ataques. Con este tipo de contador, a cada paquete de datos que se transmite se le asigna un número de secuencia. Este contador se va incrementando con cada nuevo paquete transmitido, y es verificado por el dispositivo receptor. No obstante, debido a la escasa capacidad de procesamiento de este tipo de dispositivos, este mecanismo de conteo no resulta del todo efectivo en algunos casos, pudiendo inyectar tráfico capturado y que llegue al receptor sin problema.

Este tipo de ataques se llevan a cabo para conseguir, principalmente, dos objetivos: la suplantación de identidad y la denegación de servicio.

- ✔ **Suplantación de identidad.**

Uno de los propósitos que se persiguen con este tipo de ataques es la de hacer creer al nodo receptor que la información enviada por el “supuesto” emisor es legítima, intentando provocar un mal funcionamiento del mismo con la recepción de información repetida e inconsistente. Por lo tanto, al alterar y falsificar dicha información, el receptor podría llegar a creer que es el emisor legítimo el que envió tal información.

Imaginemos que un posible atacante ha llegado a capturar el comando que abre la puerta de casa. Replicando dicho tráfico, haría hacer creer al Trust Center que se trata de tráfico legítimo, provocando que la puerta se abra.

Para poder comprobar este funcionamiento del protocolo ZigBee, se ha realizado el siguiente ataque contra éste:

1. **Configuración del enlace**: se ha configurado los nodos XBee en modo API con las siguientes características:

	Coordinador	Enrutador
Comunicación	Modo API	Modo API
Canal de comunicación	25	-
Identificador PAN	4444	4444
Clave red AES	32 caracteres hexadecimales "*A*"	-
Clave de enlace	0xABCDE	0xABCDE
Comando enviado	*0x10 - Transmit Request “OpenTheDoor”*	-

Tabla 10: Configuración enlace modo API para envío de comando "OpenTheDoor"

2. **Objetivo**: se ha capturado el mensaje enviado del nodo enrutador al coordinador, el cual se trata de un comando con la orden “*OpenTheDoor*”, para, posteriormente, reenviar dicho tráfico al coordinador, suplantando al nodo enrutador y provocar una hipotética apertura de una puerta.

3. **Resultado esperado**: ya que el stack IEEE 802.15.4 / ZigBee implementa medidas contra ataques de repetición, se espera no poder suplantar al nodo emisor.

4. **Resultado obtenido** : sorprendentemente, el nodo coordinador ha recibido y procesado gran cantidad de los paquetes reenviados por el nodo atacante, con lo que se ha podido suplantar al nodo legítimo (ver sección 4.2).

5. **Consecuencias**: se produce, pues, una vulneración en la integridad de las comunicaciones de la red ZigBee, pudiendo suplantar al nodo emisor y provocar que, a partir de una captura de tráfico previa, el nodo receptor procese dicho tráfico, independientemente del momento en el que se envíe.

✔ **Denegación de Servicio.**

El tráfico capturado por un atacante podría ser utilizado para intentar realizar un ataque de denegación de servicio a cualesquiera de los nodos que componen una red ZigBee. Mediante un sencillo script, o utilizando varias máquinas simultáneamente, se puede intentar replicar dicho tráfico y esperar un comportamiento anómalo por parte de los receptores de los paquetes enviados.

Para comprobar la viabilidad de este ataque, se ha procedido con el siguiente escenario:

1. **Configuración del enlace**: igual que en el caso anterior.

2. **Objetivo**: reenvío masivo del tráfico capturado anteriormente para intentar sobrecargar al dispositivo destino y dejarlo fuera de servicio.

3. **Resultado esperado**: se espera poder saturar al nodo coordinador, de manera que pierda la conectividad y deje de procesar paquetes.

4. **Resultado obtenido**: no ha sido posible llevar al nodo objetivo del ataque a un estado no controlado y provocar su denegación de servicio (ver sección 4.2).

5. **Consecuencias**: no se ha producido ninguna consecuencia en el desempeño de la red ZigBee.

3.4.3 Denegación de Servicio (DoS, *Denial-of-Service*)

También llamado ataque DoS (por sus siglas en inglés, *Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos [37], provocando una pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

Aparte de la posible denegación de servicio que puede provocarse aprovechando un ataque de repetición, es posible intentar provocar un mal funcionamiento de un dispositivo de la red ZigBee o, incluso, la interrupción completa

de la red ZigBee mediante ataques cuyo objetivo sea la saturación o desbordamiento de los recursos de la red.

Se ha intentado provocar una denegación de servicio en el nodo coordinador mediante el siguiente ataque:

1. **Configuración del enlace**: no ha sido necesaria una configuración especial de los dispositivos XBee.

2. **Objetivo**: se ha hecho uso de la herramienta "zbassocflood" de Killerbee para enviar masivamente solicitudes de unión a la red al nodo coordinado y provocar un mal funcionamiento de ésta.

3. **Resultado esperado**: se espera poder interrumpir el funcionamiento normal de la red ZigBee.

4. **Resultado obtenido**: no se ha podido afectar el normal funcionamiento del nodo coordinador y la red no ha sufrido ningún tipo de incidente (ver sección 4.3).

5. **Consecuencias**: no se han producido incidencias en el desempeño de la red.

Como se comenta en el punto anterior, con el hardware disponible no ha sido posible la inutilización de ninguno de los dispositivos objetivo, ya que la tasa de envío no llegaba a superar el límite de procesamiento de estos.

A modo documental, y con la intención de que pueda servir para trabajos futuros, se indicarán una serie de situaciones que podrían provocar una denegación de servicio de un nodo de la red ZigBee e, incluso, la inutilización completa de la red, utilizando las herramientas software y hardware suficientes que ayuden a conseguirlo:

- Envío de paquetes de datos con un número de secuencia elevado (tamaño de un byte, máximo valor es 254), de manera que se busque el desbordamiento y reseteo de éste. En este escenario, se buscará comprobar la existencia de mecanismos adecuados que gestionen estas tipo de situaciones, que sean capaces de identificar cuándo se alcanza el valor máximo y reestablecer e inicializar el contador sin que afecte al correcto desempeño de la red.

- Realización de ataques de fuzzing [42], enviando multitud de datos inválidos o inesperados a cada uno de los dispositivos y comprobar cómo responden a ellos. El objetivo principal es la monitorización de situaciones excepcionales que puedan provocarse al inyectar miles de paquetes por segundo con valores no controlados, lo que podría llegar a provocar caídas de nodos de la red, aserciones de código erróneas o encontrar potenciales filtraciones de memoria, que, finalmente, lleven al dispositivo a un estado no controlado.

- Envío de multitud de peticiones para unirse a la red y comprobar la respuesta de nodos coordinadores. Con este tipo de ataque se perseguirá llevar a los nodos coordinadores a una situación límite tanto de procesamiento como de recursos de memoria, en la que se pueda llegar a saturar y dejar la red con los nodos principales fuera de servicio..

3.4.4 Ataques físicos (*Physical Attacks*)

En el presente trabajo, dada la particularidad del entorno de pruebas planteado, este tipo de ataques han sido realizados de forma superflua, debido a que para su correcta realización se requieren herramientas software y hardware más avanzadas y específicas de las que se disponía. No obstante, y en la medida de lo posible, se detallarán las pruebas realizadas y los resultados obtenidos, señalando su posible resultado en caso de haber dispuesto de un material más apropiado.

Los ataques físicos en los dispositivos ZigBee se enfocan, principalmente, en dos objetivos principales:

1. **Extracción de información confidencial.**

Mediante un acceso físico al dispositivo, podrían llevarse a cabo la extracción de información protegida o instalación de puertas traseras que permitan una posterior explotación. Para ello, se debe realizar una extracción del firmware para su análisis y modificación.

Como se ha mencionado en la sección *2.4.5.3 Claves de Seguridad*, la clave de enlace de un dispositivo ZigBee se pre-configura por el fabricante durante el proceso de fabricación y configuración del mismo. Esta clave se almacena en el firmware, de manera que, si no se protege adecuadamente, podría ser accesible a un ataque físico al mismo.

Con un adecuado equipamiento, la extracción del firmware de uno de estos dispositivos puede ser relativamente fácil de realizar [44][45]. Una vez extraído, se pueden utilizar herramientas como la utilidad “strings” o “binwalk”, para, por ejemplo, buscar palabras dentro del firmware y secciones de datos que puedan llevar a extraer la clave de cifrado flasheada en el dispositivo. Además, una de las herramientas del framework utilizado Killerbee se enfoca exactamente en esto mismo, la búsqueda de la clave a partir de una captura de código cifrado o “dumpeo” de memoria legítima de un dispositivo IEEE 802.15.4 / ZigBee [29].

