Implementación de niveles de ciberseguridad óptimos a los protocolos Z-Wave y ZigBee para su uso en medidores inteligentes

Carlos Araya Guzmán, Gabriel García Calvo, Maximiliano Ortiz Gómez

Prof. Randall Barnett Villalobos

Escuela de Ingeniería
Universidad Latinoamericana de Ciencia y Tecnología,
ULACIT, Urbanización Tournón, 10235-1000
San José, Costa Rica
[carayag960, ggarciac606, mortizg051]@ulacit.ac.cr http://www.ulacit.ac.cr

Resumen Los medidores inteligentes ofrecen ventajas como información de consumo, ahorro de energía y costos y conexión con la HAN. Con estas funcionalidades, junto con domótica, se puede controlar el encendido, la temperatura, humedad, iluminación u otros detalles; sin embargo, se requiere de protocolos para la comunicación. Los principales, Z-Wave y Zigbee, usados en redes inalámbricas, son vulnerables en materia de ciberseguridad, considerando *hacking* de dispositivos, manejo de datos, cantidad de nodos y sus enlaces. Por ello, se dio el análisis de revisiones bibliográficas de las características de estos protocolos, las capas que los componen, su cifrado, tipos de ataques, mejores prácticas, entre otros aspectos. Se establece, a partir de lo todo lo anterior, la necesidad de contar con más documentación técnica asociada a Z-Wave, utilizar la encriptación y tener dispositivos preconfigurados para gestionar claves, y conocer de previo, si la red es más compleja, para lo cual, Zigbee será la opción.

Keywords: Medidor inteligente, Red inteligente, AMI, seguridad, autoconsumo, vulnerabilidades, electricidad, ZigBee, Z-Wave, SCADA.

1. Introducción

En nuestros días, la tecnología nos permite utilizar novedades en el hogar y en la industria. Es posible realizar inversiones a nivel nacional, para dotar de inteligencia a los lugares antes mencionados, con el objetivo de aprovechar la infraestructura y a las fuentes alternativas de energía. Centrándose en este último aspecto, las inversiones en domótica deben contribuir a la automatización de procesos cotidianos, como lo son el uso racional de la luz o de aparatos electrónicos, además de la gestión de servicios de seguridad y comunicación. Esto se puede aprovechar a través del uso de redes HAN, como elemento central en los hogares. Una tecnología de *hardware,* denominada medidores

inteligentes[1], permite administrar las ventajas que ofrece la domótica de forma centralizada y automatizada.

Toda red se vale de protocolos para lograr una efectiva comunicación entre los nodos que la conforman, de ahí su importancia, y según el servicio o servicios que ofrezca la red, se puede disponer de diferentes protocolos.

Dentro de las redes, existe una en particular denominada HAN o *Home Area Network*, la cual es conocida en español como una Red Inteligente para el Hogar, siendo los hogares, por lo tanto, su campo de acción.

En este trabajo, se consideran los protocolos Zigbee y Z-Wave[2], ambos son protocolos utilizados en redes HAN y se detallará más adelante los aspectos técnicos asociados a ellos, los que permiten a los dispositivos asociados a dicha red conectarse a estas HAN. Sin embargo, es necesario considerar cuál protocolo es el que se adapta mejor a las necesidades de la red por utilizar, considerando que no esté obsoleto, que el fabricante continuamente esté generando actualizaciones, que los métodos de encriptación ofrezcan bastante seguridad y garanticen que los datos, los dispositivos y por supuesto, las instalaciones físicas donde estos residan, no sean accesados de forma alguna por terceros no autorizados.

(ZigBeeAlliance, 2015c) (Z-WaveAlliance, 2015) Respecto a la domótica, cabe recalcar también que no todos los aspectos son positivos. También existen desventajas que merecen ser citadas, tales como:

- Poco conocimiento del uso de redes para el usuario promedio.
- Altos costos de instalación y mantenimiento de equipo.
- Acceso o uso indebido por parte de otras personas a la red, a sus dispositivos o los datos que estos generan y trasladan.

A pesar de que existen diferentes protocolos para estas redes, cada uno con distintas características, existe una necesidad de incorporar mayores niveles de seguridad.

Se han hecho diferentes estudios para analizar los protocolos existentes en las redes que utilizan medidores inteligentes, sin embargo, muchos de estos estudios están relacionados con el consumo energético y cómo se puede hacer un uso eficiente de este. Un ejemplo es el estudio que desarrollaron Heikki Karvonen, Carlos Pomalaza-Ráez y Matti Hamalainen[3], llamado *A Cross-Layer Optimization Approach for Lower Layers of the Protocol Stack in Sensor Networks*.

(Karvonen, 2014) (Islam, 2013)

También se han desarrollado mecanismos que permiten un acceso remoto a las redes HAN de una manera más segura, como el que desarrollaron Binod

[1] Del inglés, *Smart Meters.*
[2] En adelante, al referirse a los protocolos Z-Wave y ZigBee, se hará´ prescindiendo de la palabra "protocolo"
[3] Tomado del artículo "*A Cross-Layer Optimization Approach for Lower Layers of the Protocol Stack in Sensor Networks*".

Vaidya, Dimitrios Makrakis, Hussein Mouftah[4]. (Dimitrios Makrakis, 2011) Para el protocolo Zigbee, existe un consorcio denominado *ZigBee Alliance*, que patrocina el Estándar 802.15.4[5]. Zigbee opera en redes inalámbricas transmitiendo datos a velocidades de hasta 250 kpbs y opera en las bandas de 2.4 GHz, 928 y 868 MHz, y como su contraparte, el protocolo Z-Wave que fue desarrollado por una compañía con sede en Dinamarca llamada Zensys[6], opera entre los 868 y 908 MHz y puede transmitir a velocidades de 9.6 a 100 kpbs.

Ambos protocolos permiten el manejo de redes HAN, pero en el caso de ZWave, los datos son transferidos en un texto plano, permitiendo que su contenido sea vulnerable, a falta del uso de la encriptación, esto podría facilitar que personas inescrupulosas puedan eventualmente conocer su contenido y por lo tanto, reproducirlo con el fin de tener acceso físico a un hogar, alterar los registros asociados a los dispositivos que se conectan a este[7]. Por su parte, Zigbee usa el algoritmo de encriptación AES, el que ofrece ventajas sobre Z-Wave, tan solo por el hecho de contar con esta particularidad de encriptación.

Respecto a la latencia, es decir, la cantidad de paquetes que pueden ser transmitidos por un dispositivo, Z-Wave presenta más problemas de latencia en comparación con Zigbee, donde para este último, la latencia expresada en tiempo, podría tomar hasta 100 milisegundos, mientras que en Z-Wave, podría ser de un segundo[8].

2. Antecedentes

En la actualidad, las dos tecnologías de protocolos: Zigbee y Z-Wave, poseen ventajas y desventajas de acuerdo con M. Knight, en su artículo denominado "*How safe is Z-Wave?*" (Knight, 2006).

A continuación se citan algunas de esas ventajas y desventajas.

Ventajas:

- Son de malla.
- Baja potencia.
- Fácil integración.
- Bajo consumo de energía.

Desventajas:

- La tasa de transferencia es baja.
- Manipula textos de poco tamaño en comparación con otras tecnologías.
- No tienen las mismas trasferencias y capacidades que el protocolo
- Bluetooth. Menor cobertura por usar redes inalámbricas (WPAN).

[5] Diseñado para redes inalámbricas, utilizan, para los datos, bajas tasas de transmisión.
[6]

[4] Tomado del artículo "*Secure communication mechanism for ubiquitous*".

Al accesar http: //www.zen-sys.com, la página redirecciona a http://www.sigmadesigns.com/ ya que ZenSys fue adquirida por Sigma Designs

7 Tomado de artículo "*How safe is Z-Wave? [Wireless standards]"*

8 Tomado de artículo *"How safe is Z-Wave? [Wireless standards]"*

- Los fabricantes que usaron el primer chip de Z-Wave no quisieron utilizar el cifrado triple DES incluido.

Entre protocolos existen ventajas y desventajas, las cuales se citan a continuación:

- Zigbee puede controlar una mayor cantidad de nodos.
- ZigBee es más versátil y puede ser configurado para prácticamente cualquier trabajo inalámbrico que sea de corto alcance.
- El protocolo ZigBee es más complejo para desarrollar.
- Z-Wave utiliza un protocolo mucho más sencillo para desarrollo. ZigBee utiliza la banda ISM 2,4 GHz, muy poblada y que comparte con Wi-Fi y Bluetooth, por lo que puede producir interferencias. Z-Wave es más utilizado en productos residenciales.

A pesar de esas desventajas de seguridad, Z-Wave se ve más en el mercado residencial, por lo que para futuros productos se está planeando introducir seguridad AES de 128 Bits, en el caso de ZigBee se está enrumbando en el mercado comercial por tener importantes alianzas con empresas como Intel y Cisco.

Características técnicas Z-Wave:

- Trabaja con la frecuencia 868,42 Mhz.
- Bajo consumo de energía (tiempo de alerta = 2,5 uA).
- Alcance en espacios cerrados es de 45 metros y en los espacios libres de 150 metros.
- Opera en 908,42 MHz en los EE.UU. y Canadá, pero depende de la reglamentación de cada país.
- Modulación por desplazamiento de frecuencia gausiana (FSK).
- Velocidades de datos disponibles incluyen 9.600 bits/s y 40 kbits/s.
- La potencia de salida es de 1 mW.

Características técnicas Zigbee:

- Bajo consumo de energía en comparación con otras tecnologías como Bluetooth y WIFI.
- Bajo costo, permite reducir requisitos en el controlador de comunicación.
- Trabaja en 20 250 kbps, la cual es la tasa más baja.
- La distancia de trasmisión está en el rango de los 10 m 100 m, pero si se aumenta la potencia de trasmisión puede llegar entre 1 y 3 km y la

distancia puede ser más larga si se utiliza relay entre el enrutamiento y el nodo. Tiene la respuesta más rápida en comparación con el Bluetooth (3-10 s) y el Wi-Fi (3 s), ya que solo necesita 15 ms, en la conexión nodo 30 ms.

Permite su uso en redes estrella, árbol y malla.

Zigbee es flexible, utiliza ACL y cifrado simétrico AES128 y modo seguro en nivel 3 con banda libre de licencia y está entre las bandas ISM 2.4 GHZ, 915 Mhz y 868 MHZ.

Ambos protocolos necesitan de mejoras en su seguridad, por lo que Sergio Saponara y Tony Bacchillone, en su artículo *Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid*, proponen utilizar, para redes de malla, cifrado asimétrico PKI con el fin de mejorar la seguridad con cifrado de datos. A continuación se mencionan algunas características positivas de PKI (Saponara, 2012):

- Certificados digitales, por ejemplo X509.
- Herramientas de red inteligente.
- Seguridad anclada de confianza.
- Certificados de atributo.
- Algoritmo de cifrado del servidor *Web (SSL) Secure Socket.*

La desventaja de PKI es que necesita de servidores de seguridad, lo que implica inversiones adicionales para mantener dicha tecnología.

Los autores Khan, Shafiullah, Kok-Keong Loo, Mast, Noor Naeem, Tahir , en su investigación *"SRPM: Secure Routing Protocol for IEEE 802.11 Infrastructure Based Wireless Mesh Networks",* demostraron por medio de las métricas utilizadas cómo el protocolo SRPM es más eficiente y seguro contra una serie de ataques de seguridad, que utilizando otros protocolos con serias deficiencias en seguridad, por lo que recomiendan el protocolo SRPM como ruta segura y exclusiva por sus características más robustas y resistencia a amenazas para una red de infraestructura de malla inalámbrica (Khan, 2010).

3. Comparativa de protocolos

Ambos protocolos poseen 4 capas denominadas:

- Capa Física (PHY)
- Capa MAC (MAC)
- Capa de Red (NWK)
- Capa de Aplicación (APL)

En las siguientes secciones, se procederá a detallar el funcionamiento de cada protocolo.

3.1. Capa física

ZigBee se asocia al estándar IEEE 802.15.4 y opera en diferentes bandas según su región de uso, 868 MHz para Europa, los 915 MHz para el Norte y Sur de América y en 2.4 GHz a nivel mundial.

A continuación se presentan algunos datos asociados con la capa física:

Z-Wave está asociado al estándar ITU-T G.9959, que describe la funcionalidad de las dos capas inferiores, y a diferencia de ZigBee, opera únicamente en la frecuencia sub- 1-GHz, que varía entre 850 y 950 MHz. Esta frecuencia cambia dependiendo de la región y el país. Por ejemplo, en Estados Unidos se utiliza en los 908.42 MHz, mientras que en Europa se utiliza en los 868.42 MHz. Los dispositivos Z-Wave operan en uno de tres perfiles de RF definiendo la modelación, mecanismos de codificación y velocidad de los datos de la capa física.

Canal	**Ancho de Banda**	**Intervalo del Canal**	**Tasa de Trasmisión de Datos**
0	600 Khz	868-868.6 Mhz	100 Kbps
1-10	2 Mhz	902-928 Mhz	250 Kbps
11-26	5 Mhz	2.4-2.480 Ghz	250 Kbps

Perfil RF	**Velocidad Datos**	**Codificación**	**Modulación**	**Tamaño de paquetes**
R1	9.6 Kbps	Manchester	*Frequency shift-keying* (FSK)	64 *bytes*
R2	40 Kbps	*Non*-return-to-Zero (NRZ)	(FSK)	64 *bytes*
R3	100 Kbps	NRZ	(FSK)	170 *bytes*

3.2. Capa MAC

Al igual que en la capa física, ZigBee utiliza el estándar IEEE 802.15.4 y bajo esta capa existen diferentes dispositivos que participan en la red, los cuales tienen una tarea que se define como un rol, el que está asociado a determinadas actividades que permiten el funcionamiento y seguridad a nivel de red. Los roles y dispositivos asociados son:

- Centro de Confianza (TC) Zigbee: Es un dispositivo conocido como FFD que se encarga de autenticar dispositivos. Básicamente cuando un dispositivo requiere unirse a la red, este le consulta al *router* más cercano y será el TC quien le indique al *router* que permita o deniegue la conexión.
- Coordinador (ZC) Zigbee: Otro FFD, al igual que el *Trust Center*, permite que otros dispositivos Zigbee se conecten a la red, se encarga de gestionar el funcionamiento de la red y por cada red Zigbee solo es necesario tener un coordinador.