2. **Ataques de canal lateral (*side-channel*).**

En este tipo de ataques se persigue la extracción de información protegida del dispositivo estudiando y analizando la implementación física del sistema. Algunos tipos son [43]

   - Ataque de caché, basados en la capacidad del atacante para monitorizar la cache de la víctima en un sistema físico compartido.
   - Ataques de monitorización de consumo energético, mediante el análisis de la variación en el consumo de energía del hardware durante los cálculos.
   - Ataques electromagnéticos, basados en la fuga de radiación electromagnética, pudiendo utilizarse, por ejemplo, para deducir claves criptográficas.

Este tipo de ataques requieren de un equipamiento específico y un esfuerzo en términos temporales que superan los disponibles para la realización del presente trabajo, por lo que no se han podido llevar a cabo. No obstante, sí que se ha podido experimentar y analizar ciertos comportamientos en los dispositivos ZigBee analizados y sacar las siguientes conclusiones:

- La distancia existente entre los dispositivos XBee influía en la comunicación entre ellos. Cuando esta distancia era muy cercana o muy lejana, se han experimentado pérdidas de paquetes entre ambos nodos. Ha sido especialmente sorprendente la situación en la que ambos dispositivos se encontraban prácticamente juntos y la tasa de perdida de mensajes podía ser de 10 %, aproximadamente.

- Según el canal de comunicación utilizado, existía también una pérdida o demora en la entrega de paquetes. Esta ha sido una de las razones por las que se ha utilizado el canal 25 para las pruebas realizadas, debido a que no existe un solapamiento con otras tecnologías como Wifi que, en redes domésticas como en este caso, puedan llegar a interferir e influir en los resultados obtenidos. En este sentido, un posible atacante podría analizar el canal de comunicaciones utilizado por los dispositivos de una red ZigBee e intentar inyectar ruido e interferencias que provoquen un mal funcionamiento de ésta.

3.4.5 Contramedidas a los ataques planteados

Una vez realizado el estudio de las posibles vulnerabilidades que pueden encontrarse en dispositivos ZigBee y los ataques que pueden ser llevados a cabo para aprovecharse de ellas, se señalarán una serie de contramedidas que permitan servir de referencia a la hora de una implementación segura del protocolo:

✔ Ataques de sniffing

Para evitar que un posible atacante pueda extraer información confidencial o atentar contra la integridad de los datos transportados a través de redes IEEE 802.15.4 / ZigBee a partir de la captura de tráfico, la principal contramedida a utilizar es el **cifrado de las comunicaciones**. Este cifrado debe ser implementado utilizando algoritmos y claves lo suficientemente robustos para evitar un descifrado no sólo hoy día, sino en un futuro no muy lejano. El uso de AES y una clave de 128 bits es una medida adecuada para el uso actual de la tecnología. No obstante, en el futuro, y con la inminente llegada de la computación cuántica, esta longitud de clave puede resultar insuficiente.

En este sentido, y obviando la obsolescencia temporal de la seguridad, para una correcta configuración e implementación del cifrado en las comunicaciones y evitar este tipo de ataques, se deben tener en cuenta las siguientes consideraciones:

- La clave de enlace o transporte debe pre-configurarse en los dispositivos por el fabricante usando algún mecanismo fuera de línea (no conectado).

- Proteger la clave de enlace dentro del dispositivo mediante, por ejemplo, el cifrado del firmware.

- No enviar la clave de red en texto plano bajo ningún concepto. Si un dispositivo sin clave de enlace intenta unirse a la red ZigBee, desautorizar su unión.

✔ Ataques de repetición

Para evitar este que este tipo de ataques sean efectivos en redes IEEE 802.15.4 / ZigBee, es necesario que se implementen algunas de las siguientes contramedidas:

- Implementar mecanismos de validación del número contador de secuencia que eviten la recepción y procesamiento de paquetes repetidos, así como una marca de tiempo que sirva de referencia para evitar procesar este tipo de mensajes en un periodo de tiempo posterior a éste (teniendo en cuenta la posible latencia de la red y procesamiento del dispositivo receptor).

- Aparte de los mecanismos de validación existentes en el protocolo, diseñar un esquema de validación y comprobación de duplicados a nivel de aplicación, de forma que se asegure la integridad de la información recibida y no se atente contra el no repudio de las comunicaciones.

- Establecer un periodo breve de validez del mensaje enviado a través de redes LR-WPAN. Dada la aplicación de este tipo de redes y la cercanía de sus dispositivos, tan sólo se tendrían que considerar posibles valores de latencia de red y procesamiento por parte del receptor. Además, la información enviada suelen ser de tamaño reducido, por lo que establecer un periodo de validez excesivo puede llevar a aumentar la superficie de ataques contra este tipo de redes.

✔ Ataques de denegación de servicio

Los ataques DoS en redes ZigBee pueden llegar a dejar inutilizable la red por completo. En entornos domésticos, dependiendo del tipo de dispositivos utilizados, se podrían bloquear la apertura y cierre de puertas y ventanas, la inutilización de sistemas de ventilación y calefacción, y un largo etcétera de posibilidades. Si esta misma situación se extrapola a sistemas de monitorización y control industrial o sistemas médicos, se pueden deducir las graves consecuencias que podrían acarrear.

En este sentido, para reducir el impacto de ataques cuyo objetivo sea este, se pueden implementar las siguientes contramedidas:

- Permitir la conexión únicamente a dispositivos autorizados a unirse a este tipo de redes. Debe descartarse directamente cualquier tráfico procedente de un dispositivo no autorizado, de manera que no se pierdan recursos en procesarlo.

- Limitar el número de peticiones de acceso a la red, estableciendo un límite máximo de intentos consecutivos erróneos. Si el dispositivo no cumple con los requerimientos necesarios para unirse a la red, debe rechazarse cualquier intento de unirse a la red ZigBee lo antes posible.

- Implementar mecanismos de restablecimiento seguro de la red en caso de fallo o condición no deseada, de forma que, de nuevo, únicamente los dispositivos autorizados puedan unirse a ella.

- Utilización de una política de seguridad restrictiva, en la que se deniegue el acceso a todos los dispositivos que no estén autorizados explícitamente.

Pueden definirse listas blancas con la información de los dispositivos que tendrán permitido el acceso.

✔ Ataques físicos

En este tipo de ataques, podría hacerse la suposición de que uno o varios dispositivos han podido ser accedido físicamente por un atacante, de forma que se deduzcan qué medidas podrían implementarse en dichos dispositivos para proteger su integridad y, consecuentemente, la red 801.15.4 / ZigBee en general. A continuación se señalan algunas contramedidas que pueden ser empleadas para evitar o limitar este tipo de ataques:

- Proteger firmware del dispositivo mediante cifrado. De esta forma, ante una posible extracción del mismo, la información protegida, como claves de cifrado, estará protegida y no podrá ser extraída de forma trivial.

- Debe configurarse adecuadamente un arranque seguro del dispositivo, donde se haga una comprobación de la integridad del firmware por parte del bootloader y evitar arrancar si se comprueba una modificación en los datos.

- Implementación de mecanismos como la ceroización [39] que, ante la detección de una apertura del dispositivo o acceso indebido, elimine la información sensible de la memoria y evite su posible extracción.

- Poner en práctica mecanismos de contingencia en situaciones límite del sistema que aseguren la integridad de los datos transportados en situaciones donde se pueda estar recibiendo un ataque de denegación de servicio mediante la inyección de ruido en el canal.

4 Detalle de las pruebas realizadas

4.1 Sniffing

✔ **Comunicación no cifrada.**

Utilizando el programa XCTU, se ha procedido a la configuración de los módulos XBee en modo Transparente, donde uno de ellos actuará como Coordinador y otro como Enrutador. El Enrutador recogerá el mensaje "*HelloMiguel*" inyectado en su interfaz serial y lo enviará al Coordinador, el cual lo recibirá y mostrará a su vez por su interfaz serial.

Un tercer equipo con el Api-Mote conectado permanecerá a la escucha y tratará de capturar el tráfico entre ambos módulos.

A continuación se muestran capturas de la comunicación entre ambos nodos. En este caso, se ha programado el envío repetido cada 2 segundos del mensaje "*HelloMiguel*" desde el nodo Enrutador al Coordinador:

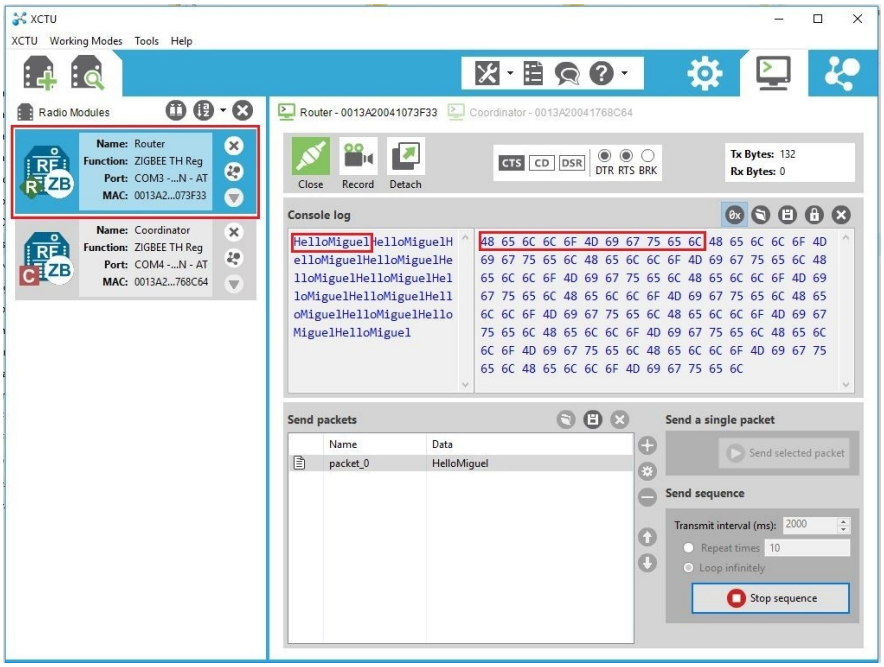


Figura 29. Configuración enlace nodo Enrutador

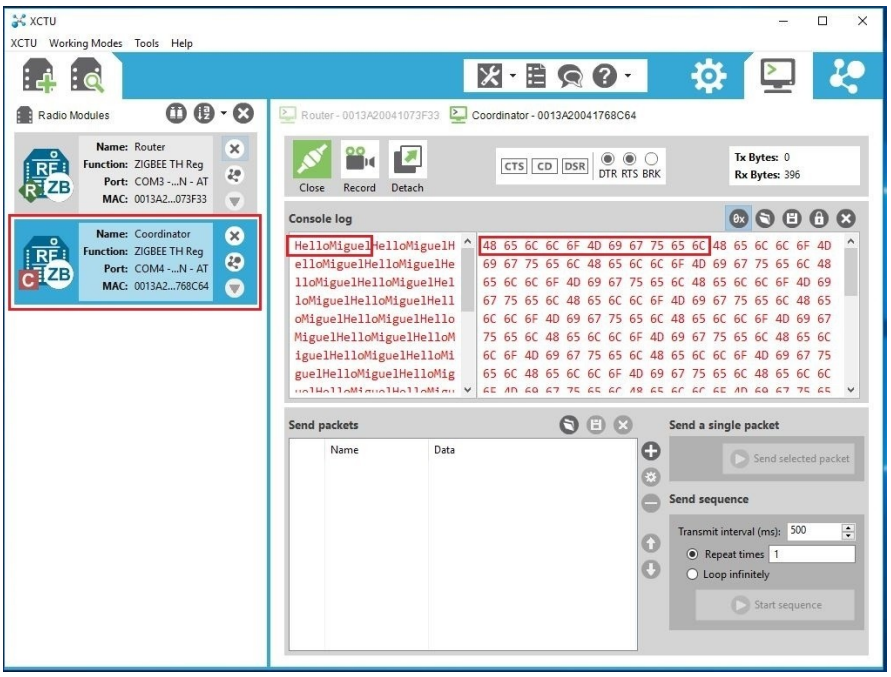


Figura 30. Recepción del mensaje en el Coordinador

Como puede apreciarse, el mensaje "*HelloMiguel*" inyectado en la interfaz serial al que se conecta el nodo Router es recogido por éste y enviado al Coordinador, el cual lo recibe y lo muestra por su interfaz serial.

Por su parte, el nodo Atacante ha estado capturando este envío de información entre los nodos XBee, tal y como se aprecia en la siguiente imagen:

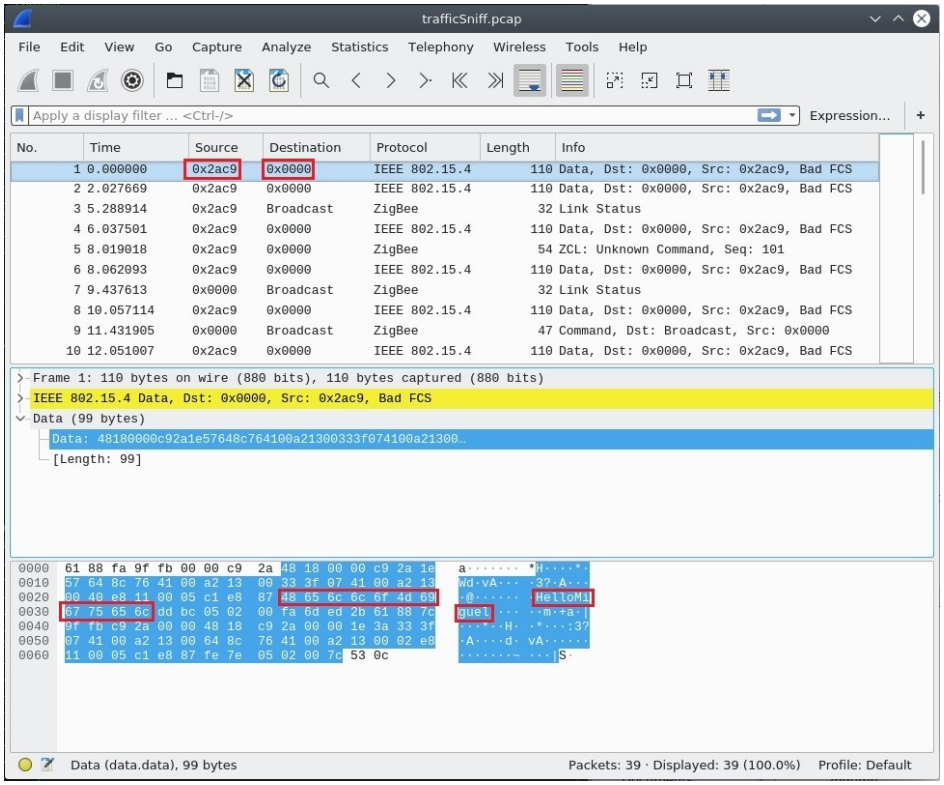


Figura 31. Captura de tráfico en claro desde el nodo Atacante

Por lo tanto, tal y como se aprecia en la imagen, se ha podido capturar información transmitida entre ambos nodos y, más concretamente, la información enviada desde el nodo Enrutador (dirección de origen 0x2ac9) al Coordinador (0x0000, por defecto para comunicaciones con el coordinador), extrayendo el mensaje en claro enviado "*HelloMiguel*".

Así pues, vemos que es posible vulnerar la confidencialidad de las comunicaciones en una red ZigBee que no implemente cifrado.