- *Router* Zigbee (ZR): Es el equivalente del coordinador pero a nivel de *hardware* y al igual que este coordinador, permite que los dispositivos Zigbee se unan a la red, coordina el tráfico de red, lo cual es inherente a cualquier red dentro de la red y por lo tanto, para lograr esta coordinación se requerirán varios de ellos en una misma red.
- Dispositivos finales Zigbee (ZED): Son aquellos que se conectan a un ZR o a un ZC.

En cuanto a Z-Wave en la capa MAC, es responsable de algunos atributos del protocolo como:

- Formateo de paquetes.
- Reconocimiento positivo.
- Detección de errores.
- Retransmisión de paquetes.
- Procesamiento unicast, broadcast y multicast.
- Funciones de selección y asignación de direcciones.

La arquitectura básica de una red basada en Z-Wave consiste de dispositivos controladores y dispositivos esclavos, donde un solo dispositivo controlador es responsable de establecer la red y seleccionar un identificador único (*HomeID*). Estos dispositivos pueden iniciar una transmisión en la red, además son los encargados de mantener la información de enrutamiento, por lo que los dispositivos esclavos simplemente siguen las instrucciones de estos controladores sin preocuparse por el enrutamiento o la necesidad de iniciar conexiones con otros dispositivos Z-Wave. Los controladores pueden ser portables, que generalmente se cargan con baterías, o estáticos, que se alimentan de manera consistente de una fuente. El formato de la trama es diferente dependiendo del perfil de RF utilizado, se utiliza un formato para los 2 primeros perfiles, y otro para el tercer perfil.

3.3. Capa de red

En esta capa ambos protocolos definen tareas como la asignación de la dirección, el enrutamiento e incluso la detección de dispositivos. La función más importante se conoce como formación o construcción de una red Zigbee y para ello, se requiere de un coordinador de la red, el cual selecciona una canal donde operará la red y, de esta forma, permite que los ZED y los ZR que soliciten el ingreso a la red, puedan asociarse a esta. En el caso de Z-Wave el proceso para involucrar o excluir nodos a la red consiste en presionar un botón tanto en el controlador como en el nodo, de manera que lo hace una característica importante de seguridad, ya que se requiere acceso físico a ambos dispositivos.

3.4. Capa de aplicación

Con esta capa se tiene acceso a la interfaz de cada dispositivo, la cual permite la comunicación con el resto de capas mencionadas dentro de un mismo dispositivo, a la vez que permite, por medio de esta interfaz, proporcionar la función de Zigbee (ZC, ZR, ZED), permite asignar y remover las llaves de encriptación y asignar la función que permite asociar o no dispositivos a la red. Esta capa posee una subcapa denominada Subcapa de Apoyo a la Aplicación (APS), que se encarga de solicitar la entrega y recepción de datos a nivel de los dispositivos inalámbricos que componen la red Zigbee. El protocolo Z-Wave utiliza clases de comandos de aplicación para diferenciar acciones y respuestas a través de la red, y cada clase de comando puede contener otros comandos.

4. Seguridad

La seguridad es una preocupación inherente en tecnología, por ello, en esta sección se desarrollará este tema, asociándolo a los protocolos bajo estudio.

4.1. Seguridad en ZigBee

Para lograr la seguridad en Zigbee se utilizan dos modos, su detalle es:

- Modo Estándar de Seguridad donde el TC utiliza las Listas de Control de Acceso (ACL) para lograr la autenticación de los dispositivos Zigbee.
-

Modo de Alta Seguridad donde el TC almacena todas las claves de encriptación y autenticación, las políticas de red y las actualizaciones que sufran las anteriores.

Encriptación en Zigbee: La encriptación se da a través del algoritmo AES[5] y para ello y con el fin de gestionar la seguridad de la red, utiliza tres tipos de claves (Joshua Wright, 2015):

- *Master key*: es opcional y se utiliza junto con SKKE para generar claves.
- *Network key*: ayuda en temas de confidencialidad e integridad de la información entre varios dispositivos y también permite que cada dispositivo logre ser autenticado dentro de la red. Todos los dispositivos utilizan esta *network key*, es decir, es conocida por todos los dispositivos y se comparte con estos como un texto plano, al momento de unirse a la red. No es compatible su uso con el Modo de Alta Seguridad, por el tema del texto, por lo tanto, se usa en el Modo de Seguridad Estándar.

[5] Tomado de *Hacking Exposed Wireless, Wireless Security Secrets and Solutions*

- *Link Key*: Ayuda, al igual que la *network key*, en temas de confidencialidad e integridad, solo que su alcance se da para dos dispositivos pero con la desventaja que también esta *key* se traslada en un texto plano, por lo tanto, solo es posible su uso en el Modo de Seguridad Estándar. La diferencia entre la *link key* y la *network key* es que la primera se utiliza entre dos dispositivos y la segunda, entre todos los dispositivos de la red.

Para la entrega de las *key* o llaves, Zigbee utiliza dos métodos[6]:

- *Key Transport*: Aquí la *network key* y *link key* son recibidas por el dispositivo que se une a la red inalámbrica, el problema aquí es que la entrega se hace en un texto plano, lo cual facilita que un atacante pueda obtener la *link key* y con esta, logre ya sea obtener acceso a la información que se traslada sobre la red o usurpar el lugar de un dispositivo y así también, lograr acceso a la red.
- *Pre-installation*: El Administrador de la red debe instalar las llaves de encriptación de forma manual en todos los dispositivos que se quieran unir a la red, el problema con ello, es cuando se debe hacer la revocación de la llave o el cambio de la *link key* y esto se debe hacer en cualquier momento.

Cuando se trata de la autenticidad, es decir, el control que debe existir sobre la información o contenido asociado a una trama, se puede utilizar CCM* (*Counter Mode with Cipher Block Chaining Message Authentication Code*), que es un algoritmo que permite tanto el uso de la encriptación como de la integridad. En el caso de esta última, lo que permite es validar el contenido de la trama, con lo cual se permite evitar que un atacante pueda modificar dicho contenido y retransmitirlo. El problema observado al aplicar CCM* para el caso de la integridad, es que generalmente en las redes Zigbee es algo opcional. En el caso de la autenticación, es decir, validar que solo dispositivos autorizados, puedan ingresar a la red, se tienen los siguientes métodos:

- Modo ACL: Cada dispositivo debe tener la lista actualizada de direcciones MAC de los dispositivos que deseen ingresar a la red, el problema es cómo lograr que esta lista se mantenga actualizada cada vez que algún dispositivo desea ingresar a la red.
- *Trust Center*: El dispositivo que quiere acceder a la red, lo hace una vez que el *Trust Center* le asigna la *network key* pero para ello el dispositivo tiene que tener instalada la *network key*, si no el *Trust Center* le envía la *key* en un texto plano y así el nodo logra comunicarse con otros nodos; sin embargo, el *Trust Center* verifica el Modo ACL y si el dispositivo no cumple con esto, el *Trust Center*, del todo, evita que el dispositivo se conecte a la red y por lo tanto, con el resto de dispositivos que están en ella.
- Sin embargo, para evitar el envío de la *network key* en un texto plano, tanto el dispositivo que se quiere asociar a la red como el *Trust Center* usan el método SKKE, que les permite a ambos se reconozcan por medio de su *link*

[6] Tomado de *Hacking Exposed Wireless, Wireless Security Secrets Solutions.*

key y una vez que estos se reconocen, se da la entrega de la *master key* al dispositivo.

4.2. Seguridad en Z-Wave

Respecto a la seguridad en Z-Wave, a pesar de que Z-Wave Alliance no provee ningún tipo de documentación que describa los mecanismos de seguridad utilizados por Z-Wave, se ha descubierto que utilizan AES-OFB *(output feedback mode)* como protocolo para proveer confidencialidad a los datos, mientras que se usa AES CBC-MAC (*message authentication code*) como protocolo para proveer integridad de los datos. Z-Wave utiliza la clase de comando *CLASS SECURITY* que se utiliza para intercambiar información considerada confidencial entre dispositivos. Cuando un dispositivo Z-Wave soporta esta clase y es incluido en la red, este completa un proceso de intercambio de llave para obtener las llaves por utilizar en encriptaciones e integridad de los datos posteriormente. Este proceso es el siguiente:

- El controlador de la red le solicita al dispositivo un valor nonce, que es un valor usado en una comunicación criptográfica.
- Con este valor el controlador encripta la llave de red utilizando una llave temporal. Cabe destacar que la llave de red es generada al azar por el controlador cuando se establece la red y es única.
- Cuando el dispositivo recibe la llave de red encriptada y el MAC del controlador, valida el MAC y desencripta el mensaje con la llave temporal. El dispositivo registra la llave de red.
- El dispositivo solicita al controlador su valor *nonce*.
- Con este valor el dispositivo encripta un mensaje informando que la llave se estableció.
- El controlador recibe este mensaje.

Sin embargo, este proceso de intercambio de llaves presenta vulnerabilidades ante dos ataques:

- Ataque de hombre en el medio: El dispositivo no valida la identidad del controlador. Si se intercepta el proceso de inclusión con un controlador ajeno a la red podría causar que el dispositivo se asocie a una red no deseada.

- Ataque de recuperación de llave: No existe confidencialidad cuando se envía la llave de la red a través de ella, ya que la llave temporal se conoce. Un atacante que observe pasivamente el proceso de inclusión puede recuperar la llave de red y utilizarla posteriormente para desencriptar y enviar paquetes a través de la red.

Debido a estas debilidades en el proceso de inclusión, la Alianza Z-Wave añadió posteriormente una mejora llamada *Low power inclusion mode*, en la que el controlador y el dispositivo usan la mínima potencia de transmisión, por lo

que requieren estar a máximo un metro de distancia para llevar a cabo este proceso. Esto no significa que las vulnerabilidades mencionadas se eliminan del todo, pero resulta más difícil atacar la red debido a esta característica y también a la poca frecuencia con que se agregan nuevos dispositivos. Este proceso asume que uno de los dispositivos es portable. Después de cargar la llave de red, el dispositivo genera dos llaves adicionales utilizando AES-ECB: la llave de encriptación de paquete y la llave de autenticidad del mensaje.

- Kc = AES-ECBKn(*Passwordc*)
- Km = AES-ECBKn(*Passwordm*)

Proceso de envío de mensajes: Cuando un controlador desea enviar un mensaje a uno de los dispositivos esclavos, primeramente debe solicitar al mismo su valor *nonce*, al recibir este valor el controlador selecciona su propio valor *nonce* y concatena ambos para formar el vector de inicialización o IV. Con este valor el controlador puede encriptar la carga útil del paquete usando el IV y la llave de encriptación de paquete, y luego calcular el MAC utilizando la llave de autenticidad del mensaje. El cálculo del MAC incluye el IV, encabezado de seguridad (HDR), ID del nodo fuente (SRC), ID del nodo de destino (DST), el tamaño de la carga útil (LEN), y la carga útil encriptada (ENC (P)).

Al incluir los campos de ID de nodos de fuente y destino en el cálculo MAC, Z-Wave resuelve los intentos de falsificación de paquetes que manipulan los campos de ID de nodos. Además Z-Wave logra tener protección contra los ataques de repetición de tráfico al solicitar el valor *nonce* del dispositivo antes de la transmisión.

5. Tipos de ataques

Un aspecto importante de valorar corresponde a los ataques a los cuales son suceptibles Z-Wave y Zigbee, por ello, se mencionan los ataques principales en los siguientes párrafos.

5.1. Ataque de espionaje en Z-Wave

El ataque denominados *Eavesdrooping* o espionaje, se da porque generalmente las redes no utilizan la encriptación, lo que facilita que se pueda dar un ataque de escucha o *eavesdropping*, el cual le permite al atacante saber dónde está y como está configurada tanto la red como los dispositivos que la conforman.

En este caso se podrían aprovechar las características de encriptación incorporadas en este protocolo, o se podría utilizar rutinas de encriptación de terceros. Sin embargo, la Alianza Z-Wave no exige el uso de encriptación en ninguno de sus productos.

5.2. Ataque de repetición de tramas en Z-Wave

Otro ataque que se da en este protocolo es el de *replay*, repetición o reenvío de tramas, los datos capturados se vuelven a transmitir al receptor original y en el caso de aquellas redes que no presentan encriptación, también son vulnerables a este tipo de ataques. El efecto de esto dependerá del tipo de resultado esperado con los datos originalmente transmitidos, por ejemplo, si transmisión de datos está orientada a la seguridad en el hogar, el impacto se ubicará en este campo.

En Z-Wave, se es vulnerable a estos ataques cuando los despliegues no utilizan los mecanismos de protección opcionales de encriptación e integridad, por lo que para mitigar estos ataques hay que aprovecharse de ellos.

5.3. Ataque de encriptación en ZigBee

La gestión de claves de encriptación es un punto complicado, ya que se debe considerar aspectos como el cambio de clave, la revocación de esta y la cantidad de dispositivos donde esta gestión debe realizarse. Además, generalmente la mayoría de los dispositivos que utilizan la red no poseen una interface de usuario, siendo este factor una limitante para poder configurar la respectiva clave. Para redes Zigbee 2012 y anteriores, cuando un dispositivo desea ser asociado a la red, solicita a TC la clave y cuando es por políticas, esto es factible, TC le envía la *network key*; sin embargo, esta *network key* se envía como un texto plano, siendo generalmente la forma en la cual se da la asignación de estas *key*, lo cual representa una amenaza.

Una herramienta asociada con los ataques de encriptación, es la *KillerBee zbdsniff key Sniffing* con una clasificación de riesgo de 6. Esta herramienta captura paquetes y dentro de estos paquetes, examina tramas con el fin de determinar en cuál de ellas está la *network key*, cuando esto se da en la trama se observa como *Network Key Found* y una vez que se encuentra la key, se puede desencriptar todos los paquetes usando, por ejemplo, WireShark.

La solución a los ataques de encriptación se da con la preconfiguración o SKKE. Su detalle es:

- Preconfiguración de claves implica que estas son incluidas desde que se fabrica el dispositivo, lo cual ayuda a la transmisión segura de datos, pero genera como problema que el cambio y revocación de claves requiere que sean gestionados de forma manual por el administrador de la red.

- SKKE permite generar claves para lograr la autenticación entre el *Trust Center* y el dispositivo que desea ser autenticado, pero ambos, es decir, el dispositivo y el *Trust Center* deben tener la *master key*, ya sea para su envío *over the air* o ya preconfigurada, generando con ello los riesgos observados en el punto anterior.