✔ **Comunicación cifrada.**

A continuación se muestran capturas de configuración de los nodos Coordinador y Enrutador, así como la transmisión del mensaje "*EncryptedHelloMiguel*" desde el nodo Enrutador y su posterior recepción en el Coordinador:

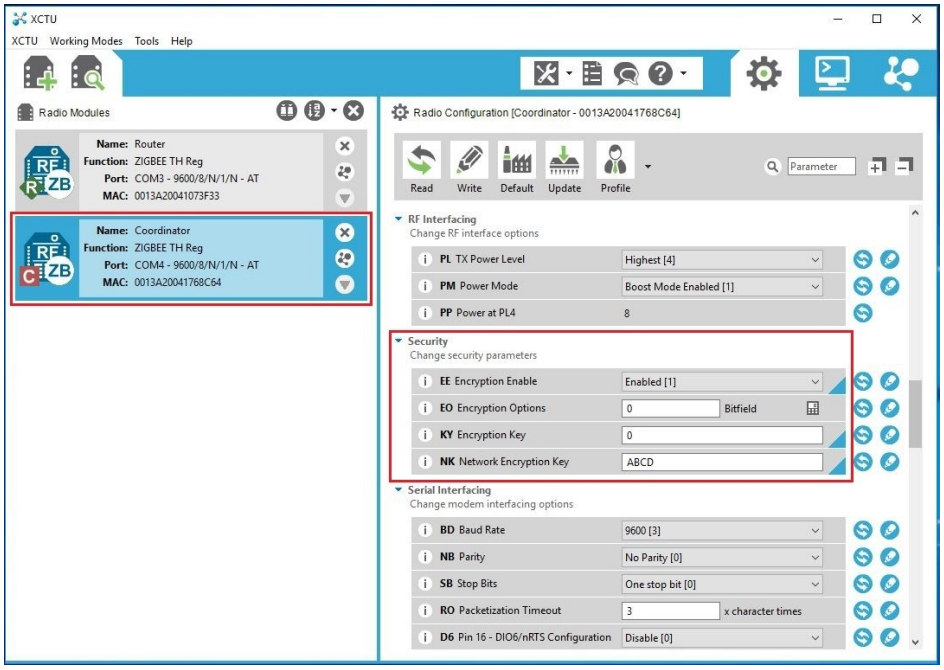


Figura 32. Configuración de seguridad en el nodo Coordinador

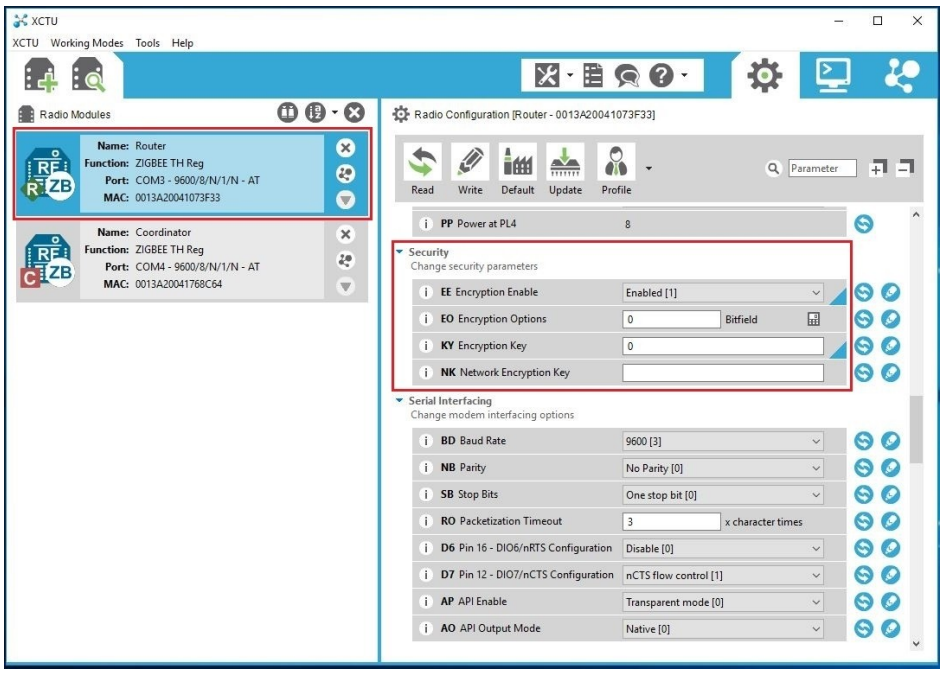


Figura 33. Configuración de seguridad en el nodo Enrutador

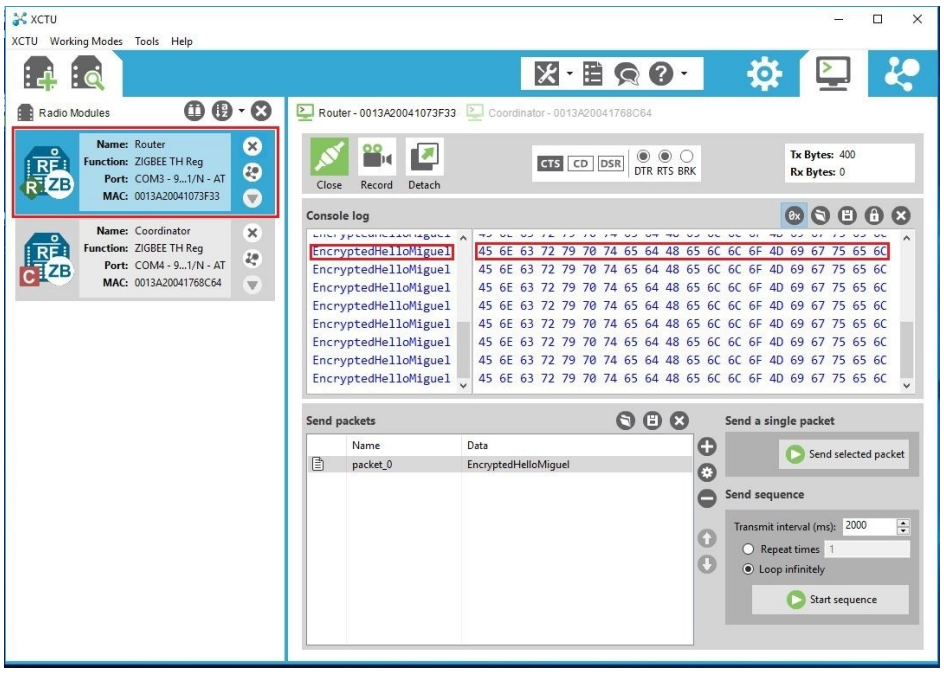


Figura 34. Envío del mensaje "EncryptedHelloMiguel" en el nodo Enrutador

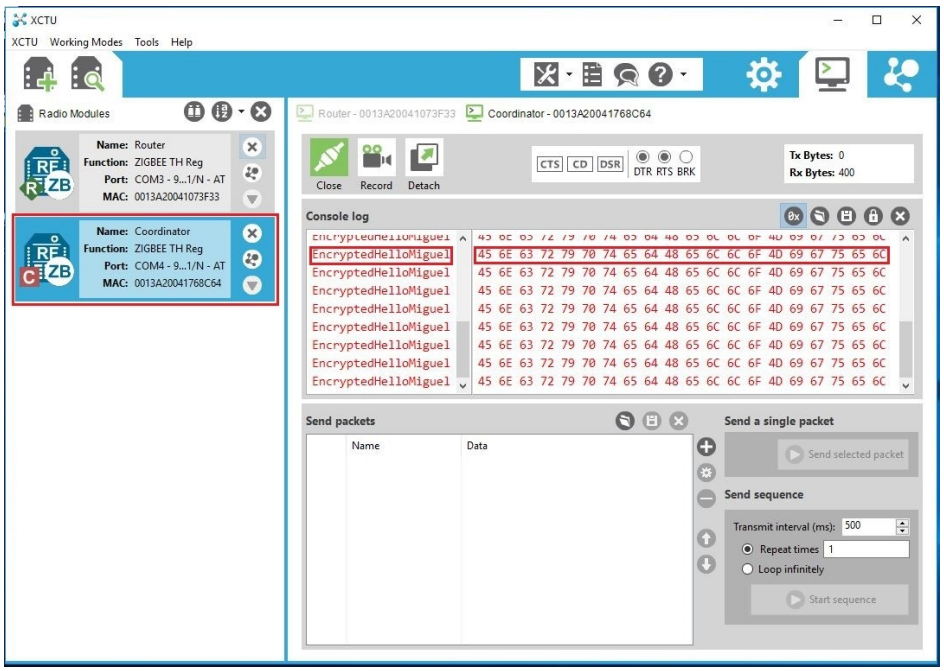


Figura 35. Recepción del mensaje en el nodo Coordinador

Previamente, hemos lanzado el programa "*zbwireshark*" en el nodo Atacante para capturar el tráfico e intentar obtener el mensaje enviado entre los dispositivos de la red ZigBee, indicando la interfaz por la que se encuentra conectado el Api-Mote (*/dev/ttyUSB0*), el canal (*25*) y el número de paquetes a capturar (*200*).

```
[root@localhost-live Attify-Zigbee-Framework]# zbwireshark -i /dev/ttyUSB0 -c 25 -n 200
zbwireshark: listening on '/dev/ttyUSB0', channel 25, page 0 (2475.0 MHz), link-type DLT_IEEE802_15_4, ca
pture size 127 bytes
```