5.4. Ataque de *Walkthrough* en ZigBee

Este ataque se orienta específicamente al ataque desde el punto de vista físico, los dispositivos que utilizan una red Zigbee, qué riesgos asociados podrían estar experimentando.

Toda red va a tener dispositivos que en mayor o menor medida son portables, y esta realidad no escapa a los dispositivos de una red Zigbee, los cuales -debido a su pequeño tamaño. Son fáciles de transportar y por lo tanto, una vez que un atacante tiene acceso físico a estos, puede tomarlos y analizarlos con el fin de determinar cómo poder atacar dicha red[7].

Una vez que el atacante tiene dichos dispositivos en su posesión, puede acceder fácilmente a su interior de forma física o lógica y con ello, por ejemplo, obtener acceso a las llaves de encriptación, las cuales constituyen la base para que los diferentes dispositivos se comuniquen entre sí. El problema al tener acceso a dichas llaves, es que el atacante puede acceder a la red Zigbee haciéndose pasar por un dispositivo asociado a la red y con ello, atacar el resto de dispositivos o los datos que están bajo el alcance de la red.

KillerBee zbfind device location analysis es una herramienta que facilita ubicar físicamente los dispositivos que constituyen la red para luego ubicar y sustraer físicamente dichos dispositivos. Esta herramienta posee una clasificación de riesgo de 6 de 10 puntos posibles, lo cual la vuelve sumamente riesgosa. La herramienta lista los dispositivos que forman parte de una red, con el fin de saber de ellos, las tramas asociadas al dispositivo y la actividad desarrollada por dicho dispositivo, para ello, el atacante, mide la intensidad de la señal con un medidor de velocidad y también puede enviar mensajes de *ping*; ambas actividades facilitarán ubicar el dispositivo Zigbee y si su acceso físico es fácil, el atacante, podrá adueñarse de él.

Después de acceder físicamente a un dispositivo, teniéndose el conocimiento técnico adecuado, se puede realizar un análisis de su arquitectura, identificando, por ejemplo, como parte de dicha arquitectura, el radio y el microprocesador del dispositivo, con lo cual se puede tener acceso a la ejecución de comandos o incluso, acceso a datos del dispositivo capturado.

Existe una herramienta denominada GoodFET, con una clasificación de riesgo de 5, que permite el acceso a la lectura del chip, extrayendo datos asociados a la memoria RAM y por lo tanto, se puede extraer información del dispositivo Zigbee que ha sido sustraído.

Otro aspecto a considerar una vez que se tiene acceso físico a un dispositivo, es el hecho de poder acceder a los datos de la RAM[8] de este dispositivo y si se logra este acceso, se puede acceder a las llaves utilizadas para encriptar y desencriptar el tráfico de datos (*encryption keys*).

Una herramienta utilizada para obtener las llaves de encriptación se denomina *KillerBee zbgoodfind key recovery*, posee una clasificación de riesgo de

[7] Tomado de *Hacking Exposed Wireless, Wireless Security Secrets Solutions.*
[8] Tomado de *Hacking Exposed Wireless, Wireless Security Secrets Solutions.*

6. La herramienta permite capturar paquetes y determinar si el paquete está encriptado. Por medio del algortimo AES, logra desencriptar el paquete capturado.

La solución contra ataques físicos en Zigbee se debe orientar al resguardo físico y para ello, el uso de dispositivos de video vigilancia y fomentar la conciencia en los mismos dueños de estos dispositivos en cuanto a permitir el acceso a los hogares solo a aquellas personas de su confianza, son elementos que contribuyen a este resguardo físico.

6. Mejores prácticas de implementación

Las mejores prácticas definen que actividades deben ser desarrolladas con el fin de lograr un manejo adecuado de los productos que utilicen Zigbee y Z-Wave. En adelante se menciona si existen mejores prácticas para los protocolos bajo estudio y el detalle de estas.

6.1. Mejores prácticas en Z-Wave

Para las redes Z-Wave no se tiene información respecto a mejores prácticas de implementación, esto se debe a que al ser un protocolo propietario, la Alliance Z-Wave no provee información sobre mejoras prácticas.

6.2. Mejores prácticas en ZigBee

En el caso de la redes ZigBee se tiene una variedad de información. Entre la documentación existente, el autor Ken Masica del *U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory* da una serie de recomendaciones para la implementación de ZigBee en redes domésticas y empresariales, que permiten tener redes ZigBee más seguras (Masica, 2007).

Consideraciones en el entorno doméstico

- Desarrollar políticas y procedimientos de seguridad por parte de la empresa que brinda estos servicios, que permitan una mejor administración, funcionamiento y manejo de las redes ZigBee, en este caso la institución que da los medidores inteligentes debe proporcionar documentación con las políticas y procedimientos de seguridad necesarios para que se puedan diseñar e implementar redes ZigBee más seguras que incluyan la gestión de las aplicaciones ZigBee, revisión y configuración de dispositivos, y actualización de las medidas de control de seguridad. Por ejemplo, los usuarios podrían estar revisando mensualmente que todos los dispositivos

Zigbee estén funcionando perfectamente, que no hayan sido saboteados o modificado su configuración.

- Protección de la infraestructura ZigBee con claves de seguridad de red: es de vital importancia que dentro de los nodos de la red ZigBee, todos los dispositivos cuenten con una clave de red, con el fin de poder enviar y recibir paquetes de datos validados, por lo que cada sensor, enrutador o puerta de enlace deben hacerlo por medio de una clave válida para poder enviar la información dentro de la red, de caso contrario serán bloqueados los paquetes, esta tarea sería asignada a los nodos de enrutamiento que validarán los paquetes de acuerdo con la clave red para poder realizar el proceso de envío de paquetes.
- Protección por medio lista de control o filtrado de direcciones (MAC): dentro del estándar IEEE 802.15.4, se tiene como seguridad baja las ACL (listas de control de acceso) que permitirían recibir tramas únicamente de los dispositivos autorizados dentro de la lista de ACL, de modo que solo los nodos autorizados puedan enviar tramas.
- Usar el cifrado AES que trae ZigBee: dentro del protocolo ZigBee se cuenta con medidas de seguridad como el cifrado AES de 128 bits, por lo que en importante que sea utilizado en las redes ZigBee para la protección de la información que se trasmita.
- Utilizar, si la red ZigBee lo permite, la autenticación nodo origen: de forma criptográfica se verifica la identidad del nodo que trasmitió la información, esta autenticación trabaja de la siguiente manera, el nodo origen envía una clave al dispositivo destino, la cual procede de las claves maestras de ambos dispositivos, por lo tanto esta clave es única y solo sirve para estos dos dispositivos, de este modo se tiene una protección más, adicional a la clave de red y solo es conocida por los dos dispositivos que interactúan.
- Implementar la coordinación de la red ZigBee, por medio de un coordinador: a pesar que el protocolo permite la auto organización y automatización, es importante poder asignar a un nodo el realizar la función de coordinador de ZigBee, para un mejor desempeño sería bueno poder utilizar uno nodo FFD. En el estándar 802.15.4 de la IEEE se permite tener un nodo que asuma el papel de coordinador, con la condición que ya no se haya establecido uno anteriormente. Este nodo coordinador tiene las responsabilidades de la seguridad de la red, envío y trasmisión y otras funciones necesarias y esenciales en la red.
- Implementar un nodo coordinador de copia de seguridad en ZigBee: Generalmente en las redes ZigBee se utiliza un único nodo coordinador, por lo que es recomendable que dichas redes cuenten con un nodo coordinador secundario. Esto quiere decir que se puede implementar un coordinador secundario, en caso que deje de funcionar el primario. Es importante realizar una adecuada configuración del nodo primario y secundario, con el fin de evitar que otros nodos traten de usurpar la función de coordinador.

- Configurar la red ZigBee para poder pre-determinar un PAN ID (*Personal Area Network Identifier)* y limitar la conectividad del nodo: el PAN ID puede ser pre-asignado o asignado dinámicamente, con el fin de limitar la inclusión a la red, de modo que solo los nodos ZigBee pueden unirse con la red con el PAN ID y operar en la misma frecuencia de canal, este es necesario si existen múltiples redes ZigBee para poder evitar conflictos entre ellas.
- Elegir métodos de carga de claves o claves fuera de banda: Dependiendo de la red ZigBee es posible tener métodos para la carga de claves, de las 3 posibles serían las siguientes: 1. Fuera de la banda, la carga de la llave se hace por medio de un dispositivo como una *laptop* ya que la condición es que no sea a través de una comunicación inalámbrica. 2. Dentro de la banda, se usa medios inalámbricos de la red para el envío de la llave, este método no es muy seguro debido a que durante el envío de la clave, esta queda sin protección, por lo que es vulnerable a un ataque. 3. Precarga de fábrica: la carga de las claves se hace en la fábrica cuando se realiza la fabricación, además el fabricante debe enviar las claves al cliente, este método no se considera seguro debido a que el fabricante tiene las claves y al ser enviadas son vulnerables. De estos métodos el más recomendable es el fuera de banda, ya que el usuario puede generar las llaves y cargarlas de manera segura.
- Utilizar los mecanismos de seguridad dentro de lo posible en la capa 2, que trae la IEEE 802.15.4, como el conjunto de cifrado para proteger el origen y destino dentro del encabezado MAC, esta opción se debe consultar con el proveedor a ver si es posible realizar en la red ZigBee.
- Implantar métodos de admisión a la red, con lo que los nodos de ZigBee se conectan a la red de forma segura si se le precarga un llave y se les admite en la red, esto se realiza por medio del Centro de Confianza que tiene ZigBee, que coordina la admisión y autenticación de los nodos que desean la admisión a la red ZigBee.
- Pre configurar nodos que tengan la dirección del Centro de Confianza (TC), En ZigBee se tiene un Centro de Confianza, por lo que sería importante precargar la dirección del TC en el nodo de ZigBee, para incrementar la seguridad, sería recomendable realizarlo cuando se precargan las claves criptográficas mencionadas anteriormente.

Consideraciones en el entorno industrial 1. Considerar interferencia: en ambiente industrial donde los equipos y máquinas industriales pueden causar ruido, así como EMI (*Electro Magnetic Interference*) que puede interferir en redes inalámbricas, debido a que la forma de encontrar el acceso es escuchar para determinar qué canal está abierto, pero al haber EMI y ruido creará problemas de rendimiento, por lo que se deben considerar los siguientes puntos:

- Elegir una banda que sea lo menos susceptible posible a la interferencias que pueda tener en entorno industrial, entre las recomendadas están entre los 900 MZ o 2.4 GHz.
- Elegir una banda de frecuencia que sea menos afectada por el EMI y configurar cada equipo ZigBee, además se debería subir el nivel de potencia, utilizando una mejor antena que dé mayor ganancia o un mejor equipo ZigBee.
- Zigbee trabaja mejor sobre topología de malla, de este modo se reducen las distancias entre equipos ZigBee y hay una mejorar señal porque le afecta menos el ruido.
- Usar salto de radio frecuencia o *Hopping* (FH), debido a que esta tecnología permite cambiar rápidamente los saltos que pueden ser configurables.

2. Considerar fiabilidad: La maquinaria puede generar ruido e interferencia, por lo que es recomendable realizar pruebas para establecer niveles críticos, así como el rendimiento de las redes para así determinar la fiabilidad de las redes en este tipo de ambiente, donde hay muchos equipos como cintas trasportadoras, robots, brazos mecánicos y otras máquinas. Se deben considerar en aspectos de fiabilidad la topología de red por usar y el tiempo de trasmisión:

- En el caso de la topología, la estrella es la que menos complejidad tiene para ZigBee, ya que solo necesita un nodo coordinador, que simplifica la comunicación, así como el enrutamiento, resulta muy fiable. Aun así, es conveniente realizar el respectivo análisis de fiabilidad y su rendimiento.
- Para el caso de la trasmisión garantizada, las redes en 802.15.4 tienen un GTS (*Guaranteed Time Slots*), donde un dispositivo opera en un canal *Carrier Sense Multiple Access* (CSMA / CA), que evita colisión, de modo que los dispositivos escucharán el acceso al canal para contender por tener el medio de trasmisión inalámbrica para trasmitir el mensaje, lo malo es que este medio no garantiza el recibido de la trama, solo la trasmisión.

3. Considerar la seguridad, donde se debe tomar en cuenta las mejores prácticas mencionadas anteriormente para mitigar las posibles vulnerabilidades que a nivel de riesgos puedan ser aceptables, ya que no se podrán eliminar por completo, debido a que las redes inalámbricas propagarán la señal más allá del edificio, por lo que es posible que atacantes puedan ver la señal y quieran *hackear* la red para enviar ataques como denegación de servicios (DOS), por lo que es recomendable seguir las prácticas mencionadas para mitigar los riesgos hasta donde sea posible.

7. Productos

A continuación se detallan algunos productos que utilizan uno u otro protocolo.

7.1. Productos Z-Wave

- Hooper DVR: Con apariencia de DVD permite controlar el encendido y apagado de las luces en el hogar, además de controlar las cámaras que se tengan en el hogar y también la cerradura, cuando el hogar cuenta con una cerradura electrónica.
- Zwave anti - antirrobo por del sensor de movimiento para el hogar sistema de seguridad: Permite detectar el movimiento del cuerpo humano y con ello, alerta al sistema de alarma, además permite controlar el clima dentro del hogar, todo de forma inalámbrica.
- Enchufe Du¨wi Dimmer Z-Wave: Es un enchufe con el cual se puede regular la intensidad de la luz, de forma inalámbrica. Permite una carga máxima de 300 watts.
- Pulsera Z-Wave con botón de emergencia Benext: En caso de emergencia, la persona toca el botón rojo y la pulsera envía una señal al controlador de la red y a su vez, el controlador, genera un correo electrónico a una persona previamente definida.
- *Intermatic MultiWave PE953 Five Channel Wireless Remote Controller*: Permite definir la temperatura que tendrá el agua en una piscina y esto se hace a través de una pantalla LCD que posee el dispositivo y que permite realizar la respectiva programación.
- Cerradura electrónica 2GIG-99100-005: Permite abrir o cerrar la puerta sin necesidad de contar con una llave y posee hasta un máximo de códigos de usuario.
- Control de persiana oculto Fibaro: cuando se cuenta con un motor eléctrico para persianas permite, al tener un controlador Z-Wave, tener el control de la persiana.
- Pack VeraLite y Karotz: Denominado Robot Inteligente Doméstico, el cual emite mensajes, por ejemplo, que la alarma está conectada o que hay movimiento en determinada zona de casa.