Figura 36: Captura de tráfico en el nodo atacante con zbwireshark

A continuación se muestra el tráfico que hemos podido capturar en dicho equipo:

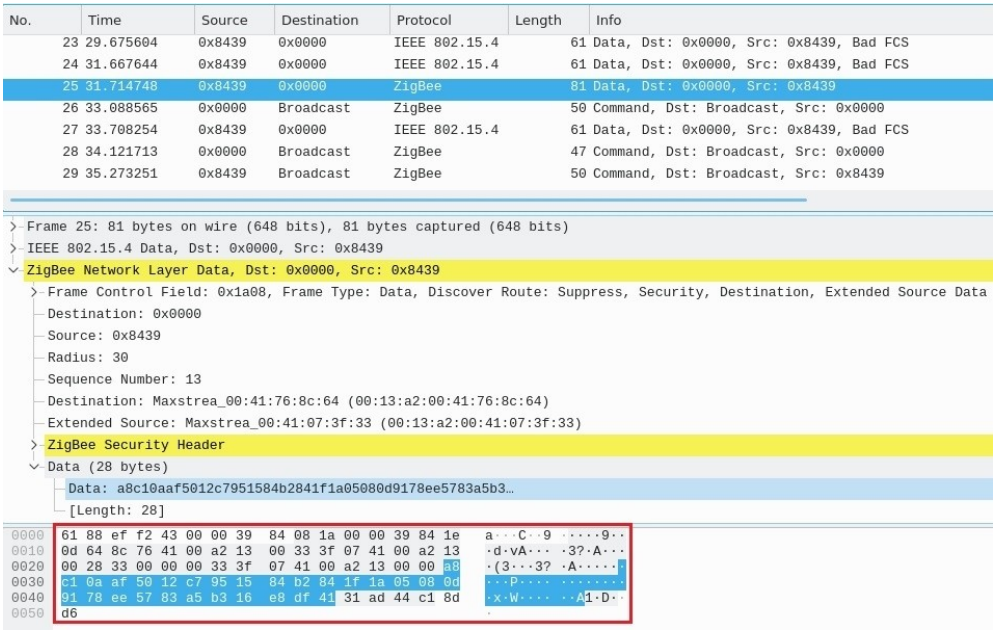


Figura 37: Captura de tráfico cifrado desde el nodo Atacante

Tal y como se aprecia, la información enviada entre los nodos Enrutador y Coordinador se encuentra cifrada, no siendo posible la extracción del mensaje enviado entre ambos.

A) Supuesto 1: Clave de Transporte no configurada.

En la siguiente imagen se aprecia la configuración del nodo coordinador. En ella puede verse la clave de cifrado utilizada:

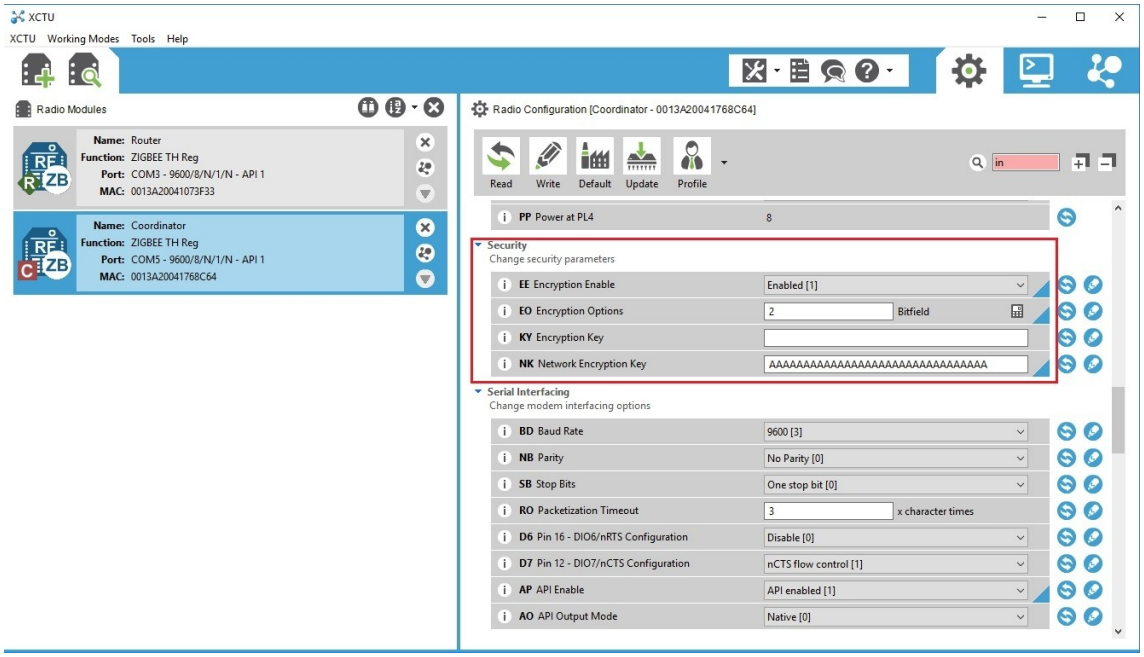


Figura 38: Configuración Clave de Red (sin Clave de Transporte)

Tras lanzar la herramienta *zbwireshark* en el nodo atacante, se ha podido identificar y obtener la clave de red sin ningún problema:

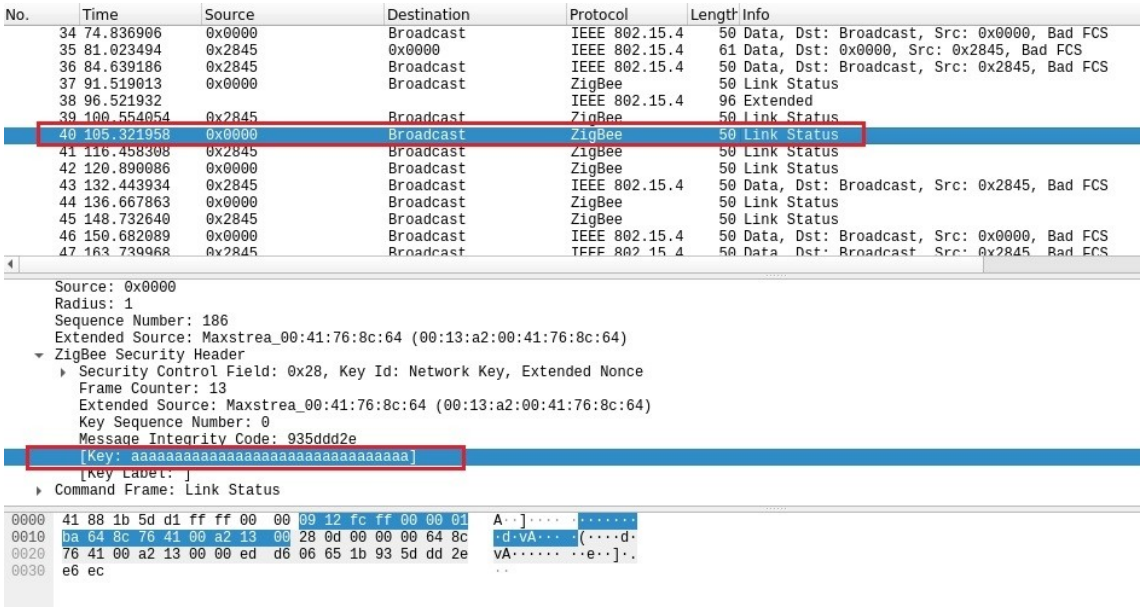


Figura 39: Captura de clave de red en el nodo Atacante

Por lo tanto, se pone de manifiesto la inseguridad existente en la propagación de la clave de red ante la unión de un nodo que no disponga de una clave de enlace pre-configurada, llegando a poder comprometer la confidencialidad de las comunicaciones de toda la red.

B) Supuesto 2: Clave de Transporte configurada.