(de Domotica DaVinci, 2014) (Alibaba.com, 2015) (Domboo, 2015a) (Domboo, 2015b) (ZWaveAlliance, 2015) (2gig, 2015) (ZWaveEcuador, s.f.) (ZWavePeru, 2015) (ZigBeeAlliance, 2015b) (ZigBeeAlliance, 2015a) (Leviton, 2012) (Netvox, 2012a)

7.2. Productos ZigBee

- Cerradura de Kwikset SmartCode: La cerradura puede comunicarse con otros dispositivos en la casa y con ello, por ejemplo, al darse la conexión con un

smartphone, se lograr monitorear y controlar estas cerraduras. La cerradura permite enviar alertas por correo electrónico.

- *Ambient Energy Joule*: Pantalla destinada al envío de información sobre el consumo de energía en tiempo real.
- Altavoces de montaje en pared/techo Leviton Architectural Edition R con tecnología de JBL: Evitan la distorsión de la señal, poseen una baja difracción y lograr compartir la música con este dispositivo, ya sea desde un *Ipod* o un televisor.
- Control remoto Z-503 utilizado para apagar dispositivos, llevar el control del consumo de electricidad y hasta puede activar/desactivar el sistema de seguridad de alarmas.
- Sirena Z602A que recibe el mensaje de alarma contra un dispositivo NIC CIE, realizado lo anterior, genera un sonido de sirena.
- Teléfono controlador Zigbee: Se realiza una llamada desde un teléfono, el dispositivo reconoce la voz y con ello, se controla la iluminación, el aire acondicionado, cortinas, entre otros puntos Netvox, 2012b).

8. Conclusiones

Las siguientes son las principales conclusiones del presente artículo:

1. En tema de mejores prácticas de implementación, para el protocolo Zigbee se provee variada información sobre este campo, mientras para el protocolo Z-Wave, a partir de la investigación realizada, se concluye que no hay documentación disponible a nivel público.
2. A pesar de la existencia de mejores prácticas para Zigbee, estas no garantizan la inviolabilidad de este protocolo, sin embargo, estas le generan un mayor nivel de dificultad al atacante al momento de tratar de ingresar a la red.
3. Ambos protocolos poseen una vulnerabilidad en común, la cual se da en el intercambio de llaves entre el controlador y el nodo que desea ingresar a la red. La vulnerabilidad consiste en transferir la llave de la red en un texto plano, por lo que uno atacante podría interceptar la trama donde se incluye esta llave de red y con ello, ingresar a la red y volverla vulnerable.
4. Z-Wave presenta mecanismos de seguridad a través del uso de dos protocolos denominados AES-OFB y AES CBC-MAC. El primero es usado para la confidencialidad de datos y el segundo para la integridad de los datos; sin embargo, la decisión de incorporar estos dependerá en mucho de si los fabricantes de los dispositivos que utilicen este protocolo deciden incorporarlos, ya que la Alianza Z-Wave no obliga a los fabricantes a agregarlos a sus productos.
5. Actualmente la versión del protocolo Zigbee utilizada es la2.0, sin embargo, ya está pronta a salir la versión 3.0, la cual traerá consigo mejoras asociadas a la escalabilidad, confiabilidad y seguridad.
6. A nivel comparativo, se tiene:

- Z-Wave es un protocolo propietario de la Alianza Z-Wave, por su lado, Zigbee no lo es, por ello, la estandarización de productos que tiene Zigbee, lo hace más seguro y fácil de adoptar a nivel mundial.
- Zigbee opera en tres rangos de frecuencias, mientras Z-Wave opera únicamente en una, además, en el caso de la frecuencia de 2.4 Ghz en la que opera Zigbee, puede presentar interferencia con la señal de los protocolos *Bluetooth* y *Wi-Fi*.

- Los dispositivos que componen una Red Zigbee son el centro de confianza, el coordinador, el *router* y el dispositivo final. Por su parte, Z-Wave considera solamente el controlador y los dispositivos esclavos, lo cual refleja que la arquitectura de Z-Wave es menos compleja que la de Zigbee, por el tipo y cantidad de dispositivos involucrados, lo cual conlleva a una mayor inversión para la creación y mantenimiento de redes Zigbee.

9. Recomendaciones

1. Para Z-Wave, es necesario que la respectiva Alianza suministre al público en general documentación asociada a mejores prácticas, con el fin de facilitar una mejor implementación en las redes o productos que utilicen este protocolo.
2. La vulnerabilidad asociada con la transferencia de la llave de red en texto plano se puede contrarrestar en Z-Wave utilizando el modo de inclusión de bajo poder (*low power inclusion mode*), que requiere que tanto el controlador como el nodo se encuentren a un metro de distancia o menos para completar el proceso de inclusión. Este modo y la baja frecuencia de incluir nodos a la red dificultan al atacante la obtención de la llave, además es recomendable agregar a la red dispositivos con el modo de inclusión mencionado.
3. En el caso de Zigbee, la vulnerabilidad mencionada en el párrafo anterior se puede contrarrestar de tres formas. La primera se denomina preinstalación, donde el administrador de la red, debe instalar las llaves de encriptación de forma manual en todos los dispositivos que se quieran unir a la red. La segunda se denomina transporte, donde el centro de confianza envía la llave a cada dispositivo que se quiera asociar a la red. El tercero corresponde al uso del protocolo SKKE, donde el dispositivo iniciador establece una clave de enlace con el receptor (*link key*), además, el Centro de Confianza genera una *master key* y se la envía a ambos nodos y de esta forma, se establece la comunicación con ambos dispositivos.
4. Para el tema de seguridad a nivel de una red Z-Wave, es necesario que se adquieran dispositivos que tengan mecanismos de seguridad incorporados o añadir dispositivos de seguridad desarrollados por terceros.
5. A futuro, es recomendable que los fabricantes que utilicen dispositivos que utilicen el protocolo Zigbee, desarrollen los análisis requeridos para adoptar la versión 3.
6. Los futuros clientes/usuarios que deseen establecer una red inalámbrica, deberán optar por una basada en el protocolo Z-Wave si la red que desean es sencilla, esto en transferencia de datos y cantidad de nodos. Por defecto, si la red que desea utilizarse en aspectos de datos y nodos es más compleja, la opción por utilizar es Zigbee.

Referencias

2gig. (2015). *Cerradura electrónica 2gig-99100-005.* http://www.inalarm.com/2gig/Default.aspx?content=productos&id=3. (Permite abrir o cerrar la puerta sin necesidad de contar con una llave) pages 17

Alibaba.com. (2015). *Zwave anti - antirrobo pir del sensor.* http://spanish.alibaba.com/product-gs/433-868-915mhz-zwave-antiburglar-pir-motion-sensor-for-home-security-system-60103869393.html. (Permite detectar el movimiento del cuerpo humano y con ello, alerta al sistema de alarma) pages 17 de Domótica DaVinci, B. (2014). *Hooper dvr.* http://blog.domoticadavinci.com/2014/01/el-stand-booth-de-la-z-wavealliance-en.html. (DVD permite controlar el encendido y apagado de las luces en el hogar) pages 17

Dimitrios Makrakis, H. M. B. V. (2011). Secure communication mechanism for ubiquitous. pages 2

Domboo. (2015a). *Enchufe du¨wi dimmer z-wave.* https://domboo.es/producto/pulsera-z-wave-con-boton-de-emergenciabenext/. (Es un enchufe con el cual, se puede regular la intensidad de la luz, de forma inalámbrica) pages 17

Domboo. (2015b). *Pulsera z-wave con botón de emergencia benext.* https://domboo.es/producto/pulsera-z-wave-con-boton-de-emergenciabenext/. (La pulsera envía una señal al controlador de la red y a su vez, el controlador, genera un mail a una persona previamente definida) pages 17

Islam, I. K., Md. Tahidul. (2013). Compressed sensing-based multi-layer data communication in smart grid systems. *IEEE Trans Smart Grid*, *9*, 22132231. pages 2

Jelena Misic, M. K., Fereshteh Amini. (2008). Performance implications of periodic key exchanges and packet integrity overhead in an 802.15.4 beacon enabled cluster. *International Journal of Sensor Networks*. pages 21

Joshua Wright, J. C. (2015). *Hacking exposed wireless* (Third ed.). McGraw-Hill Education. pages 8

Karvonen, C. H. L. I. M., H. Pomalaza-Ráez. (2014). A cross-layer optimization approach for lower layers of the protocol stack in sensor networks. , 1-31. pages 2

Khan, N. N. T., S. Kok-Keong L. Mast. (2010). Srpm: Secure routing protocol for ieee 802.11 infrastructure based wireless mesh networks. , 190-209. pages 5

Kim, C. C. J., H. Kim. (2012). A novel elliptical curve id cryptography protocol for multi-hop zigbee sensor networks. , 145-157. pages 21

Knight, M. (2006). How safe is z-wave? [wireless standards]. , 4-7. pages 3

Leviton. (2012). *Altavoces de montaje en pared/techo leviton architectural edition.* http://spanish.leviton.com/. (Altavoces de montaje en pared/techo) pages 17

Masica, K. (2007). Securing zigbee wireless networks in process control system environments. , 1-22. pages 13

Netvox. (2012a). *Control remoto z-503.* http://www.netvox.com.tw/Z-503.asp. (Apagar dispositivos, llevar el control del consumo de electricidad y activar/desactivar el sistema de seguridad de alarmas) pages 17

Netvox. (2012b). *Sirena z602a.* http://www.netvox.com.tw/Z-602.asp. (Alarma contra un dispositivo NIC CIE, realizado lo anterior, genera un sonido de sirena) pages 18

Saponara, T., S. Bacchillone. (2012). Network architecture, security issues, and hardware implementation of a home area network for smart grid. *Journal of Computer Networks & Communications*, 1-19. pages 5

Yan Y, S. H., Qian Y. (2011, mar). A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, 909 - 914. pages 21

ZigBeeAlliance. (2015a). *Ambient energy joule.* http://www.zigbee.org/products-test-page/. (Pantalla destinada al envío de información sobre el consumo de energía en tiempo real) pages 17

ZigBeeAlliance. (2015b). *Cerradura de kwikset smartcode.* https://docs.zigbee.org/zigbee-docs/dcn/09/docs-09-5248-00-0mwgzigbee-alliance-homologa-17-nuevos-productos-de-domtica-zigbee.pdf. (La cerradura puede comunicarse con otros dispositivos en la casa) pages 17

ZigBeeAlliance. (2015c). *Zigbee.* http://www.zigbee.org/. (Online; accessed Jun-2015) pages 2

ZWaveAlliance. (2015). *Intermatic multiwave pe953 five channel wireless remote controller.* http://www.inalarm.com/2gig/Default.aspx?content=productos&id=3. (Permite definir la temperatura que tendrá el agua en una piscina) pages 17

Z-WaveAlliance. (2015). *Z-wave.* http:// http://www.z-wave.com/. (Online; accessed Jun-2015) pages 2

ZWaveEcuador. (s.f.). *Control de persiana oculto fibaro.* http://zwavec.com/ year =. pages 17

ZWavePeru. (2015). *Pack veralite y karotz.* http://zwavepe.com/. (Robot Inteligente Doméstico, el cual emite mensajes) pages 17

Access Control List (ACL) Advance Encryption Standard (AES) Application Layer (APL) application support sublayer (APS) Cipher Block Chaining Message Authentication Code (CBC) Data Encryption Standard (DES) Full Function Device (FFD) Frequency Shift Keyed (FSK) Home Area Networks (HAN) Institute of Electrical and Electronics Engineers (IEEE) Industrial, Scientific and Medical

(ISM) Medium Access Control (MAC) Non return to zero (NRZ) Network Layer (NWK) Output Feedback (OFB) Personal Area Network (PAN) Physical Layer (PHY) Public Key Infrastructure (PKI) Symmetric-Key Key Establishment (SKKE) Secure Sockets Layer (SSL) Trust Center (TC) Wireless Personal Area Network (WPAN) Zigbee Coordinator (ZC) Zigbee End Device
(ZED) Zigbee Router (ZR)

Glosario

Ciberseguridad: Utiliza varios de los conceptos mencionados en este glosario y permite, a través del uso de diferentes recursos tecnológicos y de una adecuada y práctica normativa, la gestión adecuada de la información y de los usuarios que tienen acceso o son responsables de esta información. 1

Domótica: Abarca conceptos como medidores inteligentes, HAN, entre otros, y lo que permite es tener un mejor control y administración de los dispositivos conectados a esta HAN. 18

HAN: Red utilizada en hogares inteligentes, formada por medidores inteligentes, los dispositivos conectados a esta red y los paquetes que viajan por ella. 1

Medidores inteligentes: Red utilizada en Hogares Inteligentes, formada por Medidores Inteligentes, los dispositivos conectados a esta red y los paquetes que viajan por ella. 1

PKI: protocolo que sirve para el intercambio seguro de información a base de una infraestructura de red formada por servidores y servicios. 21

Protocolos: Permiten la transmisión de datos entre dos o más dispositivos conectados a una misma red. 1

***Wireshark*:** Analizador de paquetes de red. Su función es tratar de capturar los paquetes de red y mostrar los paquetes de datos de la forma más detallada posible. 12

Acrónimos

ACL: *Access Control List*. 5
AES: *Advance Encryption Standard*. 3
APL: *Application Layer*. 5
APS: *Application Support Sublayer*. 8

CBC: *Cipher Block Chaining Message Authentication Code*. 8

DES: *Data Encryption Standard*. 4

FFD: *Full Function Device*. 6
FSK: *Frequency Shift Keyed*. 4

HAN: *Home Area Networks*. 1

IEEE: *Institute of Electrical and Electronics Engineers.* 5
ISM: *Industrial, Scientific and Medical*. 4

MAC: *Medium Access Control*. 5

NRZ: *Non return to zero*. 6
NWK: *Network Layer*. 5

OFB: *Output Feedback*. 10

PAN: *Personal Area Network*. 3
PHY: *Physical Layer*. 5
PKI: *Public Key Infrastructure*. 5

SKKE: *Symmetric-Key Key Establishment*. 8
SSL: *Secure Sockets Layer*. 5

TC: *Trust Center*. 6

WPAN: *Wireless Personal Area Network*. 3

ZC *Zigbee Coordinator*. 6
ZED *Zigbee End Device*. 7
ZR *Zigbee Router.* 8