En este caso, el tráfico capturado está cifrado, por lo que no se puede obtener la clave de red de forma trivial

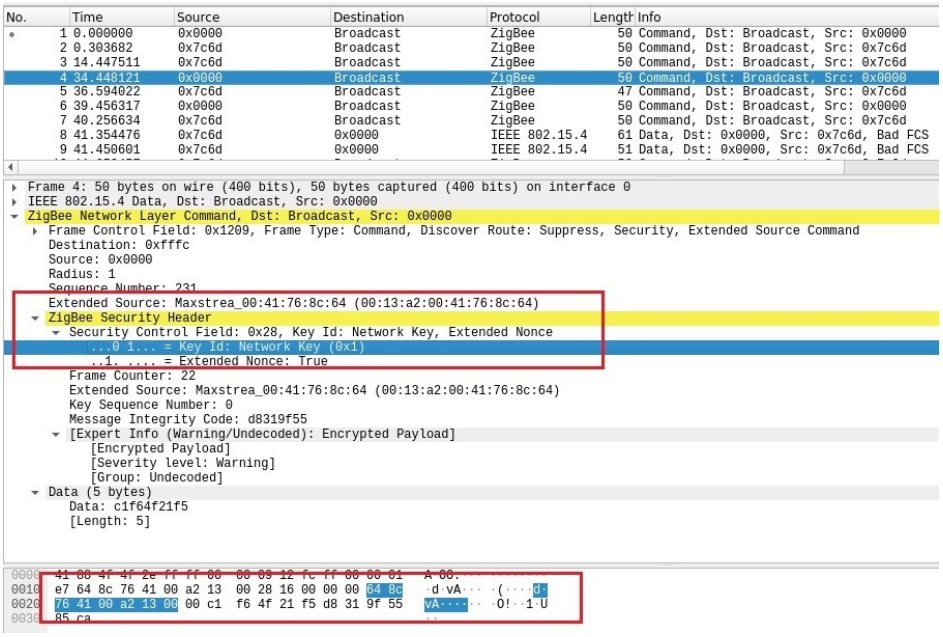


Figura 40: Intercambio de clave de red cifrada

No obstante, como se ha comentado anteriormente, para favorecer la interoperabilidad entre los dispositivos de distintos fabricantes, y tal y como se recoge en la definición del estándar, algunos productos son pre-configurados con una clave de enlace predeterminada bien conocida, siendo la codificación en hexadecimal de **ZigbeeAlliance09** (0x5A 0x69 0x67 0x42 0x65 0x65 0x41 0x6C 0x6C 0x69 0x61 0x6E 0x63 0x65 0x30 0x39)**.** Por lo tanto, configurando Wireshark con esta clave (en "reverse byte order") se puede obtener la clave de red en claro:

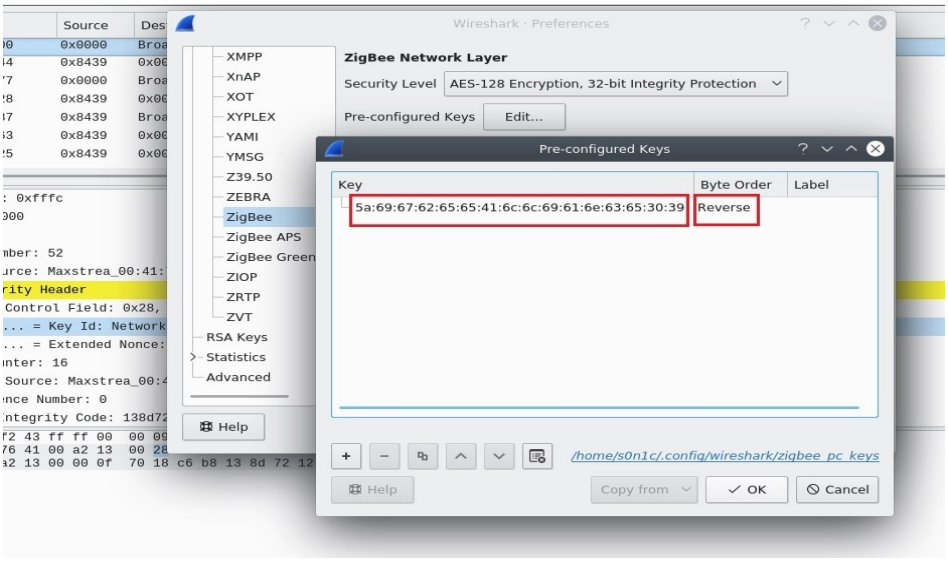


Figura 41: Configuración Clave de Enlace "ZigbeeAlliance09" en Wireshark

4.2 Ataques de Repetición (Replay attacks)

- ✔ **Suplantación de identidad.**

Para poder comprobar este funcionamiento del protocolo ZigBee, configuraremos los nodos XBee coordinador y enrutador en modo API, enviando un frame de tipo "*0x10 - Transmit Request*" desde el enrutador con el mensaje "*OpenTheDoor*". Previamente hemos puesto a la escucha el Api-Mote, de manera que pueda capturar el tráfico enviado entre los dos XBee.

Una vez capturado el intercambio de información, tratamos de replicar el tráfico y analizar el comportamiento en el nodo Coordinador:

```
[root@localhost-live tools]# zbreplay -f 25 -r replayOpenDoor.pcap -i /dev/ttyUSB0 -s 0.1
zbreplay: retransmitting frames from 'replayOpenDoor.pcap' on interface '/dev/ttyUSB0' with a delay of 0.1 seconds.
47 packets transmitted
[root@localhost-live tools]#
```

Figura 42: Ejecución de Ataque de Repetición en el nodo Atacante

Tal y como se puede comprobar a continuación, replicando el tráfico capturado, hemos sido capaces de hacer llegar al nodo Coordinador el mensaje "*OpenTheDoor*", habiendo suplantado al legítimo origen (ver direcciones de origen):

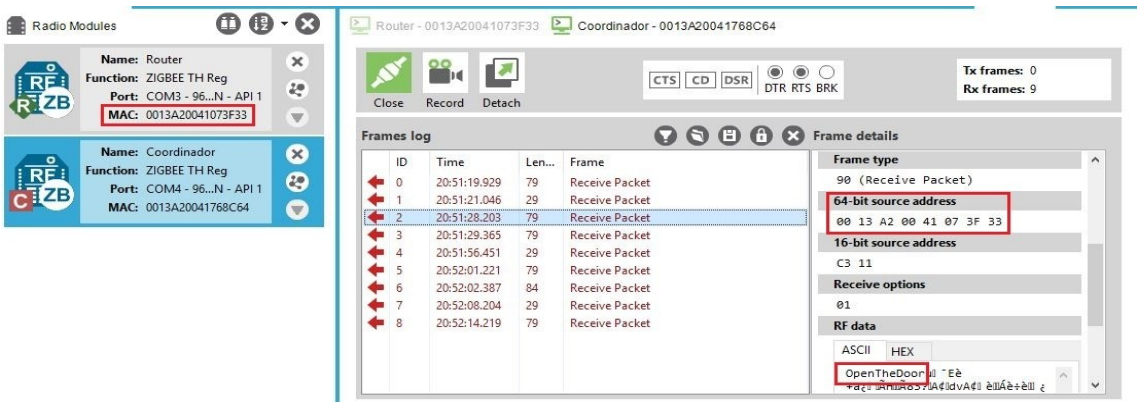


Figura 43: Suplantación de identidad mediante Ataque de Repetición

✔ **Denegación de Servicio.**

Para comprobar si este ataque podría se de aplicación en el entorno de pruebas planteado, hemos configurado el nodo Enrutador para que envíe indefinidamente un frame de tipo "*0x10 - Transmit Request*" cada mili-segundo. Hemos puesto a la escucha el nodo Atacante y, posteriormente, utilizando la herramienta "*zbreplay*" hemos intentado realizar un ataque de repetición, re-enviando el tráfico capturado (simultáneamente con el tráfico enviado por el nodo Enrutador):

```
[root@localhost-live tools]# ./zbreplay -f 25 -r dosToCoordinator.pcap -i /dev/ttyUSB0 -s 0.1
zbreplay: retransmitting frames from 'dosToCoordinator.pcap' on interface '/dev/ttyUSB0' with a delay of 0.1 seconds.
917 packets transmitted
[root@localhost-live tools]#
```

Figura 44: Ataque de repetición para conseguir denegación de servicio

No obstante, no hemos conseguido producir un comportamiento extraño en el nodo Coordinador, estando este operativo en todo momento y pudiendo, incluso, enviar mensajes al nodo Enrutador sin mayor problema. Seguramente, con algún que otro Api-Mote inyectando el mismo tráfico, se podría haber conseguido provocar un mal funcionamiento del nodo objetivo.

4.3 Denegación de Servicio (DoS, *Denial-of-Service*)

Mediante la herramienta "*zbassocflood*" el framework Killerbee, se ha intentado saturar al nodo coordinador mediante el envío de paquetes de asociación a la red.

```
[root@localhost-live tools]# zbassocflood -p 0x4444 -c 25 -s 0.1
zbassocflood: Transmitting and receiving on interface '/dev/ttyUSB0'
```

Figura 45: Ataque DoS con peticiones de asociación

Como se comenta en el punto anterior, con el hardware disponible no ha sido posible la inutilización de ninguno de los dispositivos objetivo, ya que la tasa de envío no llegaba a superar el límite de procesamiento de estos.

5. Conclusiones y líneas futuras

5.1 Conclusiones

Las vulnerabilidades trabajadas aquí son el resultado de errores de diseño o falta de implementacíión de la seguridad desde el diseño de dispositivos ZigBee. Los dispositivos XBee utilizados permiten simular la mayor parte de situaciones y entornos en los que día a día funcionan e interactúan miles de dispositivos de este protocolo. Además, aparte de los ataques remotos que puedan sufrir este tipo de dispositivos, cabe mencionar la posibilidad de

Por lo tanto, teniendo en cuenta el trabajo realizado y los resultados finales obtenidos de las pruebas realizadas, se pueden extraer las siguientes conclusiones:

- Los mecanismos de seguridad proporcionados por el estándar ZigBee se puede considerar adecuados y robustos, ya que utiliza el reconocido algoritmo AES para el cifrado y autenticación de los datos. No obstante, esta seguridad depende del secreto de las claves de cifrado, así como de una inicialización y distribución seguras de dichas claves. Dado que las claves de enlace (empleadas por la industria) con las que se cifra la clave de red son bien conocidas o han podido ser filtradas [38], la seguridad efectiva equivale a transportar las claves de red sin cifrar.

- Se ha podido verificar que se produce una vulneración de la confidencialidad de los datos transmitidos dentro de una red ZigBee cuando no se usa cifrado para proteger las comunicaciones entre los distintos elementos de la misma. Esto supone una vulneración grave al poder escuchar todo el tráfico circulante, desde comandos de control hasta mensajes de monitorización de nodos.

- Además, se han podido llevar a cabo ataques de repetición en los que se replica un mensaje legítimo enviado por otro nodo, lo que supone una vulnerabilidad grave tanto en la integridad del mensaje (al poder ser suplantado o modificado) como en el aseguramiento del no repudio del emisor, provocando que

- Se ha podido comprobar que, aunque se protejan las comunicaciones entre los distintos nodos con una clave de red, la obtención de ésta es relativamente fácil utilizando las herramientas y dispositivos adecuados. Con una inversión de poco más de cien euros, un atacante podría llegar a comprometer una red Zigbee si el Centro de Confianza está configurado para enviar la clave de red en claro a cualquier nodo que quiera unirse a la red.

- Aunque no se ha podido llegar a provocar una denegación de servicio en los dispositivos del entorno planteado, este tipo de ataque podría ser factible con toda probabilidad utilizando uno o dos dispositivos Api-Mote adicionales para enviar peticiones concurrentemente y provocar un desbordamiento del dispositivo. Por lo tanto, con una inversión reducida, un atacante podría llegar a inutilizar la red Zigbee objetivo y provocar la caída de toda la red. Esto podría suponer, en entornos domésticos, la inutilización de cerraduras, luces y sistemas de alarma. Se puede deducir que, en entornos corporativos e industriales, las consecuencias podría ser de especial gravedad si, por ejemplo, se inutilizan los sistemas de medición de gases en una fábrica, los sistemas de accionamiento de alarmas y fugas, o los sistemas de control del pH de una planta potabilizadora.

- La seguridad del protocolo ZigBee se basa en la asunción de que las claves se almacenan de forma segura: el coordinador se preconfigura con la clave de red y el resto de dispositivos se preconfiguran con la clave de enlace. Si estas claves se almacenan de forma segura, se podría llegar a extraer del firmware dichas claves, llegando a comprometer la red por completo.

Así pues, con este trabajo se intenta poner de manifiesto la importancia que la seguridad debe tener cuando se elige una tecnología de comunicaciones inalámbrica para interconectar cualquier par de dispositivos, y, más aún, cuando estos dispositivos se utilizan en el horgar, recopilando datos e información sensible, así como en entornos industriales, dada su importancia...

5.2 Recomendaciones

Las recomendaciones que se desprenden de la realización del presente trabajo y que pueden ayudar en la correcta implementación del protocolo IEEE 802.15.4 / ZigBee se recogen a continuación:

- Deben establecerse los procedimientos adecuados por parte de las organizaciones en materia de política de seguidad con el objetivo de regular la administración, implementación y operación de las redes ZigBee.
- Cuando sea posible, y siempre que el proveedor ZigBee lo admita, implementar autenticación del nodo de origen que intenta conectarse a una red o envía determinada información.
- Tanto el nodo que actúa como coordinador así como el identificador de Área de Red Personal (PAN) deben ser designados, de forma que no pueda ejercer este rol ningún dispositivo no autorizado para ello ni utilizar un PAN distinto al configurado.
- Las comunicaciones de la infraestructura de una red ZigBee deben estar siempre protegidas mediante una clave de red, la cual debe estar implementada en todos los nodos de esta, de manera que aquellos nodos que no dispongan de ella no puedan ingresar a la red (no se les otorga autorización para funcionar en ella).
- La provisión de las claves de red debe realizarse de forma offline o pre-configurando los dispositivos con dicha clave, de manera que se minimice el vector de exposición ante ataques de sniffing que capturen las comunicaciones en busca de dichas claves. Se debe implementar un mecanismo de renovación de claves que impida la transmisión de estas en claro por la red.
- Utilizar listas de control de acceso (ACL, del inglés *Access Control List*) que sirvan para realizar un flitrado de direcciones de la capa MAC con el objetivo de permitir la adición únicamente de aquellos nodos reconocidos como legítimos para una infraestructura en cuestión.
- Deben pre-configurarse todos los dispositivos de una red ZigBee con la dirección del Centro de Confianza, debido a que es el elemento central de la red ZigBee y el dispositivo en el que todos los demás nodos confían. En todos los nodos a añadir a dicha red, la dirección del TC debe ser la misma.
- Habilitar los mecanismos de seguridad de capa 2 que se admiten en IEEE 802.15.4.

- Implementar mecanismos que eviten la manipulación (anti-tampering) de aquellos ataques hardware que tienen como objetivo acceder a la memoria del dispositivo para extraer las claves de cifrado. Ante la detección de un acceso, un nodo podría eliminar información sensible de la memoria en un proceso que se conoce como ceroización [39].

5.3 Líneas futuras de investigación

A continuación se indican una serie de líneas de investigación que, en base al presente trabajo, podrían desarrollarse en un trabajo futuro:

- Ataques físicos: basándose en la información y técnicas aquí recogidas, se podría llevar a cabo un estudio de la seguridad física de algunos dispositivos comerciales ZigBee, de manera que intente extraerse información protegida en el propio dispositivo contenida en el mismo firmware, como la clave de transporte o enlace utilizada para cifrar el intercambio de la clave de red en la red ZigBee.

- Análisis de comunicaciones en dispositivos comerciales: dado que los dispositivos utilizados en este trabajo son altamente configurables, ya que se orientan al estudio del protocolo, un posible trabajo futuro sería el análisis y estudio del flujo de comunicaciones dentro de una red ZigBee compuesta por dispositivos comerciales existentes para el IoT, de manera que se pueda extraer una visión de la correcta implementación de seguridad por parte de los fabricantes de tales productos.

- Ataques de denegación de servicio distribuidos (DDoS): si se dispone más de un dispositivo Api-Mote, se podrían llegar a realizar ataques de denegación de servicio distribuidos, en los que se pueda paralelizar la inyección de tráfico hacia un determinado objetivo con la intención de provocar un mal funcionamiento o, incluso, inutilizarlo.

- Explotación de dispositivos de la red ZigBee: dado que existen dispositivos, como el Api-Mote, mediante los cuales interactuar con nodos de una red ZigBee, existe la posibilidad de analizar y explotar los servicios que implementan dichos dispositivos, sobre todo en el nodo Coordinador, de manera que pueda llegar a conseguirse una ejecución remota de código [41] que permita llegar a comprometer y controlar toda la red.

6. Glosario

ACL	Access Control List
ADC	Analog to Digial Converter
AES	Advanced Encryption Standard
AF	Application Framework
APDU	Application Protocol Data Units
APL	Application
APS	Application Support sub-layer
APSDE	Application Support Sub-Layer Data Entity
APSME	Application Support Sub-Layer Management Entity
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
COM	Communication port
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CRC	Cyclic Redundancy Checks
DAC	Digital to Analog Converter
DDoS	Distributed Denial of Service
DMA	Direct Memory Access
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
FCS	Frame Check Sequence
FFD	Full-Function Device
FTDI	Future Technology Devices International
GHz	Gigahertz
GTS	Guaranteed Time Slot
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical radio bands
IoT	Internet of Things
IPv6	Internet Protocol version 6
IV	Initialization Vector
LR-WPAN	Low-Rate Wireless Personal Area Network
MAC	Medium Access Control
MCU	Microcontroller Unit
MMO	Matyas-Meyer-Oseas hashing algorithm
NFC	Near Field Communication
NLDE	NWK layer data entity
NLME	NWK layer management entity
NPDU	Network Protocol Data Unit
NWK	Network
OSI	Open System Interconection
PAN	Personal Area Network
PCB	Printed circuit board
PHY	Physical layer
PHR	PHY header
PPDU	PHY protocol data unit
PSDU	PHY service data unit
RAM	Random Access Memory
RF	Radio frequency
RFD	Reduced-Function Device
RFID	Radio Frequency Identification
SMA	SubMiniature version A
SHR	Synchronization header
TC	Trust Center

TCLK	Trust Center Link Key
TFM	Trabajo Final de Máster
UART	Universal Asynchronous Receiver-Transmitter
USB	Universal Serial Bus
VCP	Virtual COM Port
WPAN	Wireless Personal Area Network
ZCL	ZigBee Cluster Library
ZDO	ZigBee Device Objects
ZDP	ZigBee Device Profile

7. Bibliografía

[1] - La Oberta en Abierto. Informática, Multimedia y Telecomunicación.
http://openaccess.uoc.edu/webapps/o2/handle/10609/47922

[2] - Zigbee Alliance, Zigbee Specification. Document 053474r20.
http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf

[3] - Zigbee: Securing the Wireless IoT. Zigbee Allicance
https://www.zigbee.org/download/securingthe-wireless-iot/?wpdmdl=7248

[4] - Xueqi Fan, Fransisca Susan, William Long, Shangyan Li. May 18, 2017. *Security Analysis of Zigbee.* Massachusetts Institute of Technology
https://courses.csail.mit.edu/6.857/2017/project/17.pdf

[5] - XRadosveta Sokullu, Ilker Korkmaz, Orhan Dagdeviren. GTS Attack: An IEEE 802.15.4 MAC Layer Attackin Wireless Sensor Networks. Pennsylvania State University.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.685.449&rep=rep1&type=pdf

[6] - Hipertextual. *Internet of things.*
https://hipertextual.com/2015/06/internet-of-things

[7] - Wikipedia. I*nternet de las Cosas.*
https://es.wikipedia.org/wiki/Internet_de_las_cosas

[8] - Internet Society. *The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World*.

[9] - Wikipedia. *Ley de Moore*.
https://es.wikipedia.org/wiki/Ley_de_Moore

[10] - Wikipedia. *IEEE 802.15.4*.
https://es.wikipedia.org/wiki/IEEE_802.15.4

[11] - Wikipedia. Zigbee.
https://es.wikipedia.org/wiki/Zigbee

[12] - Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate. A Developing Standard for Low-Rate, 2002.

[13] - IEEE Computer Society. IEEE Standard for Low-Rate Wireless Networks.
https://www.silabs.com/content/usergenerated/asi/cloud/attachments/siliconlabs/en/community/wireless/proprietary/forum/jcr:content/content/primary/qna/802_15_4_promiscuous-tbzR/hivukadin_vukadi-iTXQ/802.15.4-2015.pdf

[14] - Libelium World. 802.15.4 vs ZigBee.
http://www.libelium.com/802-15-4-vs-zigbee/

[15] - Libelium World. Security in 802.15.4 and ZigBee networks.
http://www.libelium.com/security-802-15-4-zigbee

[16] - Digi. Zigbee stack layers.
https://www.digi.com/resources/documentation/Digidocs/90002002/Content/Reference/r_zb_stack.htm

[17] – RF Wireless World. Zgbee vs Zigbee PRO-difference between zigbee and zigbee PRO.
http://www.rfwireless-world.com/Terminology/zigbee-vs-zigbee-PRO.html

[18] - Wireless Mesh Networking ZigBee vs. DigiMesh.

https://www.digi.com

[19] - About ZigBee Protocol.
https://sites.google.com/site/xbeetutorial/xbee-introduction/zigbee.

[20] - Zigbee 3.0 Task Force,zigbee: Securing the Wireless IoT (2017)

[21] - ZigBee 3.0 Devices. User Guide.
https://www.nxp.com/docs/en/user-guide/JN-UG-3114.pdf

[22] - Zigbee Alliance. Zigbee Certified Products.
https://www.zigbee.org/zigbee-products-2/

[23] - Zigbee Alliance. G4-MG-SE-GM-V2 Gas Meter.
https://www.zigbee.org/zigbee-products-2/#zigbeecertifiedproducts/
productdetails3/5ced196d0e7aff00060ca0e6/

[24] - Zigbee Alliance. Innr RGBW Retrofit Lights.
https://www.zigbee.org/zigbee-products-2/#zigbeecertifiedproducts/
productdetails3/5cc056cd812460322ad7ea1d/

[25] - Zigbee Alliance. Echo Plus (2ª Gen).
https://www.zigbee.org/zigbee-products-2/#zigbeecertifiedproducts/
productdetails3/5ccb1f38eae66400069573f0/

[26] - Adafruit. XBee Module - ZB Series S2C.
https://www.adafruit.com/product/968

[27] - Waveshare. XBee USB Adapter.
https://www.waveshare.com/xbee-usb-adapter.htm

[28] - APImote.
http://apimote.com/

[29] - KillerBee. Github.
https://github.com/riverloopsec/killerbee

[30] - Api-Do Project. Api-Mote Base R4.0 BETA.
https://github.com/riverloopsec/apimote/blob/master/docs/apimote_overview_v4beta.pdf

[31] - XCTU. Next Generation Configuration Platform for XBee/RF Solutions.
https://www.digi.com/products/iot-platform/xctu

[32] - VCP Drivers. FTDI Chip.
https://www.ftdichip.com/Drivers/VCP.htm

[33] - Wireshark.
https://www.wireshark.org/

[34] - Digi. Operating modes.
https://www.digi.com/resources/documentation/Digidocs/90001942-13/concepts/
c_transparent_and_api_mode.htm?TocPath=How%20XBee%20devices%20work%7CSerial
%20communication%7C_____1

[35] - Wikipedia. *Sniffing attacks*.
https://en.wikipedia.org/wiki/Sniffing_attack

[36] - Wikipedia. Ataque de Replay.
https://es.wikipedia.org/wiki/Ataque_de_REPLAY

[37] - Wikipedia. Ataque de denegación de servicio.
https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

[38] - Tobias Zillner. Zigbee Exploited.
https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

[39] - Wikipedia. Zeroisation.
https://en.wikipedia.org/wiki/Zeroisation

[40] - Github. Attify ZigBee Framework.
https://github.com/attify/Attify-Zigbee-Framework

[41] - Wikipedia. Arbitrary code execution
https://en.wikipedia.org/wiki/Arbitrary_code_execution

[42] - Wikipedia. Fuzzing.
https://www.owasp.org/index.php/Fuzzing

[43] - Wikipedia. Ataque de canal lateral.
https://es.wikipedia.org/wiki/Ataque_de_canal_lateral

[44] - Dennis Giese. Having fun with IoT: Reverse Engineering and Hacking of Xiaomi IoT Devices. DEFCON 26.
https://dgiese.scripts.mit.edu/talks/DEFCON26/DEFCON26-Having_fun_with_IoT-Xiaomi.pdf

[45] - Uri Shaked. Inside The Bulb: Adventures in Reverse Engineering Smart Bulb Firmware.
https://medium.com/@urish/inside-the-bulb-adventures-in-reverse-engineering-smart-bulb-firmware-1b81ce2694a6

[46] - Wikipedia. Z-Wave.
https://es.wikipedia.org/wiki/Z-Wave

[47] - FTDI Chip. D2XX Drivers.
https://www.ftdichip.com/Drivers/CDM/CDM%20v2.12.28%20WHQL%20Certified.zip